

# PROTOCOLES DHCP ET DNS

## Sommaire :

Intro :.....	2
1 : Observation de la résolution DNS : .....	2
1.5 : Conversion DNS d'une URL en adresse IP : .....	2
1.6 : Recherche DNS avec nslookup sur un site web : .....	2
1.6.1 : Outils en ligne :.....	3
1.7 : La recherche DNS avec la commande nslookup :.....	4
1.7.1 : Questions : .....	4
2 : Question de réflexion et de raisonnement : .....	5
2.1.1 : Commande nslookup et dig : .....	5
2.2 : DNSSEC : .....	6
2.2.3 : Exercice avec delv :.....	6
3 : Analyse approfondie des échanges sous Packet Tracer : .....	7
3.4 : Inspecter le trafic interréseau dans la filiale : .....	7
3.4.2 : Mode realtime/ mode simulation : .....	7
3.5 : Inspecter le trafic inter réseau au bureau central.....	10
3.5.1 : Configurez la capture du trafic vers le serveur Web central. ....	10
3.5.3 : Configurez la capture du trafic vers un serveur Web Internet.....	12
4 : DHCP : .....	13
4.1 : Questions :.....	13
4.2 : DHCP relais : .....	15
4.3 : Topologie : .....	15
4.3.1 : Adresses IP et Masque de sous réseau : .....	15
4.3.2 : Configurations : .....	16
4.3.3 : Vérifications : .....	17
4.3.4 : Configuration routeur : .....	18
Conclusion : .....	20

## 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 :

<pre>&gt; www.frameip.com Serveur : AL-DC-01.sio.local Address: 172.31.1.4  Réponse ne faisant pas autorité : Nom : www.frameip.com Address: 176.57.244.251</pre>	<p>On obtient :</p> <p>Le serveur interrogé et son adresse IP</p> <p>Le serveur a dû interroger un autre serveur pour avoir :</p> <p>Son nom et son adresse IP</p>
<pre>&gt; 87.98.130.52 Serveur : AL-DC-01.sio.local Address: 172.31.1.4  Nom : ip52.ip-87-98-130.eu Address: 87.98.130.52</pre>	<p>On obtient :</p> <p>Le serveur interrogé et son adresse IP</p> <p>Son nom et son adresse IP</p>
<pre>&gt; www.icann.org Serveur : AL-DC-01.sio.local Address: 172.31.1.4  Réponse ne faisant pas autorité : Nom : www.icann.org.cdn.cloudflare.net Addresses: 2606:4700::6812:25d 2606:4700::6812:35d 104.18.2.93 104.18.3.93 Aliases: www.icann.org</pre>	<p>On obtient :</p> <p>Le serveur interrogé et son adresse IP</p> <p>Le serveur a dû interroger un autre serveur pour avoir :</p> <p>Son réseau de distribution de contenu, son nom et ses adresses IPv4 et IPv6.</p>

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 :

```
> set type=NS
> 8.8.8.8
Serveur : AL-DC-01.sio.local
Address: 172.31.1.4

*** AL-DC-01.sio.local ne parvient pas à trouver 8.8.8.8 : Non-existent domain
> serveur 8.8.8.8
Serveur : [8.8.8.8]
Address: 8.8.8.8

*** 8.8.8.8 ne parvient pas à trouver serveur : Non-existent domain
> server 8.8.8.8
Serveur par défaut : dns.google
Address: 8.8.8.8

> education.fr
Serveur : dns.google
Address: 8.8.8.8

Réponse ne faisant pas autorité :
education.fr nameserver = ate-ns03.ate.info
education.fr nameserver = ate-ns02.ate.info
education.fr nameserver = ate-ns01.ate.info
```

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

Set type=mx

```
> set type=mx
> education.fr
Serveur : dns.google
Address: 8.8.8.8

Réponse ne faisant pas autorité :
education.fr MX preference = 0, mail exchanger = mx01.phm.education.gouv.fr
education.fr MX preference = 10, mail exchanger = mx02.phm.education.gouv.fr
```

