**CARON**

Atelier

B

3

-

1

*25/09/2023*

*Protocoles DHCP et DNS*

# Table des matières

[I. Table des matières 2](#_Toc150687759)

[II. Introduction 3](#_Toc150687760)

[III. Rôle du DNS 3](#_Toc150687761)

[IV. Nslookup et résolution dns 4](#_Toc150687762)

[a) Who is DNS : 5](#_Toc150687763)

[b) Test web 6](#_Toc150687764)

[V. Pare-feux et ACL : 7](#_Toc150687765)

[VI. Analyse passive 8](#_Toc150687766)

[c) RCPBIND 8](#_Toc150687767)

[VII. Différent type de dns 11](#_Toc150687768)

[VIII. Test Nslookup 12](#_Toc150687769)

[d) Nslookup résolution server messagerie : 13](#_Toc150687770)

[e) Définition d’un rcpbind : 15](#_Toc150687771)

[IX. Analyse Dns 15](#_Toc150687772)

[f) Port utilisé par le protocole DNS sur la couche de couche 4 utilisé par DNS ? 15](#_Toc150687773)

[g) RFC1035 15](#_Toc150687774)

[h) Structure des requêtes et des réponses DNS : 16](#_Toc150687775)

[X. Réflexion sur le DNS : 16](#_Toc150687776)

[i) Windows terminal : 17](#_Toc150687777)

[XI. Différent outils linux pour l’analyse DNS 18](#_Toc150687778)

[XII. Outils delv : 20](#_Toc150687779)

[XIII. Exercice 6 : Analyse approfondie des échanges sous Packet Tracer 23](#_Toc150687780)

[j) 2e partie : Inspecter le trafic interréseau au bureau central 26](#_Toc150687781)

[XIV. Étude sur le DHCP 27](#_Toc150687782)

[k) RFC 28](#_Toc150687783)

[l) Différent type d’allocation : 28](#_Toc150687784)

[m) Risque DHCP : 32](#_Toc150687785)

[n) Risque configuration clasic : 33](#_Toc150687786)

[XV. Création d’un réseaux DHCP : 34](#_Toc150687787)

[o) Problématique du DHCP : 36](#_Toc150687788)

[XVI. Mise en situation man in the middle: 37](#_Toc150687789)

[XVII. Configuration des DNS : 40](#_Toc150687790)

[XVIII. Code Html 42](#_Toc150687791)

[XIX. Protocoles vus 44](#_Toc150687792)

[XX. Conclusion: 44](#_Toc150687793)

[XXI. Sources 44](#_Toc150687794)

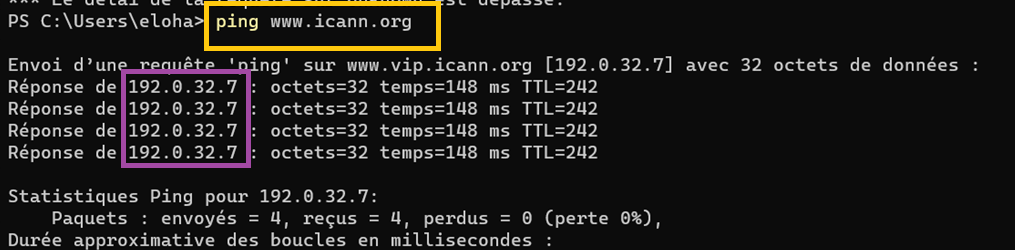
# Introduction

Cet atelier nous initie à l'utilisation du DNS, aux modes itératif et récursif, et nous aide à comprendre l'importance du DNS dans un réseau. Il nous permet également de découvrir des outils tels que "whois" ou "nslookup", qui s'avéreront particulièrement utiles pour un technicien réseau.

# Rôle du DNS

Un DNS, ou [Domain Name System](https://www.frameip.com/dns/) (Système de Noms de Domaine), est un service essentiel sur Internet. Il fonctionne comme un annuaire qui traduit les noms de domaine conviviaux que les gens utilisent en adresses IP, permettant ainsi aux ordinateurs de localiser les ressources en ligne. Voici une explication de son utilité :

* Traduction des noms de domaine en adresses IP : Les utilisateurs d'Internet accèdent aux sites web, aux services en ligne et à d'autres ressources en utilisant des noms de domaine faciles à retenir, tels que " www.icann.org ". Le DNS associe ces noms de domaine à des adresses IP numériques, telles que " IP 192.0.32.7", qui sont utilisées par les ordinateurs et les serveurs pour localiser ces ressources.
* Par exemple, si nous effectuons un ping sur **www.icann.org**, nous pouvons constater que notre requête de ping est couronnée de succès car le DNS associe le nom de domaine **www.icann.org** à l'adresse IP **192.0.32.7**. Le DNS joue un rôle essentiel dans la résolution des noms de domaine en adresses IP, permettant ainsi aux ordinateurs de localiser les ressources en ligne.

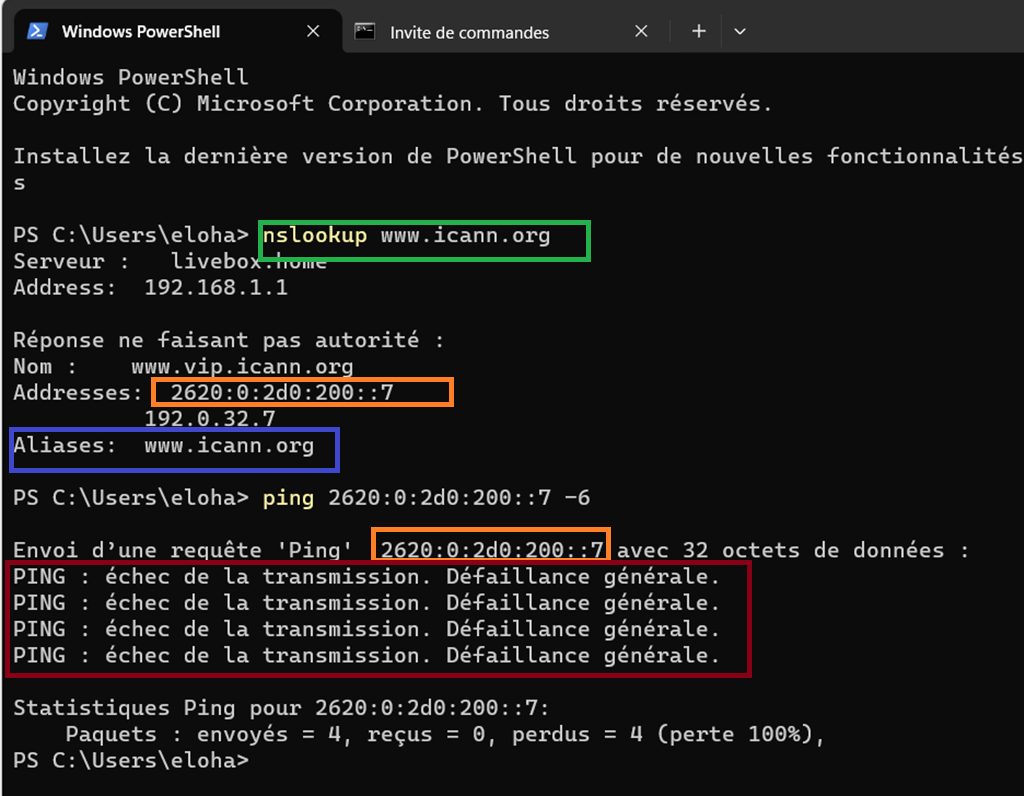


* Facilité d'utilisation : Le DNS simplifie la navigation sur Internet en permettant aux utilisateurs d'utiliser des noms de domaine plus conviviaux au lieu de se souvenir d'adresses IP complexes.
* Évolutivité : Le DNS est un système hiérarchique, ce qui signifie qu'il peut gérer un grand nombre de noms de domaine de manière efficace et évolutive.
* Redirection et équilibrage de charge : Les systèmes DNS permettent de rediriger les demandes vers les serveurs appropriés, ce qui peut être utilisé pour l'équilibrage de charge, la répartition de trafic, et la résilience.
* Localisation géographique : Le DNS peut être utilisé pour diriger les utilisateurs vers des serveurs ou des services situés géographiquement près de leur emplacement, améliorant ainsi la vitesse et la qualité de service.

