Approche théorique et pratique de TCP/IP

Sommaire :

[Script automatisation : 2](#_Toc180660135)

[Une image contenant dessin humoristique, capture d’écran, horloge, clipart

Description générée automatiquement 4](#_Toc180660136)

[Exercice 3 : Découverte TCP-IP 4](#_Toc180660137)

[3.2 : Préparation et outils : 4](#_Toc180660138)

[3.3.2 : Récupération des informations en mode commande : 4](#_Toc180660139)

[3.3.3 Accès aux informations en mode graphique 7](#_Toc180660140)

[4 : Utiliser Windows PowerShell : 12](#_Toc180660141)

[4.3 Commandes PowerShell et Invite de commande : 12](#_Toc180660142)

[4.4 : Explorez les applets de commande : 13](#_Toc180660143)

[4.5 : Commande Netstat avec PowerShell : 13](#_Toc180660144)

[4.6 Videz la corbeille avec PowerShell : 15](#_Toc180660145)

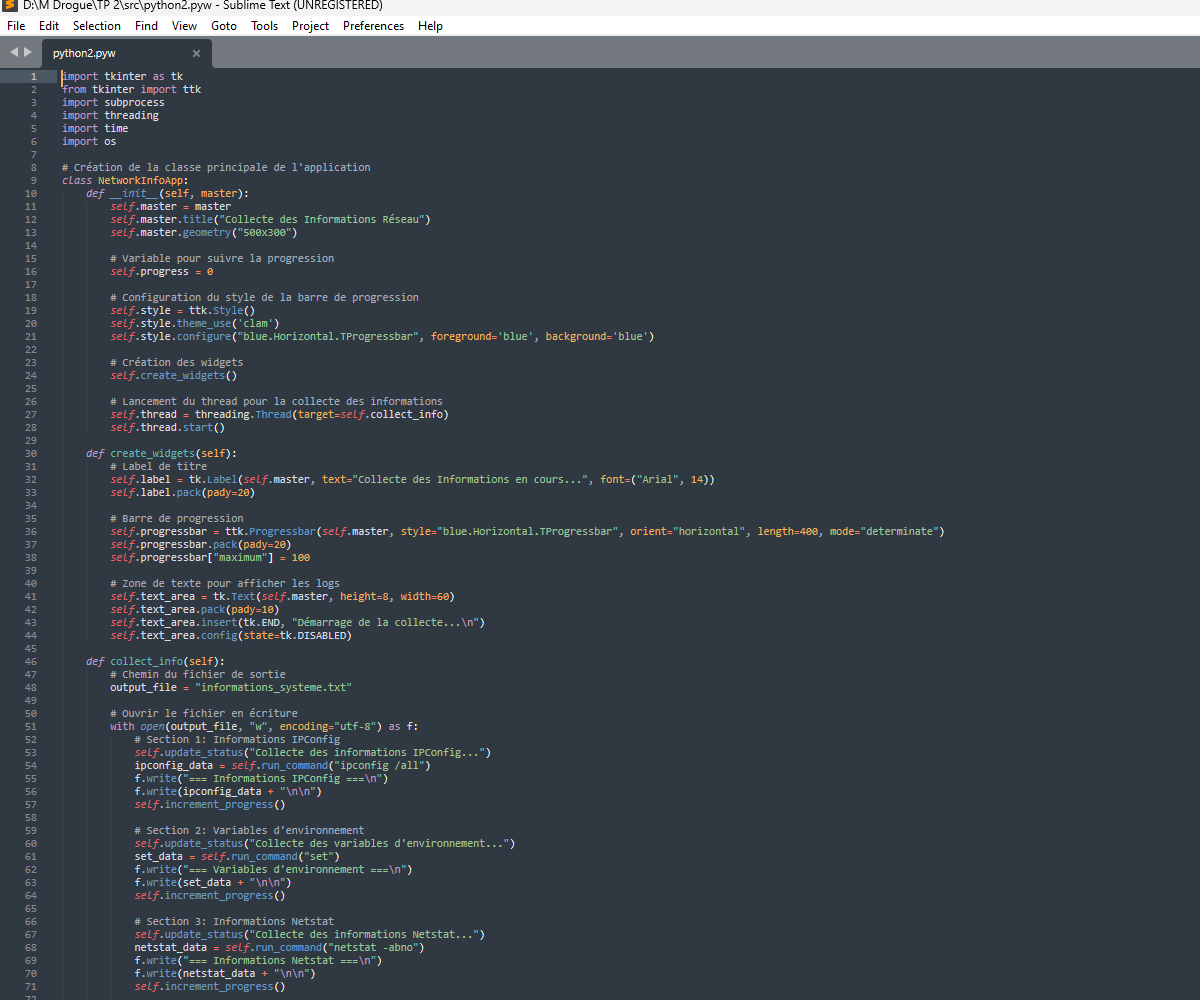
[5 : Exercices de calcul de réseaux : 19](#_Toc180660146)

