Une image contenant Graphique, capture d’écran, graphisme, conception

Description générée automatiquement

1

Atelier 8 : Mise en oeuvre d’un serveur DHCP et agent de relais DHCP, dispositif multifonction Linksys WRT300N, NAT/PAT, serveur DNS, WEB

VENTRE

ADRIEN

Table des matières

[Introduction 2](#_Toc157352342)

[Tables de routage : 3](#_Toc157352343)

[Pool DHCP et exclusions : 3](#_Toc157352344)

[Relai DHCP : 4](#_Toc157352345)

[Tables d’adresse : 4](#_Toc157352346)

[I. Contexte : 6](#_Toc157352347)

[II. Schéma réseau apprès installation de tous les appareille. 6](#_Toc157352348)

[III. Examen de la fonction NAT du routeur Linksys WTR300N 7](#_Toc157352349)

[IV. Mettre en place les scénarii d’utilisation 11](#_Toc157352350)

[V. Analyser le réseau : 16](#_Toc157352351)

[VI. Schéma réseau après réorganisation de tous les appareils : 17](#_Toc157352352)

[Tables de routage : 17](#_Toc157352353)

[Pool DHCP et exclusions : 18](#_Toc157352354)

[Relai DHCP : 18](#_Toc157352355)

[Tables d’adresse : 19](#_Toc157352356)

[VLAN 19](#_Toc157352357)

[VII. Choix de la disposition du réseau : 20](#_Toc157352358)

[VIII. Configuration approfondie du nouveau réseau : 21](#_Toc157352359)

[1. Serveurs 21](#_Toc157352360)

[2. Routeurs 24](#_Toc157352361)

[3. Swichs 24](#_Toc157352362)

[4. Telnet et SSH 24](#_Toc157352363)

[5. Sécurisation avec mot de passe 26](#_Toc157352364)

[6. Eteindre tous les ports non utilisés des swichs 27](#_Toc157352365)

[IX. Mettre en place les scénarii d’utilisation dans le nouveau réseau : 29](#_Toc157352366)

[Conclusion : 32](#_Toc157352367)

[Webographie : 33](#_Toc157352368)

# Introduction

Dans cet atelier, notre objectif est de créer un petit réseau en utilisant le dispositif multifonction commutateur-routeur-point d'accès sans fil Linksys WRT300N. Nous allons examiner la fonction NAT/PAT afin de comprendre comment elle permet la traduction des adresses et des ports entre le réseau local et le réseau public.

De plus, nous allons mettre en place un service DHCP pour faciliter la configuration automatique des adresses IP des périphériques réseau. Nous allons étudier les paramètres et les différentes options de configuration du service DHCP, ainsi que la mise en œuvre du DHCP relais pour permettre la communication entre les différents sous-réseaux.

Enfin, nous allons explorer les différents services proposés sur les serveurs du réseau. Cela comprendra l'identification et l'analyse des services tels que le serveur de fichiers, le serveur d'impression, le serveur de messagerie électronique, le serveur web, etc. Nous examinerons les fonctionnalités et les configurations nécessaires pour mettre en place ces services de manière efficace et sécurisée.

## Tables de routage :

|  |  |  |  |
| --- | --- | --- | --- |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_INT\_INT** | 200.100.51.96 | 255.255.255.224 | 200.100.51.94 |
|  | 200.100.51.64 | 255.255.255.224 | 200.100.51.94 |
|  | 200.100.51.0 | 255.255.255.224 | 200.100.51.94 |
|  | 172.16.1.0 | 255.255.0.0 | 200.100.51.94 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_EXT\_INT** | 200.100.51.32 | 255.255.255.224 | 200.100.51.93 |
|  | 200.100.51.0 | 255.255.255.224 | 200.100.51.126 |
|  | 172.16.1.0 | 255.255.0.0 | 200.100.51.126 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_EX** | 200.100.51.0 | 255.255.255.224 | 200.100.51.29 |
|  | 200.100.51.32 | 255.255.255.224 | 200.100.51.125 |
|  | 200.100.51.64 | 255.255.255.224 | 200.100.51.125 |
|  | 200.100.51.96 | 255.255.255.224 | 200.100.51.125 |
|  | 192.168.0.0 | 255.255.255.224 | 200.100.51.125 |
|  | 172.16.1.0 | 255.255.0.0 | 200.100.51.29 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **WRT300N (NAT AUTO)** | N/A | N/A | N/A |

## Pool DHCP et exclusions :

|  |  |  |
| --- | --- | --- |
| Routeurs | Pool DHCP | Exclusions |
| RO\_INT\_INT | ip dhcp pool reseaux\_interne  network 200.100.51.32 255.255.255.224  default-router 200.100.51.62  dns-server 200.100.51.97  ip dhcp pool MITM  network 200.100.51.64 255.255.255.224  default-router 200.100.51.94  dns-server 200.100.51.97  ip dhcp pool DMZ  network 200.100.51.96 255.255.255.224  default-router 200.100.51.125  dns-server 200.100.51.97 | ip dhcp excluded-address 200.100.51.33  ip dhcp excluded-address 200.100.51.34  ip dhcp excluded-address 200.100.51.62  ip dhcp excluded-address 200.100.51.35  ip dhcp excluded-address 200.100.51.97  ip dhcp excluded-address 200.100.51.125  ip dhcp excluded-address 200.100.51.126  ip dhcp excluded-address 200.100.51.94  ip dhcp excluded-address 200.100.51.93 |
| WRT300N | Start IP address 172.16.1.50  Maximum nombre d’utilisateur 29  IP address Range : 172.16.1.50 – 78  Static DNS 200.100.51.97 | Exclusions :  172.16.1.1  172.16.1.10  172.16.1.254 |

## Relai DHCP :

|  |  |
| --- | --- |
| Routeurs |  |
| RO\_INT\_INT | ip helper-address 200.100.51.93 |
| RO\_EXT\_INT | interface GigabitEthernet0/0  ip helper-address 200.100.51.94  interface GigabitEthernet0/1  ip helper-address 200.100.51.125 |

