

CREATION RESEAU

Linksys WRT300N

Table des matières

Introduction :	1
1. Réalisation	2
Ajout des différents dispositifs :	2
Connecter les différents appareils entre eux :	3
Par câble :	4
Par Wi-fi :	4
Mise en forme :	8
Adressage IP :	9
Configuration routeur :	11
Configuration des switchs :	11
Configuration des adresses IP statiques sur les PCs et serveurs :	12
Mise en place du DHCP :	13
WRT300N :	14
Routage :	15
Mise en place des différents serveurs :	17
Le serveur DNS :	17
Connecter deux réseaux :	18
2. Vérification :	20
Vérification ospf :	20
Vérification DHCP :	21
Connections sans fil (scénarios 4) :	22
Serveur DNS et http :	23
Sniffer :	23
3. Fonction NAT	24
Conclusion :	27
Sources :	27

Introduction :

Dans le cadre de cet atelier, nous avons conçu et déployé une infrastructure réseau complète centrée sur le dispositif multifonction Linksys WRT300N, en nous focalisant sur les mécanismes fondamentaux d'un réseau moderne. L'objectif principal était de maîtriser le déploiement d'un service DHCP intégré pour l'attribution dynamique d'adresses IP,

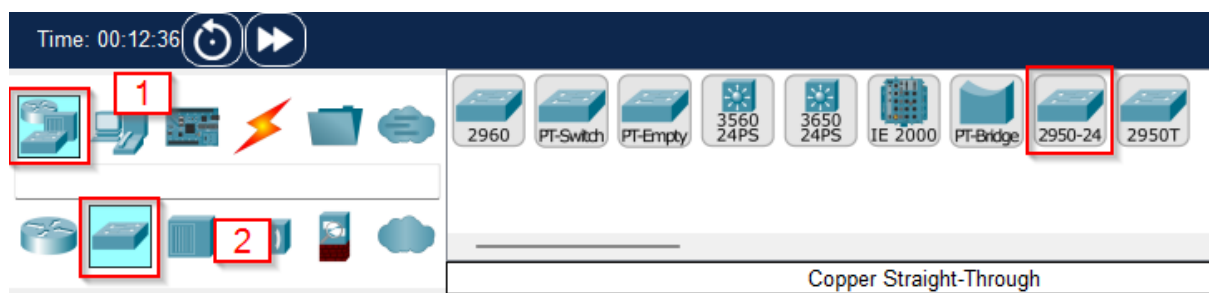
l'implémentation d'un agent relais DHCP assurant la communication entre sous-réseaux segmentés, la sécurisation avancée des équipements (chiffrement des mots de passe, restrictions d'accès) et une analyse critique de l'architecture pour identifier bonnes pratiques et limites matérielles.

1. Réalisation

Ajout des différents dispositifs :

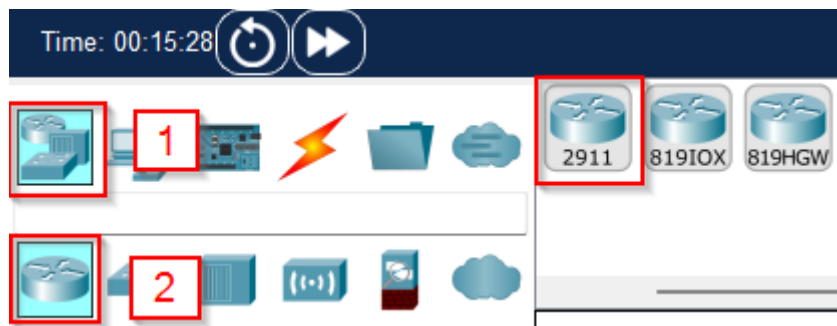
Pour assurer le bon fonctionnement d'un réseau, il faut intégrer les équipements nécessaires. Un routeur dirige les paquets entre différents réseaux. Des switchs permettent de créer et de gérer des sous-réseaux (LAN). Les serveurs jouent un rôle central, qu'il s'agisse de gérer les données, d'héberger des applications, ou d'assurer la sécurité. D'autres équipements essentiels incluent les points d'accès Wi-Fi pour permettre la connectivité sans fil et des systèmes de stockage (NAS ou SAN) pour centraliser et sécuriser les données. Il faut aussi ajouter des équipements courants en entreprise, comme une imprimante et des postes de travail pour que ca ressemble à un réseau d'entreprise.

Les Switch :



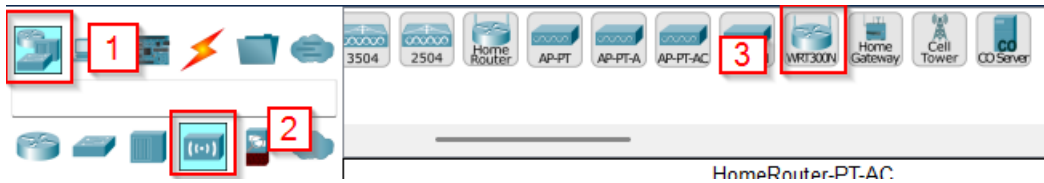
Dans la barre en bas à droite, nous avons network devices (1), là où se trouve la « réserve » d'appareils dont les switchs, dans le 2 et router. J'ai pris un switch 2950-24 comme indiqué dans le schéma réseau et il simule des réseaux avec plusieurs hôtes et est parfait pour débuter.

Routeurs :



Pour choisir le routeur, on clique toujours dans network devices (1) puis dans routers (2). J'ai pris un routeur 2911 comme indiqué dans le schéma réseau et parce qu'il prend en charge plusieurs fonctions de routage de base et des services avancés.

Le routeur WRT300N quant à lui est dans Network Devices (2), puis dans Wireless Devices (2) on trouve le routeur WRT300N (3) :



PC, serveurs, sniffer et téléphone :



Pour choisir les autres dispositifs, on clique toujours dans network devices (1) puis dans end devices (2). Il y a les PC, les PC portables, les serveurs, les smartphones et le sniffer.

Multiuser :

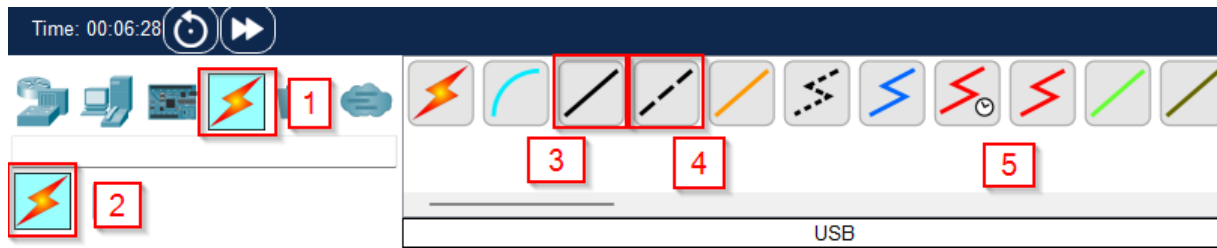


Pour ajouter un multiuser on clique sur multisuser connection puis sur mutliuser. Ça sert à connecter plusieurs pkt ou pka entre eux sur plusieurs ordinateurs pour échanger en temps réel sur les réseaux de l'autre.

Connecter les différents appareils entre eux :

Pour que les différents matériaux soient connectés entre eux, il faut les relier par des câbles le plus souvent ou sans fil, plus rare.

Par câble :



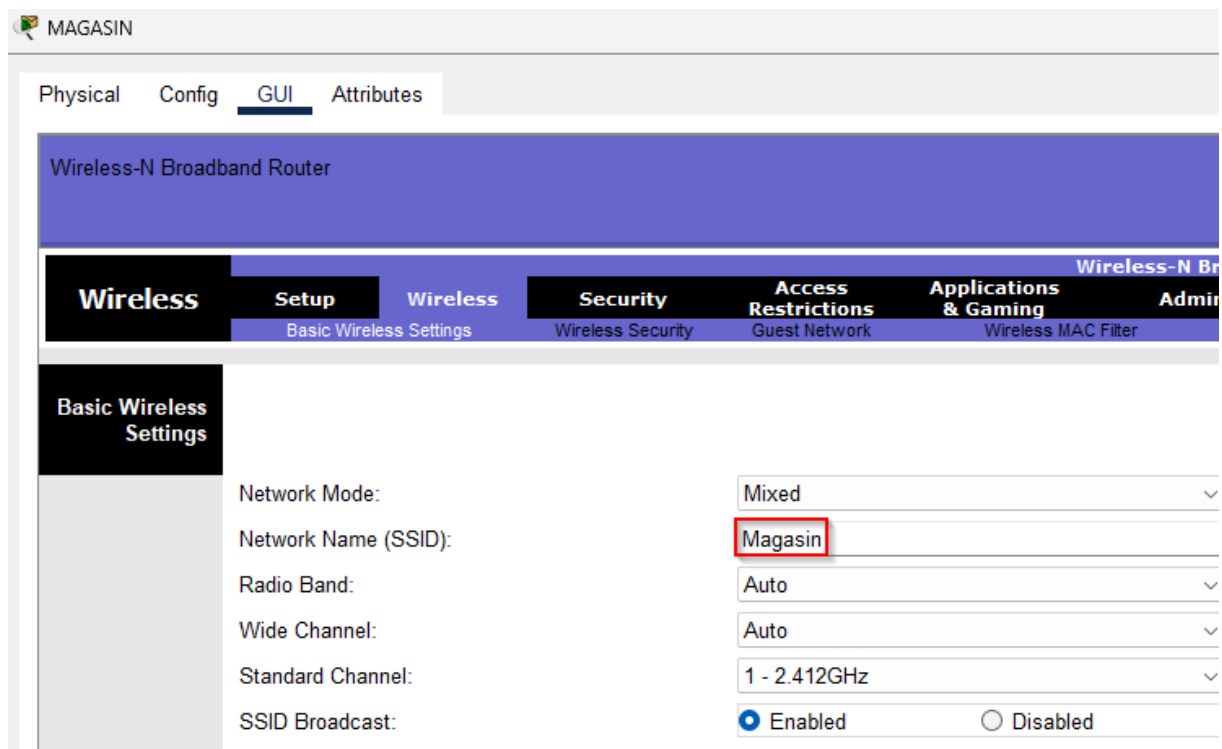
Pour ajouter des câbles, on clique sur connections (1), puis sur connections (2). Le câble 5, un câble utilisé pour connecter le peer0 au router2 car ceux sont des équipements de même type, le câble 4 est utilisé pour, entre le magasin (routeur WRT300N) et le Router2 et pour le sniffer car ceux sont des équipements différents. Le câble 5 entre toutes les autres connections sauf entre PC0, laptop0, Pda0 et le routeur WRT300N car ils ont besoin d'un accès direct au routeur.