En résumé, le DNS joue un rôle essentiel en permettant aux utilisateurs d'accéder aux ressources en ligne de manière conviviale, en garantissant la résolution des noms de domaine en adresses IP, et en facilitant la gestion du trafic Internet à grande échelle.

# Nslookup et résolution dns





nslookup est un outil de ligne de commande qui permet de **résoudre des noms de domaine** en adresses IP, d'effectuer des résolutions inverses, d'interroger des serveurs DNS spécifiques et de détecter des problèmes liés au DNS. Il est largement utilisé pour le dépannage et la gestion des systèmes réseau.

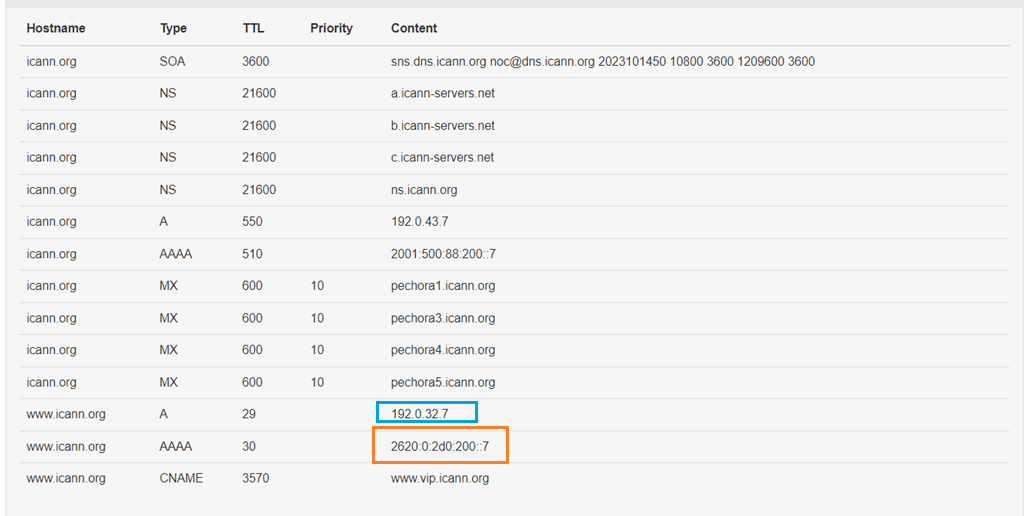
Dans notre exemple, en utilisant nslookup sur [www.icann.org](http://www.icann.org/), nous pouvons récupérer à la fois l'adresse IP version 4 (IPv4) et **l'adresse IP version 6 (IPv6)** associées au nom de domaine du site.

Maintenant, si nous souhaitons vérifier directement si le site bloque les requêtes "ping" via **IPv6**, nous pouvons prendre directement l'adresse IPv6 et effectuer notre test. Comme le montre le message d'erreur : "**Échec de la transmission. Défaillance générale**", cela suggère que les pings IPv6 ne sont pas autorisés.

**L'indication "Aliases :** [**www.icann.org**](http://www.icann.org/)**" signifie que cette adresse IP est liée au nom de domaine** [**www.icann.org**](http://www.icann.org/)**. Elle permet de faire le lien entre l'adresse IP et le nom de domaine**.

## Who is DNS :

Il existe également des outils tels que "who.is" qui permettent d'obtenir des informations sur le DNS. Comme nous pouvons le constater, ces outils fournissent des informations similaires à celles que l'on obtient avec nslookup.



## Test web

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Description générée automatiquement ici on test <https://192.0.32.7> et on tombe sur le site de maintenance de l’icann

Et quand je tape [www.icann.org](http://www.icann.org) je tombe sur ce site :

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

Description générée automatiquement

On peut observer que lorsque l'on tape directement l'adresse IP, on est redirigé vers la page de maintenance, tandis que lorsque l'on utilise le nom de domaine, on accède au bon site. Il semble que cela soit dû au fait que la page de maintenance et la page par défaut s'affichent en cas d'erreur de nom de domaine. Étant donné que la plupart des gens utilisent le nom de domaine et que le DNS n'a pas été configuré pour gérer l'accès via l'adresse IP, cela nous conduit à une page qui n'est pas destinée à servir de page d'accueil.

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

Description générée automatiquement

# Pare-feux et ACL :

Pour comprendre pourquoi les pings IPv6 ne sont pas autorisés, j'ai refait un exemple de configuration pare-feu reproduisant la situation que nous avons observée.

Voici les règles à configurer sur un routeur/pare-feu : Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

On peut aussi configurer un pare-feu pour bloquer un individu malveillant sur un ou certains ports. Pour cela, j'ai réalisé une vidéo démonstrative que vous trouverez ci-dessous : <https://youtu.be/eM6d6Mhavy4>

# Analyse passive

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

Description générée automatiquementEn saisissant l'adresse IP dans le navigateur, nous sommes automatiquement redirigés vers cette page. Par curiosité, j'ai donc effectué une analyse avec Nmap sur cette adresse :

Nmap, abréviation de "Network Mapper," est un outil informatique utilisé pour explorer et analyser les réseaux. Il permet de scanner un réseau informatique pour découvrir quels appareils sont connectés, quels ports réseau sont ouverts sur ces appareils, et quelles sont les services qui fonctionnent sur ces ports. En somme, Nmap aide à cartographier et à évaluer les dispositifs et les services d'un réseau, ce qui est précieux pour la gestion de la sécurité et la configuration des réseaux informatiques.

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

Description générée automatiquement

L'analyse Nmap révèle la présence de plusieurs ports ouverts. Le **port SSH**, par exemple, est utilisé pour une connexion sécurisée à une machine.

Il y a également un port HTTP, sur lequel je me suis connecté par défaut en entrant l'adresse IPv4. Le DNS a associé la connexion à ce port.

De plus, un port HTTPS est ouvert, renforçant la sécurité des communications.

**Enfin, j'ai identifié un port "rcpbind" dont je n'avais pas connaissance. J'ai donc effectué des recherches pour en savoir davantage sur ce protocole** :

## RCPBIND

RPCBIND, abréviation de Remote Procedure Call Binding, est un utilitaire qui joue un rôle essentiel dans les systèmes Unix et Linux. Il sert de pont entre les services RPC (Remote Procedure Call) et les ports auxquels ils écoutent. Lorsqu'un processus RPC démarre, il communique avec RPCBIND pour enregistrer le port auquel il écoute ainsi que les numéros de programme RPC qu'il prévoit de fournir. Ensuite, lorsqu'un client souhaite accéder à un service RPC spécifique, il contacte RPCBIND sur le serveur. RPCBIND redirige alors le client vers le port approprié, permettant ainsi la communication avec le service requis.

Ce processus de liaison des services RPC aux ports est essentiel, car il garantit que les clients peuvent accéder aux services de manière transparente. RPCBIND doit être disponible avant le démarrage des services RPC, car ces derniers dépendent de cette liaison pour fonctionner correctement. De plus, RPCBIND utilise des enveloppes TCP pour le contrôle d'accès, ce qui a un impact sur tous les services RPC. Il est possible de spécifier des règles de contrôle d'accès pour chaque démon RPC NFS, ce qui ajoute une couche de sécurité à ces services.