## Tables d’adresse :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Routeurs** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **RO\_INT\_INT** | Gig0/0 200.100.51.93  Gig0/1 200.100.51.62 | 255.255.255.224  255.255.255.224 | N/A | N/A |
| **RO\_EXT\_INT** | Gig0/0 200.100.51.125  Gig0/1 200.100.51.94 | 255.255.255.224 255.255.255.224 | N/A | N/A |
| **RT\_EX** | FA0/0 200.100.51.30  FA0/1 200.100.51.126 | 255.255.255.224 255.255.255.224 | N/A | N/A |
| **WRT300N** | Internet 200.100.51.29 | 255.255.255.224 | N/A | N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseaux\_interne (VERS)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **PC-Admin** | 200.100.51.33 | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |
| **PC4** | DHCP | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |
| **PC5** | DHCP | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |
| **HP181** | 200.100.51.34 | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |
| **Serveur TFTP-Sauvegarde-NTP** | 200.100.51.62 | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau MITM (BLEU)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **PC3** | DHCP | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau DMZ (ROUGE)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **Serveur http+… +DNS** | 200.100.51.97 | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |
| **PC2** | DHCP | 255.255.255.224 | 200.100.51.62 | 200.100.51.97 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau magasin (JAUNE)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **Serveur WEB** | 172.16.1.1 | 255.255.255.0 | 172.16.1.254 | 200.100.51.97 |
| **PC1** | 172.16.1.10 | 255.255.255.0 | 172.16.1.254 | 200.100.51.97 |
| **PC0** | DHCP | 255.255.255.0 | 172.16.1.254 | 200.100.51.97 |
| **Laptop0** | DHCP | 255.255.255.0 | 172.16.1.254 | 200.100.51.97 |
| **Smartphone0** | DHCP | 255.255.255.0 | 172.16.1.254 | 200.100.51.97 |

# Contexte :

On souhaite installer un réseau local dont une partie des clients hôtes seront reliés au réseau par un câble traditionnel Ethernet droit, et dont l'autre partie des clients hôtes seront reliés au réseau par Wi-Fi (c'est-à-dire sans fil).

Pour installer ce réseau, nous allons utiliser le dispositif Linksys WRT300N.

Le Linksys WRT300N est un périphérique multifonction, de la catégorie *Wireless Devices*, qui comprend :

* Un commutateur 4 ports,
* Un routeur d’accès à Internet, dans lequel est intégré un DHCP,
* Un point d’accès sans fil.

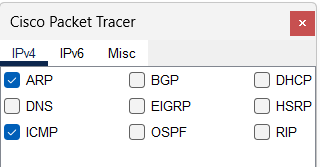
# Schéma réseau apprès installation de tous les appareille.

# Examen de la fonction NAT du routeur Linksys WTR300N

En mode Simulation, nous allons maintenant envoyer un PDU simple de PC1 vers Server1, en mode pas à pas, afin d’observer la fonction NAT du routeur WR0 :

Dans **Simulation Panel**, sélectionnez l’option **Edit Filters** et cochez uniquement les cases ARP et ICMP.

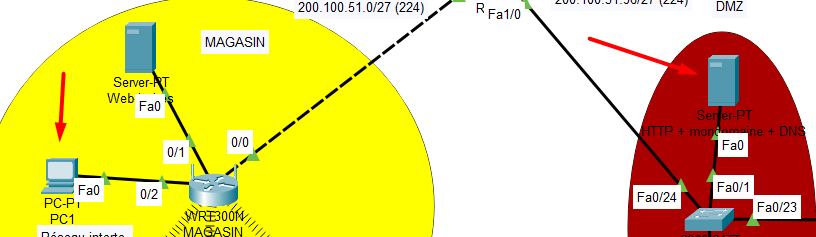




Cliquer sur l’enveloppe fermée (**Add Simple PDU**) située au-dessus de l’icône de mode de simulation.



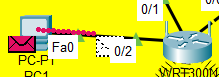
Cliquer sur le client **PC1** pour le définir comme source, puis sur le client **Server1** pour le définir comme destination.



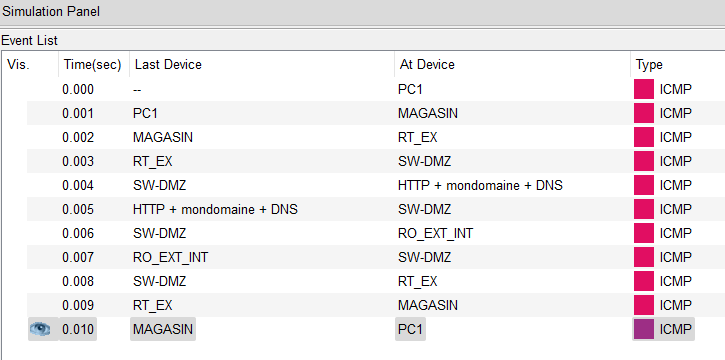
Le résultat qui doit été obtenu après cette manipulation est :



Lancer la démonstration en mode pas à pas ; lorsque le PDU est arrivé sur **WR0**, cliquer dessus et afficher son contenu (onglet *Inbound PDU Details*).

Dans le mode simulation, les enveloppes doivent se déplacer sans erreur.

Puis la requête ICMP doit revenir au PC1 car c’est lui qui a envoyé cette requête au serveur1



|  |  |
| --- | --- |
| **Trame obtenue** | **Lorsqu’il arrive dans le routeur, quelle est l’adresse IP source émetteur du paquet IP ?** |
|  | Lorsqu’il arrive dans le routeur l’adresse IP source émetteur du paquet IP et 172.16.1.10 |

Cliquer maintenant sur l'onglet *Outbound PDU Details* pour observer le contenu du PDU lorsqu’il repart du routeur **WR0**.

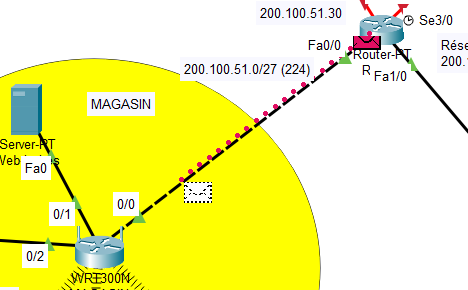
|  |  |
| --- | --- |
| **Trame obtenue** | **Lorsqu’il repart du routeur, quelle est l’adresse IP source émetteur du paquet IP ?** |
|  | Lorsqu’il repart du routeur, l’adresse IP source émetteur du paquet IP et 200.100.51.97 |

La fonction NAT du routeur a-t-elle bien opéré la translation de l’adresse IP source locale en une adresse IP globale ?

Comme nous pouvons le voir sur les deux captures d’écran l’adresse de source d’émetteur du paquet IP a bien été modifiée. Je peux donc en conclure que la translation de l’adresse IP source locale se transforme bien en adresse IP globale.

