

|  |
| --- |
|  |
| **Atelier 08**  Création réseau |
|  |

Sommaire

[1 introduction 1](#_Toc157863865)

[2 Rappel du contexte 1](#_Toc157863866)

[3 Réalisation du réseau 1](#_Toc157863867)

[4 Examen de la fonction nat du routeur LINKSYS WRT300N 6](#_Toc157863868)

[5 Réalisation d’une solution pour un réseau plus sécurise 9](#_Toc157863869)

[6 Conclusion 10](#_Toc157863870)

# 

# introduction

Cet atelier nous fait découvrir et reproduire un réseau sur le logiciel Cisco Packet Tracer en mettant en place plusieurs instructions et une certaine adresse IP à respecter. Nous allons découvrir le paramétrage d’un DHCP et DHCP Relais, la création de scénarii et une modification de notre schéma réseau pour un autre plus sécurisé selon nos constatations sur le réseau fourni de bas.

Découvrons maintenant cet atelier dans la partie 2.

# Rappel du contexte

Dans ce TP de mise en œuvre d’un serveur DHCP et agent de relais DHCP, dispositif multifonction Linksys WRT300N, NAT/PAT, serveur DNS, WEB, nous avons dû créer un petit réseau avec un dispositif multifonction commutateur-routeur-point d’accès sans fil Linksys WRT300N.

Nous avons eu pour but :

* Examinez la fonction NAT/PAT
* Mettre en place un service DHCP et DHCP Relais et le paramètre
* Étudiez les différents services proposés sur les serveurs que nous allons mettre en place

Le modèle à suivre est le suivant :

Une image contenant diagramme, ligne, carte

Description générée automatiquement

# Réalisation du réseau

Nous allons maintenant réaliser notre réseau sur Cisco Packet Tracer en nous aidant de notre modèle donner :

Une image contenant ligne, diagramme

Description générée automatiquement

Avant de commencer le paramétrage de notre réseau, nous devons créer notre table de routage pour simplifier le paramétrage de nos postes et nous y retrouver plus facilement.  Voici la table de routage que j’ai effectué :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Appareils** | **Adresse IP** | **Masque** | **Gateway** | **DNS Server** | **Static / DHCP et plage** |
| Sniffer | X | X | X | X | X |
| Printer | 200.100.42.34 | 255.255.255.224 | 200.100.42.62 | 200.100.42.97 | Static |
| PC5 | 200.100.42.33 – 200.100.42.62 | 255.255.255.224 | 200.100.42.62 | 200.100.42.97 | DHCP Plage 1 |
| PC6 | 200.100.42.33 – 200.100.42.62 | 255.255.255.224 | 200.100.42.62 | 200.100.42.97 | DHCP Plage 1 |
| Server TFTP – Sauvegarde conf + NTP | 200.100.42.35 | 255.255.255.224 | 200.100.42.62 | 200.100.42.97 | Static |
| PC Admin | 200.100.42.33 | 255.255.255.224 | 200.100.42.62 | 200.100.42.97 | Static |
| SW\_INT\_INT | Création VLAN1 200.100.42.36 | 255.255.255.224 | X | X | X |
| RO\_INT\_INT | Port Gig0/0 200.100.42.94 Port Gig0/1  200.100.42.62 | 255.255.255.224 | X | 200.100.42.97 | X |
| SW\_INT\_BORD | Création VLAN1 200.100.42.92 | 255.255.255.224 | X | X | X |
| PC3 | 200.100.42.65 – 200.100.42.92 | 255.255.255.224 | 200.100.42.94 | 200.100.42.97 | DHCP Plage 2 |
| RO\_EXT\_INT | Port Gig0/0 200.100.42.125 Port Gig0/1  200.100.42.93 | 255.255.255.224 | X | 200.100.42.97 | X |
| Switch0 | Création VLAN1 200.100.42.124 | 255.255.255.224 | X | X | X |
| Server HTTP + DNS | Activation DNS avec IP : 200.100.42.97 et comme nom : lenny.com  Activation du service HTTP | 255.255.255.224 | 200.100.42.125 | 200.100.42.97 | Static |
| PC2 | 200.100.42.98 – 200.100.42.124 | 255.255.255.224 | 200.100.42.125 | 200.100.42.97 | DHCP Plage 3 |
| Router3 | Fa0/0  200.100.42.30  Fa1/0  200.100.42.126 | 255.255.255.224 | X | X | X |
| WRT300N MAGASION | Internet setup : 200.100.42.29  Router IP : 172.16.1.254  Ip Adresse Range 172.16.1.11 -172.16.1.23 | 255.255.255.224  255.255.255.0 | 200.100.42.30  X | 200.100.42.97  200.100.42.97 | Static  DHCP |
| SmartphonePT | 172.16.1.11 -172.16.1.23 | 255.255.255.0 | 172.16.1.254 | 200.100.42.97 | DHCP Réseau interne |
| Laptop0 | 172.16.1.11 -172.16.1.23 | 255.255.255.0 | 172.16.1.254 | 200.100.42.97 | DHCP Réseau interne |
| PC0 | 172.16.1.11 -172.16.1.23 | 255.255.255.0 | 172.16.1.254 | 200.100.42.97 | DHCP Réseau interne |
| PC1 | 172.16.1.10 | 255.255.255.0 | 172.16.1.254 | 200.100.42.97 | Static |
| Server WEB-Invites | Activation du service HTTP  200.100.42.32 | 255.255.255.0 | 172.16.1.254 | 200.100.42.97 | Static |