# Script automatisation :

Pour ce TP, certaines activités ne peuvent pas se faire à domicile en raison des limitations techniques ou des ressources nécessaires. Par conséquent, une partie du travail doit être réalisée en classe pour garantir la continuité et la bonne progression des activités. Afin de faciliter le suivi de cette progression et de ne pas perdre les étapes déjà accomplies, j'ai élaboré un script automatisé.

Ce script a pour but de suivre et d'enregistrer chacune des étapes du TP dans un fichier texte. À chaque nouvelle action ou étape complétée, le script met à jour ce fichier, permettant ainsi de reprendre facilement là où nous nous étions arrêtés, que ce soit en classe ou à domicile. Il permet de :

1. Enregistrer la progression actuelle.
2. Gérer les différentes étapes à effectuer pour le TP.
3. Garantir que toutes les parties du TP soient complétées de manière ordonnée et traçable.



Le code commence par l'initialisation et la gestion de l'interface utilisateur grâce aux modules `tkinter` et `ttk`. Le constructeur `\_\_init\_\_()` crée la fenêtre principale de l'application, configure la barre de progression et installe les éléments visuels. Il utilise également un thread pour exécuter la collecte des informations réseau en arrière-plan, assurant ainsi que l'interface utilisateur reste réactive et ne se bloque pas pendant l'exécution des tâches.

Ensuite, la méthode `create\_widgets()` s'occupe de la création des composants graphiques, tels que le label de titre, la barre de progression personnalisée à l'aide de `ttk.Progressbar`, et une zone de texte pour afficher les logs. L'utilisation de `ttk.Style()` permet de définir un style visuel pour la barre de progression, offrant une meilleure personnalisation et lisibilité. Ces widgets permettent à l'utilisateur de suivre l'avancement de la collecte des informations en temps réel.

La collecte des informations système et réseau est réalisée par la méthode `collect\_info()`, qui exécute des commandes telles que `ipconfig`, `netstat` et `ping` en utilisant le module `subprocess`. Ces commandes sont exécutées dans un thread parallèle grâce à `threading.Thread`, garantissant que l'interface reste fluide pendant la collecte. Chaque étape de collecte est enregistrée dans un fichier texte, et la barre de progression est mise à jour pour refléter l'état actuel de la collecte. Le module `os` est également utilisé pour gérer l'enregistrement des résultats dans le fichier système.

Enfin, la méthode `run\_command()` exécute chaque commande système à l'aide de `subprocess.check\_output()` pour récupérer et afficher les résultats. Pendant ce temps, la méthode `increment\_progress()` met à jour la barre de progression à chaque étape accomplie. Un délai simulé est introduit avec `time.sleep(1)` pour représenter le temps nécessaire à l'exécution de chaque tâche, ce qui renforce l'interactivité et la clarté pour l'utilisateur.

Une image contenant dessin humoristique, capture d’écran, horloge, clipart

Description générée automatiquementLes modules utilisés (`tkinter`, `ttk`, `subprocess`, `threading`, `time`, et `os`) sont tous essentiels pour garantir une application fonctionnelle et réactive, capable de collecter et d'enregistrer des informations système tout en offrant un retour visuel à l'utilisateur.