### 1.6.1 : Outils en ligne :

DNS									
<p>Dns servers for <a href="#">education.fr</a></p> <table border="1"> <thead> <tr> <th>Name</th> <th>IPs</th> </tr> </thead> <tbody> <tr> <td>ate-ns01.ate.info</td> <td>198.29.138.5</td> </tr> <tr> <td>ate-ns02.ate.info</td> <td>17.229.32.3</td> </tr> <tr> <td>ate-ns03.ate.info</td> <td>198.29.138.5</td> </tr> </tbody> </table>	Name	IPs	ate-ns01.ate.info	198.29.138.5	ate-ns02.ate.info	17.229.32.3	ate-ns03.ate.info	198.29.138.5	<p>On a déjà vu les noms des serveurs DNS, mais pas leurs adresses IP</p> <p>On voit leurs serveurs DNS, leur localisation géographique et leurs adresses IP.</p>
Name	IPs								
ate-ns01.ate.info	198.29.138.5								
ate-ns02.ate.info	17.229.32.3								
ate-ns03.ate.info	198.29.138.5								

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

Cisco.fr :

<pre>&gt; cisco.com Serveur : ALG7 Address: 192.168.1.1  Réponse ne faisant pas autorité : cisco.com      MX preference = 30, mail exchanger = aer-mx-01.cisco.com cisco.com      MX preference = 10, mail exchanger = alln-mx-01.cisco.com cisco.com      MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com</pre>	<p>Cisco utilise un serveur interne car les serveurs de messagerie ont tous des noms de domaine se terminant par cisco.com.</p>
--	---

Frameip.com :

<pre>&gt; frameip.com Serveur : ALG7 Address: 192.168.1.1  Réponse ne faisant pas autorité : frameip.com    MX preference = 10, mail exchanger = smtp.frameip.com</pre>	<p>Frameip utilise aussi un serveur interne car les serveurs de messagerie ont tous le nom de domaine se terminant par frameip.com.</p>
---	---

### 1.7.1 : Questions :

- 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.
- 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.
- 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
<pre>PS C:\Users\uti029&gt; nslookup Serveur par défaut : AL-DC-01.sio.local Address: 172.31.1.4  &gt; serveur 193.54.149.20 Serveur : [193.54.149.20] Address: 193.54.149.20  *** 193.54.149.20 ne parvient pas à trouver serveur : Query refused &gt; test-yann.myshopify.com Serveur : AL-DC-01.sio.local Address: 172.31.1.4  Réponse ne faisant pas autorité : Nom : shops.myshopify.com Adresses: 2620:127:f00f:e::           23.227.38.74 Aliases: test-yann.myshopify.com</pre>	<pre>landisc@linux:~\$ dig 193.54.149.20 test-yann.myshopify.co;  ;&lt;&lt;&lt;&gt;&gt; DIG 9.20.0-Zubuntu3-Ubuntu &lt;&lt;&lt;&gt;&gt; 193.54.149.20 test-yann.myshopify.co ;; Global options: &lt;cmd ;; Got answer: ;; --HEADER-- opcode: QUERY, status: NXDOMAIN, id: 14237 ;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ;; EDNS: version: 0, flags: udp: 65494 ;; QUESTION SECTION: ;193.54.149.20.                IN      A  ;; AUTHORITY SECTION: ;899 IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2024110702 1800 900 604800 8 6400  ;; Query time: 16 msec ;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP) ;; WHEN: Fri Nov 08 07:38:43 UTC 2024 ;; MSG SIZE rcvd: 117  ;; Got answer: ;; --HEADER-- opcode: QUERY, status: NXERROR, id: 16217 ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  ;; OPT PSEUDOSECTION: ;; EDNS: version: 0, flags: udp: 65494 ;; QUESTION SECTION: ;test-yann.myshopify.co.      IN      A  ;; ANSWER SECTION: test-yann.myshopify.co. 600 IN      A      172.232.25.148 test-yann.myshopify.co. 600 IN      A      172.232.31.180 test-yann.myshopify.co. 600 IN      A      172.232.4.213  ;; Query time: 228 msec ;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP) ;; WHEN: Fri Nov 08 07:38:43 UTC 2024 ;; MSG SIZE rcvd: 99</pre>

