

Atelier 1 B-1

25/09/2023

Prise en main de Packet tracert

I. Table des matières

II.	Introduction :	3
III.	Vérifications et découvertes des services	3
a)	Configuration et teste du PC-1	3
a)	Configuration et teste du PC-2	4
b)	Vérification de la connexion avec ORANGE et FREE	4
		5
c)	Comparaison du nombre de sauts effectués par PC-MIO et PC-1 pour joindre www.google.com	6
d)	Modifier de la configuration IP de PC-3 et PC-4 pour qu'ils obtiennent une adresse IP dynamique	7
IV.	Trame Arp	7
e)	Explication de l'arp	7
f)	Simulation ARP	9
g)	Constat de l'activité	11
V.	Partie 2 : Complétion de la maquette	11
h)	Agrandissement du réseau :	12
i)	Découverte fonctionnement routeur :	13
VI.	Packet Tracer et le sans-fil	14
VII.	FTP	17
VIII.	Partie maison intelligente :	20
j)	Détecteur de fumé :	22
IX.	Conclusion :	23

II. 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

III. Vérifications et découvertes des services

a) Configuration et teste du PC-1

```
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix.:
Physical Address.....: 000C.CFB6.51EB
Link-local IPv6 Address.....: FE80::20C:CFFF:FEB6:51EB
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::

DHCP Servers.....: 192.168.1.1 gateway
                   192.168.1.200 DHCP
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-CA-10-E4-48-00-0C-CF-B6-51-EB
DNS Servers.....: ::
                  8.8.8.8

Bluetooth Connection:

Connection-specific DNS Suffix.:
Physical Address.....: 0009.7C54.7523
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-CA-10-E4-48-00-0C-CF-B6-51-EB
DNS Servers.....: ::
                  8.8.8.8
```

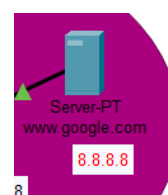
L'adresse IP est **dynamique** en raison de la présence d'un service **DHCP**.

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.



a) Configuration et teste du PC-2

```
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address...: 000C.CFB6.51EB
Link-local IPv6 Address...: FE80::20C:CFFF:FE86:51EB
IPv6 Address...: ::
IPv4 Address...: 192.168.1.102
Subnet Mask...: 255.255.255.0
Default Gateway...: ::

DHCP Servers...: 192.168.1.1
DHCPv6 IAID...: 192.168.1.200
DHCPv6 Client DUID...: 00-01-00-01-CA-10-E4-48-00-0C-CF-B6-51-EB
DNS Servers...: 8.8.8.8

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address...: 0009.7C54.7523
Link-local IPv6 Address...: ::
```

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**.

b) Vérification de la connexion avec ORANGE et FREE

Test PC-1	Test PC-2
<pre>C:\>ping www.orange.com Pinging 185.63.192.20 with 32 bytes of data: Reply from 185.63.192.20: bytes=32 time=136ms TTL=126 Reply from 185.63.192.20: bytes=32 time=66ms TTL=126 Reply from 185.63.192.20: bytes=32 time=76ms TTL=126 Reply from 185.63.192.20: bytes=32 time=89ms TTL=126 Ping statistics for 185.63.192.20: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 66ms, Maximum = 136ms, Average = 91ms C:\>ping www.free.fr Pinging 212.27.48.10 with 32 bytes of data: Reply from 212.27.48.10: bytes=32 time=139ms TTL=124 Reply from 212.27.48.10: bytes=32 time=128ms TTL=124 Reply from 212.27.48.10: bytes=32 time=116ms TTL=124 Reply from 212.27.48.10: bytes=32 time=104ms TTL=124 Ping statistics for 212.27.48.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 104ms, Maximum = 139ms, Average = 121ms</pre>	<pre>Cisco Packet Tracer PC Command Line 1.0 C:\>ping www.orange.com Pinging 185.63.192.20 with 32 bytes of data: Request timed out. Reply from 185.63.192.20: bytes=32 time=92ms TTL=126 Reply from 185.63.192.20: bytes=32 time=76ms TTL=126 Reply from 185.63.192.20: bytes=32 time=81ms TTL=126 Ping statistics for 185.63.192.20: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 76ms, Maximum = 92ms, Average = 83ms C:\>ping www.free.fr Pinging 212.27.48.10 with 32 bytes of data: Request timed out. Reply from 212.27.48.10: bytes=32 time=64ms TTL=124 Reply from 212.27.48.10: bytes=32 time=94ms TTL=124 Reply from 212.27.48.10: bytes=32 time=91ms TTL=124 Ping statistics for 212.27.48.10: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 64ms, Maximum = 94ms, Average = 83ms C:\></pre>

Effectivement, la communication 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)**, 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 tracer 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 switches a décrémenté le TTL de 1. Cela est conforme au fonctionnement normal d'un tracer, qui trace le chemin emprunté par les paquets à travers le réseau en révélant les routeurs intermédiaires et les sauts.

```

C:\>tracert www.free.fr

Tracing route to 212.27.48.10 over a maximum of 30 hops:

  1  0 ms  0 ms  0 ms  192.168.1.1
  2  27 ms 19 ms 40 ms 193.252.148.241
  3  44 ms 48 ms 39 ms 1.1.1.1
  4  53 ms 34 ms 17 ms 1.1.1.1.212
  5  32 ms 27 ms 32 ms 212.27.48.10

Trace complete.

C:\>tracert www.orange.com

Tracing route to 185.63.192.20 over a maximum of 30 hops:

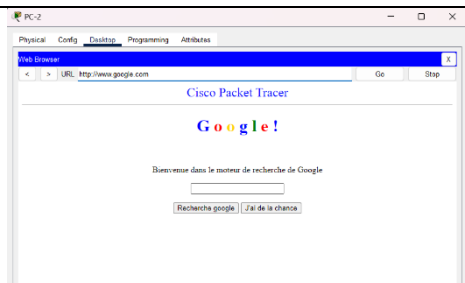
  1  0 ms  0 ms  0 ms  192.168.1.1
  2  31 ms 31 ms 32 ms 193.252.148.241
  3  23 ms 25 ms 24 ms 185.63.192.20

Trace complete.
```

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 tracer, une réduction de 3 dans les TTL indique que vous avez traversé trois switches ou routeurs intermédiaires sur votre chemin.

