protocoles dhcp et dns

Sommaire :

[Intro : 2](#_Toc182508116)

[1 : Observation de la résolution DNS : 2](#_Toc182508117)

[1.5 : Conversion DNS d’une URL en adresse IP : 2](#_Toc182508118)

[1.6 : Recherche DNS avec nslookup sur un site web : 2](#_Toc182508119)

[1.6.1 : Outils en ligne : 3](#_Toc182508120)

[1.7 : La recherche DNS avec la commande nslookup : 4](#_Toc182508121)

[1.7.1 : Questions : 4](#_Toc182508122)

[2 : Question de réflexion et de raisonnement : 5](#_Toc182508123)

[2.1.1 : Commande nslookup et dig : 5](#_Toc182508124)

[2.2 : DNSSEC : 6](#_Toc182508125)

[2.2.3 : Exercice avec delv : 6](#_Toc182508126)

[3 : Analyse approfondie des échanges sous Packet Tracer : 7](#_Toc182508127)

[3.4 : Inspecter le trafic interréseau dans la filiale : 7](#_Toc182508128)

[3.4.2 : Mode realtime/ mode simulation : 7](#_Toc182508129)

[3.5 : Inspecter le trafic inter réseau au bureau central 10](#_Toc182508130)

[3.5.1 : Configurez la capture du trafic vers le serveur Web central. 10](#_Toc182508131)

[3.5.3 : Configurez la capture du trafic vers un serveur Web Internet. 12](#_Toc182508132)

[4 : DHCP : 13](#_Toc182508133)

[4.1 : Questions : 13](#_Toc182508134)

[4.2 : DHCP relais : 15](#_Toc182508135)

[4.3 : Topologie : 15](#_Toc182508136)

[4.3.1 : Adresses IP et Masque de sous réseau : 15](#_Toc182508137)

[4.3.2 : Configurations : 16](#_Toc182508138)

[4.3.3 : Vérifications : 17](#_Toc182508139)

[4.3.4 : Configuration routeur : 18](#_Toc182508140)

[Conclusion : 20](#_Toc182508141)

# Intro :

Ce TP vise à approfondir la compréhension et la maîtrise des protocoles réseau fondamentaux, DNS et DHCP. Le protocole DNS est essentiel pour la conversion des noms de domaine en adresses IP, permettant aux utilisateurs d’accéder facilement aux ressources en ligne sans mémoriser de longues chaînes numériques. De son côté, le protocole DHCP facilite la gestion des adresses IP dans un réseau en les attribuant dynamiquement aux périphériques, ce qui simplifie le processus de configuration réseau et réduit les erreurs humaines.

# 1 : Observation de la résolution DNS :

## 1.5 : Conversion DNS d’une URL en adresse IP :

-L’adresse IPv4 de [www.icann.org](http://www.icann.org) est 104.18.3.93 et l’IPv6 est 2606:4700::6812:35d.

L’adresse IPv4 d’icann.org est 192.0.43.7 et l’IPv6 est 2001:500:88:200::7.

-On voit que ce ne sont pas les mêmes adresses car ce ne sont pas les mêmes noms domaine grâce aux « www ».

## 1.6 : Recherche DNS avec nslookup sur un site web :

|  |  |
| --- | --- |
|  | On obtient :  Le serveur interrogé et son adresse IP  Le serveur a dû interroger un autre serveur pour avoir :  Son nom et son adresse IP |
|  | On obtient :  Le serveur interrogé et son adresse IP  Son nom et son adresse IP |
|  | On obtient :  Le serveur interrogé et son adresse IP  Le serveur a dû interroger un autre serveur pour avoir :  Son réseau de distribution de contenu, son nom et ses adresses IPv4 et IPv6. |

Ce ne sont pas les mêmes adresses IPv4 et IPv6 car la commande ping se base sur la route réseau réelle, le serveur peut avoir un intermédiaire alors que la commande nslookup se base sur l'adresse directement liée au domaine (officielle).

Nslookup :

|  |
| --- |
|  |

- Il y a 3 serveurs DNS publics dont le propriétaire est ate.info, une société d’hébergement de site privée.