Nous voilà maintenant prêt à la configuration de notre réseau.

Avant de commencer, nous devons savoir que dans la mise en place d’un système DHCP nous devrons exclure certaines adresses IP. Nous commençons par configurer les postes qui poste des adresses Static, exemple ci-dessous avec le PC\_Admin :

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

Description générée automatiquement

Nous ajoutons la VLAN1 sur notre switch SW\_INT\_INT :



Et je fais de même pour les autres switch :





Par la suite nous passons à la création des exclusions des adresses que l’on va utilise sur les postes en Static ou bien même les adresses qui vont servir de broadcast pour éviter tout problème au niveau de l’adressage des IP avec le DHCP.

|  |  |
| --- | --- |
| **ip dhcp excluded-address** *@ IP exclue* *@ IP exclue* | Configuration des exclusions |

Voici la liste des adresses à exclurent :

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

Description générée automatiquement

Après avoir excluent les adresses nous pouvons commencer la création de DHCP Pool (Nos plages d’adresses).

|  |  |
| --- | --- |
| **ip dhcp pool** *nom* **network** *@ Ip du réseau* *masque* | Configuration du pool DHCP |

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

Description générée automatiquement

Nous nous retrouvons avec nos pools d’adressage d’IP de notre server DHCP, le premier pool correspond à la Plage 1.

Il faut aussi bien penser à no shutdown tous nos routeurs.

Nous devons aussi penser à mettre nos adresses IP sur les ports du routeur par exemple ici avec le port Gig0/0 et Gig0/1 du routeur RO\_INT\_INT :

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

Description générée automatiquement

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

Description générée automatiquement

Nous pouvons passer maintenant à la configuration du routeur RO\_EXT\_INT ou nous allons devoir créer notre relais DHCP. Pour commencer rappelons ce qu’est qu’un rela is DHCP :

Un relais DHCP, ou DHCP relais, est utilisé pour transmettre les demandes DHCP d'un segment de réseau à un serveur DHCP situé sur un autre segment. Cela est souvent nécessaire dans les réseaux étendus où un serveur DHCP unique est utilisé pour servir plusieurs sous-réseaux.

|  |  |
| --- | --- |
| **interface** *interface* *numéro* **ip helper-address** *@ IP du serveur DHCP* | Configuration de l’agent relais |

Nous allons donc ajouter notre relais DHCP en attribuant aussi les adresses sur nos ports Gig0/0 et Gig0/1 :

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

Description générée automatiquement

Notre DHCP est maintenant configuré et le relais DHCP aussi, nous pouvons passer nos postes en DCHP pour qu’ils se voient attribuer une adresse IP.