Vérification de l'accès aux serveurs WEB de GOOGLE

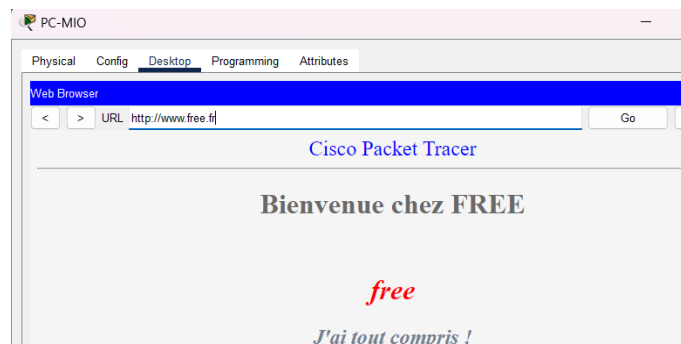
Accès à www.google.com



Accès à mail.google.com



Vérification de la communication de PC-MIO avec FREE



c) 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
<pre>C:\>ping www.google.com Pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8: bytes=32 time=143ms TTL=124 Reply from 8.8.8.8: bytes=32 time=146ms TTL=124 Reply from 8.8.8.8: bytes=32 time=105ms TTL=124 Reply from 8.8.8.8: bytes=32 time=126ms TTL=124 Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 105ms, Maximum = 146ms, Average = 130ms</pre>	<pre>C:\>ping www.google.com Pinging 8.8.8.8 with 32 bytes of data: Reply from 8.8.8.8: bytes=32 time=116ms TTL=124 Reply from 8.8.8.8: bytes=32 time=148ms TTL=124 Reply from 8.8.8.8: bytes=32 time=135ms TTL=124 Reply from 8.8.8.8: bytes=32 time=150ms TTL=124 Ping statistics for 8.8.8.8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 116ms, Maximum = 150ms, Average = 137ms</pre>
<pre>C:\>tracert www.google.com Tracing route to 8.8.8.8 over a maximum of 30 hops: 1 29 ms 0 ms 0 ms 192.168.1.1 2 54 ms 18 ms 79 ms 193.252.148.241 3 65 ms 53 ms 61 ms 1.1.3.1 4 74 ms 47 ms 69 ms 1.1.2.8 5 64 ms 58 ms 81 ms 8.8.8.8 Trace complete.</pre>	<pre>C:\>tracert www.google.com Tracing route to 8.8.8.8 over a maximum of 30 hops: 1 0 ms 0 ms 0 ms 192.168.1.1 2 50 ms 70 ms 67 ms 82.224.42.254 3 62 ms 76 ms 79 ms 1.1.1.1 4 64 ms 88 ms 23 ms 1.1.2.8 5 78 ms 73 ms 56 ms 8.8.8.8 Trace complete.</pre>

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

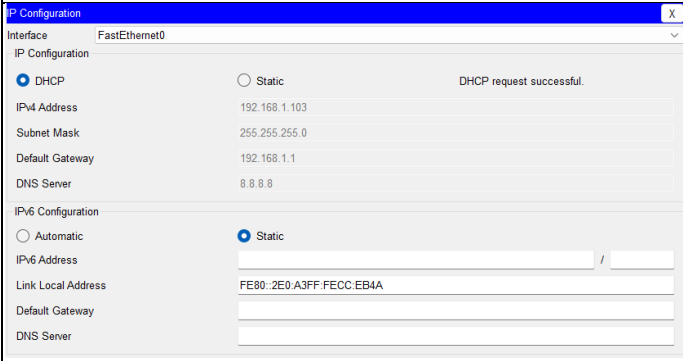
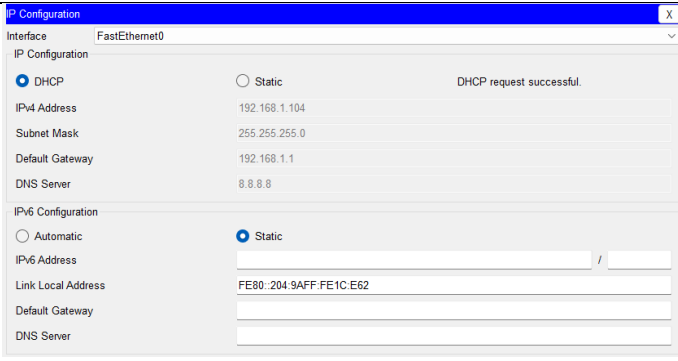
Dans les deux cas, s'il y a le même nombre de sauts, il est probable que vous ayez utilisé un paramètre spécifique dans la commande ping pour définir le nombre de sauts maximal. Cela expliquerait pourquoi le nombre de sauts est identique.

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.

d) 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
	

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.

IV. Trame Arp

e) 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.

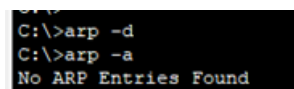
Partie pratique :

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



```
C:\>arp -d
C:\>arp -a
No ARP Entries Found
```


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/passarelle par défaut.

```
C:\>tracert www.google.com

Tracing route to 8.8.8.8 over a maximum of 30 hops:

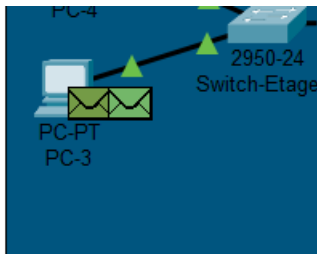
  1  0 ms    0 ms    0 ms    192.168.1.1
  2  34 ms   43 ms   34 ms   193.252.148.241
  3  21 ms   39 ms   56 ms   1.1.3.1
  4  58 ms   83 ms   27 ms   1.1.2.8
  5  54 ms   29 ms   52 ms   8.8.8.8

Trace complete.

C:\>arp -a

Internet Address      Physical Address      Type
-----
192.168.1.1           000a.41a7.aa01       dynamic
C:\>S
```

f) Simulation ARP.



