**CARON**

²

Atelier

B

1

-

1

*25/09/2023*

*Prise en main de Packet tracert*

Table des matières

[II. Introduction : 3](#_Toc146798649)

[III. Vérifications et découvertes des services 3](#_Toc146798650)

[a) Configuration et teste du PC-1 3](#_Toc146798651)

[a) Configuration et teste du PC-2 4](#_Toc146798652)

[b) Vérification de la connexion avec ORANGE et FREE 4](#_Toc146798653)

[5](#_Toc146798654)

[c) Comparaison du nombre de sauts effectués par PC-MIO et PC-1 pour joindre www.google.com 6](#_Toc146798655)

[d) Modifier de la configuration IP de PC-3 et PC-4 pour qu’ils obtiennent une adresse IP dynamique 7](#_Toc146798656)

[IV. Trame Arp 7](#_Toc146798657)

[e) Explication de l’arp 7](#_Toc146798658)

[f) Simulation ARP. 9](#_Toc146798659)

[g) Constat de l’activité 11](#_Toc146798660)

[V. Partie 2 : Complétion de la maquette 11](#_Toc146798661)

[h) Agrandissement du réseau : 12](#_Toc146798662)

[i) Découverte fonctionnement routeur : 13](#_Toc146798663)

[VI. Packet Tracer et le sans-fil 14](#_Toc146798664)

[VII. FTP 17](#_Toc146798665)

[VIII. Partie maison intelligente : 20](#_Toc146798666)

[j) Détecteur de fumé : 22](#_Toc146798667)

[IX. Conclusion : 23](#_Toc146798668)

# Introduction :

Dans ce rapport, nous allons explorer les notions essentielles pour un étudiant en BTS SIO, notamment les bases de la découverte de Packet Tracer, les réseaux, les couches du modèle OSI et les protocoles fondamentaux.

Ces bases essentielles nous seront d'une grande aide pour comprendre le fonctionnement des réseaux et des routeurs à l'avenir

# Vérifications et découvertes des services

## Configuration et teste du PC-1

|  |  |
| --- | --- |
|  | L'adresse IP est **dynamique** en raison de la présence d'un service **DHCP.**  L'adresse IP du serveur DHCP est **192.168.1.200**.  La passerelle par défaut est **192.168.1.1.**  L'adresse du serveur DNS est **8.8.8.8.**  L'adresse **8.8.8.8** correspond aux serveurs DNS publics de Google qui sont utilisés.  Une image contenant horloge, texte, Graphique, capture d’écran  Description générée automatiquement |

## Configuration et teste du PC-2

|  |  |
| --- | --- |
|  | L'adresse IP attribuée est dynamique, avec l'adresse **192.168.1.102**, tandis que le serveur DHCP à l'adresse **192.168.1.200**.  La passerelle par défaut est configurée à **192.168.1.1**.  En ce qui concerne le serveur DNS, il est défini avec l'adresse **8.8.8.8.** |

## Vérification de la connexion avec ORANGE et FREE

|  |  |
| --- | --- |
| **Test PC-1** | **Test PC-2** |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement |

Effectivement, la co**m**munication semble être valide. Il est à noter que dans les deux cas, le trafic transite par l'adresse **193.253.148.241**, qui correspond à l'adresse du switch.

Les [TTL (Time To Live),](https://ipwithease.com/what-is-time-to-live-ttl-in-networking/) ou temps de vie en français, sont des valeurs incluses dans les en-têtes des paquets de données transmis sur un réseau. Le TTL indique le nombre maximum de sauts ou de routeurs que le paquet peut traverser avant d'être abandonné ou expiré. Le TTL est généralement exprimé en secondes ou en sauts (hops).

Lorsqu'un paquet de données est émis, le TTL est initialisé à une certaine valeur par l'émetteur, souvent **64** ou **128**, selon le système d'exploitation. À chaque saut ou passage par un routeur, le TTL est décrémenté de 1. Lorsque le TTL atteint zéro, le routeur actuel jette le paquet et envoie un message d'erreur ICMP (Internet Control Message Protocol) à l'expéditeur pour l'informer que le paquet a été abandonné.