Il faut bien choisir l'entrée internet pour connecter le routeur WRT300N et firewall, sinon la connexion est impossible à faire.

Par Wi-fi :

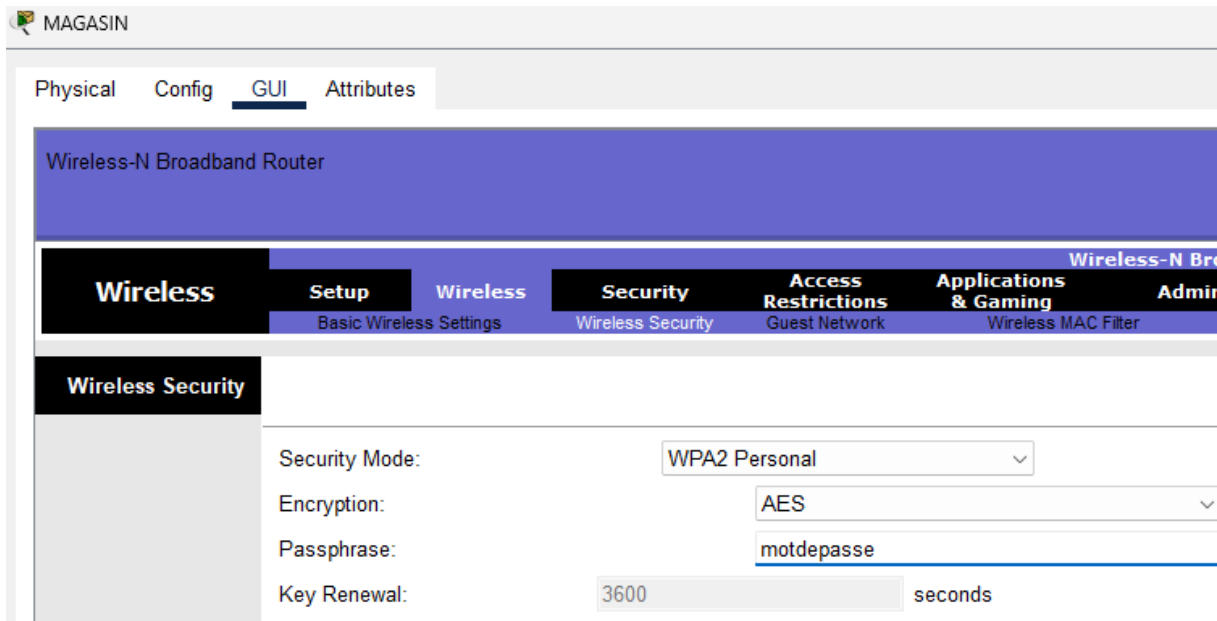
MAGASIN :

J'ai paramétré le Wireless en changeant son nom pour qu'il soit facilement repérable :

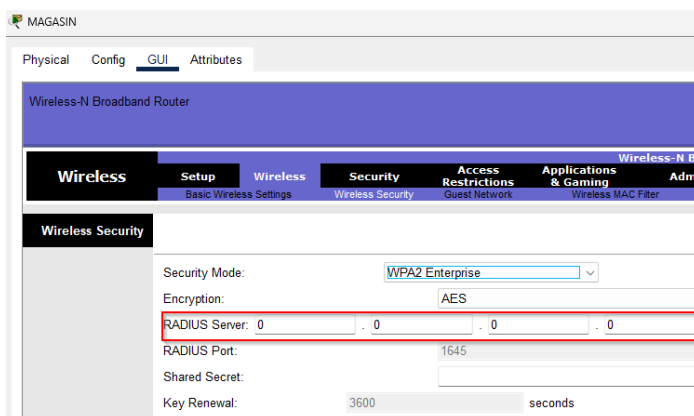


On accède à cette page juste en ouvrant le GUI.

Le GUI (Graphical User Interface), l'interface graphique utilisateur facilite la configuration du routeur et le rends accessible pour tous.

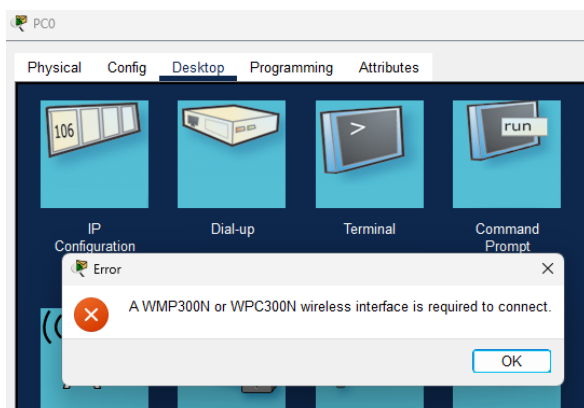


Puis dans Wireless Security j'ai sécurisé en mettant un WPA2 Personal, plus sécurisé que le 1 et le 0 et demandant juste un mot de passe, contrairement à l'entreprise où il faut un serveur radius :

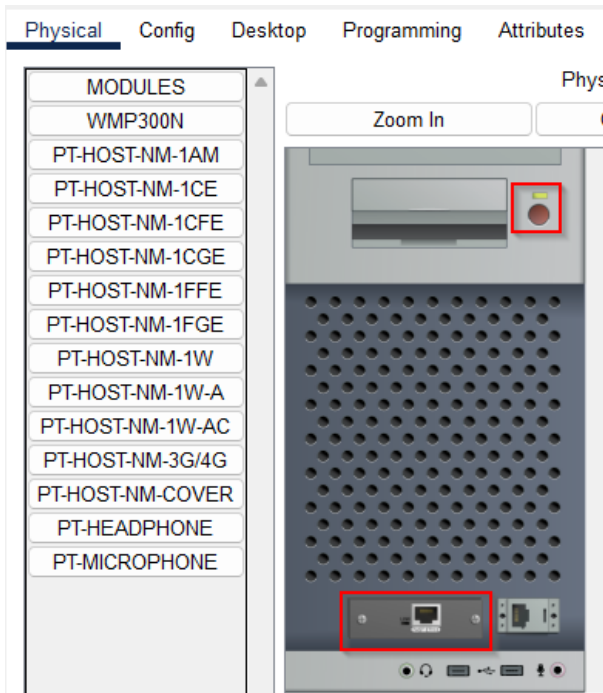


Si je configure la sécurité du réseau sans fil avec une sécurité WPA2 Enterprise, qui offre une meilleure protection mais nécessite un serveur RADIUS. Ce n'est pas indiqué dans le réseau et une sécurité WPA2 Personal suffira car elle est moins sécurisée mais nécessite pas de serveur.