PDU Information at Device: PC-3

OSI Model Outbound PDU Details

At Device: PC-3
Source: PC-3
Destination: 192.168.1.101

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3: IP Header Src. IP: 192.168.1.103, Dest. IP: 192.168.1.101 ICMP Message Type: 8
Layer2	Layer2
Layer1	Layer1

1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address is in the same subnet. The device sets the next-hop to destination.

Challenge Me << Previous Layer Next Layer >>

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.

PDU Information at Device: PC-3

OSI Model Outbound PDU Details

At Device: PC-3
Source: PC-3
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
	Layer 2: Ethernet II Header 00E0.A3CC.EB4A >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.103, Dest. IP: 192.168.1.101
Layer2	Layer 1: Port(s): FastEthernet0
Layer1	

1. The ARP process constructs a request for the target IP address.
2. The device encapsulates the PDU into an Ethernet frame.

Challenge Me << Previous Layer Next Layer >>

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.

0.003 Switch-Principal

PDU Information at Device: Switch-Etage-1

OSI Model Inbound PDU Details Outbound PDU Details

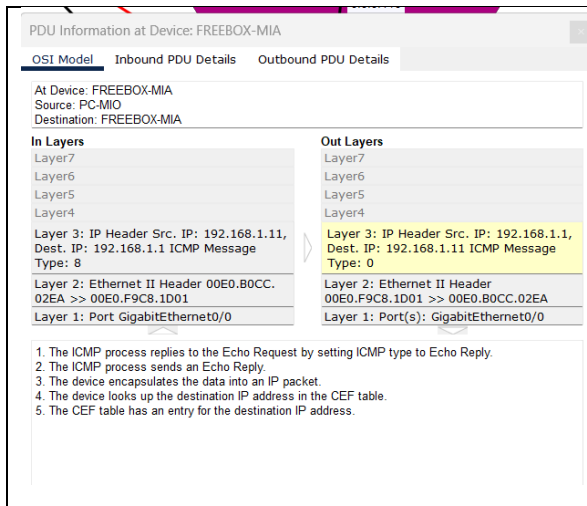
At Device: Switch-Etage-1
Source: PC-3
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 00E0.A3CC.EB4A >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.103, Dest. IP: 192.168.1.101	Layer 2: Ethernet II Header 00E0.A3CC.EB4A >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.1.103, Dest. IP: 192.168.1.101
Layer 1: Port FastEthernet0/24	Layer 1: Port(s): FastEthernet0/1 FastEthernet0/2 FastEthernet0/20

1. FastEthernet0/1 sends out the frame.
2. FastEthernet0/2 sends out the frame.
3. FastEthernet0/20 sends out the frame.

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



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 avons 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 :

```
C:\>arp -a
Internet Address      Physical Address      Type
192.168.1.1          000a.41a7.aa01       dynamic
192.168.1.101        000c.cfb6.51eb       dynamic
C:\>
```

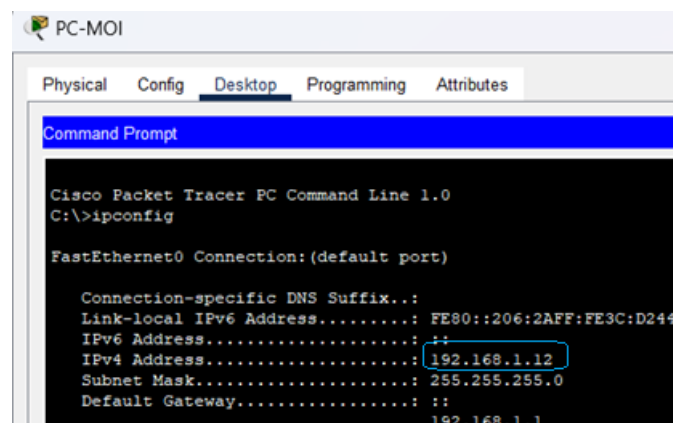
g) Constat de l'activité

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.

V. Partie 2 : Complétion de la maquette

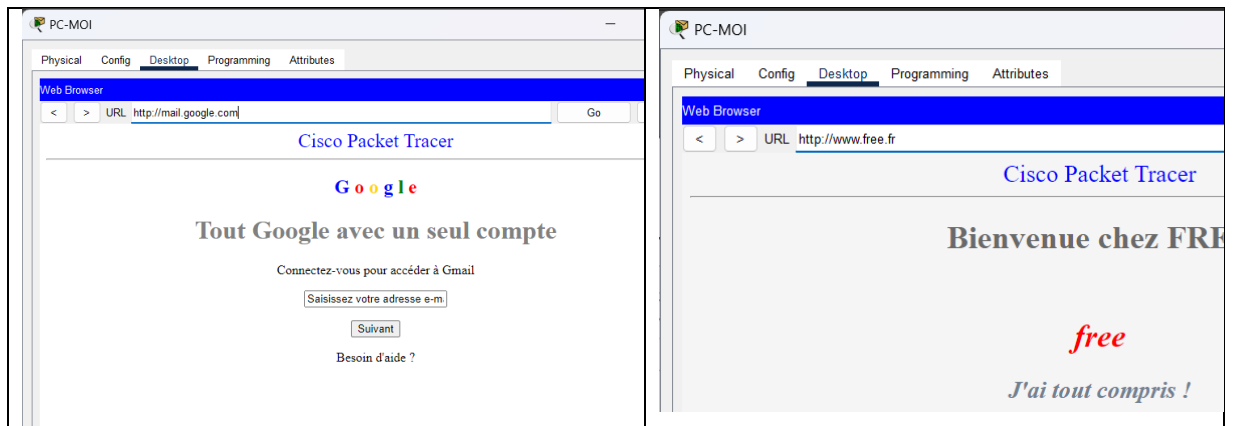
Dans cette section, nous allons ajouter plusieurs environnements réseau afin de mieux comprendre leur fonctionnement.