Dans notre cas, si le tracert montre que les TTL ont diminué de 3 à chaque saut, cela signifie que vous avez rencontré trois routeurs ou switchs intermédiaires entre votre point de départ et votre destination finale. Chacun de ces switchs a décrémenté le TTL de 1. Cela est conforme au fonctionnement normal d'un tracert, qui trace le chemin emprunté par les paquets à travers le réseau en révélant les routeurs intermédiaires et les sauts.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

En résumé, les TTL sont utilisés pour éviter que les paquets de données ne circulent indéfiniment sur le réseau en déterminant une durée de vie maximale. Dans votre tracert, une réduction de 3 dans les TTL indique que vous avez traversé trois switchs ou routeurs intermédiaires sur votre chemin.

Vérification de l’accès aux serveurs WEB de GOOGLE

## Une image contenant texte, Appareils électroniques, capture d’écran, logiciel Description générée automatiquement

|  |  |
| --- | --- |
| **Accès à www.google.com** | **Accès à mail.google.com** |
| Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement |  |

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement**Vérification de la communication de PC-MIO avec FREE**

## Comparaison du nombre de sauts effectués par PC-MIO et PC-1 pour joindre www.google.com

Cette étape est entreprise pour vérifier la connectivité à travers la **couche 3 du modèle OSI.** Il est important de noter que la vérification par le navigateur peut afficher le contenu en utilisant l'interface de la couche application, mais elle ne nous permet pas de voir les détails de la couche TCP, par exemple.

Pour comparer les sauts TTL, personnellement, je préfère utiliser l'outil **tracert**.

|  |  |
| --- | --- |
| **PC-MIO** | **PC-1** |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | Une image contenant texte, capture d’écran, Police  Description générée automatiquement |

En utilisant la commande ping, il est **IMPOSSIBLE** d'identifier quel PC a émis la requête, car les réponses ne fournissent pas cette information.

Dans les deux cas, s'il y a le même nombre de sauts, il est probable que vous ayez utilisé un paramètre spécifique dans la commande ping pour définir le nombre de sauts maximal. Cela expliquerait pourquoi le nombre de sauts est identique.

Il est vrai que le temps en millisecondes (ms) peut varier légèrement d'une tentative à l'autre en raison de facteurs tels que la charge du réseau et la latence.

Cependant, le nombre de sauts, lui, reste constant en fonction de la configuration spécifiée dans la commande ping. C'est pourquoi l'utilisation d'outils comme tracer peut-être plus précise pour cartographier le chemin suivi par les paquets à travers le réseau.

## Modifier de la configuration IP de PC-3 et PC-4 pour qu’ils obtiennent une adresse IP dynamique

Utiliser l’outil « **IP Configuration** »

|  |  |
| --- | --- |
| **PC-3** | **PC-4** |
| Une image contenant texte, capture d’écran, logiciel, nombre  Description générée automatiquement | Une image contenant texte, capture d’écran, logiciel, nombre  Description générée automatiquement |

L'utilisation du protocole DHCP (Dynamic Host Configuration Protocol) attribue des adresses IP différentes à chaque poste de manière intentionnelle pour éviter toute confusion.

Dans notre cas, les adresses IP attribuées par le DHCP sont logiquement ordonnées :

PC 3 a reçu l'adresse IP : 192.168.1.103

PC 4 a reçu l'adresse IP : 192.168.1.104

Cette méthodologie d'attribution d'adresses IP par le DHCP permet de gérer efficacement les ressources IP disponibles tout en garantissant une connectivité réseau sans conflits entre les appareils.

# Trame Arp

## Explication de l’arp

Dans cette partie, nous allons explorer le fonctionnement de l'ARP (Address Resolution Protocol) et sa fonction.

L'ARP est un protocole essentiel au bon fonctionnement des réseaux locaux. Il permet de faire la **correspondance** entre une **adresse IP** (Internet Protocol) et une **adresse MAC** (Media Access Control). Voici comment il fonctionne :

1. Besoin de correspondance IP-MAC : Lorsqu'un appareil dans un réseau local souhaite communiquer avec un autre appareil, il utilise l'adresse IP de la cible pour l'atteindre. Cependant, pour envoyer effectivement les données, il a besoin de l'adresse MAC de la cible, car les appareils se reconnaissent au niveau matériel par leurs adresses MAC.