# Introduction :

# Dans ce TP, nous allons découvrir le protocole TCP/IP en utilisant des commandes comme « ipconfig », « ping » et « netstat ». Nous utiliserons aussi des commandes PowerShell pour gérer les connexions et les processus du système. De plus, nous ferons des calculs de sous-réseaux pour mieux comprendre comment les adresses IP sont organisées. Nous travaillerons à la fois sur un réseau réel, celui du BTS, et sur le simulateur Cisco Packet Tracer pour bien comprendre chaque manipulation.

# Exercice 3 : Découverte TCP-IP

## 3.2 : Préparation et outils :

### 3.3.2 : Récupération des informations en mode commande :

|  |
| --- |
| Le chemin d’accès est:  C:\Users\UTI029\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools |

|  |  |
| --- | --- |
|  | -Il sert à communiquer des informations sur la nature du document.  -L’emplacement permet d’indiquer l’endroit où se trouve l’application.  -C’est le fichier dans lequel on retrouve l’application (et tous les autres indispensables de Windows). Il est toujours utilisé pour exécuter l’invite de commande.  -Il indique le répertoire de démarrage.  -Pour voir quelle touche permet d’ouvrir directement l’application.  -Choisir la taille de l’application lorsqu’elle est ouverte.  -Résumé de ce que fait l’application. |

Carte réseau réelle :

|  |  |
| --- | --- |
|  | - Suffixe Serveur DNS sert à compléter les noms de domaine.  -Adresse MAC (Media Acces Contrôle) est un identifiant unique servant à identifier un appareil sur un réseau local  -Adresse IP qui sert à identifier le poste sur Internet.  -Masque de sous-réseau sert à définir les limites des sous-réseaux.  -Passerelle par défaut sert à communiquer autre part que dans son réseau local. |

DNS (Domain Name System) traduit les noms de domaines en adresse IP.

Différence entre ipconfig et ipconfig /all :

|  |  |
| --- | --- |
| Dans les deux images il y a des suffixes DNS propres à la connexion les adresses IPv4 et IPv6, les masques de sous-réseau et la passerelle par défaut. Dans ipconfig /all il y a en plus le suffixe DNS principal et de recherche, le DHCP et DNS et le nom de l’hôte. |  |

DHCP (Dynamic Host Configuration Protocol) permet de donner une adresse IP automatiquement, une passerelle par défaut et les serveurs DNS.

Informations sur la configuration IP :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement | -Pour identifier le poste sur un réseau  - Définir ma méthode de résolution de noms de réseau  -le poste utilise DNS et WINS pour résoudre les noms de domaines  -Le poste ne peut pas servir de routeur  -Le proxy n’aide pas WINS à résoudre les noms NetBIOS  -Compléter les noms de domaine partiels |

WINS (Windows Internet Name Service) traduit les noms NetBIOS en adresses IP dans les réseaux, il ressemble au DNS (utilisé pour les noms de domaine internet).

#### 3.3.2.1 : Déterminer les paramètres réseau d’un poste :

|  |  |
| --- | --- |
| Nom de poste client (nom NetBIOS) | B181-102 |
| Nom de domaine | sio.local |
| WINS est-il activé ? |  |
| Adresse IP du serveur WINS, si actif | Il n’est pas actif |

NetBIOS (Network Basic Input/Output System) est plusieurs interfaces et de services pour que des ordinateurs puissent communiquer sur un réseau local.