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 :



- Test couche 3 commande :

```
C:\>ping www.free.fr

Pinging 212.27.48.10 with 32 bytes of data:

Reply from 212.27.48.10: bytes=32 time=61ms TTL=126
Reply from 212.27.48.10: bytes=32 time=66ms TTL=126
Reply from 212.27.48.10: bytes=32 time=78ms TTL=126
Reply from 212.27.48.10: bytes=32 time=93ms TTL=126

Ping statistics for 212.27.48.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 93ms, Average = 75ms

C:\>ping mail.google.com

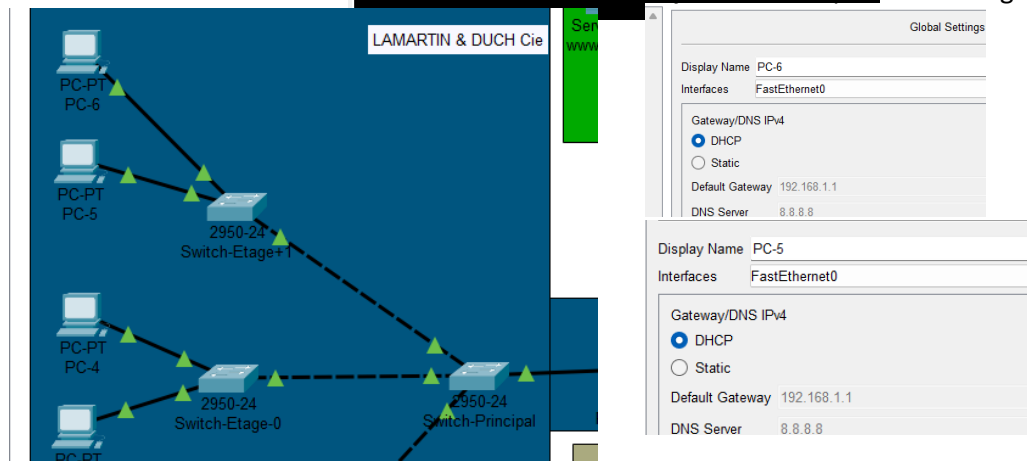
Pinging 8.8.8.96 with 32 bytes of data:

Reply from 8.8.8.96: bytes=32 time=78ms TTL=124
Reply from 8.8.8.96: bytes=32 time=68ms TTL=124
Reply from 8.8.8.96: bytes=32 time=82ms TTL=124
Reply from 8.8.8.96: bytes=32 time=72ms TTL=124

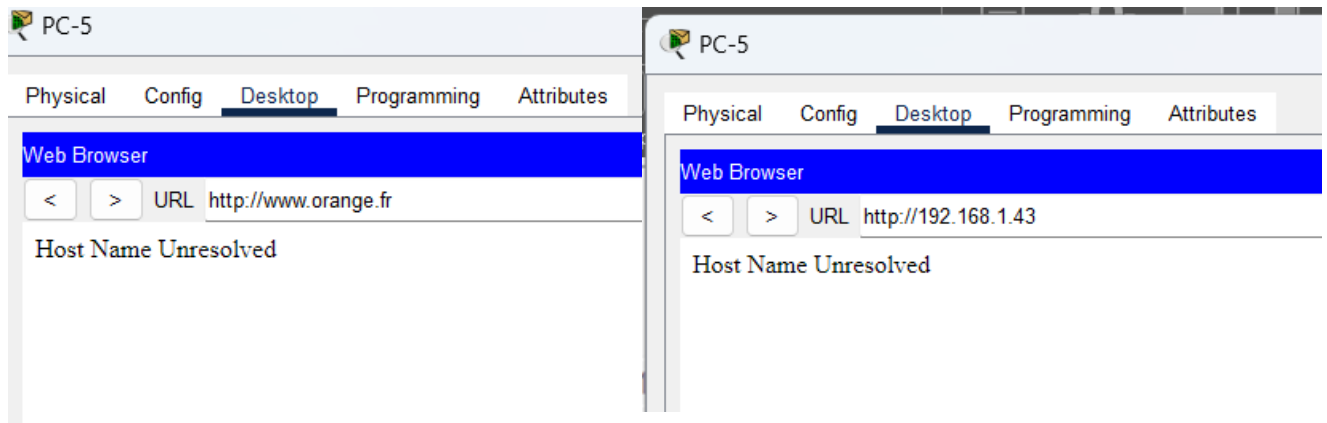
Ping statistics for 8.8.8.96:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 66ms, Maximum = 82ms, Average = 75ms
```

h) Agrandissement du réseau :

Vous trouverez ci-dessous un schéma de la configuration de nos équipements et leurs configurations :



Teste de la connectivité a orange :



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

i) Découverte fonctionnement routeur :

Sous l'outil 'packet tracer', 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

Router#?	Router#t?	Router#te?
clear clock configure connect copy	telnet terminal traceroute	telnet terminal
Router#c	Router#t	Router#te

La commande enable permet d'activer le mode privilégié

Montrer que vous obtenez bien le résultat demandé	<pre>Router#clock set 15:00:00 31 Jan 2035 Router# Router(config)#end Router# %SYS-5-CONFIG_I: Configured from console by console Router#show clock 15:4:41.341 UTC Wed Jan 31 2035 Router#</pre>
---	---

```
% Incomplete command.  
Router#clock set 15:00:00 ?  
<1-31> Day of the month  
MONTH Month of the year  
Router#clock set 15:00:00
```