Le mécanisme NAT (Network Address Translation) opère à la couche de réseau (couche 3) du modèle OSI. Plus précisément, il intervient généralement au niveau de la couche de réseau Internet (couche 3 dans le modèle TCP/IP). Le NAT est utilisé pour traduire les adresses IP et les numéros de port entre les réseaux locaux (LAN) privés et Internet.

Poursuivre la simulation jusqu’à ce que l’enveloppe atteigne la destination, puis jusqu’à ce qu’elle revienne dans le routeur **WR0** (lors du retour de la réponse).



Lorsque l’enveloppe est dans le routeur, on pourra vérifier dans les onglets *Inbound PDU Details* et *Outbound PDU Details* le mécanisme inverse de translation.

|  |  |
| --- | --- |
|  | Une image contenant texte, capture d’écran, Parallèle, reçu  Description générée automatiquement |
| On peut voir dans Inbound PDU que l’adresse IP source est 200.100.51.97 ce qui est l’adresse publique utilisée par le serveur1. Nous voyons également que l’adresse de destination n’est pas celle du pc1 mais bien celle du routeur. | Dans Outbond nous voyons que l’adresse source na pas changé mais nous voyons que l’adresse de destination n’est plus une adresse publique mais est une adresse privée donc le NAT a bien fonctionné. |

A la fin de la simulation nous avons le résultat suivant.



Conjointement au protocole NAT, le protocole PAT (Port Address Translation) utilise le champ Port Source du segment TCP pour y stocker un identifiant de la machine source

Le routeur garde la correspondance entre ce numéro identifiant la machine et son adresse IP source, dans une table NAT**.**

Cliquer sur le bouton **Inspect** représenté par une loupe, puis cliquer sur le routeur **WR0**. Dans le menu contextuel, sélectionnez **NAT Table** : une fenêtre affichant la table NAT du routeur s'ouvre :



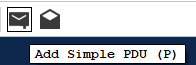
|  |  |
| --- | --- |
| **Résultats** | **Quel est le numéro identifiant la machine d’adresse IP 172.16.1.10 (PC1) ?** |
|  | On peut voir sur la capture d’écran que l’identifiant de la machine IP 172.16.1.10 (PC1) est 17. |

# Mettre en place les scénarii d’utilisation

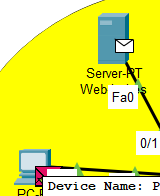
Tout d'abord, pour s'assurer que tout fonctionne, nous pouvons tester les différents réseaux. Pour cela, nous allons utiliser des scénarios pour simplifier la mise en place de ces tests.

Pour ajouter un scénario, il faut :

Récupérer un PDU ;



Cliquer sur un poste puis sur un autre ;



La conclusion des trames ICMP se met dans la fenêtre de droite.

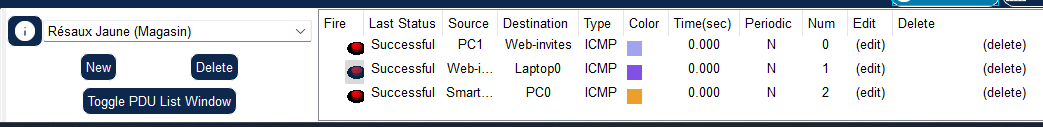


Pour commencer la réalisation des tests on peut commencer par vérifier si une machine communique avec une machine dans son réseau.

Pour le réseau Jaune (Magasin) :

Les tests qui sont réalisés consistent à vérifier la communication entre les différentes machines via des câbles RJ45. Tout d'abord, un test est effectué du serveur vers le PC1 pour vérifier si les machines peuvent communiquer entre elles via un câble RJ45. Ensuite, un test est réalisé du serveur vers le Laptop pour vérifier si le réseau câblé peut communiquer avec le réseau sans fil. Enfin, un test est effectué entre le PC0 et le Smartphone0 pour vérifier si les appareils câblés peuvent communiquer entre eux.

Sur cette image, on peut constater que la communication entre tous les appareils fonctionne correctement.

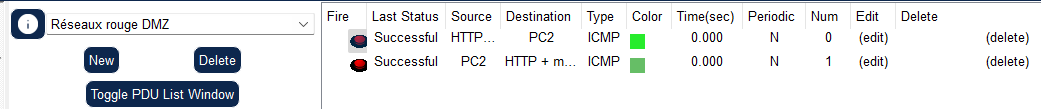


Pour le réseau Rouge (DMZ) :

Nous pouvons accéder à la configuration du PC2 pour vérifier si le DHCP a bien été récupéré à partir du routeur le plus à droite.Une image contenant texte, capture d’écran, logiciel, ligne

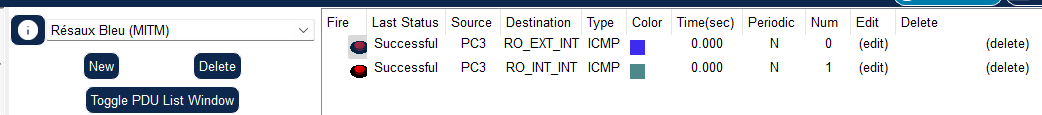
Description générée automatiquement

On peut voir qu'il a bien une adresse en DHCP.

Maintenant nous allons faire un ping entre le PC2 et le Serveur.

Comme nous le voyons, le ping entre le serveur et le PC2 a fonctionné, et inversement, le ping de PC2 vers le serveur a également fonctionné.

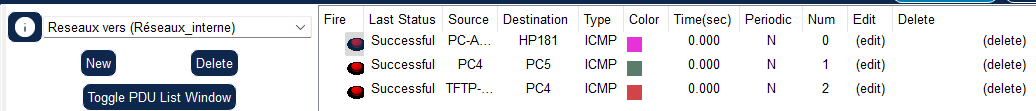
Pour le réseau bleu (MITM)

Dans ce réseau, il n'y a que PC3. Donc, les tests doivent partir de PC3 vers les deux routeurs pour vérifier s'il peut communiquer avec eux. Sur cette image, on peut voir que PC3 parvient à communiquer avec les deux routeurs avec succès.

Pour le réseau vers (Réseaux\_interne)

Les tests qui vont être réalisés sont de deux types : du PC admin vers l'imprimante, qui sont tous les deux en IP statique, puis des deux PC en DHCP (PC4 et PC5), puis du serveur en IP statique vers PC4 en dynamique. Ceci permet de voir si toutes les machines peuvent communiquer ensemble, peu importe si elles sont en statique ou en dynamique.

On peut voir que tout fonctionne correctement.