J'ai tenté de me connecter via HTTPS, et cela a résulté en l'apparition d'un nouveau site :

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

Description générée automatiquement

Un nouveau site est apparu, affichant le message suivant : "Cette page est utilisée pour tester le bon fonctionnement du serveur Apache HTTP après son installation. Si vous pouvez lire cette page, cela signifie que ce site fonctionne correctement. Ce serveur est propulsé par CentOS."

Il y a également un lien vers un service "Whois ICANN". Un site Whois est précisément lié au cours car il permet d'analyser un DNS de manière similaire à un NSLookup.Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

# Différent type de dns

Le DNS (Domain Name System) est un système essentiel qui traduit les noms de domaine en adresses IP, permettant ainsi aux ordinateurs de localiser les serveurs correspondants sur Internet. Les modes itératif et récursif sont deux méthodes utilisées dans le processus de résolution DNS pour obtenir cette correspondance entre les noms de domaine et les adresses IP. Voici les différences entre ces deux modes :

|  |  |
| --- | --- |
| **Le mode Itératif** | **Le mode Récursif** |
| dns mode iteratif root cache zone | dns mode recursif root cache zone |

**Mode Itératif :** Ce mode est le plus simple du point de vue du serveur. Les serveurs répondent directement à la requête sur la base seule de ses informations locales. La réponse peut contenir la réponse demandée, ou bien donne la référence d’un autre serveur qui sera « plus susceptible » de disposer de l’information demandée. Il est important que tous les serveurs de noms puissent implémenter ce mode itératif et désactive la fonction de récursivité.

Le mode Récursif : Le mode récursif est plus simple du point de vue du client. Dans ce mode, le premier serveur prend le rôle de résolveur.

L’utilisation du mode récursif est limitée aux cas qui résultent d’un accord négocié entre le client et le serveur. Cet accord est négocié par l’utilisation de deux bits particuliers des messages de requête et de réponse :

Le bit Ra (Récursion admissible), est marqué ou non par le serveur dans toutes les réponses. Ce bit est marqué si le serveur accepte à priori de fournir le service récursif au client, que ce dernier l’ait demandé ou non. Autrement dit, le bit RA signale la disponibilité du service plutôt que son utilisation.

# Test Nslookup

|  |  |
| --- | --- |
| Linux mint | Windows terminal |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement |  |

Au départ, j'avais l'impression que l'outil nslookup de Windows était moins complet que celui de Linux. Cependant, après avoir refait le test sur Kali Linux, j'ai conclu que les résultats pouvaient varier en fonction du moment où les tests ont été effectués. Il se peut que le site education.fr ait eu un serveur DNS public différent à un moment donné.

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

Description générée automatiquement

Il est également possible d'utiliser le site "ns.Tools" pour effectuer des tests :Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

## Nslookup résolution server messagerie :

La commande "set type=MX" dans nslookup permet d'obtenir des informations sur les serveurs de messagerie associés à un domaine, facilitant la configuration des services de messagerie.

Elle donne les indications suivantes :

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

Description générée automatiquement

Une image contenant texte, capture d’écran, Police

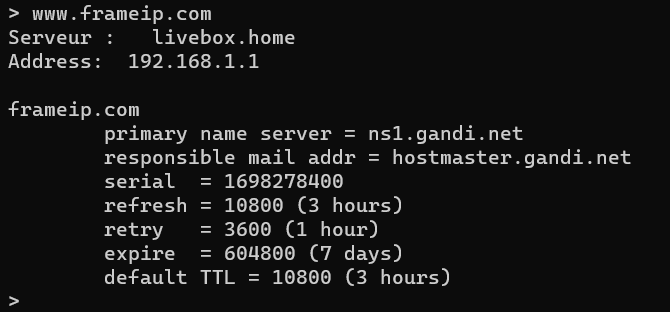
Description générée automatiquement

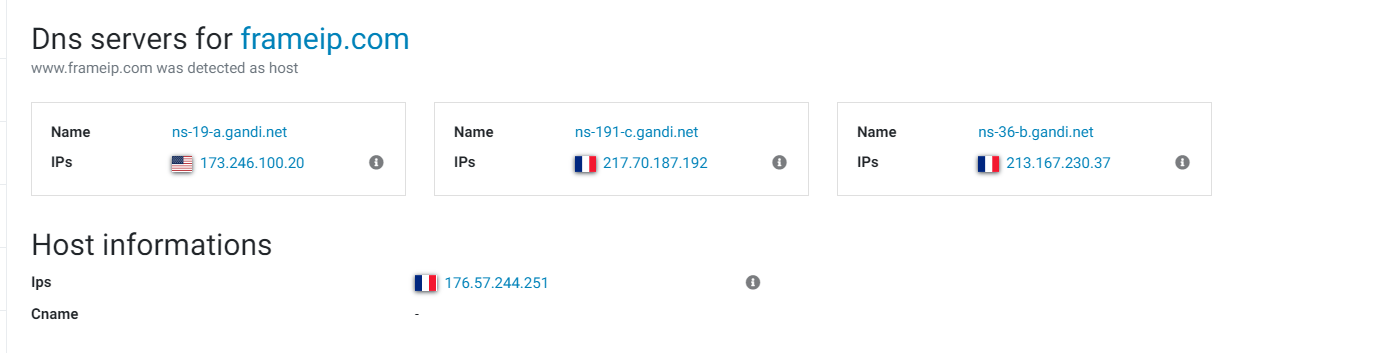
Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

Cisco utilise <https://www.akamai.com/fr/products/edge-dns>

Pour la gestion interne des courriels





Frame IP utilise également un site pour la gestion des courriels sur un serveur interne, qui est <https://www.gandi.net/fr>.

## Définition d’un rcpbind :

Rcpbind est un service Unix qui associe des numéros de port aux services RPC. Il permet aux clients RPC de trouver les ports associés aux services, facilitant ainsi la communication. Dans le contexte de Red Hat, il peut être utilisé pour gérer les numéros de port des services RPC sur des systèmes Linux basés sur Red Hat.

# Analyse Dns

## Port utilisé par le protocole DNS sur la couche de couche 4 utilisé par DNS ?

Le DNS (Domain Name System) utilise principalement le port 53 en tant que port de couche 4. Cependant, il peut également utiliser le port 5353 en UDP pour des fonctionnalités spécifiques, telles que la découverte de services multicouches (mDNS) avec Bonjour.

Donc, il y a plus d'un port utilisé, mais 53 est le plus couramment associé au DNS.

## RFC1035

La RFC 1035 a été rédigée par plusieurs personnes au sein de l'Internet Engineering Task Force (IETF), notamment Paul Mockapetris, qui est largement crédité comme l'auteur principal du protocole DNS. Elle a été publiée en novembre 1987.

La RFC 1035 a remplacé la RFC 882 et la RFC 883, qui étaient les spécifications précédentes du DNS. Ces deux RFC antérieures définissaient le Domain Name System, mais la RFC 1035 a été élaborée pour combler certaines lacunes et améliorer le protocole.

Le fondement du protocole DNS est de fournir une méthode hiérarchique et distribuée pour résoudre les noms de domaine en adresses IP. Il s'agit de l'un des éléments fondamentaux de l'infrastructure d'Internet, permettant aux utilisateurs d'accéder aux sites Web et aux services en utilisant des noms de domaine conviviaux plutôt que de devoir se rappeler des adresses IP numériques. Le DNS repose sur une structure d'arborescence de noms de domaine et sur des serveurs de noms qui se répartissent à différents niveaux de cette hiérarchie pour gérer la résolution des noms. Cela permet une navigation plus conviviale sur le Web et simplifie la gestion des adresses IP à l'échelle mondiale.

## Structure des requêtes et des réponses DNS :

Les requêtes et les réponses DNS suivent une structure commune, et elles comprennent des en-têtes ainsi que des sections qui transportent des informations spécifiques. Voici la structure typique des requêtes et des réponses DNS :

En-tête DNS :

ID (Identifiant) : Un numéro unique permettant d'associer les réponses aux requêtes correspondantes.