VI. Packet Tracer et le sans-fil

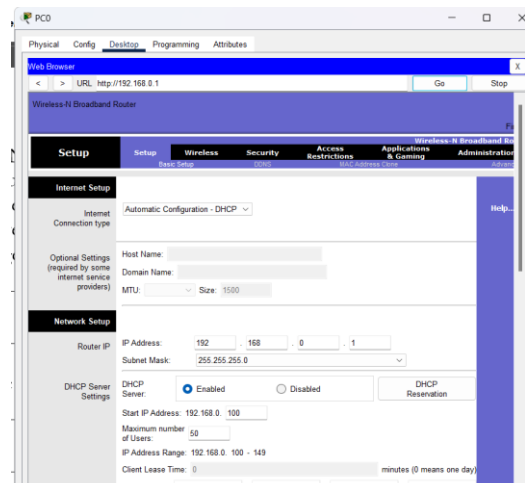
Dans cette section, nous allons configurer PC0 pour utiliser DHCP. Voici les paramètres obtenus :

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



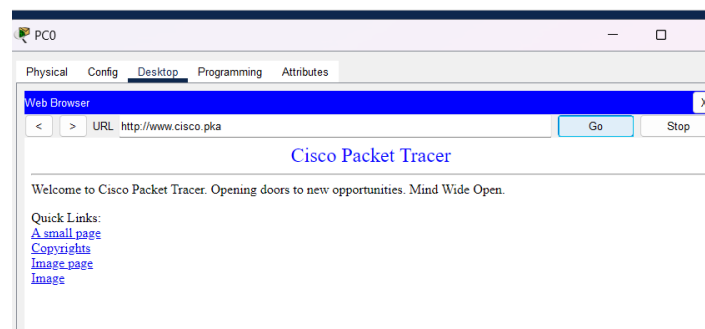
Setup	Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Wireless
	Basic Setup		DDNS		MAC Address Clone	
Internet Setup						
Internet Connection type: Static IP						
Internet IP Address: 209 . 165 . 200 . 225						
Subnet Mask: 255 . 255 . 255 . 252						
Default Gateway: 209 . 165 . 200 . 226						
DNS 1: 0 . 0 . 0 . 0						
DNS 2 (Optional): 0 . 0 . 0 . 0						
DNS 3 (Optional): 0 . 0 . 0 . 0						
Host Name:						
Optional Settings						

s: 30
ress Range: 192.168.0. 100 - 149
ress Time: 0

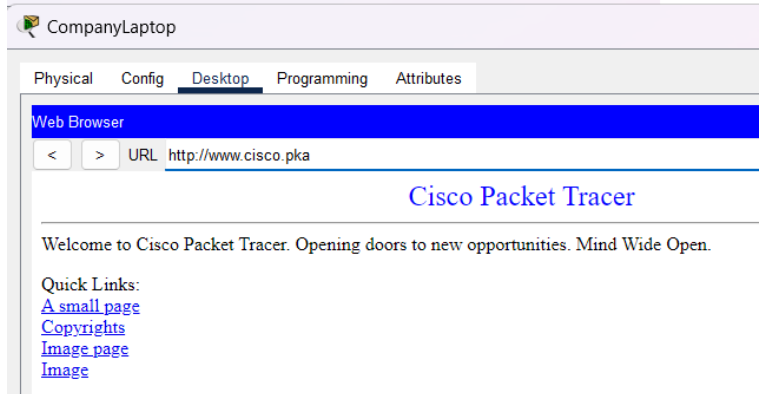
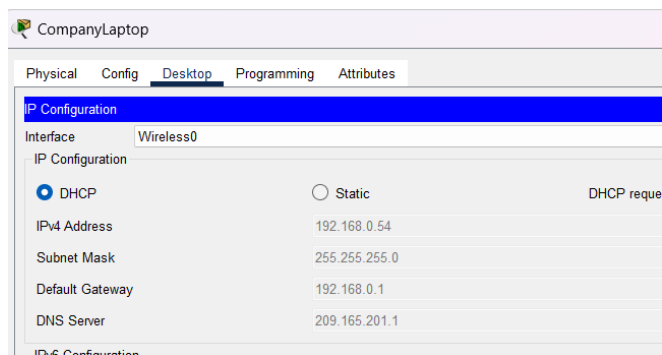
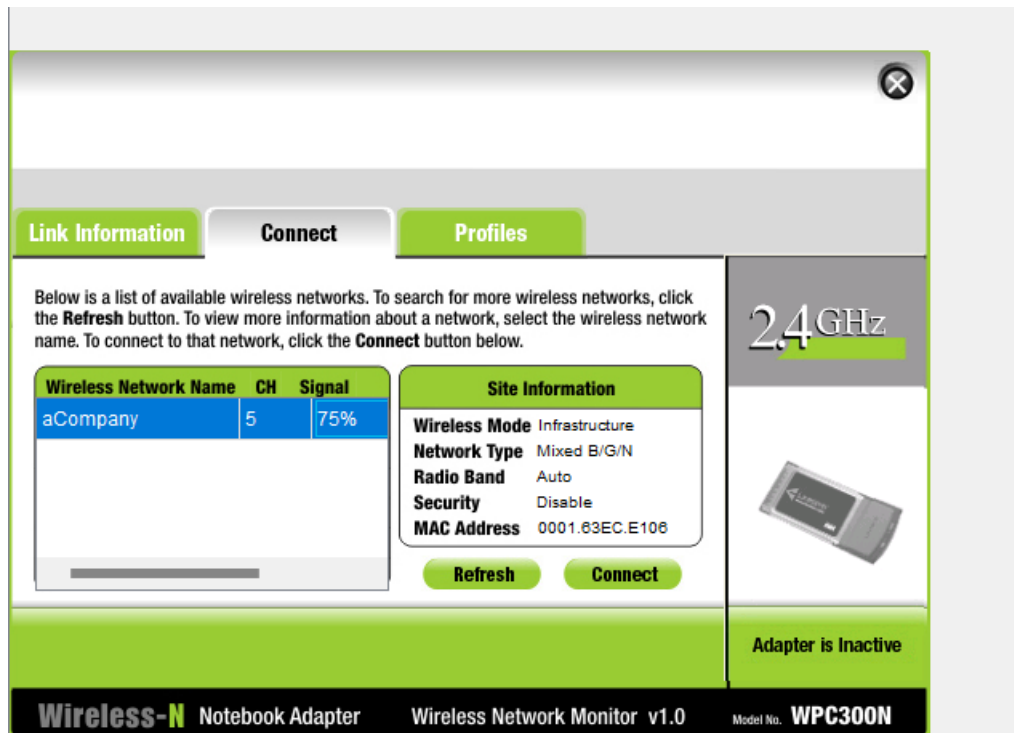
IP Address: 192 . 168 . 50 . 1
Subnet Mask: 255.255.255.252
DHCP ☒ Enabled ☐ Disabled

```
C:\>ipconfig /renew  
  
IP Address.....: 192.168.0.50  
Subnet Mask.....: 255.255.255.0  
Default Gateway.....: 192.168.0.1  
DNS Server.....: 209.165.201.1
```