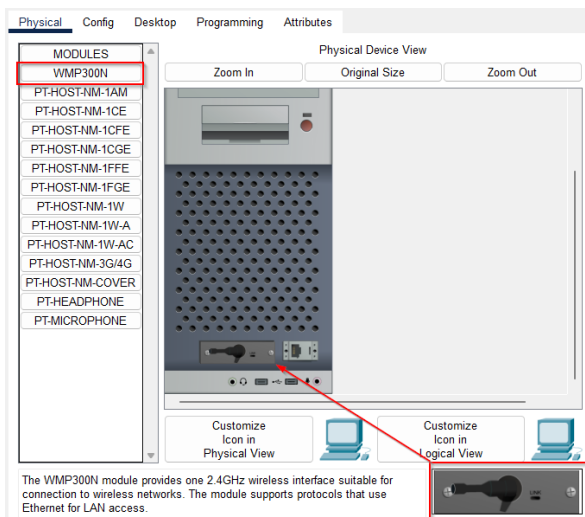
PC et laptop :



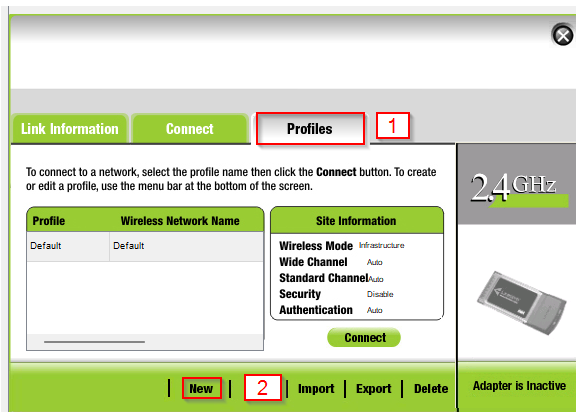
Le sans-fil n'est pas mis automatiquement sur les postes, je vais donc le mettre en place :



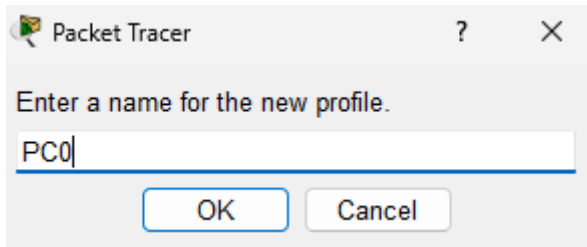
On doit d'abord éteindre le poste sur le bouton en dessous de la led verte, rouge pour les PC puis enlever le câble Ethernet pour mettre une carte réseau sans fil (WMP300N).



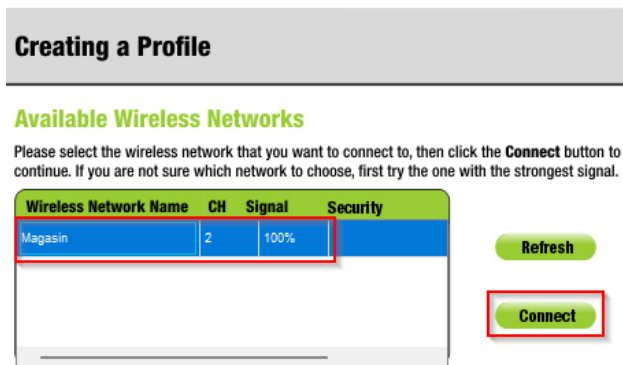
Il faut ensuite cliquer sur WMP300N et faire glisser le câble à la place libre. Il reste juste à allumer l'ordinateur et à le connecter au Wireless.



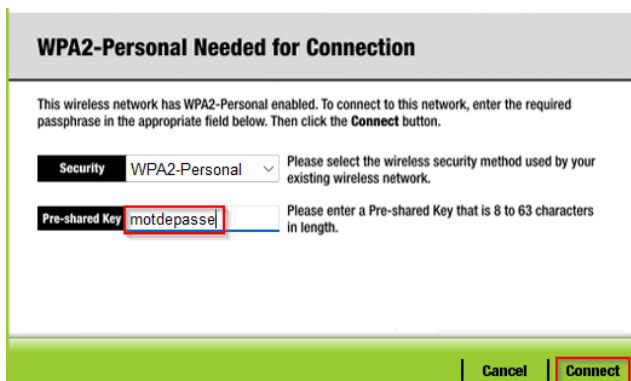
Je crée un nouveau profil pour me connecter à un réseau. Je clique sur l'onglet Profiles (1), qui me permet de gérer les connexions enregistrées. Ensuite, j'appuie sur le bouton New (2) pour démarrer la création d'un nouveau profil. Cela est nécessaire pour définir des paramètres spécifiques au réseau auquel je veux accéder.



Nous devons donner un nom à l'utilisateur du réseau, j'ai choisi le même pour le reconnaître facilement.



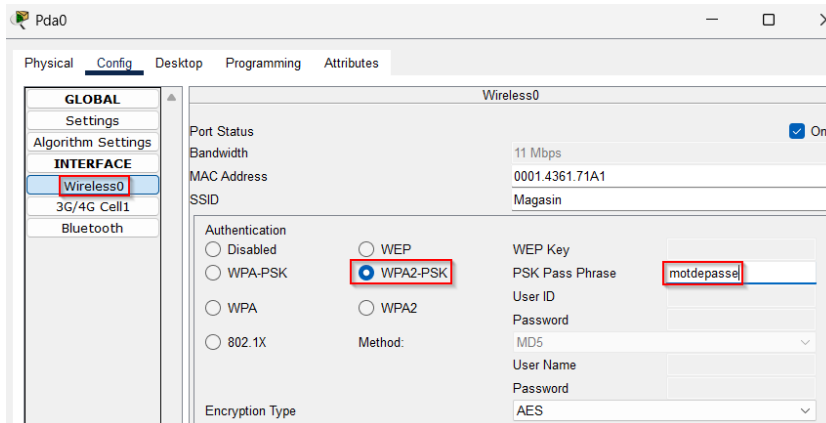
Je sélectionne le réseau sans fil Magasin. Ensuite, je clique sur le bouton Connect pour établir la connexion.



Puis on rentre le mot de passe pour se connecter, c'est une étape obligatoire pour se connecter au réseau. Ce qui garantit que je me connecte de manière sécurisée en utilisant une clé de chiffrement fiable.

Les interfaces sont identiques pour le PC et l'ordinateur portable.

Smartphone :

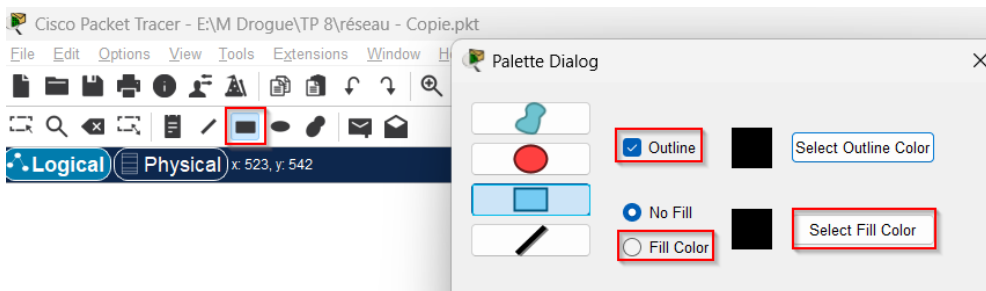


Dans l'onglet configuration, puis dans Wireless0 (pour le connecter sans fil), j'ai choisi le WPA-2-PSK car c'est le WPA2 Personal, car il est en rapport avec la connexion sans fil de mon routeur. J'ai ensuite tapé le mot de passe dans PSK Pass Phrase.

J'ai pingé entre le smartphone et le routeur WRT300N (magasin).

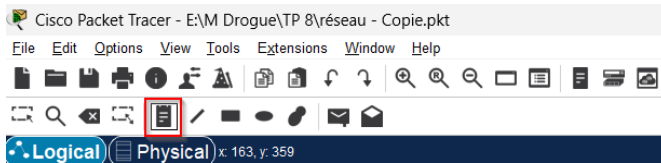
Mise en forme :

Pour créer des réseaux avec des couleurs pour améliorer la lisibilité du réseau :



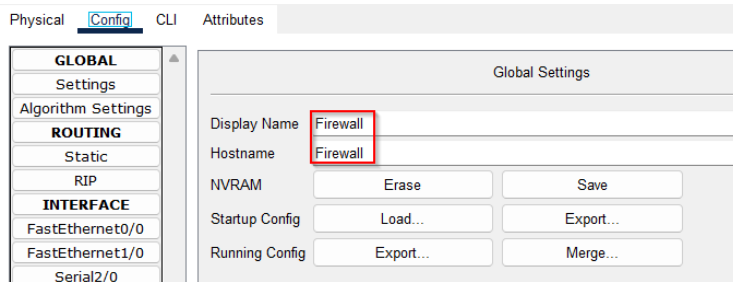
Pour insérer et personnaliser des formes dans l'interface, on commence par accéder aux outils de dessin sur la barre des tâches, puis sélectionnez l'icône représentant un carré noir. Une fenêtre de configuration s'ouvrira, vous permettant de personnaliser les formes. Si vous souhaitez créer un carré vide, sélectionnez l'option Outline pour dessiner uniquement les contours et choisissez la couleur de votre choix via la palette. Pour créer un carré rempli de couleur, activez l'option Fill Color et décochez l'option Outline si vous ne souhaitez pas afficher les contours. En plus des carrés, vous pouvez dessiner d'autres formes telles que des traits, des cercles ou des figures spécifiques en fonction du modèle sélectionné. Une fois les options configurées, dessinez votre forme à l'endroit souhaité sur le réseau.

Pour mettre du texte sur notre réseau, par exemple pour écrire le nom des sous-réseaux ou des adresses IP.