QR (Query/Response) : Un seul bit indiquant s'il s'agit d'une requête (0) ou d'une réponse (1).

Opcode : Un champ de 4 bits définissant le type d'opération (standard, inverse, etc.).

AA (Authoritative Answer) : Un seul bit indiquant si la réponse provient d'un serveur DNS autorisé.

TC (Truncated) : Un seul bit indiquant si la réponse est tronquée en raison de sa longueur.

RD (Recursion Desired) : Un seul bit indiquant si le client souhaite une résolution récursive.

RA (Recursion Available) : Un seul bit indiquant si le serveur DNS supporte la résolution récursive.

Z (Reserved) : Trois bits réservés à l'usage futur.

RCODE (Response Code) : Un champ de 4 bits indiquant le résultat de la requête (réussie, échec, etc.).

QDCount (Question Count) : Le nombre de questions dans la requête.

ANCount (Answer Count) : Le nombre de réponses dans la réponse.

NSCount (Name Server Count) : Le nombre de serveurs de noms dans la réponse.

ARCount (Additional Record Count) : Le nombre d'enregistrements supplémentaires dans la réponse.

# Réflexion sur le DNS :

Pour un utilisateur, le système DNS (Domain Name System) sert principalement à deux fonctionnalités essentielles :

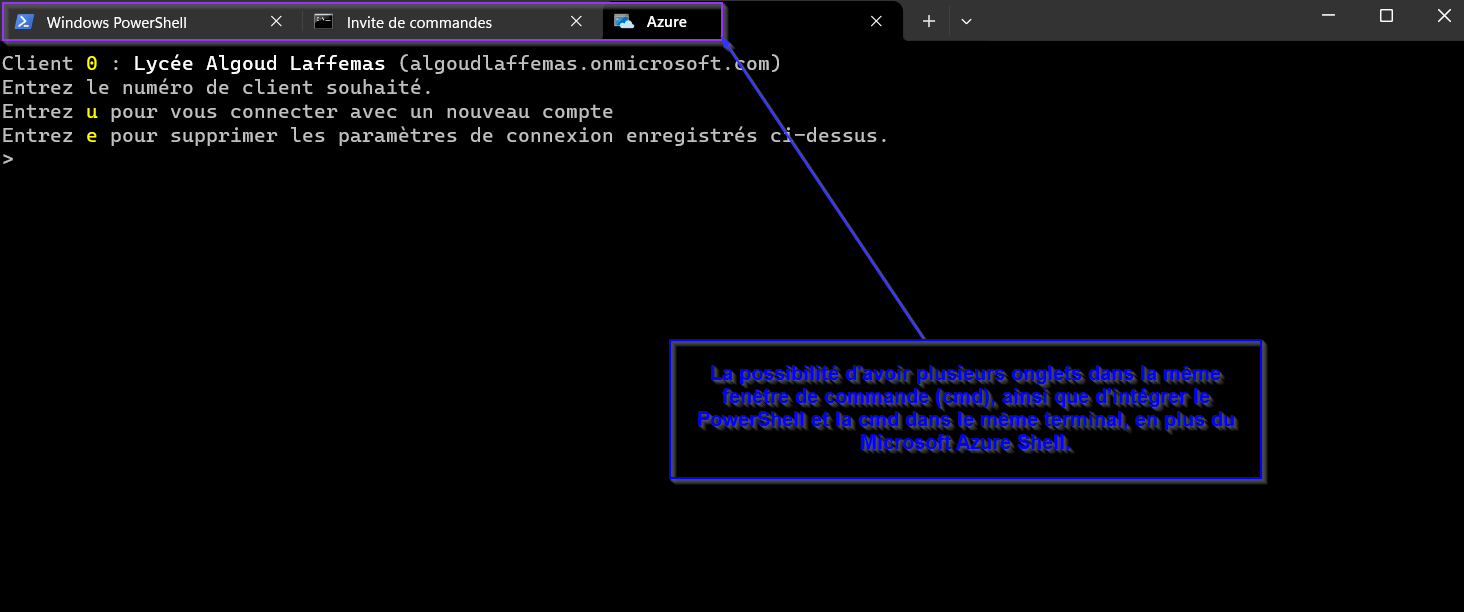
* Faciliter l'accès aux sites Web et aux services en ligne : Le DNS permet aux utilisateurs de saisir des noms de domaine conviviaux (comme " https://www.frameip.com/") dans leur navigateur au lieu de devoir mémoriser des adresses IP numériques compliquées. Il traduit ces noms de domaine en adresses IP, permettant ainsi la navigation sur le Web et l'accès à des services en ligne de manière conviviale.
* Assurer la communication par e-mail : Le DNS est également crucial pour le système de messagerie électronique. Il permet de trouver les serveurs de messagerie (enregistrements MX) associés à un nom de domaine. Cela garantit que les e-mails sont correctement acheminés vers les serveurs de messagerie appropriés.

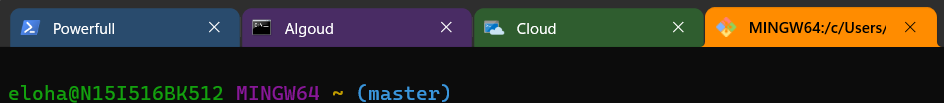
Pour un serveur, le DNS offre également des fonctionnalités cruciales. Voici comment le DNS est utilisé du côté serveur :

* Résolution des noms de domaine : Les serveurs utilisent le DNS pour résoudre les noms de domaine en adresses IP. Cela leur permet de communiquer avec d'autres serveurs et de fournir des services aux clients via Internet.
* Enregistrements DNS personnalisés : Les serveurs peuvent utiliser des enregistrements DNS pour définir des alias (CNAME), des serveurs de messagerie (MX), des serveurs de noms (NS), etc. Ces enregistrements personnalisés permettent de configurer les services offerts par le serveur.
* Résolution de noms internes : Les serveurs utilisent le DNS pour résoudre les noms de domaine internes à leur réseau, ce qui facilite la communication entre les différents services et dispositifs au sein de l'infrastructure d'une entreprise.
* Gestion de la sécurité : Le DNS peut être utilisé pour renforcer la sécurité en mettant en place DNSSEC pour vérifier l'authenticité des réponses DNS et en empêchant la falsification de données (DNS spoofing).
* Mise à jour dynamique : Les serveurs peuvent prendre en charge la mise à jour dynamique des enregistrements DNS, ce qui est utile dans des environnements où les adresses IP des dispositifs changent fréquemment, comme dans le cas de serveurs DHCP.
* Gestion des domaines : Les serveurs DNS autorisés sont responsables de la gestion des domaines et de leurs enregistrements. Ils peuvent ajouter, supprimer ou modifier des enregistrements pour gérer le domaine.
* Diagnostic des problèmes : Les serveurs DNS peuvent générer des journaux qui aident à diagnostiquer les problèmes liés à la résolution des noms. Cela facilite la maintenance et la résolution des problèmes.

En résumé, pour un serveur, le DNS est essentiel pour la résolution des noms de domaine, la configuration des services, la gestion de la sécurité, la répartition de la charge et la communication au sein de l'infrastructure. C'est un élément central de la connectivité et des services Internet.

## Windows terminal :

Le Windows terminal est nettement supérieur pour moi par rapport à une cmd classique, car il offre la possibilité d'avoir plusieurs onglets dans la même fenêtre de commande (cmd) tout en intégrant le PowerShell, la cmd, et même le [Microsoft Azure Shell](https://learn.microsoft.com/fr-fr/training/paths/azure-linux/).

Il intègre également Git, un outil permettant de configurer un dépôt GitHub. De plus, il offre la possibilité d'ouvrir la session précédente avec l'historique des commandes, ce qui s'avère utile pour un administrateur. Vous avez également la possibilité de configurer les onglets disponibles :

De plus, la possibilité de configurer des raccourcis, offrant ainsi un gain de temps considérable au quotidien.