Nous savons que tout fonctionne en local dans chaque réseau. Il nous manque plus qu’à vérifier si les réseaux communiquent entre eux.

En deuxième, nous allons vérifier si les réseaux communiquent entre eux. Pour cela, nous allons le faire en deux parties : d'abord du réseau le plus à droite vers celui le plus à gauche, puis inversement, afin que les requêtes ICMP puissent passer entre tous les routeurs.

Les tests réaliser sont :

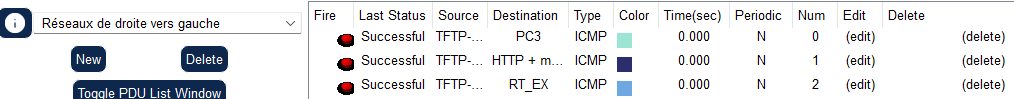
De serveur-interne vers PC3

De serveur-interne vers serveur DMZ

De serveur-interne vers Routeur-PT

De serveur-interne vers WRT300N magasin

On peut voir sur les captures d’écran que tous fonctionnent sauf le dernier



Le dernier ne fonctionne pas, car lors du ping avec l’enveloppe PDU, l’adresse IP de destination est une adresse privée et quand elle arrive sur le routeur sans fil, il rejette cette adresse. Il est impossible de faire un ping entre les appareils du réseau externe et le réseau interne du magasin, car le NAT personnalisé sur le routeur sans fil n’est pas pris en charge, ni le routage. Ainsi, les seules communications possibles seront si un appareil de l’intérieur du réseau magasin pingue vers l’extérieur, car il utilisera l’adresse IP publique du routeur sans fil au lieu de son adresse privée.

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

Description générée automatiquement

Tests de gauche vers droite.

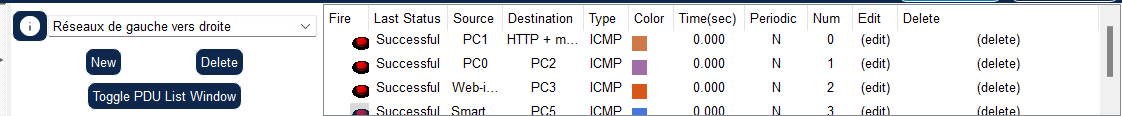
Les tests réalisés sont :

De PC1 vers serveur DMZ

De PC0 vers PC2

De serveur magasin vers PC3

Du smartphone0 vers PC5

Tous les tests ont été réalisés avec succès, on peut donc dire que les communications sont possibles entre les différents réseaux.

Le dernier test est l'interconnexion entre plusieurs Packet Tracer. Dans ce test, je suis connecté avec deux personnes : Anissa et Nathan.

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

Description générée automatiquementComme nous pouvons le voir, la connexion entre les deux réseaux fonctionne car il y a la présence des flèches pointant vertes.

Pour être parfaitement sûre que les réseaux sont bien connectées, il faut faire un ping entre les réseaux pour cela il faut mettre des adresse IP sur les deux ports.

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

Une fois les adresse IP rentrées il faut faire les pings pour voir s’il y a une réponse.

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

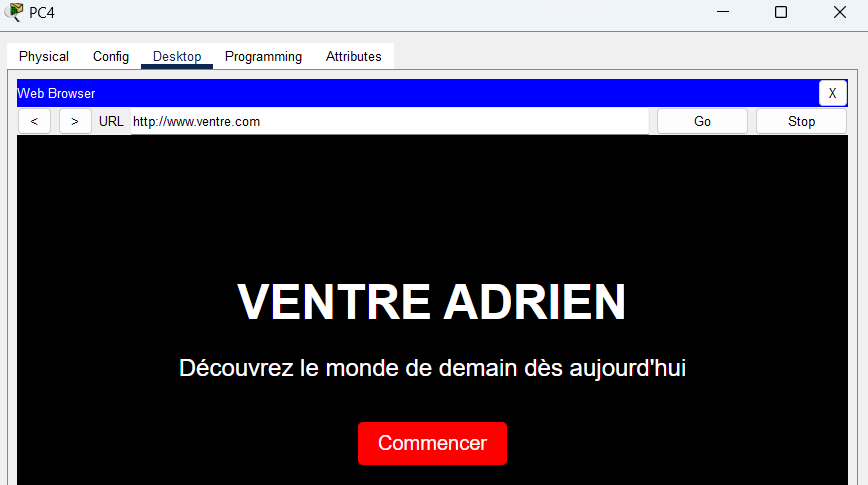
Description générée automatiquement

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

Description générée automatiquement

On peut voir que la connexion entre les routeurs fonctionne pour les deux réseaux.

Le dernier test à faire est de vérifier si le site est disponible sur l'un des postes. Pour cela, il faut ouvrir le navigateur web et saisir son nom de domaine. Cela permet de vérifier plusieurs aspects tels que la bonne communication avec le serveur, le DNS et le protocole HTTP du serveur.

On peut constater que tous les protocoles fonctionnent correctement."

# Analyser le réseau :

|  |  |  |
| --- | --- | --- |
| Point forts | Points faibles | Incohérences |
| Séparation du réseau en plusieurs zone. | Poste dans la DMZ  DNS dans la DMZ  DHCP qui rentre dans la DMZ  Plage de restriction du DHCP | PC dans la DMZ  Un seul poste dans la zone bleue (seuil au milieu des deux réseaux). |

|  |
| --- |
| Pistes d’améliorations |
| 1. Enlever toutes les adresses publiques pour en avoir plus que 2 (une dans le magasin et une pour l’autre réseaux) 2. Mettre des masques les plus rapproche des machines existent pour éviter les insertions de machine non désirée. 3. Simplification des tables de routage avec deux tables de routage pour chaque routeur. 4. Mettre le serveur DNS dans la zone la plus éloignée 5. Mettre un serveur DHCP dédié dans la zone la plus éloignée. 6. Mettre les postes dans la deuxième zone. 7. Replacer le http par https 8. Sécuriser les accès console, VTY 0 15, enable et mettre une bannière pour indiquer les risques en rentrant dans les routeurs. 9. Mettre des mots de passe sur toutes les entrées possibles. 10. Configurer un port en mode mirroring sur la DMZ avec un snifer pour voir tout ce qui rentre et sort du réseau. 11. Éteindre les ports non utilisés sur les switchs et mettre en place des VLAN pour l'administration. 12. Mettre en place une connexion gigabits sur tous les swichs et routeurs. 13. Utiliser un connexion fibre sur le routeur de sortie vers Internet. 14. Rajout d’un serveur AAA avec des utilisateurs spécifiques pour chaque routeur. 15. Redondance avec 2 routeurs de sorties, deux serveurs DNS, deux sortie internet, deux routeurs entre les réseaux et deux switchs dans les réseaux internet. 16. Mise en place du SSH sur les routeurs et swichs pour pouvoir les commandes depuis le PC\_admin. 17. Mise en place du NAT sur les routeurs de sortie sur internet. |