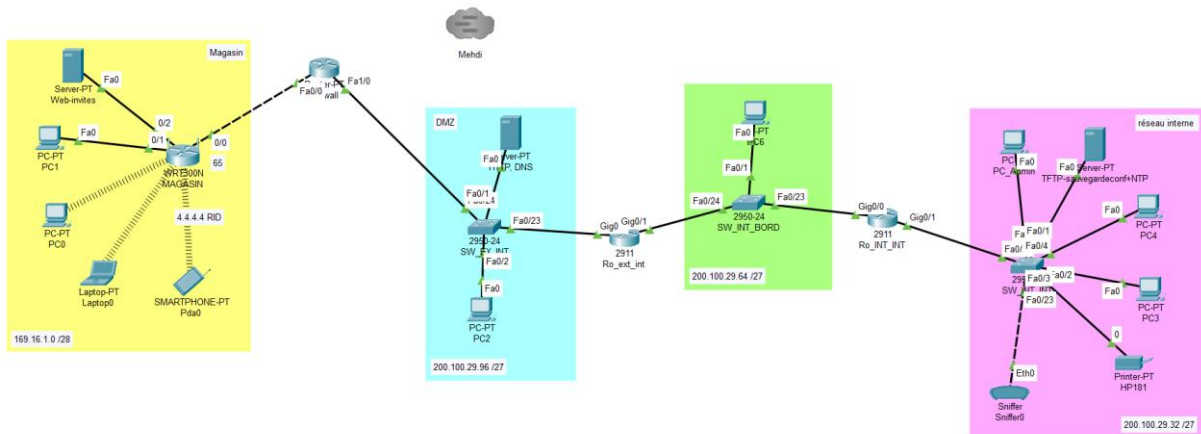
On sélectionne l'outil de texte, l'icône avec une feuille dans la barre d'outils. Une fois l'outil activé, cliquez sur l'espace de travail à l'endroit où vous souhaitez insérer le texte. Une boîte de dialogue s'ouvrira pour que vous puissiez entrer le texte.

Pour changer les noms :



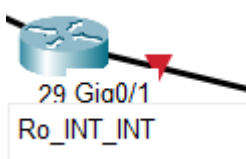
Pour modifier le nom des équipements on change directement le nom dans l'onglet Config, sous la section Name (une seule pour les PC et serveurs), le Display name pour changer le visuel dans le réseau et Hostname pour le changer dans le CLI. Il suffit de taper le nom souhaité dans le et le changement sera appliqué immédiatement.

Voilà ce que ça donne avec toutes les modifications visuelles :



Adressage IP :

On va attribuer des adresses IP sur chaque interface pour que les paquets puissent être transmis, reçus et validés correctement :



On voit que la connexion n'est pas valide.

Le masque de sous réseau /27 est de 27 bits, on fait $32-27 = 5$ bits qu'on met en puissance pour 2, $2^{*5}=32$ adresses mais on en enlève 2 car il y a l'adresse réseau et de broadcast. Il y a donc 32 adresses disponibles.

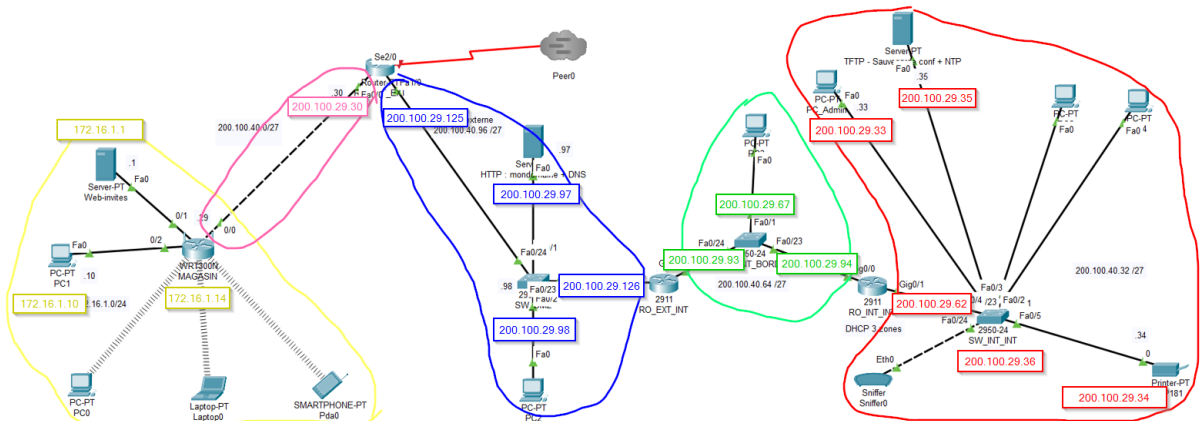
J'ai changé le masque de sous réseau du magasin car il était beaucoup trop grand pour un masque de /28 avec seulement 16 adresses disponibles contre 254. Les adresses utilisables sont de 172.16.1.1 à 172.16.1.14.

Les adresses utilisables de la connexion au routeur firewall sont de 200.100.29.1 à 200.100.29.30.

Les adresses utilisables de SW_ex_int sont de 200.100.40.97 à 200.100.40.126.

Les adresses utilisables de SW_INT_BORD sont de 200.100.29.65 à 200.100.29.94.

Les adresses utilisables de SW_int_int sont de 200.100.29.33 à 200.100.29.62.



Noms	Adresses IP	Masque de sous-réseau	Passerelle par default
Firewall gig 0/0	200.100.29.30	255.255.255.224	/
Firewall gig 0/1	200.100.29.125	255.255.255.224	/
RO_EXT_INT gig0/0	200.100.29.126	255.255.255.224	/
RO_EXT_INT gig0/1	200.100.29.93	255.255.255.224	/
RO_INT_INT gig0/0	200.100.29.94	255.255.255.224	/
RO_INT_INT gig0/1	200.100.29.62	255.255.255.224	/
SW_INT_BORD	200.100.29.67	255.255.255.224	/

WRT300N	172.16.1.14	255.255.255.240	/
SW_INT_INT	200.100.29.36	255.255.255.224	/
SW_EXT_INT	200.100.29.124	255.255.255.224	/
Serveur HTTP	200.100.29.97	255.255.255.224	200.100.29.124
Serveur TFTP	200.100.29.35	255.255.255.224	200.100.29.36
Serveur Web	172.16.1.1	255.255.255.240	172.16.1.14
PC_admin	200.100.29.33	255.255.255.224	200.100.29.36
PC1	172.16.1.10	255.255.255.240	172.16.1.14
HP181	200.10.29.34	255.255.255.224	200.100.29.36

Chaque carré en gris pourra être adapté en changeant des numéros ou des interfaces. J'ai fait ça car les manipulations se répètent d'un appareil à un autre et ce n'est pas toujours très pertinent de montrer pratiquement les mêmes captures.

Configuration routeur :

```
--- System Configuration Dialog ---  
  
Would you like to enter the initial configuration dialog? [yes/no]: n  
  
Press RETURN to get started!
```

Lors de l'initialisation d'un routeur, celui-ci propose d'appliquer une configuration automatique. J'ai choisi de refuser cette option car ça me permet d'éviter d'avoir à entrer des mots de passe à chaque étape de la configuration ce qui rendant le processus plus fluide et efficace. Une fois la configuration réseau terminée, je les appliquerais.

```
Router(config)#interface FastEthernet1/0  
Router(config-if)#no ip address  
Router(config-if)#ip address 200.100.29.126 255.255.255.224
```

Dans cette capture, je configure l'interface FastEthernet1/0 du routeur. Je commence par entrer dans le mode de configuration de cette interface avec la commande interface FastEthernet1/0. Ensuite, j'utilise la commande no ip address pour supprimer toute adresse IP précédemment configurée sur cette interface. Je configure ensuite une nouvelle adresse IP avec un masque de sous-réseau. J'ai attribué une adresse ip à l'interface, ici FastEthernet1/0.

Configuration des switches :

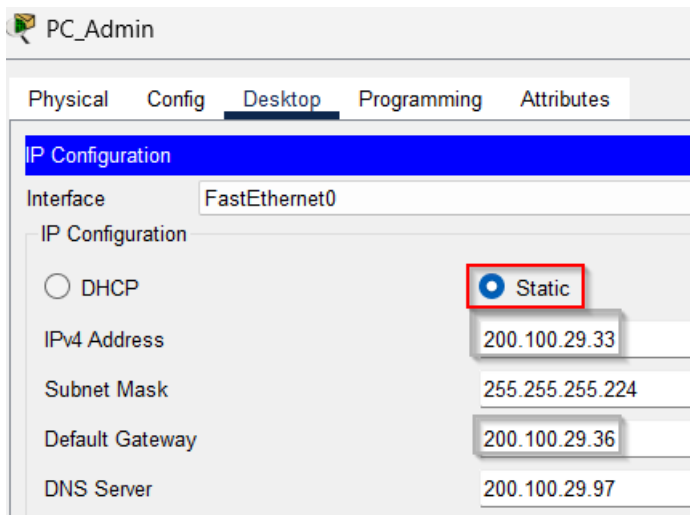
```
Switch(config)#interface vlan 1  
Switch(config-if)#ip address 200.100.29.98 255.255.255.224  
Switch(config-if)#no shutdown
```

Ici, je configure l'interface VLAN 1 d'un switch. Je commence par entrer dans la configuration de cette interface avec interface vlan 1. Ensuite, j'attribue une adresse IP statique avec un masque de sous-réseau. J'active l'interface VLAN avec no shutdown pour qu'elle soit opérationnelle. Cela permet au switch de communiquer sur le réseau via cette adresse IP.

```
Switch(config)#ip default-gateway 200.100.29.62
```

J'ai aussi ajouté une passerelle par défaut pour que le switch ait accès à d'autres sous-réseaux.