- 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 :

<pre>Candice@Linux:~\$ delv trustee.ietf.org ;; no valid RRSIG resolving 'org/DS/IN': 127.0.0.53#53 ;; broken trust chain resolving 'trustee.ietf.org/A/IN': 127.0.0.53#53 ;; resolution failed: broken trust chain</pre>	<p>L'erreur "broken trust chain" provient du résolveur DNS local (127.0.0.53), géré par 'systemd-resolved', qui gère mal DNSSEC.</p>
<pre>Candice@Linux:~\$ delv trustee.ietf.org @8.8.8.8 ; fully validated trustee.ietf.org. 300 IN A 104.16.44.99 trustee.ietf.org. 300 IN A 104.16.45.99 trustee.ietf.org. 300 IN RRSIG A 13 3 300 20241109155600 20241107135600 34505 ietf.org. 6mgiaqPoJgyO6MLFT/kVdkNFnyO3wnlhJh5FR8JuPMP+izYLqWst/v7U NnoCTW+wdH+7sWc13SnN+Tps/WFCW==</pre>	<p>Pour régler le problème, il faut utiliser un résolveur DNS supportant DNSSEC, comme Google (@8.8.8.8).</p>

#### 2.2.3.2 : Enregistrement inexistant :

<pre>Candice@Linux:~\$ delv nonexistent.ietf.org @8.8.8.8 ;; resolution failed: ncache nxrrset ; negative response, fully validated ; nonexistent.ietf.org. 1800 IN \-A ;-\$NXRRSET ; ietf.org. SOA jill.ns.cloudflare.com. dns.cloudflare.com. 2356443086 10000 2400 604800 1800 ; ietf.org. RRSIG SOA ... ; nonexistent.ietf.org. RRSIG NSEC ... ; nonexistent.ietf.org. NSEC \000.nonexistent.ietf.org. RRSIG NSEC TYPE128</pre>
---

#### Sous wsl :

<pre>(Message from Kali developers)  This is a minimal installation of Kali Linux, you likely want to install supplementary tools. Learn how: =&gt; https://www.kali.org/docs/troubleshooting/common-minimum-setup/  (Run: "touch ~/.hushlogin" to hide this message) (candice@kali:~)\$ delv trustee.ietf.org ;; DNS format error from 10.255.255.254#53 resolving org/DS for &lt;unknown&gt;: question section mismatch: got org.sio.local/IN/DS ;; DNS format error from 10.255.255.254#53 resolving org/DS for &lt;unknown&gt;: question section mismatch: got org.sio.local/IN/DS ;; DNS format error from 10.255.255.254#53 resolving org/DS for &lt;unknown&gt;: question section mismatch: got org.sio.local/IN/DS ^C;; broken trust chain resolving 'trustee.ietf.org/A/IN': 10.255.255.254#53 ;; resolution failed: broken trust chain  (candice@kali:~)\$ delv trustee.ietf.org @8.8.8.8 ;; resolution failed: ncache nxrrset ; negative response, fully validated ; trustee.ietf.org. 1800 IN \-A ;-\$NXRRSET ; ietf.org. SOA jill.ns.cloudflare.com. dns.cloudflare.com. 2356443086 10000 2400 604800 1800 ; ietf.org. RRSIG SOA ... ; trustee.ietf.org. RRSIG NSEC ... ; trustee.ietf.org. NSEC \000.trustee.ietf.org. RRSIG NSEC TYPE128  (candice@kali:~)\$</pre>
---