Set type=mx

|  |
| --- |
| Une image contenant texte, capture d’écran, Police, noir  Description générée automatiquement |

### 1.6.1 : Outils en ligne :

|  |  |
| --- | --- |
|  | On a déjà vu les noms des serveurs DNS, mais pas leurs adresses IP  On voit leurs serveurs DNS, leur localisation géographique et leurs adresses IP. |

## 1.7 : La recherche DNS avec la commande nslookup :

Une image contenant texte, capture d’écran, Police

Description générée automatiquementCisco.fr :

|  |  |
| --- | --- |
|  | Cisco utilise un serveur interne car les serveurs de messagerie ont tous des noms de domaine se terminant par cisco.com. |

Frameip.com :

|  |  |
| --- | --- |
|  | Frameip utilise aussi un serveur interne car les serveurs de messagerie ont tous le nom de domaine se terminant par frameip.com. |

### 1.7.1 : Questions :

a) Il y a qu’un seul serveur DNS actif, qui a comme adresse IP 192.168.1.1. Les serveurs de Google ont 8.8.8.8 comme adresse IP et les serveurs dit libre 1.1.1.1 et 1.0.0.1.

b) Le DNS utilise seulement le port 53 mais avec deux protocoles différents, UDP 53 pour les requêtes standard et TCP 53 pour les requêtes de plus de 512 octets.

c) La RFC 1035 décrit le protocole DNS.

RFC (Request For Comments) est un document officiel qui décrit les normes, protocoles procédures et concepts utilisés sur internet.

d) La structure des requêtes et réponses DNS est composée de, Header qui contient des champs de contrôle pour identifier la requête/réponse, des indicateurs de statut et de réponse et des compteurs de sections, indiquant le nombre de questions, de réponses, d’autorités, et de ressources supplémentaires. Question qui contient le nom de domaine demandé, le type de requête et la classe, Answer qui contient les enregistrements correspondants à la question posée, Authority qui communique des informations sur les serveurs DNS faisant autorité pour le nom de domaine en question. Et Additional qui donne des informations supplémentaires, comme des enregistrements A associés aux serveurs NS mentionnés dans la section Authority, pour une résolution plus rapide.

# 2 : Question de réflexion et de raisonnement :

a) Les principales fonctionnalités du système DNS sont la résolution de noms, le routage et la redirection, ainsi que la différenciation des adresses.

b) Le message « Réponse ne faisant pas autorité » apparaît parce que les réponses obtenues viennent d'un serveur DNS récursif qui n'est pas le serveur faisant autorité pour le domaine en question. Ces serveurs fournissent des réponses à partir de leur cache, mais ils ne détiennent pas la gestion directe du domaine. Pour obtenir une réponse faisant autorité, on doit interroger directement le serveur DNS faisant autorité du domaine en configurant nslookup pour cibler spécifiquement ce serveur.

c) Windows Terminal apporte un plus par rapport à l'invite de commande grâce à sa personnalisation, sa prise en charge de plusieurs shells (PowerShell, WSL, Azure Cloud Shell) et la possibilité de l'ouvrir avec plusieurs onglets.

### 2.1.1 : Commande nslookup et dig :

|  |  |
| --- | --- |
| nslookup | dig |
|  |  |

-Le serveur interrogé est AL-DC-01.sio.local pour l’ordinateur fixe (nslookup) et 127.0.0.53 pour la machine virtuelle (dig).

-On cherche l’adresse 193.54.149.20.

-La commande dig fournit plus d’informations notamment en donnant le temps de la requête et les adresses IP multiples.

## 2.2 : DNSSEC :

### 2.2.3 : Exercice avec delv :

#### 2.2.3.1 : Enregistrement existant :

|  |  |
| --- | --- |
|  | L'erreur "broken trust chain" provient du résolveur DNS local (127.0.0.53), géré par ‘systemd-resolved', qui gère mal DNSSEC. |
| Une image contenant texte, capture d’écran, carte de visite, Police  Description générée automatiquement | Pour régler le problème, il faut utiliser un résolveur DNS supportant DNSSEC, comme Google (@8.8.8.8). |

#### 2.2.3.2 : Enregistrement inexistant :

|  |
| --- |
|  |

##### Sous wsl :

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

Nous avons les mêmes erreurs. Il faut spécifier le DNS par lequel nous passons, car cela est bloqué au niveau du DNS.