Les mots de passes :

* Mode enable : sio180e
* Mode privilégié : sio180p
* Ligne console : sio180c
* Lignes virtuelles : sio180v

# Schéma réseau après réorganisation de tous les appareils :

## Tables de routage :

|  |  |  |  |
| --- | --- | --- | --- |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_INT\_INT** | 10.255.1.0 | 255.255.255.248 | 192.168.30.1 |
|  | 10.255.2.0 | 255.255.255.252 | 192.168.30.1 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_EXT\_INT** | 192.168.40.0 | 255.255.255.248 | 192.168.30.2 |
|  | 10.255.2.0 | 255.255.255.252 | 10.255.1.1 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **RO\_EX** | 192.168.30.0 | 255.255.255.0 | 10.255.1.2 |
|  | 192.168.40.0 | 255.255.255.0 | 10.255.1.2 |
| **Routeur** | **Network** | **Masque** | **Next Hop** |
| **WRT300N (NAT AUTO)** | N/A | N/A | N/A |

## Pool DHCP et exclusions :

|  |  |  |
| --- | --- | --- |
| Routeurs | Pool DHCP | Exclusions |
| RO\_INT\_INT |  | Pas d’exclusions car les 10 premières adresses ne sont pas dans la plage DHCP. Le nombre d'appareils est limité à 100. |
| WRT300N | Start IP address 172.16.1.50  Maximum nombre d’utilisateur 29  IP address Range : 172.16.1.50 – 78  Static DNS 192.168.40.4 | Exclusions :  172.16.1.1  172.16.1.10  172.16.1.254 |

## Relai DHCP :

|  |  |
| --- | --- |
| Routeurs |  |
| RO\_INT\_INT | interface GigabitEthernet0/0  ip helper-address 192.168.40.3  interface GigabitEthernet0/1  ip helper-address 192.168.30.2 |

## Tables d’adresse :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Routeurs** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **RO\_INT\_INT** | Gig0/0 192.168.30.2  Gig0/1 192.168.40.1 | 255.255.255.0  255.255.255.248 | N/A | N/A |
| **RO\_EXT\_INT** | Gig0/0 10.255.1.2  Gig0/1 192.168.30.1 | 255.255.255.248  255.255.255.0 | N/A | N/A |
| **RT\_EX** | Gig0/8 10.255.1.1  Gig0/9 10.255.2.1 | 255.255.255.248  255.255.255.252 | N/A | N/A |
| **WRT300N** | Internet 10.255.2.2 | 255.255.255.252 | N/A | N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau\_interne (VERS)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **Serveur DHCP** | 192.168.40.3 | 255.255.255.248 | 192.168.40.1 | 192.168.40.4 |
| **Serveur DNS** | 192.168.40.4 | 255.255.255.248 | 192.168.40.1 | 192.168.40.4 |
| **Serveur TFPT+NTP** | 192.168.40.5 | 255.255.255.248 | 192.168.40.1 | 192.168.40.4 |
| **Serveur AAA** | 192.168.40.6 | 255.255.255.248 | 192.168.40.1 | 192.168.40.4 |
| **PC\_ADMIN** | 192.168.40.2 | 255.255.255.248 | 192.168.40.1 | 192.168.40.4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau\_Utilisateur (BLEU)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **Utilisateur\_1** | DHCP | 255.255.255.0 | 192.168.30.2 | 192.168.40.4 |
| **Utilisateur\_2** | DHCP | 255.255.255.0 | 192.168.30.2 | 192.168.40.4 |
| **Utilisateur\_3** | DHCP | 255.255.255.0 | 192.168.30.2 | 192.168.40.4 |
| **Utilisateur\_4** | DHCP | 255.255.255.0 | 192.168.30.2 | 192.168.40.4 |
| **Impriment** | 192.168.30.3 | 255.255.255.0 | 192.168.30.2 | 192.168.40.4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Réseau DMZ (ROUGE)** | **Adresse IP** | **Masque** | **Passerelle par défaut** | **Serveurs DNS** |
| **Serveur https** | 10.255.1.3 | 255.255.255.248 | 10.255.1.2 | 192.168.40.4 |
| **Sniffer** | N/A | N/A | N/A | N/A |

## VLAN

|  |  |
| --- | --- |
| Swich interne | VLAN 10 ADMIN  G0/1 et G0/2 Truck  G0/2 VLAN 10 |

# Choix de la disposition du réseau :

Une image contenant diagramme, cercle, horloge

Description générée automatiquement

Comme nous le voyons, le réseau principal a été séparé en trois parties. Une partie est utilisée pour la sortie vers Internet avec un serveur HTTPS et un sniffer pour surveiller les informations entrantes et sortantes du réseau.

La deuxième partie est dédiée aux utilisateurs et à l'imprimante pour leur permettent d'imprimer leurs documents.

La troisième partie comprend les serveurs et le poste administrateur, qui sont placés en arrière-plan en raison de leur sensibilité. Ces serveurs remplissent des rôles importants dans la gestion efficace du réseau, et le poste administrateur, disposant de tous les droits sur le réseau, doit être protégé contre les attaques.

Également, la redondance a été mise en place, même si elle n'est pas parfaite et pourrait être largement améliorée avec plus d'équipements. La redondance a été mise en œuvre sur le pool DHCP du réseau dans la zone utilisateur, avec un DHCP de secours en cas de panne du premier. De plus, une redondance a été établie sur la sortie Internet grâce à l'utilisation de deux routeurs pour éviter les interruptions de connexion. Idéalement, il serait recommandé d'avoir également deux commutateurs par réseau et quatre routeurs en sortie vers Internet, en utilisant deux fournisseurs d'accès à Internet (FAI). Cependant, il est important de prendre en compte le coût de tout cet équipement supplémentaire, ainsi que les exigences et les besoins réels de l'entreprise. Il est préférable d'ajuster la mise en place en fonction des besoins spécifiques plutôt que de chercher à tout mettre en place de manière exhaustive.