#### 3.3.2.2 : Vérifier les paramètres TCP/IP :

|  |  |
| --- | --- |
| Comment la station obtient-elle son adresse IPv4 ? | Grâce au DHCP qui en attribue une automatiquement |
| Adresse IPv4 de la station | 172.31.1.172 |
| Masque de sous-réseau | 255.255.255.0 |
| Passerelle par default | 172.31.1.254 |
| DNS est-il activé ? | Oui car les serveurs DNS sont listés |
| Adresse IP du serveur DNS | 172.16.40.1 |
| Durée du bail si DHCP activé | 8 jours |
| Comment la station obtient-elle son adresse IPv6 ? | Grâce à DHCP qui en attribue une automatiquement |
| Adresse IPv6 de la station | fe80::dd7c:ed8b:e875:d983%14 |
| IAID DHCP v6 | 115373031 |
| DUID de client DHCP v6 | 00-01-00-01-2C-91-20-A6-E0-73-E7-B2-64-D7 |

DHCP (Dynamic Host Configuration Protocol) permet de donner une adresse IP automatiquement, une passerelle par défaut et les serveurs DNS.

**Questions :**

-L’adresse IP sert à amener les paquets sur le réseau, sans elle, le poste ne peut pas aller sur internet. De plus, les adresses IP sont reliées à un fournisseur d’accès internet.

-L’adresse MAC est reliée à une interface réseau. L’ordinateur peut en avoir plusieurs donc plusieurs adresses MAC.

L'adresse MAC (Media Access Control) sert à identifier le poste et à communiquer sur un réseau local.

- L’adresse MAC est aussi appelée l’adresse Ethernet (les plus couramment utilisées) ou adresse de couche 2 (là où elles interviennent).

- IAID (Identity Association Identifier) permet d’identifier une adresse IPv6 avec une interface réseau. Et DUID (DHCP Unique Identitifier) permet au serveur DHCP de reconnaître un client spécifique.

|  |  |  |
| --- | --- | --- |
| COMPUTERNAME | B181-102 | C’est pour identifier l’appareil sur un réseau |
| USERDOMAIN | SIO | C’est le nom du domaine dans lequel il se trouve, pour le localiser plus facilement dans les grandes entreprises |
| USERDNSDOMAIN | SIO.LOCAL | C’est l’adresse du nom de domaine complet |
| USERNAME | UTI029 | Le nom de l’utilisateur |
| LOGONSERVER | \\AL-DC-02 | C’est pour savoir qui à authentifié l’utilisateur |

### 3.3.3 Accès aux informations en mode graphique

#### 3.3.3.1 Informations système

|  |  |
| --- | --- |
|  | On peut voir les spécifications de l’appareil, son nom, le nom du processeur, la RAM, le système d’exploitation et le processeur.  Et celles de Windows avec son édition, sa version, la date d’installation du système d’exploitation et la build du système d’exploitation. |

Mémoire RAM (Random Access Memory) sert de mémoire temporaire le temps que le processeur les traite ou les utilise.

Build est la version exacte du système d’exploitation de l’ordinateur.

#### 3.3.3.2 : Informations réseau

|  |  |
| --- | --- |
| *Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement* | On voit la carte réseau utilisée, plusieurs protocoles et les services et composants de la connexion réseau. On a déjà vu les protocoles IPv4 et IPv6 car la fenêtre montre la configuration des protocoles et des services réseaux activés de la connexion Ethernet. |

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement | On voit le modèle de la carte réseau utilisée, l’adresse MAC, le DHCP activé, les informations de l’IPv4 et l’IPV6 et leurs passerelles, le masque de sous-réseau, le bail obtenu et expirant, le DHCP, le DNS, le WINS et le NetBIOS. On a déjà rencontré ces informations dans les paramètres TCP/IP car ça concerne aussi les protocoles IP. |

Carte réseau :

|  |  |
| --- | --- |
| Constructeur de la carte réseau | Intel |
| La carte réseau fonctionne-elle correctement ? |  |
| Date du pilote | 05/05/2024 |
| Indiquez un des fichiers du pilote | Une image contenant texte, Police, capture d’écran, ligne  Description générée automatiquement |

Connexion Ethernet :

|  |
| --- |
| Une image contenant texte, capture d’écran, nombre, Police  Description générée automatiquement |

Ordinateur :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, Police  Description générée automatiquement | On voit les détails des informations comme  La connexion IPv4 et IPv6,  L’état du média (carte réseau active),  La durée de la connexion au réseau,  Sa vitesse à la connexion au réseau  Les données reçues et  Les données envoyées |

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquementTous les contrôleurs de domaine :

|  |
| --- |
|  |

|  |
| --- |
| Une image contenant texte, Police, ligne, nombre  Description générée automatiquement. |

- Ce sont les noms qui ont un compte utilisateur du système.