Configuration des adresses IP statiques sur les PCs et serveurs :



Je sélectionne l'option "Static" dans la section de configuration IP et entre l'adresse IP le masque de sous-réseau, la passerelle par défaut et le serveur DNS. J'ai configuré le PC admin, les serveurs, l'imprimante et le PC1 en statique car pour configurer une communication fiable entre les appareils du réseau.

Configuration du WRT300N :

The screenshot shows the MAGASIN router configuration interface. At the top, there are tabs for Physical, Config, GUI, and Attributes. The 'Config' tab is selected, and the 'Internet Setup' section is active. The 'Internet Connection type' is set to 'Static IP'. Below this, the following fields are filled in:

Field	Value
Internet IP Address	200 . 100 . 29 . 30
Subnet Mask	255 . 255 . 255 . 224
Default Gateway	200 . 100 . 29 . 30
DNS 1	200 . 100 . 29 . 97
DNS 2 (Optional)	0 . 0 . 0 . 0

Ici, je configure l'adresse IP qui permet au routeur de se connecter à internet en utilisant l'interface graphique. Je sélectionne "Static IP" comme type de connexion Internet et je remplis, l'adresse IP le masque de sous-réseau, la passerelle par défaut et le DNS

The screenshot shows the MAGASIN router configuration interface. At the top, there are tabs for Physical, Config, GUI, and Attributes. The 'Config' tab is selected, and the 'Internet Settings' section is active. The 'IP Configuration' is set to 'Static'. The following fields are filled in:

Field	Value
IPv4 Address	200.100.29.30
Subnet Mask	255.255.255.224
Default Gateway	200.100.29.30
DNS Server	

Dans cette capture, je configure l'adresse IP du routeur dans l'onglet "Config", section "Internet". J'ai sélectionné l'option "Static" pour attribuer manuellement une adresse IP fixe et j'ai mis les informations de l'interface entre le routeur magasin et le firewall pour qu'il puisse communiquer entre eux.

Mise en place du DHCP :

Le DHCP attribue automatiquement des adresses IP. Je le mets en place sur les routeurs pour éviter des erreurs d'adressage IP et gagner du temps. J'exclue toutes les adresses IP statiques pour ne pas avoir de conflits.

```
Ro_INT_INT(config)#ip dhcp pool PoolRouge
Ro_INT_INT(dhcp-config)#network 200.100.29.32 255.255.255.224
Ro_INT_INT(dhcp-config)#default-router 200.100.29.62
Ro_INT_INT(dhcp-config)#ex
Ro_INT_INT(config)#ip dhcp excluded-address 200.100.29.33 200.100.29.35
Ro_INT_INT(config)#ip dhcp excluded-address 200.100.29.36 200.100.29.34
Ro_INT_INT(config)#ip dhcp excluded-address 200.100.29.62
```

Ici, je configure un pool DHCP. Je définis le réseau comme sur le schéma réseau avec un masque de sous-réseau et la passerelle par défaut. J'exclus ensuite les adresses IP déjà utilisées pour les appareils statiques pour éviter qu'elles ne soient attribuées dynamiquement.

```
Ro_INT_INT(config)#ip dhcp pool PoolBleu
Ro_INT_INT(dhcp-config)#dns 200.100.29.97
```

Je configure adresse IP du serveur DNS (200.100.29.97) pour que les clients puissent résoudre les noms de domaine.

Le Pool Rouge est attribué au sous-réseau int_int, le Pool Bleu au sous-réseau ext_int et le Pool vert au sous-réseau int_board. Je trouve que mettre des couleurs étaient plus facile pour désigner chaque réseau.

Pour rediriger la demande de DHCP vers le bon routeur, il faut aider le routeur concerné en entrant l'adresse IP du routeur DHCP:

```
Firewall(config)#int fa1/0
Firewall(config-if)#ip helper-address 200.100.29.94
```

J'ai choisi le firewall qui est la passerelle par default de la DMZ car les paquets seront redirigé vers se routeur. J'ai sélectionné l'interface correspondante (fa1/0) et entrer la commande « ip helper-address » et l'adresse IP du routeur DHCP 200.100.29.94.

WRT300N :

Network Setup

Router IP

IP Address: 169 . 16 . 1 . 14

Subnet Mask: 255.255.255.240

DHCP Server Settings

DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 169.16.1. 1

Maximum number of Users: 14

IP Address Range: 169.16.1. 1 - 14

DHCP Reservation

Je configure ici l'adresse IP du routeur (169.16.1.14) et son masque de sous-réseau (255.255.255.240). J'active le serveur DHCP pour attribuer des adresses IP dynamiques aux clients, en définissant une plage d'adresses de 169.16.1.1 à 169.16.1.14. J'ai limité le nombre d'utilisateurs à 14 pour limiter le nombre de personnes connecté au réseau.

Pour exclure les adresses IP, il faut aller dans l'onglet GUI puis dans DHCP Reservation.

Internet Setup

Internet Connection type: Static IP

Internet IP Address: 200 . 100 . 29 . 30

Subnet Mask: 255 . 255 . 255 . 224

Default Gateway: 200 . 100 . 29 . 30

DNS 1: 200 . 100 . 29 . 97

DNS 2 (Optional): 0 . 0 . 0 . 0

DNS 3 (Optional): 0 . 0 . 0 . 0

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU: Size: 1500

Network Setup

Router IP: IP Address: 172 . 16 . 1 . 14

Subnet Mask: 255.255.255.240

DHCP Server Settings

DHCP Server: ☒ Enabled ☐ Disabled

DHCP Reservation

DHCP Reservation

Wireless-N Broadband Router

Firmware Version: v0.93.3

DHCP Reservation

Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
	LAN	172.16.1.1	00:00:0C:75:02:74	<input type="checkbox"/>
	LAN	172.16.1.3	00:01:43:61:71:A1	<input type="checkbox"/>
	LAN	172.16.1.5	00:0C:CF:3A:98:24	<input type="checkbox"/>

Add Client

Manually Adding Client

Enter Client Name	Assign IP Address	To This MAC Address	Add
	172.16.1.0	00:00:00:00:00:00	Add

Dans cette interface de réservation DHCP, je peux attribuer des adresses IP fixes à des clients spécifiques. Trois clients sont déjà listés, avec leurs adresses IP, adresses MAC et l'interface associée. Pour sélectionner un client existant, je coche la case correspondante et confirme la réservation. Si je veux ajouter un nouveau client manuellement, je renseigne un nom dans le champ "Enter Client Name", l'adresse IP souhaitée dans "Assign IP Address" et l'adresse MAC correspondante dans "To This MAC Address". Ensuite, je clique sur "Add Client" pour ajouter la réservation.

Routeur :

Le routage permet que 2 LANs communiquent entre eux. J'ai choisi un routage OSPF car il est sécurisé (authentification MD5), il est rapide et efficace (mise à jour de routage automatique).



On commence par associer les interfaces du routeur à OSPF via leur sous-réseau en spécifiant une zone OSPF :


```
Router(config)#router ospf 10
Router(config-router)#router-id 3.3.3.3
Router(config-router)#log-adjacency-changes
Router(config-router)#network 200.100.29.0 0.0.0.31 area 0
Router(config-router)#network 200.100.29.96 0.0.0.31 area 0
Router(config-router)#
00:38:51: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on FastEthernet1/0 from LOADING to FULL, Loading Done
```

Dans cette configuration OSPF, je définis le processus OSPF avec l'ID 10, puis j'attribue un identifiant de routeur (3.3.3.3) car elle est unique, indépendante des adresses IP des interfaces et c'est une adresse IPv4. Cet identifiant est utilisé pour identifier de manière unique ce routeur dans le protocole OSPF. J'ajoute les réseaux 200.100.29.0/31 et 200.100.29.96/31 à l'aire OSPF 0. Cela permet au routeur de faire participer ces sous-réseaux à l'échange des routes via OSPF. J'active également la journalisation des changements d'adjacence pour surveiller les transitions des voisins dans OSPF.

L'ID du routeur ro_int_int est 1.1.1.1, celui du routeur ro_ext_int est 2.2.2.2 et celui du routeur firewall est 3.3.3.3.

Mais je n'arrivais pas à envoyer un paquet ICMP du routeur firewall au routeur SW_INT_INT :

 Failed Ro_IN... Firewall ICMP  0.000 N 6

J'ai donc utilisé « clear ip ospf process », qui est utilisée pour redémarrer les processus OSPF sur les deux routeurs :

```
Router#clear ip ospf process
Reset ALL OSPF processes? [no]: y

Router#
00:44:40: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Adjacency forced to reset

00:44:40: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

00:44:41: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0 from LOADING to FULL, Loading Done

Router#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
2.2.2.2          1     FULL/DR         00:00:30    200.100.29.93  GigabitEthernet0/0
```

Je redémarre tous les processus OSPF avec la commande clear ip ospf process. Lorsque le message de confirmation apparaît, je réponds "y" pour confirmer le redémarrage. Cela force le protocole à rétablir toutes les adjacences, ce qui peut résoudre des problèmes de connectivité ou actualiser la table de routage.