# Configuration approfondie du nouveau réseau :

### Serveurs

Dans ce nouveau réseau nous avons plusieurs nouveau appareils mis en place comme le serveur DHCP, serveur DNS, serveur NTP, serveur AAA.

#### Le serveur DHCP

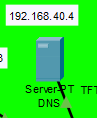
Une image contenant texte, capture d’écran, Police, diagramme

Description générée automatiquement

Le serveur sert aux utilisateurs dans le réseau bleu. Utilisez une plage d'adresses IP de 192.168.30.10 à 192.168.30.110. Grâce à cette plage, le nombre d'utilisateurs est assez important pour permettre une évolutivité du réseau, tout en ayant des adresses statiques qui commencent par 192.168.30.1 à 9 et de 192.168.30.111 à 192.168.30.254, ce qui laisse la possibilité d'ajouter des machines statiques.Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

#### Le serveur DNS

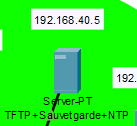


Le serveur DNS était déjà présent dans l'ancien réseau, mais il était situé dans la DMZ, ce qui n'était pas sécurisé. Maintenant, il est dans la zone la plus sécurisée du réseau. Le DNS permet de lier un nom de domaine à l'adresse IP du serveur HTTPS.

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

Description générée automatiquement

#### Le serveur NTP et TFTP



Ce serveur a deux fonctions. Le NTP synchronise l'horloge des dispositifs du réseau, tandis que le TFTP facilite le transfert de fichiers dans un réseau qui ne prend en charge que les fichiers texte.

La clé du services NTP est 1 et son mot de passe est 123.

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

Description générée automatiquement

Pour les services TFTP l’utilisateur est cisco avec le mot de passe cisco, cet utilisateur a toutes les permissions en tant qu’administrateur.

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

Description générée automatiquement

#### Le serveur AAA

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

Description générée automatiquement

Le serveurs AAA (Authentication, Authorization, and Accounting) est utilisé pour gérer l'authentification, l'autorisation et la comptabilisation des utilisateurs dans un réseau.

Ils permettent de contrôler l'accès des utilisateurs aux ressources du réseau et de collecter des informations sur leur utilisation.

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

Description générée automatiquement

### Routeurs

En plus des serveurs, les routeurs ont été légèrement modifiés. Les routeurs de sortie, appelés "router-PT-empty", sont spécifiques car ils ne disposent pas de cartes réseau installées par défaut. Ainsi, il est nécessaire d'en installer. Dans cette configuration, j'ai utilisé deux cartes Gigabit Ethernet et deux cartes Gigabit Ethernet en fibre optique pour la sortie vers Internet. De nos jours, il est important pour toute entreprise de disposer d'un réseau Gigabit pour obtenir des débits élevés et éviter les problèmes de temps de chargement, que ce soit sur Internet ou en local. C'est pourquoi l'utilisation de la fibre optique pour la sortie vers Internet est essentielle.

Les cartes utilisées sur ces routeurs (RT\_EX) sont deux PT\_ROUTER\_NM\_CGE pour les ports RJ45 et deux PT\_ROUTER\_NM\_FGE pour la fibre optique.

Une image contenant texte, logiciel, Logiciel multimédia, Icône d’ordinateur

Description générée automatiquement

### Swichs

Dans l'ensemble du réseau, les commutateurs utilisent des ports RJ45 en Gigabit, ce qui était déjà le cas dans l'ancien réseau. Cela permet d'avoir des débits élevés pour les connexions au sein du réseau local.

### Telnet et SSH

Telnet et SSH sont des protocoles de communication utilisés pour établir des connexions distantes sécurisées ou pas avec des systèmes informatiques. Le protocole le plus facile mais qui n’est pas sécurisé est Telnet. SSH est le protocole qui va être utilisé dans le réseau pour établir une connexion entre le PC\_ADMIN et les différents routeurs du réseau.

En premier, nous allons mettre en place la sécurisation des ports VTY de 0 à 15 avec un mot de passe.

Pour commencer, il faut entrer dans le mode de configuration globale en utilisant la commande 'configure terminal'. Ensuite, vous devez accéder aux lignes VTY 0 15 pour sélectionner les ports de 0 à 15. Vous pouvez ensuite définir un mot de passe en utilisant la commande 'password' suivie du mot de passe souhaité, par exemple 'sio180v'. Enfin, pour activer le mot de passe, vous pouvez utiliser la commande 'login'.

Commande routeurs :

configure terminal

service password-encryption

line vty 0 15

password sio180v

login

Une fois cette étape faite le protocole Telnet peut être utiliser directement, ce qui n’est pas très sécurisé mais possible.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Description générée automatiquement

Pour mettre en place le SSH il faut utiliser les commandes suivantes.

Mettre un nom au routeur :

Router(config)#hostname R3

Créer un domaine

R3(config)#ip domain-name ADMIN

Créer une Clé de chiffrement

R3(config)#crypto key generate rsa general-keys modulus 1024

The name for the keys will be: R3.ADMIN

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

\*Mar 1 0:24:42.893: %SSH-5-ENABLED: SSH 2 has been enabled

Activer la version 2 de ssh

R3(config)#ip ssh version 2

Se mettre sur les lignes VTY pour que le ssh soit utilisé sur ces lignes.

R3(config)#line vty 0 15

R3(config-line)#transport input ssh

R3(config-line)#access-class acl-ssh-permit inUne image contenant texte, logiciel, nombre, Police

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

Description générée automatiquement

Cette étape doit être faite sur tous les routeurs.

### Sécurisation avec mot de passe

Il est important de sécuriser toutes les entrées d'un routeur. Pour ce faire, il est nécessaire de mettre en place des politiques de sécurité, et l'une d'entre elles consiste à configurer des mots de passe sur toutes les interfaces du routeur.

Pour mettre en place les mots de passe, vous pouvez suivre les étapes suivantes :

Entrez dans le mode de configuration globale en utilisant la commande "configure terminal".

Pour définir le mot de passe d'accès global (enable password), utilisez la commande "enable password [mot de passe]". Par exemple, vous pouvez utiliser "enable password sio180e".

Pour définir le mot de passe d'accès privilégié (enable secret), utilisez la commande "enable secret [mot de passe]". Par exemple, vous pouvez utiliser "enable secret sio180p". Cette commande crypte le mot de passe de manière sécurisée.

Pour protéger l'accès à la console, utilisez la commande "line console 0" pour accéder à l'interface de la console.

Utilisez la commande "password [mot de passe]" pour définir le mot de passe de la console. Par exemple, vous pouvez utiliser "password sio180c".