Postes de la salle :

|  |  |
| --- | --- |
|  | Il n’y a que le poste B181\_PROF qui est sur ETCD, ayant plus de droits que les élèves.  Les autres postes sont sur ETTD. |

ETTD (Équipement Terminal de Traitement de Données) permet aux utilisateurs de traiter les données.

ETCD (Équipement Terminal de Concentration de Données) permet de gérer la transmission des données.

Contrôleurs de domaine :

|  |  |
| --- | --- |
|  | On voit une liste des contrôleurs du domaine sio.local. Ils servent la sécurité, l’authentification et les services de nos comptes. |

On n’a jamais vu ses noms.

Utilisateur voisin :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement | On effectue une recherche des utilisateurs dans le réseau sio.local pour trouver le nom de ma voisine (uti022). |
| Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement | On n’a pas accès aux informations concernant l’utilisateur, je ne peux donc pas vérifier si c’est bien elle.  (Je lui ai demandé son utilisateur pour effectuer une recherche sur elle). |

Utilitaire ping et résolution de noms :

Les adresses IP privées sont utilisées essentiellement pour les tests locaux. Elles permettent aux appareils de se connecter et de communiquer entre eux sans être accessibles directement depuis Internet. Ce type d’adresses est très utile pour effectuer des tests en toute sécurité, car elles ne sont pas visibles de l’extérieur.

Ping :

|  |
| --- |
|  |
|  |
|  |
|  |

-C’est un protocole ICMP (Internet Control Message Protocol) qui communique des informations sur le réseau et sert principalement à diagnostiquer d’éventuels problèmes.

-Il y a les 3 couches mises en œuvre, la couche 1 et 2 ne sont pas visibles mais permettent de structurer et transporter les paquets et la couche 3 se voit avec l’utilisation de l’ICMP et du ping.

-Les adresses IP privées sont utilisées pour les réseaux privés dans les communications dans ce réseau, afin éviter qu’elles soient attaquables de l’extérieur.

« ping %LOGONSERVER:\=% » :

|  |
| --- |
|  |

-L’adresse IP de Shayma est 172.31.1.106 et son nom de poste est B18122.

# 4 : Utiliser Windows PowerShell :

## 4.3 Commandes PowerShell et Invite de commande :

Commande dir :

|  |  |
| --- | --- |
|  | La commande dir affiche le contenu du répertoire C:\Windows\System32, le volume, le numéro de série du disque et la date de modification de chaque fichier. Elle permet de voir le détail des fichiers et dossiers dans C:\Windows\System32. |

|  |  |
| --- | --- |
| Ping |  |
| Cd | On est passé du répertoire C:\Windows\System32 à C:\Users |
| Ipconfig |  |

## 4.4 : Explorez les applets de commande :

- La commande PowerShell pour dir est « Get-ChildItem ».

## 4.5 : Commande Netstat avec PowerShell :

Commande Netsat -h :

|  |
| --- |
|  |

- La commande qui permet d’afficher la table de routage de l’ordinateur avec les routes actives est « route print».

Route print :

|  |  |
| --- | --- |
|  | Nous voyons  La liste des interfaces, Ethernet Intel I219-LM et Software Loopback Interface,  La table de routage IPv4 avec les itinéraires actifs  Des exemples d’entrée,  La table de routage IPv6 et  Les itinéraires persistants. |

- La passerelle IPv4 est un routeur qui dirige le trafic vers d'autres réseaux quand la destination n’est pas sur le même réseau.

Informations PID :

|  |
| --- |
|  |

PID (Process Identifier) est un identifiant unique pour les processeurs qui sert à suivre et gérer chaque processeur.

## 4.6 Videz la corbeille avec PowerShell :

- Grâce à la commande « Clear-RecycleBin » sur PowerShell, la poubelle est vidée.