2. Recherche dans le cache ARP : Tout d'abord, l'ordinateur qui souhaite communiquer vérifie son cache ARP local pour voir s'il possède déjà l'association entre l'adresse IP cible et l'adresse MAC correspondante. Si cette association est déjà présente, aucune action supplémentaire n'est nécessaire, et la communication peut avoir lieu.

3. Demande ARP : Si l'association IP-MAC n'est pas dans le cache ARP, l'appareil envoie une requête ARP de diffusion (ARP Request) à l'ensemble du réseau local. Cette requête ARP contient l'adresse IP de la cible et demande à tout appareil qui possède cette adresse IP de répondre avec son adresse MAC.

4. Réponse ARP : L'appareil cible, en recevant la requête ARP qui lui est destinée, répond avec un message ARP de réponse (ARP Reply) contenant son adresse MAC. Ce message est alors capturé par l'ordinateur émetteur de la requête ARP.

5. Mise à jour du cache ARP : Une fois que l'adresse MAC de la cible est reçue, l'ordinateur émetteur met à jour son cache ARP avec cette nouvelle association IP-MAC pour des communications futures.

L'ARP est crucial dans les réseaux locaux car il permet de traduire efficacement les adresses IP en adresses MAC, facilitant ainsi la communication entre les appareils. Sans ARP, la communication serait difficile, voire impossible, car les ordinateurs ne pourraient pas déterminer comment atteindre d'autres appareils sur le réseau.

Partie pratique :

Je vais illustrer chacune de ces parties à travers une démonstration pratique :

Sous Windows la commande ARP – D permet de vider le cache arp.

Et ARP – A d’afficher notre table arp

Dans l'exemple ci-dessous, si l'on exécute la commande arp -d avant arp -a, on remarque que rien ne s'affiche, ce qui est normal car le cache ARP vient d'être vidé

|  |  |
| --- | --- |
| Pour obtenir une réponse affichée, on peut utiliser la commande tracert vers google.com.  Dans notre cas, nous allons suivre la route du paquet jusqu'à l'adresse **8.8.8.8**, qui est automatiquement associée à google.com grâce au DNS  En effectuant à nouveau un arp -a, on peut constater que notre table ARP s'est remplie et que nous avons associé une adresse physique au routeur/passerelle par défaut. |  |

## Une image contenant texte, Appareils électroniques, capture d’écran, affichage Description générée automatiquementSimulation ARP.

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

Description générée automatiquement

Dans le contexte de la démonstration, voici comment vous pourriez formuler cette partie :

"En mode simulation, nous allons maintenant essayer d'envoyer une requête ping. Lorsque nous cliquons sur l'enveloppe, nous pouvons collecter les informations suivantes :

* Il s'agit d'un message de type ping du réseau, spécifiquement un « echo request ».
* Cette communication se situe au niveau de la couche 3, la couche de liaison.
* L'adresse source de cette requête est 192.168.1.103.
* L'adresse de destination est 192.168.1.101."

Cela rendra la description plus claire et structurée dans un rapport.

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement | En poursuivant notre analyse :  À la couche 2, qui est la couche physique, nous pouvons identifier les détails suivants :  L'adresse source de niveau 2 est : 00E0.A3CC.EB4A.  L'adresse FF:FF:FF:FF:FF:FF est une adresse de broadcast, ce qui est caractéristique du fonctionnement en broadcast du protocole ARP. |

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, Police  Description générée automatiquement | La différence majeure réside dans l'introduction d'un élément appelé 'Layers In', qui était absent des trames précédentes. De plus, cette fois-ci, les masques de sous-réseaux sont indiqués.  Il y a une seule entrée dans la table ARP, ce qui s'explique par le fait que nous communiquons uniquement avec une seule interface du switch. Cependant, il est important de noter que le switch communique avec plusieurs autres postes, ce qui signifie qu'il 'diffuse' la trame ARP pour que les autres appareils puissent également mettre à jour leur cache ARP |