# Différent outils linux pour l’analyse DNS

Nous allons étudier les différents outils Dig et nslookup. Dig est plus puissant et flexible, ce qui le rend idéal pour les utilisateurs avancés et les tâches complexes. En revanche, nslookup reste simple et convivial, adapté aux utilisateurs moins expérimentés ou pour des opérations basiques de résolution de noms.

Démonstration :

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

Description générée automatiquement

Plusieurs requêtes DNS ont été effectuées pour le domaine "test-yann.myshopify.com" en utilisant les commandes **dig** et **nslookup**. Les résultats indiquent que le serveur DNS situé à l'adresse IP 193.54.149.20 refuse la requête avec le statut "REFUSED", indiquant un refus de répondre à la demande.

Dans notre exemple e serveur interrogé est à l'adresse IP 193.54.149.20.

L'adresse recherchée est pour le domaine "test-yann.myshopify.com".

Et nous voyons que la commande dig semble fournir plus d'informations détaillées, notamment en affichant le temps de requête, les options EDNS, et d'autres détails.

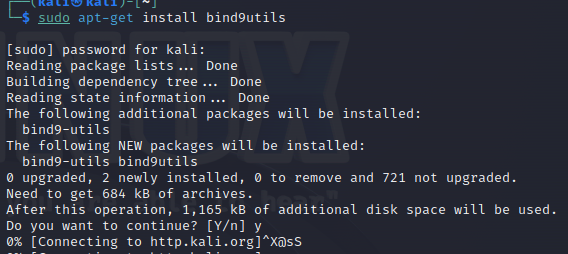
Une image contenant texte, capture d’écran, Police

Description générée automatiquement

J'ai remarqué après que vous aviez délibérément introduit une erreur dans la requête que vous nous aviez fournie, comportant une erreur. J'ai donc réeffectué la requête et obtenu de meilleurs résultats.

# Outils delv :

Installation de l’outils Delv



La commande `**delv**` est plus complexe à utiliser qu'une commande de type `**nslookup**` ou `**dig**`. Si elle est mal configurée, elle interrogera notre DNS local, et nous sommes obligés de forcer l'utilisation de Google à la fin. Les options sont indispensables pour obtenir un résultat. Voici un exemple de ce qui se passe si l'analyse est mal effectuée :Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Et voici comment il faut s'y prendre pour obtenir des résultats convenables :

delv +cd +dnssec trustee.ietf.org @8.8.8.8

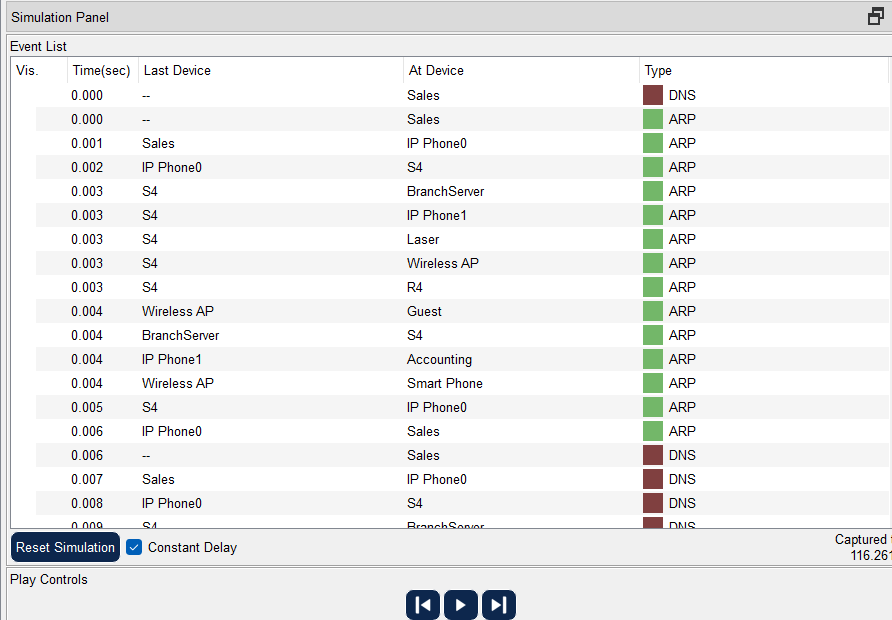
Une image contenant texte, capture d’écran, Police

Description générée automatiquement

On peut également utiliser un outil web pour compléter notre recherche :Une image contenant texte, capture d’écran, document, Police

Description générée automatiquement

# Exercice 6 : Analyse approfondie des échanges sous Packet Tracer



La première trame qui est envoyée est une trame de type DNS multicast.

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

Description générée automatiquement

Toutes les prochaines trames sont de type Arp qui servent à l’identification du réseau



Malheureusement, dans les premiers paquets, l'adresse MAC manque, ce qui nous empêche de contacter directement le DNS. C'est pourquoi des trames ARP sont envoyées pour identifier le réseau. 

On peut voir que les trames ARP ont traversé tous les éléments du réseau Branch pour associer chaque élément à une adresse MAC :

|  |  |
| --- | --- |
| Une image contenant texte, carte, capture d’écran, diagramme  Description générée automatiquement |  |

Si on fait défiler jusqu'à ce que le périphérique cible soit Branch Server :Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

Le serveur DNS trouve une adresse IP associée à ce domaine branchserver.pt.pta. Il renvoie une réponse.

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

Description générée automatiquement

L'adresse qui répond est 172.16.0.3, celle du serveur.Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement | Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement |

Une requête HTTP traverse plusieurs couches du modèle OSI pour atteindre sa destination. Voici une explication brève de l'utilisation des couches 7, 4, 3, 2, et 1 dans le modèle OSI pour une requête HTTP :

* Couche 7 (Application) : C'est la couche où se situe le protocole HTTP. La requête HTTP est créée au niveau de l'application, définissant la manière dont les données doivent être présentées et interprétées.
* Couche 4 (Transport) : Le protocole de transport utilisé pour les requêtes HTTP est généralement TCP (Transmission Control Protocol). La couche de transport assure la fiabilité de la transmission en établissant, maintenant, et terminant des connexions entre les points finaux.
* Couche 3 (Réseau) : Cette couche gère la transmission des paquets à travers le réseau. Les adresses IP sont utilisées pour router les paquets de la source à la destination. La requête HTTP est encapsulée dans des paquets IP pour être transportée sur le réseau.
* Couche 2 (Liaison de données) : À ce niveau, les données sont encapsulées dans des trames. Cette couche gère l'accès au support physique (comme l'Ethernet) et fournit des mécanismes de détection d'erreur.
* Couche 1 (Physique) : Cette couche concerne le support physique réel utilisé pour la transmission des données, tel que les câbles, les commutateurs, et autres composants matériels. Les bits sont convertis en signaux électriques, optiques, ou radiofréquences, selon le support physique.

En résumé, une requête HTTP traverse ces différentes couches du modèle OSI car chaque couche a une fonction spécifique dans le processus de transmission d'informations à travers un réseau, depuis la création de la requête au niveau de l'application jusqu'à la transmission physique des données.

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

Description générée automatiquement

Le client HTTP reçoit une réponse HTTP du serveur. Il affiche la page dans le navigateur web.

## 2e partie : Inspecter le trafic interréseau au bureau central

Contrairement à la requête précédente, il n'y a pas de recherche ARP car le réseau a déjà été identifié.