Programme pour afficher les processus actifs et les backdoor existants :

|  |  |
| --- | --- |
|  | Fichier contenant le code pour afficher les processus actifs et les backdoors existants : |
|  |  |
| Il n’y a donc pas de backdoors suspicieux |

- Je m’attendais à ne pas trouver de backdoors suspicieux, ce qui est arrivé mais pour améliorer le programme et le rendre plus intéressant, on pourrait analyser tous les ports ouverts et pas seulement les ports 4444, 1337 et 8080.

Explications du programme :

* « Write-Host "Listing active processes..."» :  Affiche un message informant l'utilisateur que les processus actifs sont en cours d'énumération.
* « Get-Process » : Récupère la liste de tous les processus en cours d'exécution sur la machine.
* « Select-Object Id, ProcessName, CPU, StartTime » : Sélectionne les informations importantes sur chaque processus.
* « Sort-Object -Property CPU -Descending » : Trie les processus par l'utilisation du CPU, du plus élevé au plus bas.
* « Format-Table -AutoSize » : Formate la sortie sous forme de table.
* « $backdoorPorts = @(4444, 1337, 8080) » : Déclare une liste de ports considérés comme suspects (4444, 1337, et 8080).
* « Write-Host "Searching for potential backdoors..." -ForegroundColor Red » : Affiche un message en rouge pour indiquer qu'une recherche de backdoors est en cours sur les ports spécifiés.
* « Get-NetTCPConnection » : Récupère toutes les connexions TCP actives sur la machine.
* « Where-Object { $backdoorPorts -contains $\_.LocalPort -and $\_.State -eq 'Listen' } » : Filtre les connexions TCP pour ne garder que celles qui écoutent sur les ports spécifiés (4444, 1337, 8080) et dont l'état est 'Listen' (en attente de connexion).
* « if ($networkConnections) »: Vérifie s'il existe des connexions réseau suspectes sur les ports spécifiés.
* « foreach ($backdoor in $networkConnections) »: Parcourt chaque connexion réseau suspecte.
* « $process = Get-Process -Id $backdoor.OwningProcess  » : Récupère le processus correspondant à la connexion réseau suspecte en utilisant l'ID du processus propriétaire de la connexion.
* « ErrorAction SilentlyContinue » : ignorer les erreurs si le processus n'est pas trouvé.
* « Write-Host "Potential Backdoor Detected..." » : Si un processus est trouvé, le script affiche un avertissement en rouge, indiquant qu'un backdoor potentiel a été détecté, en fournissant le nom du processus, son PID (Process ID), et le port sur lequel il écoute.
* « else { Write-Host "No suspicious backdoors found..." } » : Si aucune connexion suspecte n'est trouvée, le script affiche un message en vert pour indiquer qu'il n'y a pas de backdoors détectés sur les ports spécifiés.

Commandes pour simplifier les tâches d’un analyste en sécurité :

|  |  |
| --- | --- |
| Get-Process | Récupérer des informations sur les processus qui s’exécutent sur le système.  Pour surveiller les processus actifs sur le système |
| Get-Service | Where-Object { $\_.Status -eq 'Running' } | Lister les services qui sont en cours d'exécution sur le système.  Visualiser tous les services en cours d'exécution. |
| Get-NetTCPConnection | Obtenir des informations détaillées sur les connexions TCP actives sur le système.  Afficher des informations détaillées sur les connexions réseau actives. |
| netstat -an | findstr LISTENING | Lister uniquement les connexions réseau TCP en état "LISTENING" (en écoute). C’est le mélange des commandes netstat -an et findstr LISTENING.  Identifier rapidement les ports ouverts. |
| Get-LocalUser | Lister et récupérer des informations sur les utilisateurs locaux d'un système.  Identification des comptes non autorisés ou des comptes créés récemment. |

TCP (Transmission Control Protocol) est responsable de la connexion fiable entre deux machines.