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



Connexion a distance de puis le pc



VII. 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

```
ftp>put sample.txt
Writing file sample.txt to ftp.cisco.pka:
File transfer in progress...

[Transfer complete - 17 bytes]

17 bytes copied in 0.083 secs (204 bytes/sec)
ftp>dir

Listing /ftp directory from ftp.cisco.pka:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : cl841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : cl841-ipbase-mz.123-14.T7.bin 13832032
4 : cl841-ipbasek9-mz.124-12.bin 16599160
5 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
6 : c2600-i-mz.122-28.bin 5571584
7 : c2600-ipbasek9-mz.124-8.bin 13169700
8 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
9 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
10 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
11 : c2800nm-ipbasek9-mz.124-8.bin 15522644
12 : c2950-i6q412-mz.121-22.EA4.bin 3058048
13 : c2950-i6q412-mz.121-22.EA8.bin 3117390
14 : c2960-lanbase-mz.122-25.FX.bin 4414921
15 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
16 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
17 : c3560-advipservicesk9-mz.122-37.SEE1.bin 8662192
18 : pt1000-i-mz.122-28.bin 5571584
19 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
20 : sample.txt 17
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

1/1/1970    1:0 PM                24      sample.txt
                24 bytes                1 File(s)

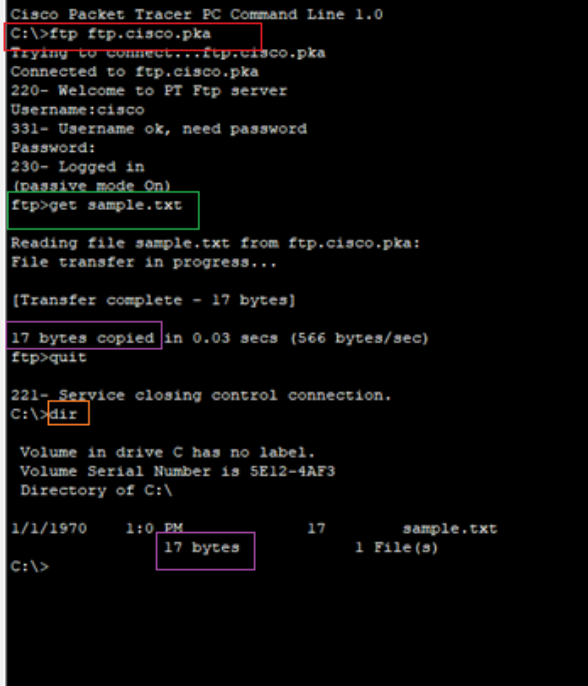
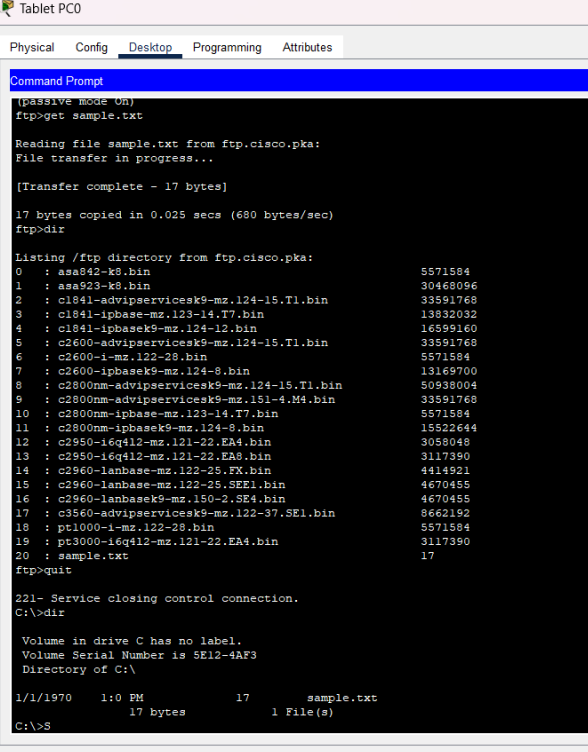
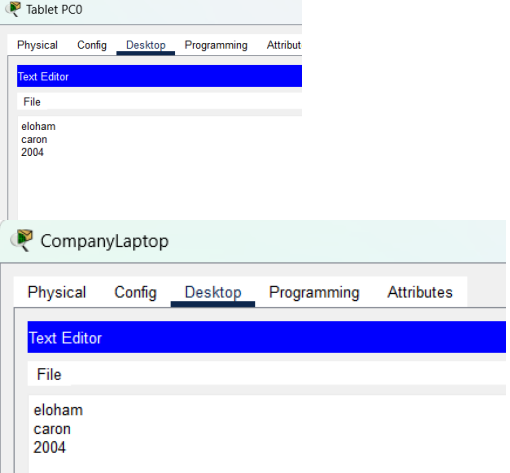
C:\>
```

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

Il y a actuellement 20 fichiers dans le répertoire.