#### 2.2.3.3 : outil web :

|  |  |
| --- | --- |
|  | La racine «. »et le domaine «.fr » ont des enregistrements DNSKEY et DS fonctionnels.  « education.fr » ne possède ni d’enregistrements DS ni d’enregistrements DNSKEY pour son propre domaine. Il n’y a pas non plus de signature de la DNSSEC. Ce qui ne protège pas ce site des manipulations DNS. Mais les serveurs autoritaires répondent correctement. |

DNSKEY contient la clé pour signer et vérifier les enregistrements DNS d’un domaine

DS (Delegation Signer) relie une zone parent avec un zone enfant pour valider l’authenticité des enregistrements DNS.

Le domaine de la zone parent délègue la gestion des sous-domaines à la zone enfant.

DNSSEC (Domain Name System Security Extensions) est une extension DNS qui ajoute des signatures numériques afin de garantir l’authenticité et l’intégrité des enregistrements DNS.

# 3 : Analyse approfondie des échanges sous Packet Tracer :

## 3.4 : Inspecter le trafic interréseau dans la filiale :

### 3.4.2 : Mode realtime/ mode simulation :

c)

|  |  |
| --- | --- |
|  | Le premier type d’évènement qui apparait est le DNS car c’est lui qui transforme les noms de domaine en adresse IP. |

d)

|  |  |
| --- | --- |
|  | Il manque les informations de la couche 2, les adresses MAC de source et de destination. Elles permettent de diriger les paquets au bon destinataire. |

e) La requête ARP traverse 14 périphériques différents.

f)

|  |  |
| --- | --- |
|  | Le DNS est protocole appliqué dans la couche 7. C’est donc une requête de résolution de nom de domaine. |

g)

|  |
| --- |
|  |

h)

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

i)

|  |  |
| --- | --- |
|  | Il y a seulement 2 couches actives car un périphérique intermédiaire ne traite pas le contenu de la requête http. Mais elle regarde que les adresses MAC pour diriger les paquets correctement. |

j)

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

## 3.5 : Inspecter le trafic inter réseau au bureau central

Dans la Partie 2 de cet exercice, vous allez utiliser le mode Simulation de Packet Tracer (PT) pour afficher et examiner le mode de traitement du trafic quittant le réseau local.

### 3.5.1 : Configurez la capture du trafic vers le serveur Web central.

d)

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement | Le protocole ARP est activé seulement si un échange direct a lieu, mais avant le poste doit chercher l’adresse IP de BranchServeur. |

e)

|  |  |
| --- | --- |
|  | Le client DNS a reçu l’adresse IP résolue, le serveur sait sur quelle adresse IP envoyer les requêtes pour ce domaine. |

f)

|  |
| --- |
| Une image contenant texte, capture d’écran, reçu, nombre  Description générée automatiquement |

g)

|  |  |
| --- | --- |
|  | C’est 0001.969A.1003 car il a la même adresse IPv4 que celle de source. |

h)

|  |  |
| --- | --- |
|  | L’adresse MAC source est 00D0.D3D7.5B29 et celle du prochain saut est 000A.F3E4.EB0. |

i)

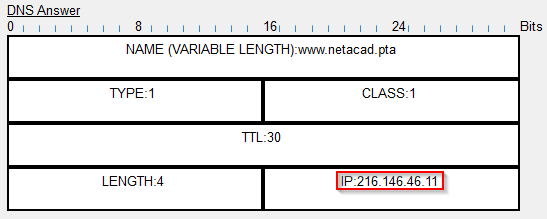
|  |  |
| --- | --- |
|  | Intranet utilise Frame Relay pour la connexion d’un réseau étendu (WAN), sinon Ethernet serait utilisé. |

Frame Relay= protocole de transmission pour connecter des périphériques sur de longues distances.