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 :

.	<ul style="list-style-type: none"><li>✔ Found 2 DNSKEY records for .</li><li>✔ DS=20326/SHA-256 verifies DNSKEY=20326/SEP</li><li>✔ Found 1 RRSIGs over DNSKEY RRset</li><li>✔ RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset</li></ul>
fr	<ul style="list-style-type: none"><li>✔ Found 1 DS records for fr in the . zone</li><li>✔ DS=51508/SHA-256 has algorithm ECDSA256SHA256</li><li>✔ Found 1 RRSIGs over DS RRset</li><li>✔ RRSIG=11019 and DNSKEY=11019 verifies the DS RRset</li><li>✔ Found 3 DNSKEY records for fr</li><li>✔ DS=51508/SHA-256 verifies DNSKEY=51508/SEP</li><li>✔ Found 2 RRSIGs over DNSKEY RRset</li><li>✔ RRSIG=29133 and DNSKEY=29133/SEP verifies the DNSKEY RRset</li></ul>
education.fr	<ul style="list-style-type: none"><li>✖ No DS records found for education.fr in the fr zone</li><li>✖ No DNSKEY records found</li><li>✔ ate-ns01.ate.info is authoritative for education.fr</li><li>✔ education.fr A RR has value 185.75.143.93</li><li>✖ No RRSIGs found</li></ul>
education.fr	<ul style="list-style-type: none"><li>✔ ate-ns04.ate.info is authoritative for education.fr</li><li>✔ education.fr A RR has value 185.75.143.93</li><li>✖ No RRSIGs found</li></ul>
education.fr	<ul style="list-style-type: none"><li>✔ ate-ns03.ate.info is authoritative for education.fr</li><li>✔ education.fr A RR has value 185.75.143.93</li><li>✖ No RRSIGs found</li></ul>
education.fr	<ul style="list-style-type: none"><li>✔ ate-ns02.ate.info is authoritative for education.fr</li><li>✔ education.fr A RR has value 185.75.143.93</li><li>✖ No RRSIGs found</li></ul>

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 interrèseau dans la filiale :

##### 3.4.2 : Mode realtime/ mode simulation :



c)

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

d)

<b>Out Layers</b> Layer 7: DNS Layer6 Layer5 Layer 4: UDP Src Port: 1025, Dst Port: 53 Layer 3: IP Header Src. IP: 172.16.0.8, Dest. IP: 172.16.0.3 Layer 2: Layer1	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)

<b>In Layers</b> Layer 7: DNS Layer6 Layer5 Layer 4: UDP Src Port: 1025, Dst Port: 53 Layer 3: IP Header Src. IP: 172.16.0.7, Dest. IP: 172.16.0.3 Layer 2: Ethernet II Header 00D0.D3D7.5B29 >> 0060.5C93.13A4 Layer 1: Port FastEthernet0	Le DNS est protocole appliqué dans la couche 7. C'est donc une requête de résolution de nom de domaine.
---	---

g)

DNS Answer	
0	Bits
NAME (VARIABLE LENGTH): branchserver.pt.pta	
TYPE:1	CLASS:1
TTL:86400	
LENGTH:4	IP:172.16.0.3

h)

PDU Information at Device: Sales

**OSI Model**   Inbound PDU Details   **Outbound PDU Details**

At Device: Sales  
Source: Sales  
Destination: 172.16.0.3

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1025	Layer 4: TCP Src Port: 1025, Dst Port: 80
Layer 3: IP Header Src. IP: 172.16.0.3, Dst. IP: 172.16.0.7	Layer 3: IP Header Src. IP: 172.16.0.7, Dst. IP: 172.16.0.3
Layer 2: Ethernet II Header 0060.5C93.13A4 >> 00D0.D3D7.5B29	Layer 2: Ethernet II Header 00D0.D3D7.5B29 >> 0060.5C93.13A4
Layer 1: Port FastEthernet0	Layer 1: Port(s): FastEthernet0