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, Police  Description générée automatiquement | Dans l'étape suivante, nous ne traitons plus une requête de ping, mais plutôt une réponse au ping précédent. Il s'agit d'un message de type 'echo reply |

Après avoir effectué ces tests en simulation, nous avons maintenant deux adresses MAC associées à des adresses IP dans la table ARP

Étant donné que l'ARP est un protocole de découverte basé sur la diffusion (broadcast), et que nous avions précédemment vidé notre table ARP en utilisant 'arp -d', celle-ci était initialement vide. Cependant, du fait de l'envoi d'ARP en diffusion, la table ARP a été à nouveau remplie :

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

Description générée automatiquement

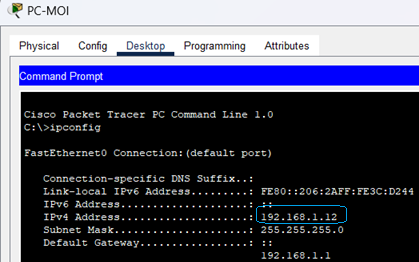
## Constat de l’activité

Nous pouvons désormais constater que notre table ARP est plus remplie. Si nous effectuons à nouveau un ping du PC-3 vers le PC-1, la différence majeure est que cette fois-ci, nous n'envoyons pas de requête vers une adresse de diffusion (broadcast), mais plutôt vers l'adresse MAC spécifique du PC-1, car nous la connaissons.

# Partie 2 : Complétion de la maquette

Dans cette section, nous allons ajouter plusieurs environnements réseau afin de mieux comprendre leur fonctionnement.

Pour ma part, sur le poste que j'ai configuré en IP dynamique, j'ai obtenu l'adresse IP suivante : **192.168.1.12.** Cette information peut être vérifiée à l'aide du terminal, comme illustré ci-dessous



Ensuite, j'ai vérifié que mon poste avait bien accès aux différents réseaux et équipements locaux. J'ai réalisé ces tests, que je vais diviser en deux parties :

* Test graphique couche application :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement |  |

* Test couche 3 commande :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

## Agrandissement du réseau :

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

Description générée automatiquementUne image contenant texte, capture d’écran, affichage, Police

Description générée automatiquementVous trouverez ci-dessous une liste des postes que j'ai ajoutés, ainsi que leurs configurations :Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquement

Teste de la connectivité a orange :

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquementUne image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

L'hôte est introuvable car le DNS ne le résout pas, c'est-à-dire qu'aucune association n'est trouvée.

## Découverte fonctionnement routeur :

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

Description générée automatiquementSous l'outil 'packet tracert', une variété d'aides sont mises à disposition pour nous guider, notamment sur la manière de compléter une commande ou pour trouver les commandes qui commencent par une certaine lettre

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

Description générée automatiquementUne image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

La commande enable permet d’activer le mode préviligier

|  |  |
| --- | --- |
| Montrer que vous obtenez bien le résultat demandé | Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement  Une image contenant texte, Police, capture d’écran, blanc  Description générée automatiquement |

# Packet Tracer et le sans-fil

Dans cette section, nous allons configurer PC0 pour utiliser DHCP. Voici les paramètres obtenus :

Adresse IP : 192.168.0.100

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 192.168.0.1

|  |  |
| --- | --- |
| Dans la configuration DHCP, on remarque que l'adresse IP est attribuée dans la plage appropriée, ce qui est tout à fait normal. Étant donné que cette plage s'étend de 100 à 149, le serveur DHCP a attribué la première adresse disponible, qui est 192.168.0.100, étant donné que PC0 est le seul appareil configuré en dynamique | Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur  Description générée automatiquement |

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

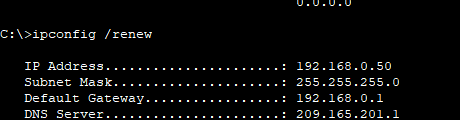
Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement



Après avoir changé la plage d'adresses IP, ma nouvelle adresse IP est 192.168.0.50.