Nous avons configuré notre server HTTP + DNS en activant ses deux services.

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

Description générée automatiquement

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

Description générée automatiquement

Nous ajoutons notre adresse qui servira de DNS 200.100.42.97.

Nous pouvons continuer la configuration de notre réseau en passant à la configuration du Router3

On configure aussi nos ports Fa0/0 et Fa1/0 :

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

Description générée automatiquement

Ici pas besoin de faire de DHCP.

Nous devons maintenant configurer notre dernier routeur WRT300N MAGASIN.  
Ce routeur est un routeur doté d’un affichage pour le configuré plus facilement mais aussi possible de connecter des appareils en Wifi qui servira de Wifi public pour le magasin.

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

Description générée automatiquement

Nous rentrons les informations que nous avons marquées dans notre tableau d’adressage pour l’internet setup. Il faut bien penser à passer le « Internet Connection type » en Static IP.

Pour le network setup donc notre dernier réseau :

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

Description générée automatiquement  
Il faut aussi faire attention de bien activer le DHCP Server qui va ici nous donner des adresses pour notre appareils qui vont se connecter en Wifi.

Nous devons aussi activer le service http sur notre server Web-invites :

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

Description générée automatiquement

La configuration de notre réseau semble maintenant terminer !

# Examen de la fonction nat du routeur LINKSYS WRT300N

Nous allons maintenant envoyer un PDU simple du PC1 vers le Server1 en mode pas à pas afin d’observer la fonction NAT de notre Routeur WR0.

Nous passons en mode simulation et nous éditons les filtres pour ne laisser de cocher que les requêtes ARP et ICMP comme ci-dessous :

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

Description générée automatiquement

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

Description générée automatiquement**

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

Description générée automatiquement**

Nous lançons une simulation en prenant l’enveloppe fermée (Add Simple PDU), et nous cliquons sur le client PC1 pour le définir comme source, puis sur le client Server1 pour le définir comme destination.

On peut maintenant lancer la démonstration en mode pas à pas, lorsque le PDU est arrivé sur le WR0, nous allons afficher et regarder le contenu de se paquet (onglet Inbound PDU Details).

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

Après avoir regardé dans l’onglet Inbound PDU Details, nous allons observer le contenu du PDU lorsqu’il repart du routeur WR0 :

|  |  |
| --- | --- |
| **Trame obtenue** | **Lorsqu’il repart du routeur, quelle est l’adresse IP source émettrice du paquet IP ?** |
| **Une image contenant texte, capture d’écran, nombre, Parallèle  Description générée automatiquement** | **200.100.42.29** |

La fonction NAT du routeur a bien opéré la translation de l’adresse IP source locale 172.16.1.10 en une adresse IP globale 200.100.42.29.

Le mécanisme NAT opère dans la couche 3 du modèle OSI, la couche réseau.

Nous continuons la simulation jusqu’au retour de notre paquet dans le routeur WR0, et nous allons regarder dans l’onglet Inboud PDU Details vérifier le mécanisme inverse de translation :

L'adresse IP source de l'enveloppe envoyée est 200.100.42.29 et l'adresse IP de destination est 200.100.42.97. On peut donc voir que le routeur a traduit l'adresse IP source de l'enveloppe reçue en adresse IP de destination de l'enveloppe envoyée, et vice-versa.

|  |  |
| --- | --- |
| **Résultats** | **Quel est le numéro identifiant la machine d’adresse IP 172.16.1.10 (PC1) ?** |
| **Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement** | Le numéro identifiant la machine PC1 est 200.100.42.29:8080 |

Nous pouvons créer quelques scénarii pour vérifier la connectivité entre nos postes et server :

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

Description générée automatiquement

Nous allons aussi mettre en place une sécurité d’accès sur nos switchs et routeurs avec les mots de passe suivants :

* Mode enable : sio180\_e
* Mode privilégié : sio180\_p
* Ligne console : sio180\_c
* Lignes virtuelles : sio180\_v

On réalise cette manipulation sur chacun de nos switchs et routeur :

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

Description générée automatiquement

Voilà nos switchs et routeurs sécurisé avec des mots de passes.