- The device receives a TCP SYN+ACK segment on the connection to 172.16.0.3 on port 80.
- Received segment information: the sequence number 0, the ACK number 1, and the data length 24.
- The TCP segment has the expected peer sequence number.
- The TCP connection is successful.
- TCP retrieves the MSS value of 536 bytes from the Maximum Segment Size Option in the TCP header.
- The device sets the **connection state to ESTABLISHED**

i)

PDU Information at Device: IP Phone0	
<p><b>OSI Model</b>   Inbound PDU Details   Outbound PDU Details</p> <p>At Device: IP Phone0 Source: Sales Destination: HTTP CLIENT</p> <p><b>In Layers</b></p> <p>Layer7</p> <p>Layer6</p> <p>Layer5</p> <p>Layer4</p> <p>Layer3</p> <p>Layer 2: Ethernet II Header 00D0.D3D7.5B29 &gt;&gt; 0060.5C93.13A4</p> <p><b>Layer 1: Port PC</b></p>	<p>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.</p>

j)

PDU Information at Device: Sales

**OSI Model**   Inbound PDU Details   Outbound PDU Details

At Device: Sales  
Source: Sales  
Destination: HTTP CLIENT

In Layers
Layer 7: HTTP
Layer6
Layer5
Layer 4: TCP Src Port: 80, Dst Port: 1025
Layer 3: IP Header Src. IP: 172.16.0.3, Dst. IP: 172.16.0.7
Layer 2: Ethernet II Header 0060.5C93.13A4 >> 00D0.D3D7.5B29
Layer 1: Port FastEthernet0

### 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)

Sales	DNS	Le protocole ARP est activé seulement si un échange direct a lieu, mais avant le poste doit chercher l'adresse IP de BranchServeur.
Sales	ARP	
IP Phone0	ARP	
S4	ARP	
BranchServer	ARP	

e)

1. The DNS client receives an A DNS response. 2. The received A DNS response contains a resolved IP address for the queried domain.	Le client DNS a reçu l'adresse IP résolue, le serveur sait sur quelle adresse IP envoyer les requêtes pour ce domaine.
--	--

f)

DNS Answer	
0 8 16 24	
NAME (VARIABLE LENGTH):centraiserver.pt.pta	
TYPE:1	CLASS:1
TTL:86400	
LENGTH:4	IP:10.10.10.2

g)

Ethernet II	
PREAMBLE: 101010...10	DEST ADDR: 0001.969A.1D03
SRC ADDR: 0060.4753.45E1	TYP: E:0x
DATA (VARIABLE LENGTH)	FCS: 0x00000000
Arp	
HARDWARE TYPE: 0x0001	PROTOCOL TYPE: 0x0800
HLEN: 0x06	PLEN: 0x04
OPCODE: 0x0002	
SOURCE MAC: 0060.4753.45E1	
SOURCE IP: 10.10.10.2	
TARGET MAC: 0001.969A.1D03	
TARGET IP: 10.10.10.1	

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

h)

Out Layers	
Layer 7: HTTP	
Layer 6	
Layer 5	
Layer 4: TCP Src Port: 1026, Dst Port: 80	
Layer 3: IP Header Src. IP: 172.16.0.8, Dest. IP: 10.10.10.2	
Layer 2: Ethernet II Header	
00D0.D3D7.5B29 >> 000A.F3E4.EB01	
Layer 1: Port(s):	

L'adresse MAC source est 00D0.D3D7.5B29 et celle du prochain saut est 000A.F3E4.EB01.

i)

PDU Information at Device: Intranet	
OSI Model	Inbound PDU Details
At Device: Intranet	
Source: Sales	
Destination: HTTP CLIENT	
In Layers	
Layer 7	
Layer 6	
Layer 5	
Layer 4	
Layer 3	
Layer 2: Frame Relay FRAME RELAY	
Layer 1: Port Serial1	