On observe que l'adjacence avec le voisin 2.2.2.2 passe d'un état "FULL" à "DOWN", suivi d'une nouvelle négociation qui revient à l'état "FULL". Cela montre que le processus OSPF s'est réinitialisé correctement et que les voisins sont de nouveau synchronisés.

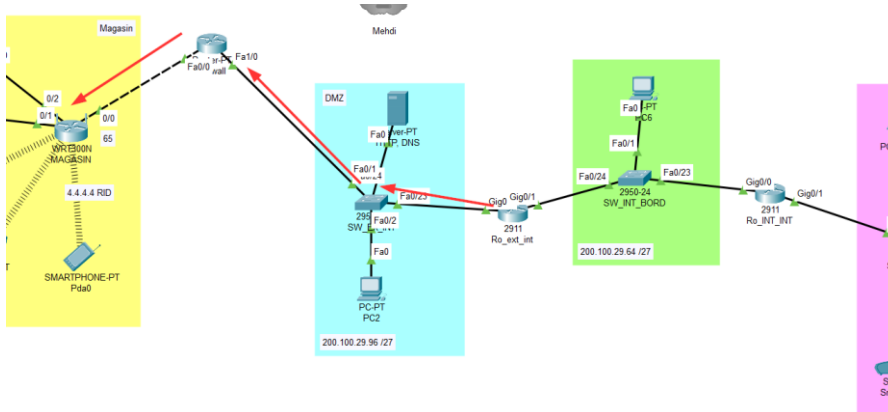
Enfin, la commande `show ip ospf neighbor` est utilisée pour vérifier l'état des voisins OSPF. Le voisin 2.2.2.2 est affiché avec l'état "FULL/DR", indiquant qu'il est pleinement opérationnel et agit comme routeur désigné (DR). L'interface utilisée est GigabitEthernet0/0, et l'adresse IP correspondante est 200.100.29.93. Cette vérification assure que la connectivité OSPF est restaurée.

Le paquet ICMP est bien arrivé :

Successful Ro_IN... Firewall ICMP 0.000 N 6

Le WRT300N ne prends pas en compte le routage ospf, on le configure donc sur le routeur voisin, le firewall :

```
Firewall(config)#router ospf 10
Firewall(config-router)# network 200.100.29.0 0.0.0.31 area 0
```

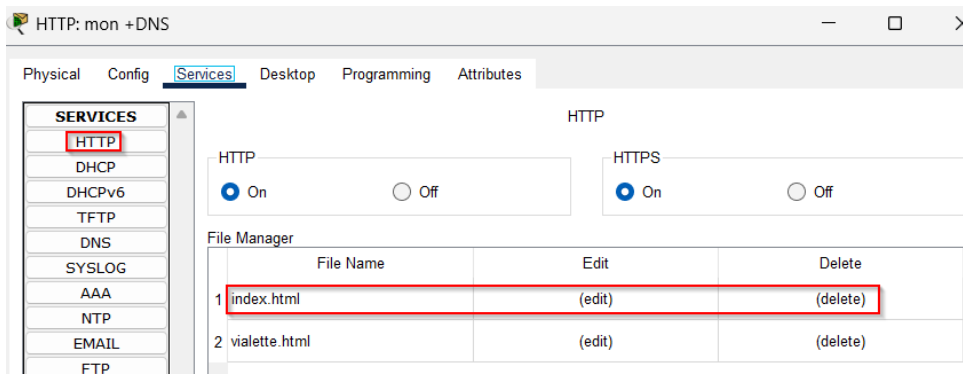


Ce qui permet les routeurs d'envoyer des données au routeur magasin.

Mise en place des différents serveurs :

Le serveur DNS :

J'ai repris le site web que j'avais fait dans le TP3 car il contient mon nom et mon prénom.



Je suis allée sur le serveur http, puis dans services, http et j'ai créé un site (index.html). J'y est ensuite copié mon site web.

Connecter deux réseaux :

Protégez votre ordinateur avec le Pare-feu Windows Defender

Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

Mettre à jour les paramètres du pare-feu

Le Pare-feu Windows Defender n'utilise pas les paramètres recommandés pour protéger votre ordinateur.

Utiliser les paramètres recommandés

Quels sont les paramètres recommandés ?

Réseaux avec domaine Connecté ^

Réseaux en entreprise, qui appartiennent à un domaine

État du Pare-feu Windows Defender : Désactivé

Connexions entrantes : Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

Réseaux avec domaine actifs : sio.local

État de notification : M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application

Réseaux privés Non connecté v

Réseaux publics ou invités Non connecté v

Je désactive le pare-feu Windows pour autoriser toutes les connexions entrantes le temps de me connecter avec mon camarade. Je le réactiverais après.

Multiuser Listen

172.25.0.1:38000
172.31.1.67:38000
192.168.56.1:38000
127.0.0.1:38000

Local Listening Address:

Port Number 38000

Password

Existing Remote Networks

☒ Always Accept
☐ Always Deny
☐ Prompt

New Remote Networks

☒ Always Accept
☐ Always Deny
☐ Prompt

Ici, je configure un service de type "Multiuser Listen" avec un port d'écoute (38000) et un mot de passe cisco (le même pour les deux réseaux) pour sécuriser les connexions. J'ai défini que les réseaux existants et les nouveaux réseaux distants sont toujours acceptés (Always Accept) pour faciliter la connexion entre les 2.

```
Firewall(config)#ip route 0.0.0.0 0.0.0.0 se2/0
```

Je crée une route statique vers l'extérieur pour que la connexion se fasse.

Sécurisation des routeurs :

```
Firewall>enable
Firewall#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Firewall(config)#enable secret candice
Firewall(config)#line console 0
Firewall(config-line)#password candice
Firewall(config-line)#login
Firewall(config-line)#exit
Firewall(config)#line vty 0 4
Firewall(config-line)#password candice
Firewall(config-line)#login
Firewall(config-line)#transport input ssh
Firewall(config-line)#exit
```

Dans cette capture, je configure la sécurité de l'accès au firewall :

- Mot de passe d'administration globale :
J'utilise enable secret candice pour définir un mot de passe chiffré pour accéder au mode privilégié. Cela renforce la sécurité par rapport à un mot de passe en clair.
- Configuration de la console :
Je passe sur la ligne console avec line console 0, puis je configure un mot de passe (password candice) et j'active l'obligation de connexion avec la commande login. Cela sécurise l'accès physique à l'appareil.
- Configuration des lignes VTY (accès distant) :
Avec line vty 0 4, je sécurise les connexions distantes en définissant un mot de passe (password candice) et en activant l'authentification (login). J'autorise uniquement les connexions SSH grâce à transport input ssh, garantissant un accès sécurisé à distance.

Ces configurations sont essentielles pour protéger l'accès local et distant à l'appareil et prévenir tout accès non autorisé.

```
Firewall(config)#crypto key generate rsa
% Please define a domain-name first.
Firewall(config)#ip domain-name cvialette
Firewall(config)#line vty 0 4
Firewall(config-line)#transport input ssh
Firewall(config-line)#exit
```

Dans cette étape, une clé RSA est générée pour sécuriser les connexions SSH, mais une erreur indique qu'il faut d'abord définir un nom de domaine. En conséquence, la commande ip domain-name cvialette est exécutée pour définir le domaine nécessaire à la création de la clé. Ensuite, la configuration des lignes VTY (télésession virtuelle) est ajustée pour permettre uniquement les connexions SSH avec la commande transport input ssh. Cela renforce la sécurité en limitant les types d'accès autorisés.

```
Firewall(config)#username admin privilege 15 secret candice
Firewall(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
```

Ici, un utilisateur avec des privilèges administratifs est créé en utilisant username admin privilege 15 secret candice. La commande ip ssh version 2 est utilisée pour activer la version 2 de SSH, qui est plus sécurisée que la version 1. Cependant, un message rappelle qu'une clé RSA de taille minimale de 768 bits est nécessaire pour cette version. Cela garantit une configuration moderne et sécurisée pour SSH.

```
Firewall(config)#service password-encryption
```

La commande service password-encryption est activée pour chiffrer les mots de passe dans la configuration. Cela empêche l'exposition en clair des mots de passe sensibles, renforçant ainsi la sécurité globale de l'appareil.

```
Firewall(config)#access-list 10 permit 200.100.29.33
Firewall(config)#line vty 0 4
Firewall(config-line)#access-class 10 in
Firewall(config-line)#exit
```

Un contrôle d'accès est mis en place avec la commande access-list 10 permit 200.100.29.33 pour autoriser uniquement cette adresse IP à accéder aux lignes VTY. Ensuite, la liste d'accès est appliquée avec access-class 10 in. Cette configuration limite l'accès SSH à des sources spécifiques, empêchant ainsi des connexions non autorisées.

```
Firewall(config)#line console 0
Firewall(config-line)#exec-timeout 5 0
Firewall(config-line)#exit
Firewall(config)#line vty 0 4
Firewall(config-line)#exec-timeout 5 0
Firewall(config-line)#exit
Firewall(config)#end
Firewall#copy running-config startup-config
Destination filename [startup-config]?
%SYS-5-CONFIG_I: Configured from console by console
```

Les délais d'inactivité sont configurés à 5 minutes avec exec-timeout 5 0 sur la console et les lignes VTY. Cela déconnecte automatiquement les sessions inactives pour réduire les risques d'accès non surveillés. Enfin, la configuration courante est sauvegardée dans la configuration de démarrage avec copy running-config startup-config, ce qui garantit que toutes les modifications sont conservées après un redémarrage.