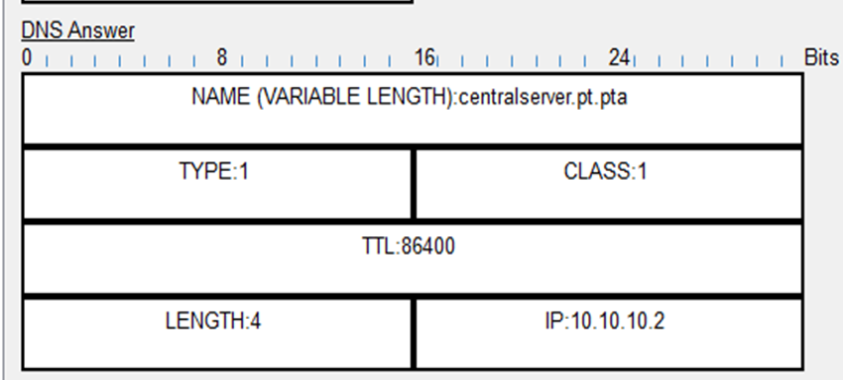
Une image contenant texte, nombre, Police, ligne

Description générée automatiquement

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

Description générée automatiquement

Ensuite, le serveur DNS reçoit une réponse où il résout le DNS.



# Étude sur le DHCP

DHCP signifie Dynamic Host Configuration Protocol. Il s’agit d’un protocole qui permet à un ordinateur qui se connecte sur un réseau local d’obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l’administration d’un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l’on installe une machine à travers un réseau (on peut effectivement installer complètement un ordinateur, et c’est beaucoup plus rapide que de le faire en à la main). Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionne pour [IPv4](http://www.frameip.com/entete-ip/) (adresses IP sur 4 octets). Une spécification pour [IPv6](http://www.frameip.com/entete-ipv6/) (adresses IP sur 16 octets) est en cours de développement par l’IETF.

Le protocole DHCP (Dynamic Host Configuration Protocol) opère à la couche applicative du modèle OSI. Il utilise la couche applicative car il s'agit d'un protocole réseau qui fournit des informations de configuration aux périphériques sur un réseau. La couche applicative est la couche la plus élevée du modèle OSI et englobe les protocoles qui permettent la communication entre les applications sur des appareils différents.

DHCP est conçu pour simplifier la configuration des adresses IP et d'autres paramètres réseau sur les périphériques clients. En utilisant la couche applicative, il peut transmettre des informations telles que l'adresse IP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc. Ces informations sont essentielles pour permettre aux appareils de communiquer efficacement sur un réseau.

## RFC

La RFC (Request for Comments) qui décrit le protocole DHCP est la RFC 2131. Elle a été publiée en mars 1997. Cette RFC spécifie la version 4 du protocole DHCP (DHCPv4), qui est la version la plus couramment utilisée pour la configuration dynamique des adresses IP sur les réseaux IPv4.

Le protocole DHCP s'appuie sur le protocole Bootstrap Protocol (BOOTP). BOOTP est un protocole plus ancien qui a été conçu pour fournir des configurations réseau initiales aux clients lorsqu'ils démarrent (bootstrap) sur un réseau. DHCP a évolué à partir de BOOTP pour offrir une configuration dynamique et étendue, permettant notamment la réattribution dynamique des adresses IP.

Bien que DHCP ait évolué à partir de BOOTP, BOOTP est encore utilisé dans certaines situations spécifiques. Par exemple, dans le processus d'amorçage réseau, où un périphérique démarre et cherche une adresse IP initiale pour se connecter au réseau. Dans ce contexte, BOOTP peut être utilisé pour fournir une adresse IP initiale aux clients lors du démarrage, mais DHCP est souvent préféré pour ses fonctionnalités plus avancées de configuration dynamique. Ainsi, bien que BOOTP soit moins couramment utilisé que DHCP, il reste pertinent dans des scénarios spécifiques tels que l'amorçage réseau.

## Différent type d’allocation :

Les trois types d'allocations possibles pour les adresses IP dans le contexte du protocole DHCP sont :

* Allocation Dynamique : Dans ce mode, une adresse IP est attribuée à un client par le serveur DHCP pour une durée déterminée, appelée bail. Le client peut renouveler le bail avant son expiration.
* Allocation Statique : Une adresse IP spécifique est attribuée à un client de manière permanente. Contrairement à l'allocation dynamique, l'adresse IP ne change pas à chaque nouvelle connexion du client. Cela nécessite une configuration manuelle sur le serveur DHCP.
* Allocation Automatique : Dans ce mode, le serveur DHCP attribue une adresse IP au client pour une durée déterminée, mais contrairement à l'allocation dynamique, le client ne renouvelle pas automatiquement son bail. Si le client se reconnecte, il peut recevoir une adresse IP différente.

Ces différentes méthodes d'allocation offrent une flexibilité dans la gestion des adresses IP au sein d'un réseau en fonction des besoins spécifiques de l'environnement.

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

Description générée automatiquement

Les trames DHCP fonctionnent de la manière suivante :Une image contenant texte, capture d’écran, conception

Description générée automatiquement

**1er paquet :**

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

Description générée automatiquement**

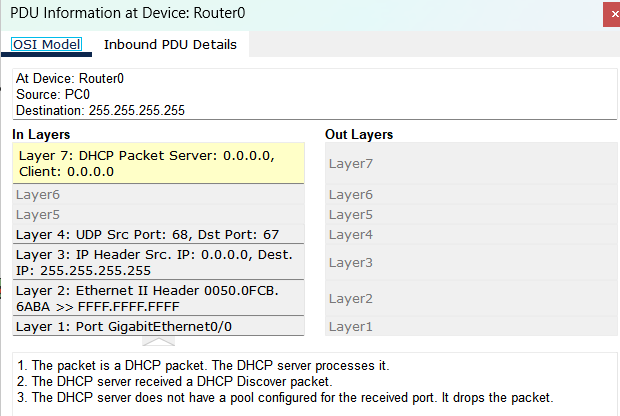
Le premier paquet est de type "discover" ; notre ordinateur découvre les réseaux via une diffusion en broadcast.Une image contenant diagramme, capture d’écran, ligne, carte

Description générée automatiquement

Ensuite, chaque périphérique du réseau reçoit et transmet la trame jusqu'à ce qu'elle trouve un serveur DHCP.

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

Description générée automatiquement



1. Le paquet est un paquet DHCP. Le serveur DHCP le traite.

2. Le serveur DHCP a reçu un paquet DHCP Discover.

3. Le serveur DHCP n'a pas de pool configuré pour le port reçu. Il rejette le paquet.

## Risque DHCP :

Le problème avec le mode DHCP réside dans le fait que le poste qui demande une adresse IP via DHCP le fait en diffusant une requête de broadcast. Cela signifie que n'importe quel élément du réseau peut identifier cette demande et potentiellement fournir une adresse IP.

Vous aurez plus de détails dans la partie suivante avec un exemple pratique.

## Risque configuration clasic :

Avec une configuration DHCP classique, plusieurs problèmes peuvent survenir, notamment

* Épuisement de la plage d'adresses IP : Si la plage d'adresses IP configurée dans le pool DHCP est trop petite pour le nombre de périphériques sur le réseau, il peut y avoir une pénurie d'adresses IP disponibles, entraînant des problèmes de connectivité pour les nouveaux périphériques.
* Conflits d'adresses IP : Il est possible que deux périphériques se voient attribuer la même adresse IP, provoquant des conflits et des perturbations dans le réseau.
* Durée de bail inappropriée : Si la durée de bail (temps pendant lequel une adresse IP est attribuée à un périphérique) est configurée de manière inappropriée, cela peut entraîner des renouvellements excessifs ou des interruptions de connexion.
* Problèmes de routage : Des erreurs dans la configuration du serveur DHCP peuvent entraîner la fourniture de paramètres de routage incorrects, perturbant la connectivité du réseau.
* Serveur DHCP indisponible : Si le serveur DHCP est hors service, les périphériques ne pourront pas obtenir de configuration réseau, ce qui peut entraîner des problèmes de connectivité.
* Attaques DHCP : Des attaques telles que les attaques de déni de service (DoS) visant le serveur DHCP peuvent perturber le processus de configuration et causer des problèmes sur le réseau.