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)

DNS Answer																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
0														8																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		</

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

g)

In Layers	
Layer7	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.
Layer6	
Layer5	
Layer4	
Layer 3: IP Header Src. IP: 200.200.200.1, Dest. IP: 216.146.46.11	
Layer 2: PPP Frame PPP	
Layer 1: Port Serial0/1/0	

h)

1. The device receives a TCP SYN+ACK segment on the connection to 216.146.46.11 on port 80.
2. Received segment information: the sequence number 0, the ACK number 1, and the data length 24.
3. The TCP segment has the expected peer sequence number.
4. The TCP connection is successful.
5. TCP retrieves the MSS value of 536 bytes from the Maximum Segment Size Option in the TCP header.
6. The device sets the connection state to ESTABLISHED.

## 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)

<p><b>Out Layers</b></p> <p>Layer 7: DHCPv6 Frame</p> <p>Layer 6</p> <p>Layer 5</p> <p>Layer 4: UDP Src Port: 546 Dst Port: 547</p> <p>Layer 3: IPv6 Header Src. IP: FE80::2D0:58FF:FEA7:87A1, Dest. IP: FF02::1:2</p> <p>Layer 2: Ethernet II Header 00D0.58A7.87A1 &gt;&gt; 3333.0001.0002</p> <p>Layer 1: Port(s): FastEthernet0</p>	<p>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.</p> <p>Les ports 546 et 547 sont aussi utilisés par DHCP.</p>
---	---

f)

<p>OSI Model Inbound PDU Details</p> <p>At Device: Server0 Source: PC0 Destination: 255.255.255.255</p> <p><b>In Layers</b></p> <p>Layer 7: DHCP Packet Server: 0.0.0.0, Client: 0.0.0.0</p> <p>Layer6</p> <p>Layer5</p> <p>Layer 4: UDP Src Port: 68, Dst Port: 67</p> <p>Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255</p> <p>Layer 2: Ethernet II Header 0050.0FCB.6ABA &gt;&gt; FFFF.FFFF.FFFF</p> <p>Layer 1: Port FastEthernet0</p> <p>1. The packet is a DHCP packet. The DHCP server processes it. 2. The DHCP server received a <b>DHCP Discover packet</b>. 3. The DHCP server does not have an existing binding to this host. It looks up DHCP pools for a new IP address. 4. The DHCP server finds the next available IP address in the pool.</p>	DHCP Discover, pour localiser les serveurs DHCP disponibles.
<p>OSI Model Inbound PDU Details Outbound PDU Details</p> <p>At Device: PC0 Source: Server0 Destination: Broadcast</p> <p><b>In Layers</b></p> <p>Layer 7: DHCP Packet Server: 192.168.1.1, Client: 0.0.0.0</p> <p>Layer6</p> <p>Layer5</p> <p>Layer 4: UDP Src Port: 67, Dst Port: 68</p> <p>Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 255.255.255.255</p> <p>Layer 2: Ethernet II Header 0004.9A46.7DB7 &gt;&gt; FFFF.FFFF.FFFF</p> <p>Layer 1: Port FastEthernet0</p> <p>1. The packet is a DHCP packet. The DHCP client processes it. 2. The DHCP client received a <b>DHCP offer packet</b>.</p>	DHCP Offer, une proposition d'adresses IP et de configuration réseau.
<p>OSI Model Inbound PDU Details Outbound PDU Details</p> <p>At Device: Server0 Source: Server0 Destination: Broadcast</p> <p><b>In Layers</b></p> <p>Layer 7: DHCP Packet Server: 192.168.1.1, Client: 0.0.0.0</p> <p>Layer6</p> <p>Layer5</p> <p>Layer 4: UDP Src Port: 68, Dst Port: 67</p> <p>Layer 3: IP Header Src. IP: 0.0.0.0, Dest. IP: 255.255.255.255</p> <p>Layer 2: Ethernet II Header 0050.0FCB.6ABA &gt;&gt; FFFF.FFFF.FFFF</p> <p>Layer 1: Port FastEthernet0</p> <p>1. The packet is a DHCP packet. The DHCP server processes it. 2. The DHCP server received a <b>DHCP Request packet</b>. 3. The DHCP server binds the requested IP address from the pool to the host's MAC address.</p>	DHCP Request, acceptation de l'adresse IP.
<p>OSI Model Inbound PDU Details</p> <p>At Device: PC0 Source: Server0 Destination: Broadcast</p> <p><b>In Layers</b></p> <p>Layer 7: DHCP Packet Server: 192.168.1.1, Client: 0.0.0.0</p> <p>Layer6</p> <p>Layer5</p> <p>Layer 4: UDP Src Port: 67, Dst Port: 68</p> <p>Layer 3: IP Header Src. IP: 192.168.1.1, Dest. IP: 255.255.255.255</p> <p>Layer 2: Ethernet II Header 0004.9A46.7DB7 &gt;&gt; FFFF.FFFF.FFFF</p> <p>Layer 1: Port FastEthernet0</p> <p>1. The packet is a DHCP packet. The DHCP client processes it. 2. The DHCP client received a <b>DHCP acknowledge packet</b>. 3. The DHCP client receives an Ack packet and sets its IP address configuration.</p>	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 :

```
Router(config)#interface fa1/0
Router(config-if)#ip address 192.168.4.6 255.255.255.248
Router(config-if)#duplex auto
Router(config-if)#speed auto
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp pool Pool1
Router(dhcp-config)#network 192.168.2.0 255.255.255.240
Router(dhcp-config)#default-router 192.168.2.14
Router(dhcp-config)#
% Invalid input detected at '^' marker.
Router(dhcp-config)#default-router 192.168.2.14
Router(dhcp-config)#ip dhcp excluded-address 192.168.2.12 192.168.2.14
```