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Connexion a distance de puis le pc

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

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

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

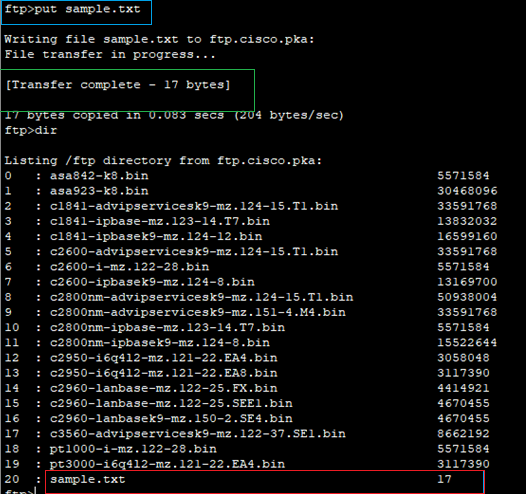
# FTP

Un serveur FTP (File Transfer Protocol) est un type de serveur utilisé pour le transfert de fichiers entre un client et un serveur via un réseau, en particulier sur Internet. Voici une définition concise et professionnelle :

Définition d'un serveur FTP : Un serveur FTP est un logiciel ou un système informatique dédié qui permet le transfert de fichiers entre des ordinateurs connectés à un réseau. Il utilise le protocole FTP pour gérer l'authentification des utilisateurs, l'accès aux répertoires et la transmission de fichiers.

Importance du FTP pour un administrateur réseau : Le FTP revêt une importance cruciale pour un administrateur réseau, car il lui permet de :

* Transférer efficacement des fichiers entre différents serveurs, facilitant ainsi la mise à jour de logiciels et la gestion des configurations.
* Assurer la sauvegarde et la restauration des données, élément essentiel pour la continuité des opérations.
* Collaborer avec des utilisateurs distants en partageant des fichiers rapidement et en toute sécurité

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

En bleu la commande pour mettre le

La commande **put sample.txt** permet de déposer le fichier dans le serveur FTP.

Il y a actuellement 20 fichiers dans le répertoire.

Mon fichier a une taille de 17 octets.

Vérification du téléchargement :

|  |  |
| --- | --- |
|  | * **En rouge : La commande pour se connecter au FTP de Cisco.** * **En vert : La commande qui nous permet de télécharger notre fichier que nous avons exporté sur le FTP.** * **En mauve : L'indication du nombre de bytes de notre fichier.** * **Dir : Une fois que nous avons quitté le mode FTP, nous permet d'afficher le fichier que nous avons téléchargé.** |
|  | * Une image contenant texte, capture d’écran, logiciel, affichage    Description générée automatiquement * Une image contenant texte, capture d’écran, affichage, logiciel    Description générée automatiquement |

|  |  |
| --- | --- |
| **Avantage de server FTP :** | **Inconvénient** |
| * Facilité de Configuration : Les serveurs FTP sont relativement simples à mettre en place et à utiliser, en particulier avec des logiciels tels que FileZilla, qui permettent de créer facilement des serveurs FTP. * Compatibilité Étendue : Le protocole FTP est compatible avec une large gamme d'appareils et de systèmes d'exploitation, y compris Linux, Windows et macOS. * Gestion de Gros Fichiers : Le FTP prend en charge le transfert de gros fichiers, ce qui en fait une option pratique pour le partage et la distribution de données volumineuses. | * Sécurité Limitée : Le FTP présente des limitations en termes de sécurité, car il ne crypte pas les données lors du transfert, les exposant ainsi aux interceptions. Les données sont transmises en texte clair. * Configuration Requise : Comme pour tout service de ce type, la mise en place d'un serveur FTP nécessite l'ouverture de ports, ce qui exige une configuration minutieuse pour garantir la sécurité. * Complexité de Configuration : Pour rendre opérationnel un serveur FTP, il faut souvent effectuer de nombreuses configurations, gérer les droits d'utilisateur et obtenir des confirmations, ce qui peut être une tâche complexe. |

# Partie maison intelligente :

Sur ce schéma, nous pouvons observer que le premier câble est connecté à la télévision, tandis que le deuxième câble est relié à un 'cable modem'. Comme je n'étais pas familier avec cet appareil, j'ai effectué des recherches pour en apprendre davantage. Sa principale fonction est de convertir le signal provenant du câble coaxial en un signal réseau utilisable par un routeur ou un ordinateur. Il diffère ainsi d'un routeur classique, qui utilise l'Ethernet pour sa connectivité

Le câble modem sert d'interface entre le réseau du FAI (Fournisseur d'Accès à Internet) et le home gateway, qui, dans ce contexte, est un routeur connecté au modem câble.