Enfin, utilisez la commande "login" pour activer l'exigence du mot de passe lors de la connexion à la console.

Il ne faut pas oublier de rajouter un message qui permet d’avoir une assurance légale. Le message choisi est « Accès restreint : Seuls les utilisateurs autorisés sont autorisés à accéder à cet équipement. Toute tentative d'accès non autorisée est strictement interdite et peut entraîner des poursuites pénales. »

Voici la configuration complète qui a été mise en place sur les routeurs.

Command sur le routeur RO\_INT\_INT

Enable

configure terminal

enable password sio180e

enable secret sio180p

line console 0

password sio180c

login

exit

configure terminal

service password-encryption

line vty 0 15

password sio180v

login

hostname RO\_INT\_INT

service password-encryption

crypto key generate rsa general-keys modulus 1024

ip domain-name ADMIN

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

access-class acl-ssh-permit in

configure terminal

banner login #

Accès restreint : Seuls les utilisateurs autorisés sont autorisés à accéder à cet équipement. Toute tentative d'accès non autorisée est strictement interdite et peut entraîner des poursuites pénales.

#

Command sur le routeur RO\_EXT\_INT

Enable

configure terminal

enable password sio180e

enable secret sio180p

line console 0

password sio180c

login

exit

configure terminal

service password-encryption

line vty 0 15

password sio180v

login

hostname RO\_EXT\_INT

service password-encryption

crypto key generate rsa general-keys modulus 1024

ip domain-name ADMIN

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

access-class acl-ssh-permit in

configure terminal

banner login #

Accès restreint : Seuls les utilisateurs autorisés sont autorisés à accéder à cet équipement. Toute tentative d'accès non autorisée est strictement interdite et peut entraîner des poursuites pénales.

#

Command sur le routeur RO\_EX

Enable

configure terminal

enable password sio180e

enable secret sio180p

line console 0

password sio180c

login

exit

configure terminal

service password-encryption

line vty 0 15

password sio180v

login

hostname RO\_EX

service password-encryption

crypto key generate rsa general-keys modulus 1024

ip domain-name ADMIN

crypto key generate rsa general-keys modulus 1024

ip ssh version 2

line vty 0 15

transport input ssh

access-class acl-ssh-permit in

configure terminal

banner login #

Accès restreint : Seuls les utilisateurs autorisés sont autorisés à accéder à cet équipement. Toute tentative d'accès non autorisée est strictement interdite et peut entraîner des poursuites pénales.

#

### Eteindre tous les ports non utilisés des swichs

Pour finaliser la sécurité du réseau, il est essentiel de désactiver tous les ports inutilisés des commutateurs afin de prévenir toute utilisation non autorisée. Pour ce faire, vous pouvez utiliser la commande "shutdown" pour mettre le port hors service. Assurez-vous également de spécifier l'interface appropriée.

Voici un exemple de configuration pour mettre un port non utilisé hors service :

Switch(config)#interface FastEthernet0/13

Switch(config-if)#shutdown

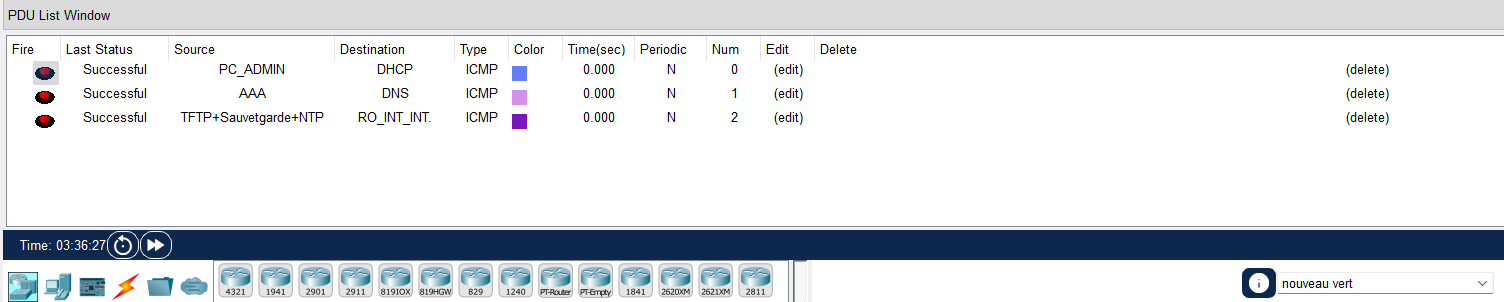
Une fois que vous avez appliqué cette configuration sur tous les ports inutilisés, il existe une autre méthode pour vous assurer que seuls les utilisateurs autorisés peuvent utiliser le commutateur. Cette méthode consiste à configurer le port pour n'autoriser que les adresses MAC valides. Si une adresse MAC non autorisée est détectée, le port se bloque automatiquement.

Pour bloquer un port avec une adresse MAC il faut :

1. Accédez au mode de configuration globale du commutateur en utilisant la commande "configure terminal".
2. Sélectionnez l'interface sur laquelle vous souhaitez configurer la sécurité du port en utilisant la commande "interface [interface]" (par exemple, "interface FastEthernet0/1").
3. Activez la fonctionnalité de sécurité du port en utilisant la commande "switchport port-security".
4. Définissez le nombre maximal d'adresses MAC autorisées sur le port en utilisant la commande "switchport port-security maximum [nombre]" (par exemple, "switchport port-security maximum 1" pour autoriser une seule adresse MAC).
5. Configurez le mode de violation pour spécifier le comportement lorsque des adresses MAC non autorisées sont détectées. Vous pouvez utiliser la commande "switchport port-security violation [mode]" pour définir le mode de violation. Par exemple, les modes courants sont :
   * "protect" : Ignore les paquets provenant d'adresses MAC non autorisées sans bloquer le port.
   * "restrict" : Ignore les paquets provenant d'adresses MAC non autorisées et génère un journal d'événements.
   * "shutdown" : Met le port en état d'erreur-désactivé si une adresse MAC non autorisée est détectée.