### 3.5.3 : Configurez la capture du trafic vers un serveur Web Internet.

c) Il y a 5 évènements DNS à la suite puis 15 autres après des ARP enfin 22 à la fin.

d) Les périphériques se trouvent tous dans le réseau Branch, plus précisément c’est le chemin le plus court pour accéder au BranchServer.

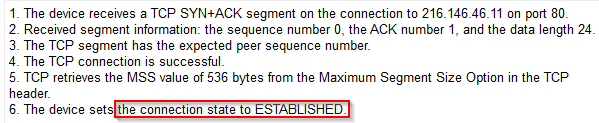
e)

|  |
| --- |
|  |

f) Il y a 38 routeurs qui ont été traversés.

g)

|  |  |
| --- | --- |
|  | Cet évènement maintient la connexion pour que la transmission des données soit fiable entre le client et le serveur HTTP. Les couches 1, 2 et 3 servent pour le transfert d’un paquet entre routeur. |

h)

|  |
| --- |
|  |

# 4 : DHCP :

## 4.1 : Questions :

a) Le DHCP (Dynamic Host Configuration Protocol) simplifie la gestion des adresses IP et réduit leurs conflits en les automatisant. C’est un protocole réseau qui évolue dans la couche 7 OSI. Il délivre une adresse IP, un masque de sous-réseau, une passerelle par défaut, une adresse de serveur DNS et la durée du bail.

b) La RFC 2131 décrit le protocole DHCP.

RFC (Request For Comments) est un document officiel qui décrit les normes, protocoles, procédures et concepts utilisés sur internet.

c) Il s’appuie sur le protocole BOOTP (Bootstrap Protocol), encore utilisé principalement dans l’administration réseau ou des anciennes infrastructures. Il est maintenu pour sa compatibilité ascendante.

d) L’allocation manuelle (fixe), automatique et dynamique (temporaire).

e)

|  |  |
| --- | --- |
|  | Le protocole utilisé est UDP Src, un protocole spécialisé dans la transmission de données rapide et sans connexion. Elle ne vérifie pas si les données sont arrivées entière et dans le bon ordre.  Les ports 546 et 547 sont aussi utilisé par DHCP. |

f)

|  |  |
| --- | --- |
|  | DHCP Discover, pour localiser les serveurs DHCP disponibles. |
|  | DHCP Offer, une proposition d’adresses IP et de configuration réseau. |
|  | DHCP Request, acceptation de l’adresse IP. |
|  | DHCP Acknowledgment, confirmation de l’adresse IP. |

g) Il y a plusieurs risques, une usurpation de serveur DHCP, une attaque de déni de service ou encore une interception du trafic.

## 4.2 : DHCP relais :

a) On peut rencontrer un conflit d’adresses IP (si deux appareils reçoivent la même adresse IP), une panne de serveur DHCP, une limitation de la plage d’adresses IP ou encore des erreurs de configuration.

b) Un relais DHCP est une fonction réseau qui permet aux clients d’avoir une adresse IP d’un serveur DHCP situé sur un autre sous-réseau.

c) La commande pour activer la fonction de relais DHCP sur un routeur est « ip helper-address <adresse\_IP\_du\_serveur\_DHCP> », elle doit être saisie en mode configuration d’interface. Elle a le même rôle qu’un relais DHCP.