Il est essentiel de surveiller et de configurer correctement le serveur DHCP pour éviter ces problèmes potentiels et assurer un fonctionnement fluide du réseau.

Un relais DHCP est un dispositif réseau qui facilite la communication entre les clients DHCP et les serveurs DHCP situés sur des sous-réseaux différents en transmettant les messages DHCP entre eux. Il permet aux clients de recevoir une configuration réseau même s'ils ne sont pas directement connectés au serveur DHCP.

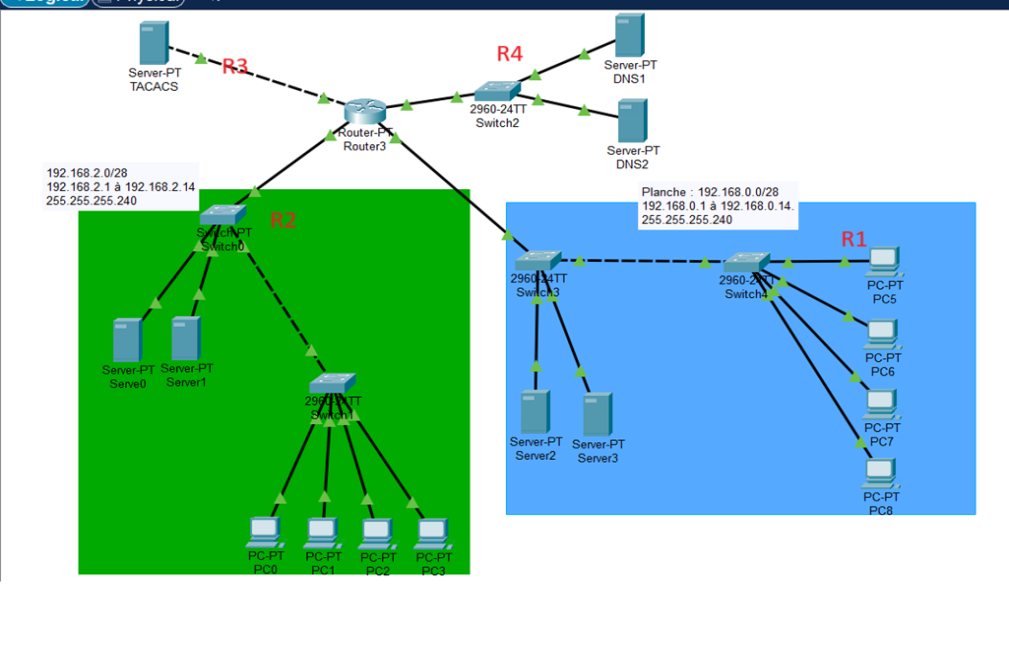
Sur Cisco, on peut l'activer avec la commande suivante :

interface Ethernet0/0

ip helper-address 192.168.1.1

# Création d’un réseaux DHCP :

Par défaut, sous Cisco, les adresses DHCP sont des adresses APIPA.



Choix des plages d'adresses pour les différents réseaux :

Pour les réseaux R1 et R2, je désirais 10 adresses utilisables car j'avais 7 adresses IP à attribuer dans les deux réseaux. Je souhaitais limiter le nombre d'adresses IP, car nous n'en avions pas besoin. Je suis parti du principe que nous visons un réseau sécurisé au maximum. Pour cela, j'ai attribué le masque 255.255.255.240 à chacun des deux réseaux.

Pour le réseau R3, j'ai autorisé 2 adresses utilisables, car je n'avais pas besoin de plus. Ici, nous évitons au maximum les attaques de type "man-in-the-middle" en utilisant le masque 255.255.255.252 (/30).

Pour le réseau R4, j'ai attribué le masque 255.255.255.248 (/29) pour les mêmes raisons que pour les autres réseaux. J'avais 6 adresses disponibles, car j'avais 3 adresses IP à attribuer, et le /30 ne m'aurait pas permis de donner une adresse à chaque poste.

|  |  |  |
| --- | --- | --- |
| Table d’interface R1 : | | |
| Interface Fa7/0 | 192.168.2.14 | 255.255.255.240 |
| Interface Fa0/0 | 192.168.0.14 | 255.255.255.240 |
| Interface Fa0/0 | 192.168.3.2 | 255.255.255.252 |
| Interface Fa0/1 | 192.168.4.6 | 255.255.255.248 |

|  |  |  |  |
| --- | --- | --- | --- |
| Configuration du server | | | |
| Nom server : | Adresse IP : | Sous réseaux : | Passerelle : |
| Server 0 | 192.168.2.12 | 255.255.255.240 | 192.168.2.14 |
| Server 1 | 192.168.2.13 | 255.255.255.240 | 192.168.2.14 |
| Server 2 | 192.168.0.12 | 255.255.255.240 | 192.168.0.14 |
| Server 3 | 192.168.0.13 | 255.255.255.240 | 192.168.0.14 |
| DNS 1 | 192.168.4.1 | 255.255.255.248 | 192.168.4.6 |
| DNS 2 | 192.168.4.2 | 255.255.255.248 | 192.168.4.6 |
| Tabac | 192.168.3.1 | 255.255.255.252 | 192.168.3.2 |
|  |  |  |  |

ip dhcp excluded-address 192.168.0.12 192.168.0.14

ip dhcp excluded-address 192.168.2.12 192.168.2.14

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

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

## Problématique du DHCP :

Le problème avec le mode DHCP réside dans le fait que le poste qui demande une adresse IP via DHCP le fait en diffusant une requête de broadcast. Cela signifie que n'importe quel élément du réseau peut identifier cette demande et potentiellement fournir une adresse IP. Comme illustré dans cet exemple :

Cette situation peut être particulièrement dangereuse, car elle expose à tous les éléments du réseau l'information selon laquelle nous recherchons un serveur DHCP, et le premier serveur qui répond remporte la connexion. Par conséquent, si un hacker est présent dans le réseau, il pourrait aisément se faire passer pour un serveur DHCP légitime.Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

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

Description générée automatiquement Une image contenant capture d’écran, texte, Police, conception

Description générée automatiquement

# Mise en situation man in the middle:

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

Description générée automatiquementDans ce scénario, imaginons qu'un hacker se soit dissimulé dans le réseau et se fasse passer pour le serveur DHCP officiel. Il aura connecté un sniffer pour récupérer des informations confidentielles.

Voici la configuration du routeur qui fait office de serveur DHCP. Je ne me suis pas embêté, elle a été faite facilement, car de toute façon, elle ne sert pas à faire fonctionner le réseau.Une image contenant texte, capture d’écran, nombre, document

Description générée automatiquement

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

Description générée automatiquement

On peut ensuite constater que notre routeur du hacker est bien celui qui a attribué en premier lieu l'adresse au PC. Il est donc associé en tant que passerelle par défaut pour le PC, ce qui signifie que toutes les requêtes du PC passeront par lui. Il pourra ainsi récupérer toutes les informations, ce qui est extrêmement dangereux. Cette simulation nous montre clairement qu'il est crucial de faire preuve de prudence sur un réseau public, car nous n'avons aucun moyen immédiat de nous rendre compte que nous sommes victimes. Il pourrait ainsi récupérer l'ensemble de nos informations.

# Configuration des DNS :

J'ai configuré les DNS pour qu'ils pointent vers le serveur de tabacs.com lorsque l'on tape le nom de domaine. J'ai associé l'adresse IP.Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Ensuite, j'ai dû configurer mes pools DHCP afin qu'ils associent automatiquement le serveur DNS, permettant ainsi une résolution DNS.