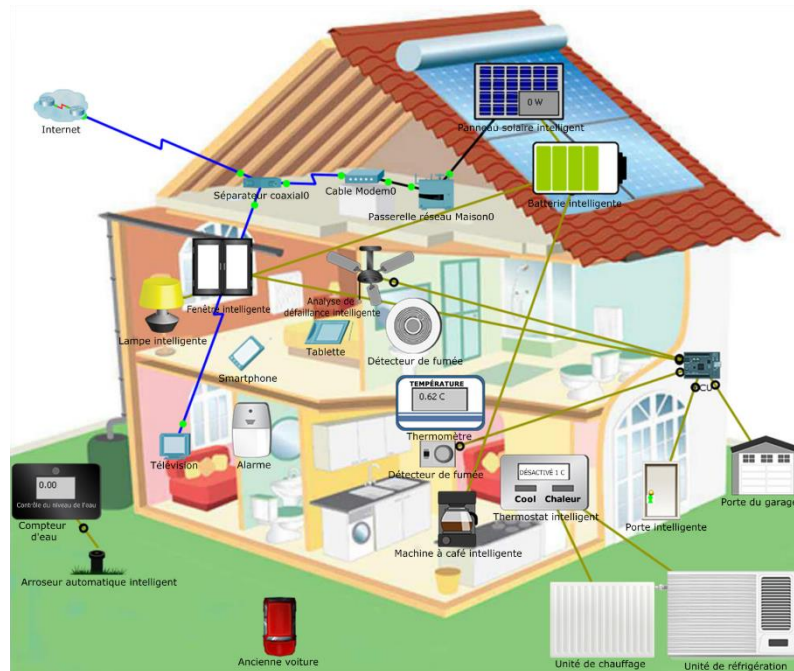
Mon fichier a une taille de 17 octets.

Vérification du téléchargement :

 <pre>Cisco Packet Tracer PC Command Line 1.0 C:\>ftp ftp.cisco.pka Trying to connect...ftp.cisco.pka Connected to ftp.cisco.pka 220- Welcome to FT Ftp server Username:cisco 331- Username ok, need password Password: 230- Logged in (passive mode On) ftp>get sample.txt Reading file sample.txt from ftp.cisco.pka: File transfer in progress... [Transfer complete - 17 bytes] 17 bytes copied in 0.03 secs (566 bytes/sec) ftp>quit 221- Service closing control connection. C:\>dir Volume in drive C has no label. Volume Serial Number is 5E12-4AF3 Directory of C:\ 1/1/1970 1:0 PM 17 sample.txt 17 bytes 1 File(s) C:\></pre>	<ul style="list-style-type: none">• 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.
 <pre>Tablet PC0 Physical Config Desktop Programming Attributes Command Prompt (passive mode On) ftp>get sample.txt Reading file sample.txt from ftp.cisco.pka: File transfer in progress... [Transfer complete - 17 bytes] 17 bytes copied in 0.025 secs (680 bytes/sec) ftp>dir Listing /ftp directory from ftp.cisco.pka: 0 : asa842-k8.bin 5571584 1 : asa823-k8.bin 30468096 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768 3 : c1841-ibase-mz.123-14.T7.bin 13832032 4 : c1841-ibasek9-mz.124-12.bin 16599160 5 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768 6 : c2600-i-mz.122-28.bin 5571584 7 : c2600-ibasek9-mz.124-8.bin 13169700 8 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004 9 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768 10 : c2800nm-ibase-mz.123-14.T7.bin 5571584 11 : c2800nm-ibasek9-mz.124-8.bin 15522644 12 : c2950-16q412-mz.121-22.EA4.bin 3058048 13 : c2950-16q412-mz.121-22.EA8.bin 3117390 14 : c2960-lanbase-mz.122-35.FX.bin 4414921 15 : c2960-lanbase-mz.122-35.SE11.bin 4670455 16 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455 17 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192 18 : pt1000-i-mz.122-28.bin 5571584 19 : pt3000-16q412-mz.121-22.EA4.bin 3117390 20 : sample.txt 17 ftp>quit 221- Service closing control connection. C:\>dir Volume in drive C has no label. Volume Serial Number is 5E12-4AF3 Directory of C:\ 1/1/1970 1:0 PM 17 sample.txt 17 bytes 1 File(s) C:\>S</pre>	 <pre>Tablet PC0 Physical Config Desktop Programming Attributes Text Editor File eloham caron 2004 CompanyLaptop Physical Config Desktop Programming Attributes Text Editor File eloham caron 2004</pre>

Avantage de server FTP :	Inconvénient
<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.

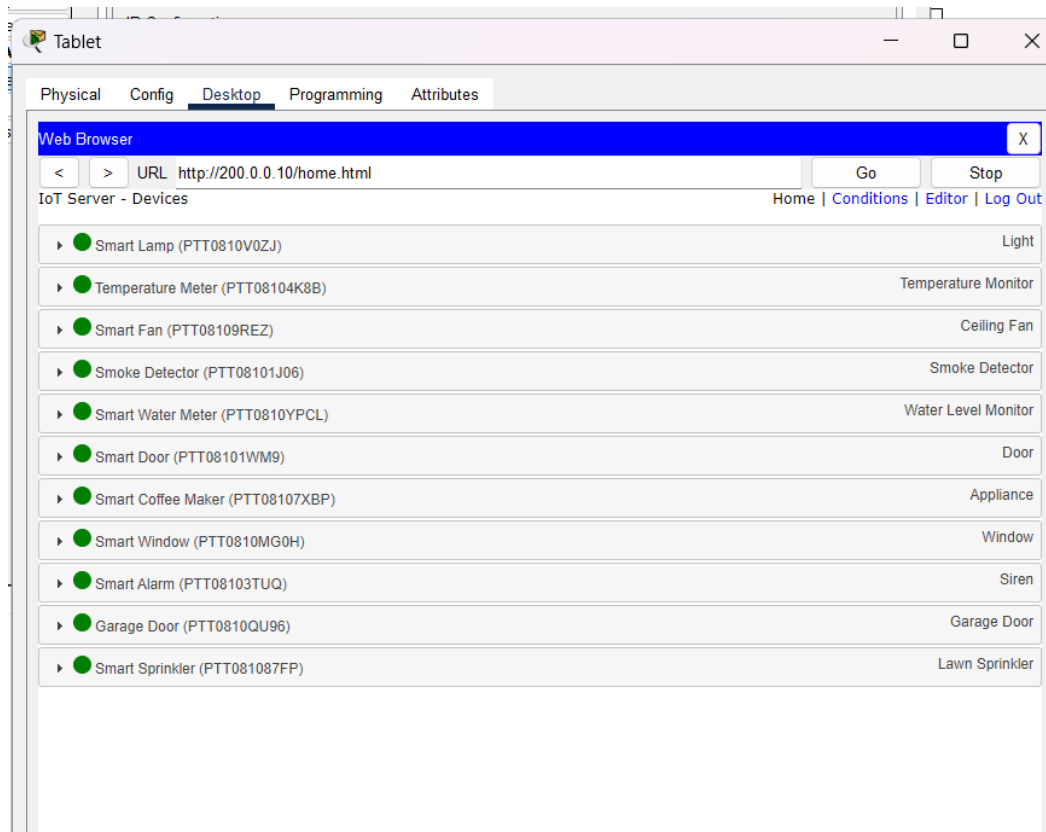
VIII. Partie maison intelligente :