J'ai configuré les 3 routeurs exactement de la même manière car utiliser des mots de passe différents serait plus sécurisé mais moins facile à retenir. Comme nous sommes juste dans une simulation j'ai choisi de garder le même.

2. Vérification :

Vérification ospf :

```
Ro_ext_int#show ip ospf neighbor
```

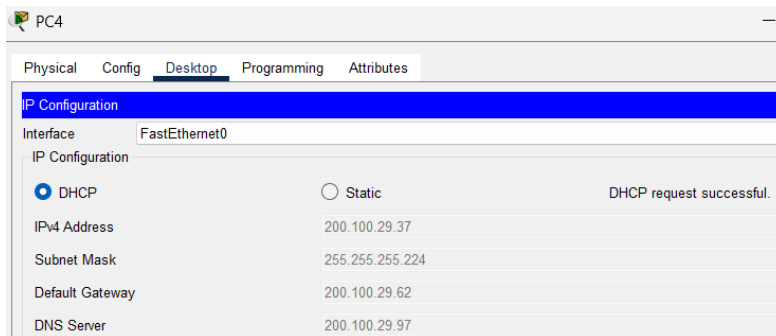
Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	00:00:36	200.100.29.94	GigabitEthernet0/1
3.3.3.3	1	FULL/DR	00:00:36	200.100.29.125	GigabitEthernet0/0

Avec la commande `show ip ospf neighbor`, je vérifie l'état des voisins OSPF. Deux voisins sont listés. Les voisins sont dans l'état FULL/BDR, ce qui indique qu'ils sont complètement synchronisés et agissent comme routeur désigné de secours (BDR). Cette vérification me permet de m'assurer que les relations de voisinage OSPF sont établies et fonctionnelles.

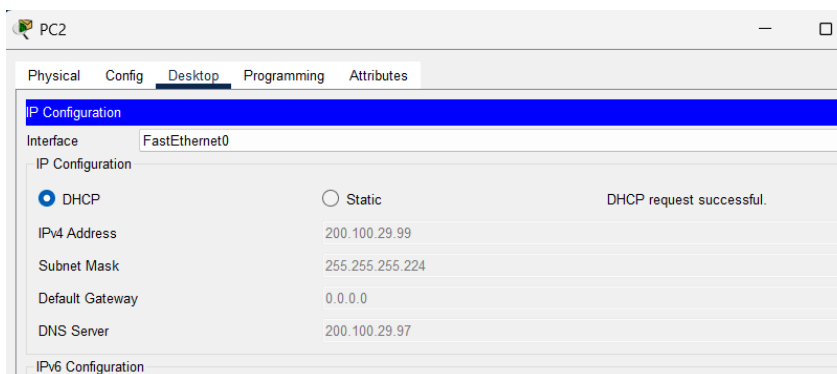
```
Ro_INT_INT#show ip route ospf
200.100.29.0/24 is variably subnetted, 6 subnets, 2 masks
O       200.100.29.0 [110/3] via 200.100.29.93, 00:14:19, GigabitEthernet0/0
O       200.100.29.96 [110/2] via 200.100.29.93, 00:14:19, GigabitEthernet0/0
```

Avec la commande `show ip route ospf`, je consulte les routes apprises via OSPF pour le réseau 200.100.29.0/24. Ce réseau est subdivisé en 6 sous-réseaux avec 2 masques différents. La route 200.100.29.0 est apprise avec une métrique de coût [110/3] via le prochain saut 200.100.29.93, utilisant l'interface GigabitEthernet0/0. La route 200.100.29.96 est également apprise avec une métrique [110/2] via le même saut et interface. Ce qui montre que le routage dynamique OSPF fonctionne correctement en intégrant plusieurs sous-réseaux.

Vérification DHCP :



J'ai vérifié le DHCP dans un premier temps dans un réseau appartenant au routeur DHCP. On voit que le masque de sous-réseau (255.255.255.224), la passerelle par défaut (200.100.29.62) et le Serveur DNS (200.100.29.97) sont configurés correctement. De plus l'adresse IP est dans la plage d'adresse IP du réseau rouge. Ces paramètres permettent à l'ordinateur de communiquer avec d'autres appareils sur le réseau et d'accéder à des ressources externes via le DNS et la passerelle.



J'ai aussi vérifié que le DHCP marchait dans un réseau ne lui appartenant pas. On voit que le masque de sous-réseau (255.255.255.224), la passerelle par défaut (200.100.29.62) et le Serveur DNS (200.100.29.97) sont configurés correctement. De plus l'adresse IP est dans la





plage d'adresse IP du réseau bleu. Ces paramètres permettent à l'ordinateur de communiquer avec d'autres appareils sur le réseau et d'accéder à des ressources externes via le DNS et la passerelle.

```
Ro_INT_INT#show running-config | include excluded-address
ip dhcp excluded-address 200.100.29.94
ip dhcp excluded-address 200.100.29.125
ip dhcp excluded-address 200.100.29.33 200.100.29.35
ip dhcp excluded-address 200.100.29.36 200.100.29.34|
ip dhcp excluded-address 200.100.29.62
ip dhcp excluded-address 200.100.29.94 200.100.29.93
ip dhcp excluded-address 200.100.29.67
ip dhcp excluded-address 200.100.29.98 200.100.29.125
ip dhcp excluded-address 200.100.29.97 200.100.29.126
```



J'ai aussi vérifié les adresses IP exclues, elles sont correctes et là. Le DHCP ne pourra donc pas les attribuer .

Le DHCP est donc configuré comme il faut et marche.

Connections sans fil (scénarios 4) :

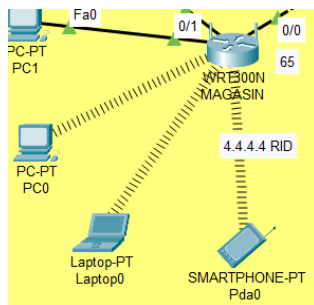
	Successful	Laptop0	MAGASIN	ICMP		0.000	N	0	(edit)
	Successful	PC0	MAGASIN	ICMP		0.000	N	1	(edit)

Entre le routeur WRT300N (magasin) et le PC et l'ordinateur portable. On voit qu'il est réussi.

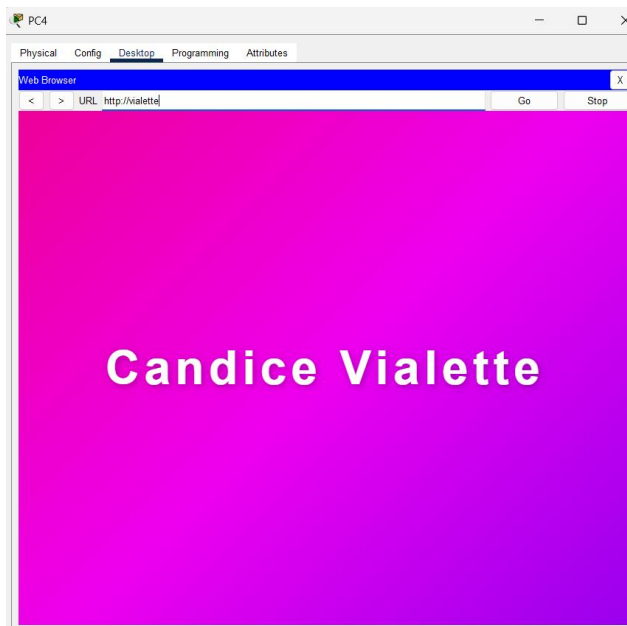
	Successful	Pda0	MAGASIN	ICMP		0.000	N	0	(edit)
---	------------	------	---------	------	---	-------	---	---	--------

Et là entre le smartphone et le routeur WRT300N. On voit que ça marche.

De plus on voit les connections entre le routeur magasin et les matériels sans fil :

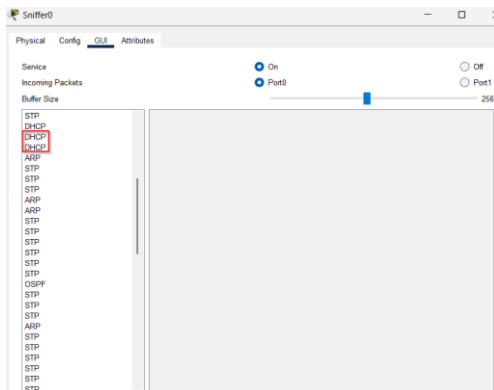


Serveur DNS et http :



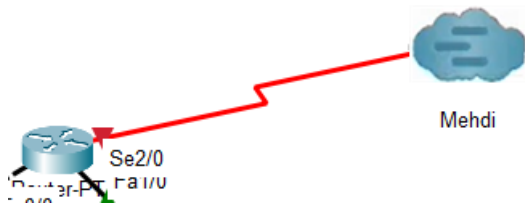
J'ai rentré le nom de mon site sur un poste qui n'est pas dans la dmz, le même réseau que le serveur et le service DNS a bien traduit le nom de domaine. De plus le service http a bien afficher mon site web.