Commande PowerShell en ligne de commande :

|  |  |  |  |
| --- | --- | --- | --- |
| Get-Process |  | tasklist |  |
| Get-Service | Where-Object { $\_.Status -eq 'Running' } |  | sc query state= running |  |
| Get-NetTCPConnection |  | netstat -ano |  |
| netstat -an | findstr LISTENING |  | netstat -an | findstr LISTENING |  |
| Get-LocalUser |  | net user |  |

# 5: Exercices de calcul de réseaux:

## 5.1: Activitée 5:

Adresse IP du serveur 3: 89.0.223.96 car c’est la première du réseau 4

Adresse IP du serveur 2 : 150.179.0.4 car c’est la quatrième du réseau 2

Adresse IP du serveur 1 : 199.64.196.4 car c’est la quatrième du réseau 2

## 5.2 : Activité 6 :

* Le sous-réseau A a besoin de 50 équipements, un masque de /26 pour avoir 64 adresses IP, de 192.168.1.1 à 192.168.1.63, la première et la dernière adresse sont réservées à l’adresse réseau (192.168.1.0) et l’adresse de diffusion (192.168.1.64). Le masque de sous-réseau est 255.255.255.192 car il a potentiellement 64 adresses IP. Le PC A a donc l’adresse IP 192.168.1.1 et l’interface l’adresse IP 192.168.1.62 (la 192.168.1.63 étant déjà prise mais pas sur les interfaces visibles)

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

L’adresse réseau désigne uniquement le réseau, elle ne peut pas être rattachée à un appareil.

L’adresse de diffusion envoie des messages à tous les appareils du sous-réseau, elle ne peut pas non plus être attribuée à un réseau.

* Le sous-réseau B a besoin de 35 équipements, un masque de /26 permet d’avoir 64 adresses IP, de 192.168.1.66 à 192.168.1.126, la première et la dernière adresse sont réservées à l’adresse réseau (192.168.1.65) et l’adresse de diffusion (192.168.1.127). Le masque de sous-réseau et le même que pour le sous-réseau A (255.255.255.192) car il a le même nombre d’adresses IP possible. L’adresse IP de l’interface sera donc 192.168.1.126 et celle du PC B 192.168.1.66.
* Le réseau C a besoin de 20 équipements, un masque de /27 permet d’avoir 32 adresses IP de 192.168.1.129 à 192.168.1.158, la première et la dernière adresse sont réservées à l’adresse réseau (192.168.1.128) et l’adresse de diffusion (192.168.1.159). le masque de sous-réseau est 255.255.255.224, car il a potentiellement 32 adresses IP. L’interface a donc 192.168.1.126 comme adresse IP et PC C 192.168.1.129
* Le sous-réseau D a besoin de 25 équipements, un masque de /27 permet d’avoir 32 adresses IP de 192.168.1.161 à 192.168.1.189, la première et la dernière adresse sont réservées à l’adresse réseau (192.168.1.160) et l’adresse de diffusion (192.168.1.191). Le masque de sous-réseau est le même que pour le sous-réseau C (192.168.1.128) car il a le meme nombre d’adresses IP possible. L’interface a donc 192.168.1.191 comme adresse IP et PC D 192.168.1.161.
* Le sous-réseau pour la liaison des bâtiments n’a besoin que de 2 adresses IP (pour chaque routeur), un masque de /30 permet d’avoir 4 adresses IP de 192.168.1.193 à 192.168.1.194, la première et la dernière adresse sont réservées à l’adresse réseau (192.168.1.192) et l’adresse de diffusion (192.168.1.195). Le masque de sous-réseau sera de 255.255.255.252 comme il y a maximum 2 adresses IP. L’adresse IP du routeur 1 sera donc 192.168.1.193 et celle du routeur 2 192.168.1.194.

# Conclusion:

Ce TP nous a permis de découvrir le protocole TCP/IP, un élément important pour la communication du réseau. Nous avons appris à récupérer des informations réseau, automatiser certaines tâches via PowerShell et effectuer des calculs de sous-réseaux. Ce qui a développé notre capacité à diagnostiquer et administrer un réseau de manière autonome.