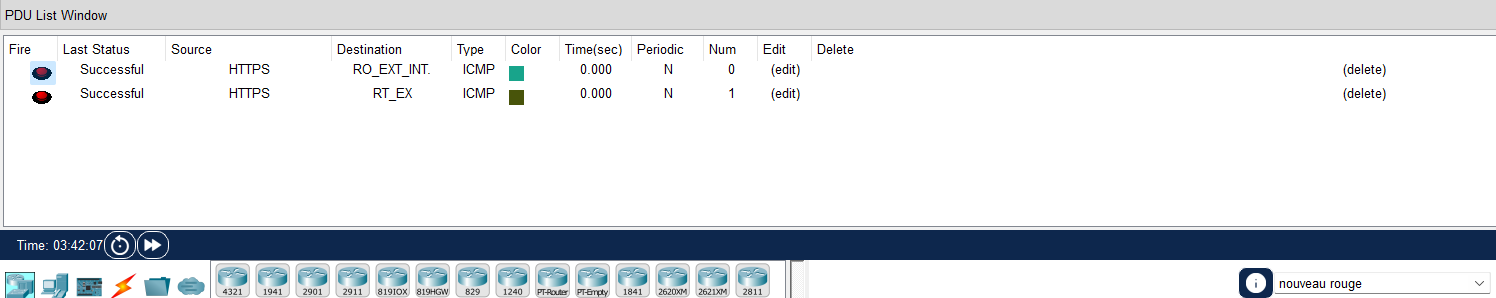
# Mettre en place les scénarii d’utilisation dans le nouveau réseau :

Pour tester le bon fonctionnement du réseau, nous allons procéder par étapes. Tout d'abord, nous utiliserons un scénario pour tester chaque réseau Internet.

Pour le réseau vert, il y a seulement 3 pings à effectuer : un du PC\_ADMIN vers un serveur (DHCP), puis un autre d'un serveur vers un autre serveur (AAA vers DHCP), et enfin d'un serveur vers la passerelle par défaut.

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

Description générée automatiquementPour le réseau bleu, il y a seulement 3 pings à effectuer : un du PC utilisateur vers l'imprimante, puis d'un utilisateur vers un autre utilisateur, et enfin d'un utilisateur vers le routeur de gauche pour vérifier si la passerelle fonctionne et si la table de routage est correcte.

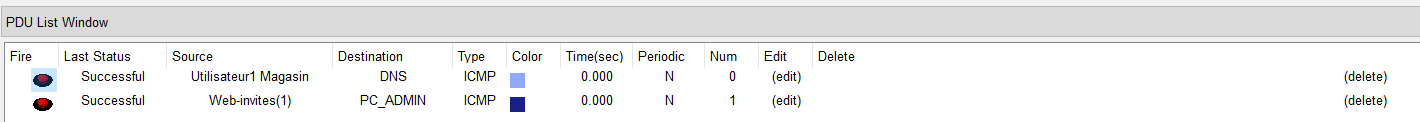
Pour le réseau rouge, il y a seulement 2 pings à effectuer : un du serveur HTTPS vers sa passerelle par défaut, et l'autre vers le routeur Internet.

Une image contenant capture d’écran, texte, logiciel, Icône d’ordinateur

Description générée automatiquementPour le réseau jaune, il faut effectuer 4 pings : Du serveur web vers le smartphone. De l'utilisateur 1 vers le serveur web. De l'utilisateur 2 vers le smartphone. Du routeur magasin vers le routeur Internet.

Pour finaliser ces tests, il reste à vérifier la connectivité d'une machine accessible depuis un réseau le plus éloigné.

Pour réaliser ce test, j’ai testé la communication entre les deux machines les plus éloignées qui sont Utilisateur1 magasin au DNS et Serveur WEB magasin ver PC\_ADMIN



Nous pouvons également vérifier le fonctionnement du DNS et du serveur HTTPS en tapant le nom de domaine dans la barre de recherche de plusieurs ordinateurs.Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

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

# Conclusion :

Dans cet atelier, nous avons pu explorer et mettre en place différents aspects d'un réseau en utilisant le dispositif multifonction Linksys WRT300N. Nous avons étudié la fonction NAT/PAT pour permettre la traduction des adresses et des ports entre le réseau local et le réseau public, facilitant ainsi la communication avec l'extérieur. De plus, nous avons configuré le service DHCP pour attribuer automatiquement les adresses IP aux périphériques du réseau, en utilisant également le DHCP relais pour permettre la communication entre les sous-réseaux.

Nous avons également examiné les différents services offerts par les serveurs du réseau, tels que le serveur de fichiers, le serveur d'impression, le serveur de messagerie électronique et le serveur web. Nous avons étudié les configurations nécessaires pour mettre en place ces services de manière sécurisée.

Enfin, nous avons analysé et réorganisé le réseau en fonction des besoins, en examinant les tables de routage, les pools DHCP, les relais DHCP et les tables d'adresse. Nous avons également pris en compte la mise en place de VLAN pour segmenter le réseau de manière logique.

Cet atelier nous a permis de comprendre les principes fondamentaux de la configuration et de la gestion d'un réseau, ainsi que les différentes fonctionnalités offertes par le dispositif Linksys WRT300N. En utilisant les scénarios d'utilisation, nous avons pu tester et valider le bon fonctionnement du réseau.

Cet atelier a été une excellente opportunité d'apprendre et de mettre en pratique les connaissances liées à la configuration réseau et à l'utilisation des dispositifs de réseau. Il a permis d'acquérir une expérience concrète dans la mise en place et la gestion d'un réseau fonctionnel.

Cet outil logiciel, Packet Tracer, peut être utilisé en entreprise pour la préproduction de réseaux. Il permet de tester un réseau théorique avant son installation physique.

# Webographie :

Semperboni, Fabio. « NAT and PAT: A Complete Explanation ». *CiscoZine* (blog), 16 février 2013. <https://www.ciscozine.com/nat-and-pat-a-complete-explanation/>.

Semperboni, Fabio. « How to Allow Multi IP Address from the Same Wireless Client ». *CiscoZine* (blog), 2 mars 2021. <https://www.ciscozine.com/allow-multi-ip-address-from-wireless-client/>.

Cisco. « Configuration VLAN via l’interface de ligne de commande sur les commutateurs gérés de la gamme 300/500 ». Consulté le 28 janvier 2024. <https://www.cisco.com/c/fr_ca/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4986-vlan-configuration-via-cli-on-300-500-series-managed-switche.html>.

« Configurer le service DHCP sur un routeur Cisco | Cisco | IT-Connect ». Consulté le 7 novembre 2023. <https://www.it-connect.fr/configurer-le-service-dhcp-sur-un-routeur-cisco/>.

Cisco. « Configurer l’AAA de base sur un serveur d’accès ». Consulté le 28 janvier 2024. <https://www.cisco.com/c/fr_ca/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>.