Sniffer :



Le sniffer capte bien les échanges qui se passent sur le réseau, comme les requêtes et réponses DHCP. J'ai testé en demandant une adresse IP dynamique, et j'ai bien vu passer les messages DHCP (Discover, Offer, Request et Acknowledgment) dans les trames capturées. Cependant, il faut faire attention à ce que le sniffer ne soit pas isolé dans un VLAN. Sinon, il ne pourra pas voir les échanges entre différents VLAN ou les trames envoyées sur d'autres parties du réseau, ce qui empêcherait d'avoir une vue complète de ce qui se passe.

La connexion entre deux pkt :



On voit bien que le nuage est devenu bleu, la connexion a donc été établie avec succès.

Sécurité :

User Access Verification

Password:

Firewall>en

Password:

Password:

Firewall#

On voit bien qu'il faut un mot de passe pour se connecter à l'interface du routeur. Ce que j'ai fait a donc bien fonctionné.

3. Fonction NAT

La fonction NAT sera mise en place lors du tp 09 sur le NAT et le PAT.

Je me suis renseigné dessus :

Fonctionnement du NAT-PAT :

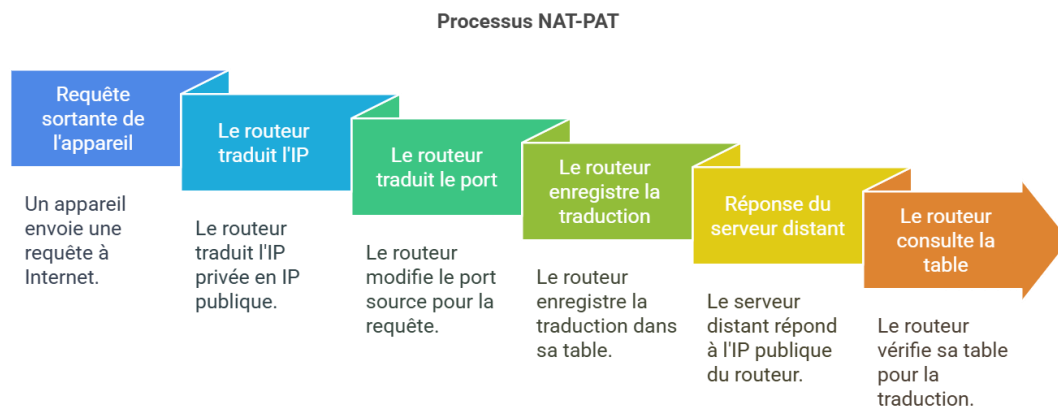
1. Contexte :

- Les adresses IP publiques sont limitées (IPv4), donc les réseaux locaux utilisent des IP privées (ex. 192.168.x.x, 10.x.x.x).
- Le routeur (ou box Internet) doit "traduire" ces IP privées en une IP publique pour communiquer avec Internet.

2. Étape 1 : Requête sortante (de l'appareil vers Internet) :

- Un appareil (ex. smartphone 192.168.1.10) envoie une requête (ex. accéder à un site web).
- Le routeur remplace :
 - IP source privée (192.168.1.10) → IP publique du routeur (ex. 203.0.113.5).
 - Port source aléatoire (ex. 5000) → Nouveau port unique (ex. 12345).

- Le routeur garde une table de traduction (NAT table) pour mémoriser cette correspondance.
3. Étape 2 : Réponse entrante (d'Internet vers l'appareil) :
- Le serveur distant répond à l'IP publique (203.0.113.5) et au port 12345.
 - Le routeur consulte sa table de traduction :
 - Il retrouve que 203.0.113.5:12345 correspond à 192.168.1.10:5000.
 - Il redirige la réponse vers le bon appareil.



NAT-PAT (ou NAT Overload) :

✓ But : Partager 1 IP publique entre plusieurs appareils (PC, smartphone, etc.).

✓ Comment :

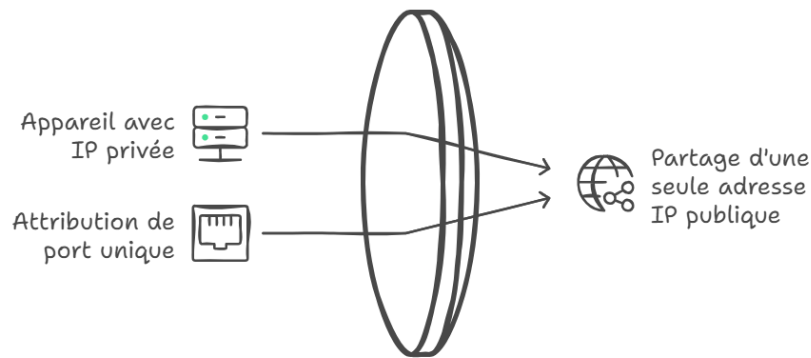
→ Chaque appareil à une IP privée locale (ex : 192.168.1.10).

→ Le routeur remplace l'IP privée par son IP publique en sortie.

→ + Ports TCP/UDP : Le routeur attribue un port unique par connexion (ex : 203.0.113.5:12345).

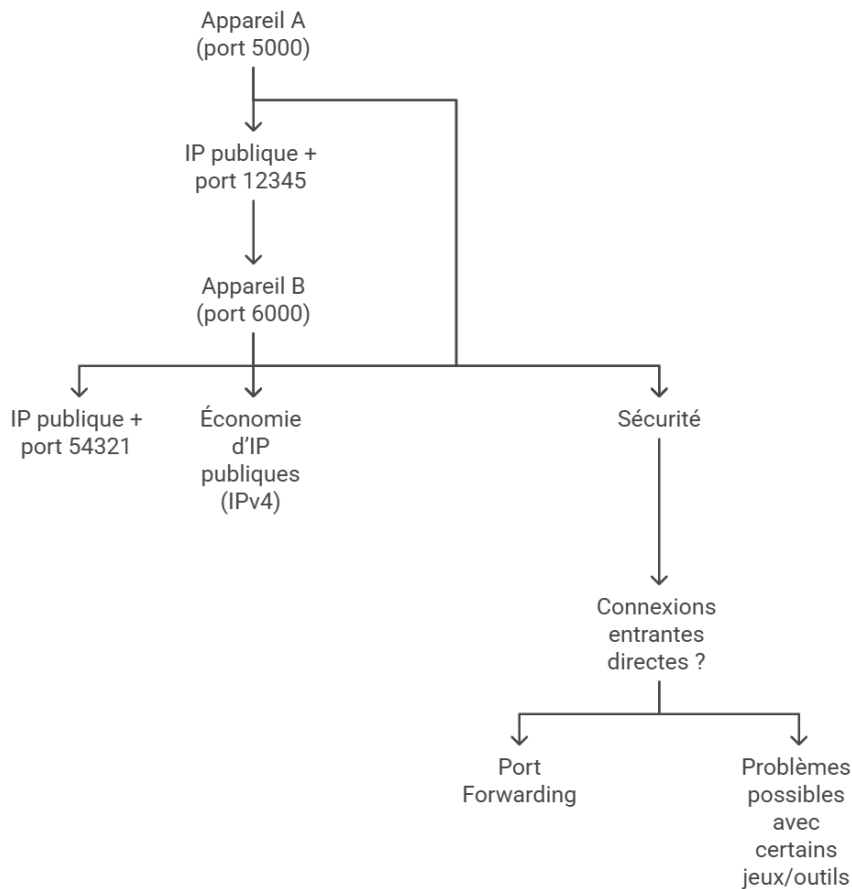
Exemple :

Mécanisme NAT-PAT



- Appareil A (port 5000) → IP publique + port 12345.
- Appareil B (port 6000) → IP publique + port 54321.
- :
- → Économie d'IP publiques (IPv4).
- → Sécurité (masque le réseau local).
-
- Les connexions entrantes directes nécessitent du *Port Forwarding*.
- Problèmes possibles avec certains jeux/outils (ex : P2P).

Fonctionnement du NAT-PAT



En gros : le NAT-PAT est le traducteur malin qui gère le trafic Internet de toute la maison avec une seule IP !

Conclusion :

Cet atelier a permis de concevoir et d'implémenter une infrastructure réseau complète en exploitant les fonctionnalités du routeur Linksys WRT300N. L'accent a été mis sur le déploiement des services essentiels tels que le DHCP et l'agent relais pour gérer les communications entre sous-réseaux, tout en assurant une sécurisation avancée des équipements et une gestion rigoureuse des ressources réseau. Cette approche a permis de mettre en pratique les bonnes pratiques de segmentation, de contrôle d'accès et d'analyse des limites matérielles pour répondre aux besoins d'un réseau moderne.

Sources :

[Prise en main de Cisco Packet Tracer pour créer un lab](#)

https://en.wikipedia.org/wiki/VLAN_hopping

<https://openclassrooms.com/fr/courses/7192261-simulez-le-schema-de-votre-reseau-avec-cisco-packet-tracer/7444197-ajoutez-un-point-d-acces-sans-fil-au-reseau-de-la-metropole>

<https://www.youtube.com/watch?v=gTkEyKbN1qg>

<https://www.youtube.com/watch?v=aW4A8ffMx9g>

<https://app.napkin.ai>