## Ip 4.3 : Topologie :

### 4.3.1 : Adresses IP et Masque de sous réseau :

|  |  |  |  |
| --- | --- | --- | --- |
| Equipements | Adresse IP | Masque de sous réseau | Passerelle |
| Routeur (Fa0/0) | 192.168.0.14 | 255.255.255.240 | / |
| Serveur2 | 192.168.0.12 | 255.255.255.240 | 192.168.0.14 |
| Serveur3 | 192.168.0.13 | 255.255.255.240 | 192.168.0.14 |
| Routeur (Fa1/0) | 192.168.4.6 | 255.255.255.248 | / |
| DNS1 | 192.168.4.1 | 255.255.255.248 | 192.168.4.6 |
| DNS2 | 192.168.4.2 | 255.255.255.248 | 192.168.4.6 |
| Routeur (Fa7/0) | 192.168.2.14 | 255.255.255.240 | / |
| Serveur0 | 192.168.2.12 | 255.255.255.240 | 192.168.2.14 |
| Serveur1 | 192.168.2.13 | 255.255.255.240 | 192.168.2.14 |
| Routeur (Fa6/0) | 192.168.3.2 | 255.255.255.252 | / |
| TACACS | 192.168.3.1 | 255.255.255.252 | 192.168.3.2 |

TACACS (Terminal Access Controller Access Control System) est un protocole d’authentification pour contrôler l'accès aux équipements réseau.

Pour les réseaux Serveur 0,1,2 et 3 seulement 7 adresses IP sont nécessaire. Le masque 255.255.255.240 suffit à couvrir 10 adresses IP.

Pour le réseau Serveur TACACS, seulement 2 adresses IP sont nécessaires, donc un masque de 255.255.255.252 convient parfaitement.

Pour le réseau Serveur DNS1 et DNS2, il y a besoin de seulement 6 adresses, un masque de 255.255.255.252 est parfait.

Adresses IP exclues :

Les adresses 192.168.0.12, 192.168.0.14,192.168.2.12 et 192.168.2.14 sont exclu pour les réserver pour les serveurs 2 et 0 et pour les connexions Fa7/0 et Fa0/0.

### 4.3.2 : Configurations :

|  |
| --- |
|  |

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

Description générée automatiquementLes marques en gris sont les éléments qui changent pour la configuration des autres interfaces/Pools/exclusions.

|  |  |
| --- | --- |
|  | J’ai configuré un site simple avec seulement un fond et mon nom en html, sur le serveur web TACAS. |

### 4.3.3 : Vérifications :

Adresses exclues :

|  |
| --- |
|  |

Enveloppe IMCP (ping) réussie :

|  |
| --- |
|  |

DHCP :

|  |  |
| --- | --- |
|  | Le DHCP attribue l’adresse IP, le masque de sous-réseau et le serveur DNS automatiquement correctement, le routeur est donc bien configuré. |

Site internet :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, logiciel, ordinateur  Description générée automatiquement | J’ai aussi testé avec un appareil sur un autre réseau, on obtient ce site web. |

### 4.3.4 : Configuration routeur :

Pour sécuriser le routeur, on met un mot de passe pour l’accès a la ligne de commande et un SSH.

SSH (Secure Shell) permet de se connecter à un routeur en toute sécurité.

J’ai choisi le mot de passe « candice ».

Configuration :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, document  Description générée automatiquement | Ce script sécurise le routeur en configurant un accès administrateur, des mots de passe chiffrés pour l'accès local et distant, et en définissant des paramètres de sécurité pour limiter les tentatives d'accès. |

Il faut donner un nom au router avec hostname  pour avoir une connexion SSH fonctionnelle :

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

Ce qui donne se script que l’on peut mettre sur tous nos router : enable secret candice

Pour accéder au routeur :

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement | Le mot de passe a été tapé après Password mais pour des raisons de sécurité, Cisco n’affiche rien quand on le tape |

# Conclusion :

Ce TP m'a permis de comprendre et de maîtriser les protocoles DHCP et DNS, essentiels pour la gestion des réseaux. À travers les exercices, j'ai configuré et testé un serveur DHCP sur un routeur, attribuant dynamiquement des adresses IP à différents sous-réseaux. J’ai également observé comment le DNS résolvait les noms de domaine en adresse IP. Cette configuration a permis d'automatiser la distribution des paramètres réseau, simplifiant ainsi la gestion des adresses IP tout en évitant les conflits potentiels. Les tests effectués ont confirmé la bonne configuration et la distribution correcte des adresses IP aux différents postes clients. J'ai également pris en compte les aspects de sécurité en protégeant l'accès au routeur avec un mot de passe.