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

	<p>J'ai configuré un site simple avec seulement un fond et mon nom en html, sur le serveur web TACAS.</p>
--	---





### 4.3.3 : Vérifications :

Adresses exclues :

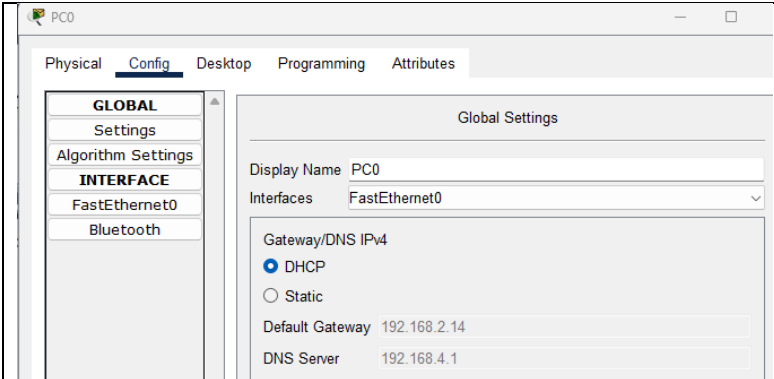
```
R3#show running-config
Building configuration...

Current configuration : 1857 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable secret 5 $1$mERr$koVKGXkyO8L7qhomZCdqk0
!
!
ip dhcp excluded-address 192.168.2.12 192.168.2.14
ip dhcp excluded-address 192.168.0.12 192.168.0.14
!
ip dhcp pool Pool1
network 192.168.2.0 255.255.255.240
default-router 192.168.2.14
--More--
```

Enveloppe ICMP (ping) réussie :