# Réalisation d’une solution pour un réseau plus sécurisé

Nous passons maintenant à réalisation de modification de notre réseau en apportant des pistes d’améliorations pour rendre le réseau plus optimisé et sécurisé.

Une image contenant ligne, diagramme

Description générée automatiquement

Voici une proposition de nouveau format du réseau en regroupant les postes des utilisateurs en 1 seul endroit, on regroupe aussi nos serveurs.  
  
  
Dans notre ancien réseau, constitué d’adresse en 200.100.42.XX, nous pouvons ici le masque en /30, mettre des adresses en privé,et configurées directement notre pool DHCP sur notre server ce qui va nous simplifié la tâche :

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

Description générée automatiquement

Nous nous retrouvons maintenant avec un réseau devenu bien plus sécurisé avec des adresses IP utilisé à l’intéreur de notre réseau local LAN et qui n’est pas directement accessible depuis Internet. Ces adresses sont généralement utilisées pour l’adressage des appareils dans un réseau local privé et sont souvent masquées derrière un routeur ou par-feu.

En général, une adresse IP privée est considérée comme plus sécurisée qu'une adresse IP publique, car elle n'est pas directement accessible depuis Internet.

# Conclusion

En conclusion, notre atelier sur la configuration d'un réseau sur Cisco Packet Tracer a été une expérience intéressante. Nous avons pu explorer les fondamentaux de la configuration réseau, depuis la mise en place des équipements jusqu'à la sécurisation des communications.

La première partie de l'atelier nous a permis de créer un petit réseau sur Cisco Packet Tracer, où nous avons configuré chaque équipement de A à Z. Cette étape nous a donné une compréhension pratique des concepts de base de la configuration des routeurs, des commutateurs et des périphériques réseau.

Ensuite, nous avons étudié la fonction NAT en utilisant un routeur Linksys WRT300N. Cette exploration nous a permis de comprendre comment NAT fonctionne pour permettre la communication entre un réseau privé et Internet en traduisant les adresses IP.

Enfin, nous avons abordé la question de la sécurité du réseau en proposant une solution pour améliorer la sécurité de notre infrastructure. En masquant les adresses IP avec un masque en /30, en utilisant des adresses privées et en configurant un pool DHCP sur notre serveur, nous avons pu renforcer la sécurité de notre réseau. Cette approche nous permet de mieux contrôler l'accès aux ressources réseau et de limiter les risques d'intrusion.

En résumé, cet atelier nous a permis d'acquérir des compétences pratiques et théoriques dans la configuration et la sécurisation des réseaux informatiques. Nous sommes désormais mieux équipés pour gérer et maintenir des réseaux efficaces et sécurisés dans des environnements professionnels.

# Webographie

[1] « ChatGPT ». Consulté le: 12 novembre 2023. [En ligne]. Disponible sur: https://chat.openai.com

[2] « Configurer le service DHCP sur un routeur Cisco | Cisco | IT-Connect ». Consulté le: 1 février 2024. [En ligne]. Disponible sur: https://www.it-connect.fr/configurer-le-service-dhcp-sur-un-routeur-cisco/

[3] « Mise en place d’un agent relais DHCP | Cisco | IT-Connect ». Consulté le: 12 novembre 2023. [En ligne]. Disponible sur: https://www.it-connect.fr/mise-en-place-dun-agent-relais-dhcp/

[4] « NAT PAT : Fiche Résumé ». Consulté le: 3 février 2024. [En ligne]. Disponible sur: https://www.formip.com/pages/blog/nat-pat