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

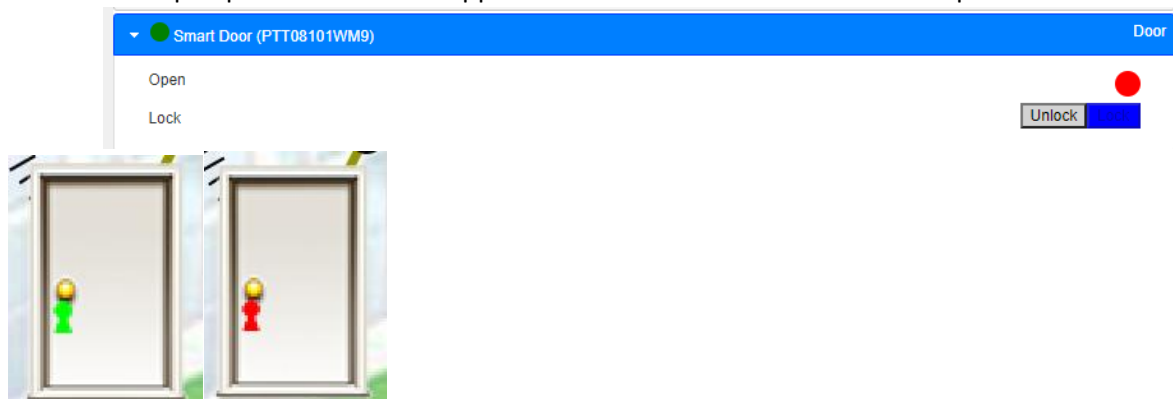
Le câble modem sert d'interface entre le réseau du FAI (Fournisseur d'Accès à Internet) et le home gateway, qui, dans ce contexte, est un routeur connecté au modem câble.

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.



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



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'

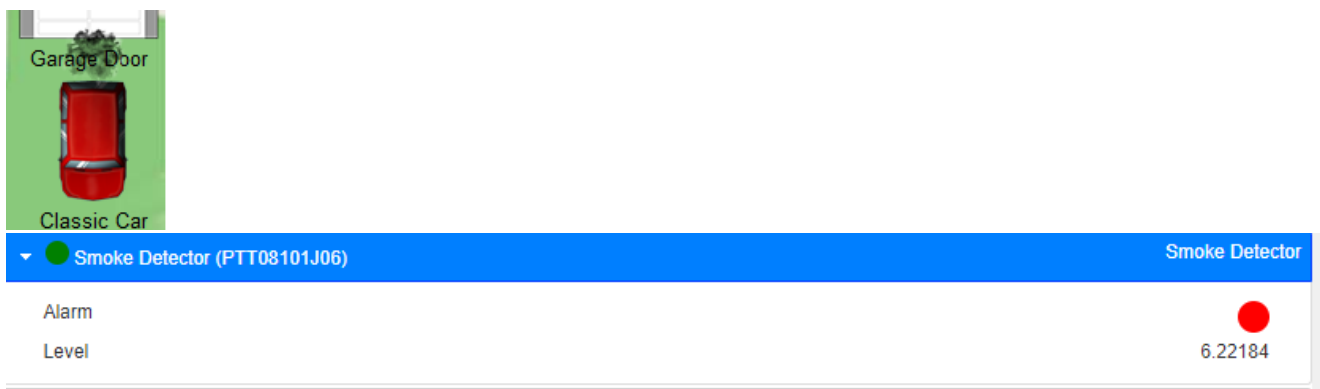
j) Détecteur de fumé :

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.

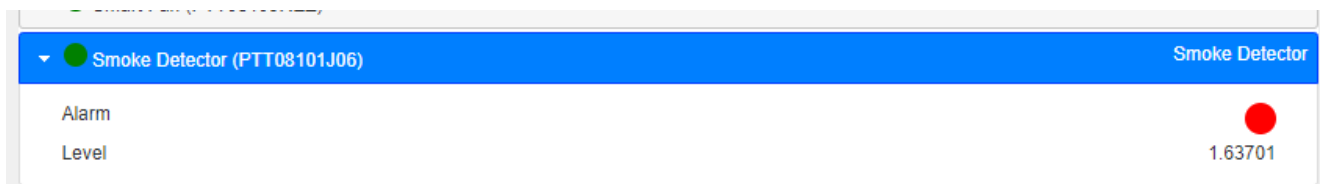
Cependant, la surveillance à distance peut être utile dans certaines situations. De plus, je pense qu'il pourrait être possible d'influer sur ses valeurs en utilisant une méthode autre que l'interface graphique, un peu comme une injection SQL. Certaines technologies utilisent également des signaux électroniques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



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.



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.

IX. 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.

X. 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%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/>