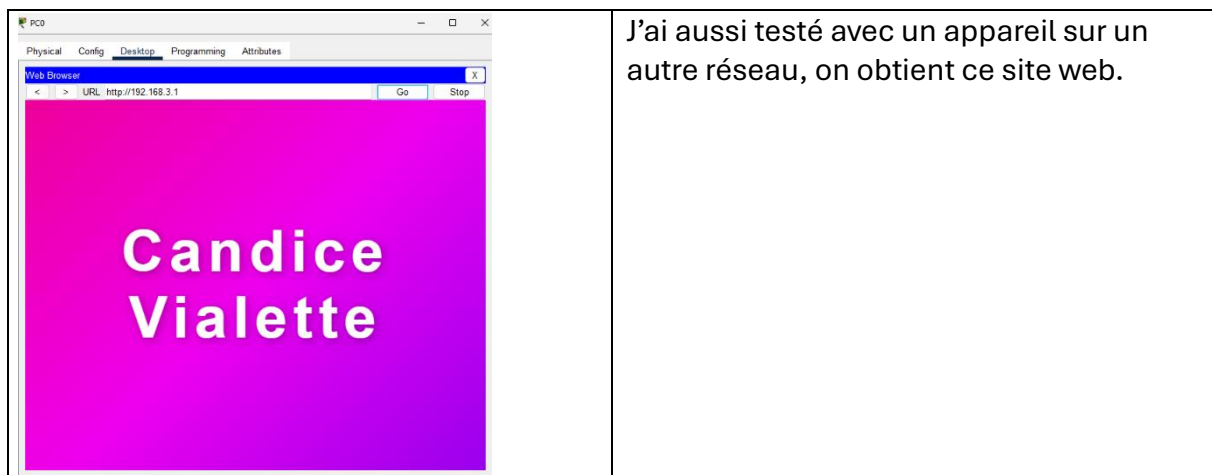
	Successful	PC0	DNS1	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC0	DNS1	ICMP		0.000	N	5	(edit)	(delete)

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 :



#### 4.3.4 : Configuration routeur :

Pour sécuriser le routeur, on met un mot de passe pour l'accès à 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 :

<pre>Router(config)#enable secret candice Router(config)#ip domain-name tp.drogue Router(config)#crypto key generate rsa % Please define a hostname other than Router. Router(config)#username candice privilege 15 secret candice Router(config)#line vty 0 4 Router(config-line)#transport input ssh Router(config-line)#login local Router(config-line)#exit Router(config)#line console 0 Router(config-line)#password candice Router(config-line)#login Router(config-line)#logging synchronous Router(config-line)#exit Router(config)#service password-encryption Router(config)#ip ssh version 2 Please create RSA keys (of at least 768 bits size) to enable SSH v2. Router(config)#ip ssh authentication-retries 2 Router(config)#ip ssh time-out 90 Router(config)#</pre>	<p>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.</p>
--	--

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

```

R3(config)#enable secret candice
R3(config)#ip domain-name tp.drogue
R3(config)#crypto key generate rsa
% You already have RSA keys defined named R3.tp.drogue .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R3.tp.drogue
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

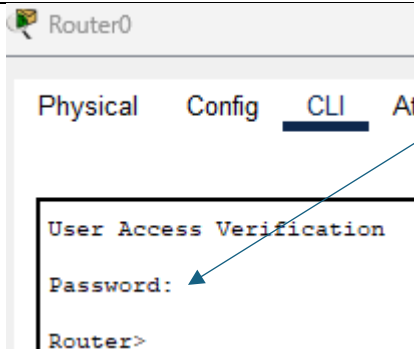
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#
R3(config)#username candice privilege 15 secret candice
*Mar 1 0:36:28.213: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#line console 0
R3(config-line)#password candice
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#ip ssh version 2
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh time-out 90
R3(config)#

```

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

Pour accéder au router :

	<p>Le mot de passe a été tapé après Password mais pour des raisons de sécurité, Cisco n'affiche rien quand on le tape</p>
---	---

## 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.