Ce routeur joue le rôle de point central pour la distribution du réseau. Il dispose de ports Ethernet pour connecter des appareils par câble, ainsi que de fonctionnalités Wi-Fi pour permettre la connectivité sans fil.

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Nous pouvons contrôler les différentes STA qui sont connectées à la passerelle par défaut.

Il est à noter que quasiment tous les appareils de la maison sont connectés à la passerelle de la maison Une image contenant texte, logiciel, capture d’écran

Description générée automatiquementUne image contenant Rectangle, tableau blanc

Description générée automatiquementUne image contenant Rectangle, cadre photo, tableau blanc

Description générée automatiquement

La couleur verte est utilisée pour indiquer 'ouvert', tandis que la couleur rouge est utilisée pour 'fermer', ce qui correspond bien à l'anglais, où 'lock' signifie 'verrouiller' et 'unlock' signifie 'déverrouiller

## Détecteur de fumé :

Nous avons également la possibilité d'accéder au détecteur de fumée à distance et de surveiller son état. Cependant, il est important de noter que nous ne pouvons pas le contrôler à distance, ce qui est parfaitement compréhensible, car la fonction principale d'un détecteur de fumée est de protéger contre les incendies, et non pas d'être un gadget contrôlable à distance pour le divertissement.

Cependant, la surveillance à distance peut être utile dans certaines situations. De plus, je pense qu'il pourrait être possible d'influer sur ses valeurs en utilisant une méthode autre que l'interface graphique, un peu comme une injection SQL. Certaines technologies utilisent également des signaux électroniques pour cette communication

Cependant, il est important de noter qu'on peut démarrer la voiture dans le garage, ce qui peut entraîner une augmentation du taux de fumée détecté par le détecteur."

Cette reformulation rend l'information plus concise et compréhensible dans un rapport

Une image contenant texte, rouge

Description générée automatiquementUne image contenant texte, logiciel, Police, capture d’écran

Description générée automatiquement

Cependant, il est à noter que la MCU s'active automatiquement lorsque le taux de fumée augmente, ce qui a pour effet de réduire ce taux.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Elle ouvre automatiquement les portes et les fenêtres lorsque la fumée est détectée, puis les referme lorsque la fumée cesse.

Lorsque la voiture s'arrête, l'air se 'purifie', et il n'y a plus de fumée détectée.

# Conclusion :

Dans ce rapport, nous avons mis en évidence l'importance de sécuriser nos équipements et de les isoler pour mieux comprendre les risques associés aux appareils connectés et à l'IoT (Internet des objets). De plus, nous avons exploré les notions essentielles du fonctionnement des réseaux. Il est crucial de prendre conscience des risques qui nous entourent et de l'importance de la vigilance dans la gestion de ces divers équipements tout en les limitant.

Une approche intéressante aurait été de réaliser une analyse de la maison avec Wireshark ou un sniffer, malheureusement, nous n'avons pas eu accès à GNS3 pour cette expérience.

# Sources

**Source DNS :**

[**https://www.ionos.fr/digitalguide/serveur/know-how/le-serveur-dns-ne-repond-pas-que-faire/#:~:text=Les%20adresses%208.8.8.8%20et,l'adresse%20IP%20en%20cons%C3%A9quence**](https://www.ionos.fr/digitalguide/serveur/know-how/le-serveur-dns-ne-repond-pas-que-faire/#:~:text=Les%20adresses%208.8.8.8%20et,l'adresse%20IP%20en%20cons%C3%A9quence)**.**

**Type de requête ICMP :**

<https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-le-protocole-icmp/>

FTP :

https://filezilla-project.org/

TTL :

https://ipwithease.com/what-is-time-to-live-ttl-in-networking/