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

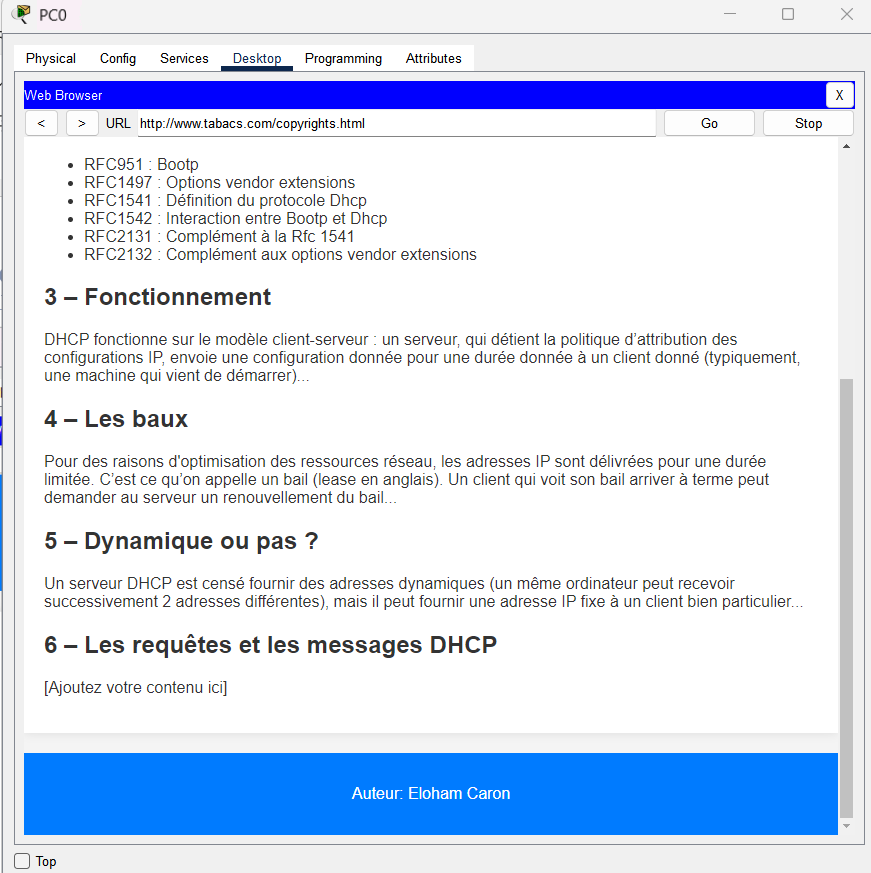
Description générée automatiquement

J'ai débranché le routeur hackeur pour éviter tout problème. La configuration est enregistrée. Si vous souhaitez effectuer des tests, il est toujours en place et fonctionnel. Je l'ai simplement débranché pour éviter tout problème, car il n'avait pas été configuré pour activer le réseau, mais plutôt pour montrer les dangers.

Une image contenant texte, capture d’écran, conception, illustration

Description générée automatiquement

Ensuite, à titre d'exemple, j'ai créé rapidement mon code HTML que j'ai directement implémenté sur le serveur www.tabac.com, accompagné de CSS. Pour l'exemple, j'ai mis le cours de FrameIP sur le DHCP et j'ai signé avec mon nom et prénom. Voici ce que cela donne lorsque je me connecte depuis le PC 0 :



# Code Html

HTML (HyperText Markup Language):

HTML est un langage de balisage utilisé pour structurer le contenu d'une page web. Il a été inventé par Tim Berners-Lee en 1991. HTML utilise des balises pour définir des éléments tels que des titres, des paragraphes, des liens, des images, etc. Ces balises permettent aux navigateurs web de comprendre la structure d'une page et d'afficher le contenu de manière appropriée. HTML est la base de la plupart des sites web et constitue l'ossature sur laquelle d'autres technologies, telles que CSS (Cascading Style Sheets) et JavaScript, s'appuient pour améliorer l'aspect et le comportement des pages.

CSS (Cascading Style Sheets):

CSS est un langage de feuilles de style utilisé pour décrire la présentation visuelle d'un document HTML. Il a été proposé par Håkon Wium Lie et Bert Bos en 1996. Alors qu'HTML se concentre sur la structure et le contenu, CSS permet de styliser et de mettre en forme ce contenu. En utilisant des règles de style, on peut définir des aspects tels que la couleur, la police, la disposition et d'autres propriétés visuelles d'une page web. CSS permet une séparation claire entre le contenu d'une page (HTML) et sa présentation, favorisant ainsi la maintenabilité et la flexibilité dans la conception web.

Complémentarité :

HTML et CSS sont complémentaires car ils travaillent ensemble pour créer une expérience utilisateur cohérente et esthétique. HTML structure le contenu, tandis que CSS stylise ce contenu. Cette séparation des responsabilités permet aux concepteurs et aux développeurs de se concentrer sur leurs domaines respectifs, simplifiant ainsi le processus de développement et de maintenance des sites web. Par exemple, HTML détermine qu'un texte est un titre, tandis que CSS spécifie comment ce titre doit être présenté à l'utilisateur, que ce soit en termes de taille, de couleur ou d'autres propriétés visuelles.

En résumé, HTML et CSS sont deux langages fondamentaux pour le développement web, travaillant de concert pour créer des pages web structurées et visuellement attrayantes. HTML définit la structure du contenu, tandis que CSS contrôle son apparence.

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

Description générée automatiquement

# Protocoles vus

|  |  |  |
| --- | --- | --- |
| Protocoles : | | |
| Protocole : | Ports | Description |
| TCP | 0-65535 | Assure une transmission fiable des données en établissant une connexion et en gérant la séquence d'échange. |
| SSH | 22 | Permet une connexion sécurisée à distance en chiffrant les communications entre les deux points. |
| RCPBIND | 111 | Associe les numéros de port RPC (Remote Procedure Call) aux services correspondants sur un système. |
| HTTP | 80 | Protocole de transfert hypertexte utilisé pour le transfert de données sur le World Wide Web. |
| HTTPS | 443 | Version sécurisée de HTTP, crypte les données pour assurer une communication web sécurisée. |
| UDP | 0-65535 | Protocole de datagramme utilisateur, offre une communication plus rapide mais non fiable sans établir de connexion. |
| DNS | 53 | Traduit les noms de domaine en adresses IP, facilitant la navigation sur Internet. |
| DHCP |  | Permet l'attribution dynamique d'adresses IP aux dispositifs sur un réseau, simplifiant la configuration réseau.  Haut du formulaire |
| ARP |  | Protocole qui mappe une adresse IP à une adresse physique (MAC) dans un réseau local, facilitant la communication au niveau de la couche de liaison de données. |
| IPv4 |  | Protocole de réseau qui attribue des adresses uniques à chaque appareil connecté à Internet pour faciliter l'acheminement des données. |
| IPv6 |  | Version améliorée d'IPv4, utilisée pour résoudre la pénurie d'adresses en attribuant un identifiant unique à un nombre considérablement plus grand d'appareils connectés à Internet |

# Conclusion:

Dans cet atelier, nous avons vu plusieurs protocoles tels que le DNS, qui est indispensable pour faciliter la vie des utilisateurs. Il nous serait impossible de naviguer sur Internet sans celui-ci. Cet atelier met également en évidence l'importance de faire attention avec le DHCP, en comprenant à la fois son utilité et les risques et dangers qu'il présente sur les réseaux publics. Il est crucial de rester vigilant avec ces protocoles qui simplifient notre vie, mais qui peuvent tout autant servir de porte d'entrée pour les pirates.

Nous pouvons également conclure que Packet Tracer est un outil de simulation limité, car nous ne pouvons pas tout configurer comme dans un vrai réseau, tel que les baux DHCP, par exemple.

# Sources

<https://www.frameip.com/dns/>

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/s2-nfs-methodology-portmap>

<https://unix.stackexchange.com/questions/234154/exactly-what-does-rpcbind-do>

<https://learn.microsoft.com/fr-fr/training/paths/azure-linux/s>

<https://www.frameip.com/rfc-2131-fr-protocole-de-configuration-dynamique-de-machine-dhcp/>

https://www.frameip.com/dhcp/