

Objectif : Observer le fonctionnement du protocole DHCP et analyser les différents échanges entre un client et un serveur DHCP à l'aide de Wireshark.

1. Relâchement de l'adresse IP avec ipconfig /release

- **Action** : Dans la fenêtre de commande (cmd), entrez la commande ipconfig /release.
 - **But** : Cette commande force votre machine à libérer son adresse IP actuelle. En réponse, l'adresse IP de votre interface réseau sera mise à 0.0.0.0 (si le client est configuré en DHCP).

```
C:\Users\laulf>ipconfig /release
```

Configuration IP de Windows

Aucune opération ne peut être effectuée sur Connexion au réseau local* 1 lorsqu'aucun média n'est connecté.

Aucune opération ne peut être effectuée sur Connexion au réseau local* 2 lorsque son média est déconnecté.

Aucune opération ne peut être effectuée sur Wi-Fi lorsque son média est déconnecté.

Aucune opération ne peut être effectuée sur Connexion réseau Bluetooth lorsque son média est déconnecté.

Carte Ethernet Ethernet :

Suffixe DNS propre à la connexion. . . :

Adresse IPv6 de liaison locale: : fe80::5054:97d3:8464:98ad%3

Passerelle par défaut.

Carte réseau sans fil Connexion au réseau local* 1 :

Statut du média : Média déconnecté

Suffixe DNS propre à la connexion. . . .

Carte réseau sans fil Connexion au réseau local* 2 :

Statut du média : Média déconnecté

Suffixe DNS propre à la connexion.

Carte réseau sans fil Wi-Fi :

Statut du média : Média déconnecté

Suffixe DNS propre à la connexion

Carte Ethernet Connexion réseau Bluetooth :

Statut du média : Média déconnecté

Suffixe DNS propre à la connexion

2. Lancer Wireshark

- **Action** : Démarrer Wireshark et sélectionnez l'interface réseau appropriée pour capturer les paquets
 - **But** : Vous allez capturer tous les paquets transitant par votre machine, y compris ceux liés à DHCP.

3. Commencer la capture des paquets

- **Action** : Démarrer la capture sur Wireshark en cliquant sur l'interface réseau appropriée.
 - **But** : Cela permettra d'enregistrer tous les paquets réseau, ce qui inclut les échanges DHCP.

No.	Time	Source	Destination	Protocol	Length	Info
372	2.943145	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
373	2.952641	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
374	2.962133	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
375	2.971618	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
376	2.981121	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
377	2.990612	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
378	3.000105	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
379	3.009596	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
380	3.019092	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
381	3.028582	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
382	3.038077	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
383	3.040682	HewlettPacka_4c:2c:...	Broadcast	ARP	60	Who has 192.168.28.25? T
384	3.047589	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
385	3.057076	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
386	3.066564	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
387	3.076093	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
388	3.085550	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
389	3.095042	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914
390	3.104549	Cisco_4c:c9:15	CDP/VTP/DTP/PAgP/UD...	CDP	208	Device ID: 2c36f84cc914

Frame 1: 208 bytes on wire (1664 bits), 208 bytes	0000	01 00 0c cc cc cc cc 2c 36 f8 4c c9 15 00 c2
► IEEE 802.3 Ethernet	0010	03 00 00 0c 20 00 02 b4 3e 40 00 01 00 10
► Logical-Link Control	0020	33 36 66 38 34 63 63 39 31 34 00 02 00 2d
► Cisco Discovery Protocol	0030	00 02 01 01 cc 00 04 c0 a8 1c f3 02 08 aa
	0040	00 00 00 86 dd 00 10 fe 80 00 00 00 00 00 00
	0050	36 f8 ff fe 4c c9 14 00 03 00 07 67 69 31
	0060	00 08 00 00 00 28 00 05 00 0c 31 2e 34 2e
	0070	2e 35 00 06 00 27 43 69 73 63 6f 20 53 47
	0080	30 2d 32 30 20 28 50 49 44 3a 53 52 57 32
	0090	36 2d 4b 39 29 2d 56 53 44 00 0a 00 06 00
	00a0	0b 00 05 01 00 0e 00 07 01 00 03 00 12 00
	00b0	00 13 00 05 00 00 14 00 0b 53 77 2d 50 52
	00c0	00 1a 00 10 00 00 75 da 00 00 00 00 ff ff

4. Lancer la commande ipconfig /renew

- **Action** : Dans la fenêtre de commande (cmd), entrez ipconfig /renew.
 - **But** : Cette commande force la machine à envoyer une requête DHCP pour obtenir une nouvelle adresse IP. Le processus DHCP de quatre étapes sera lancé : **Discover, Offer, Request, ACK**.

5. Vérifier la nouvelle adresse IP avec ipconfig

- **Action** : Après l'échange DHCP, entrez ipconfig dans la fenêtre de commande.
- **But** : Vérifiez que votre machine a reçu une nouvelle adresse IP attribuée par le serveur DHCP.

6. Effectuer un deuxième ipconfig /renew

- **Action** : Tapez à nouveau ipconfig /renew dans la fenêtre de commande.
- **But** : Demander une nouvelle adresse IP au serveur DHCP. Cela vous permet de voir s'il y a un changement ou non (par exemple, si l'adresse IP a été renouvelée ou réattribuée).

7. Effectuer un ipconfig /release

- **Action** : Tapez ipconfig /release dans la fenêtre de commande.
- **But** : Relâchez à nouveau l'adresse IP attribuée à votre machine.

8. Effectuer un ipconfig /renew à nouveau

- **Action** : Exécutez à nouveau ipconfig /renew pour demander une nouvelle adresse IP après avoir libéré l'adresse précédente.
- **But** : Cela permet de voir si le serveur DHCP attribue la même ou une nouvelle adresse IP.

9. Stopper la capture Wireshark

- **Action** : Une fois que vous avez effectué toutes les étapes ci-dessus et observé les paquets échangés, arrêtez la capture dans Wireshark.
- **But** : Cela vous permet d'analyser les paquets capturés et de répondre aux questions suivantes.

Filtrage des paquets DHCP dans Wireshark

- **Filtre Wireshark** : Dans la barre de filtre en haut de Wireshark, entrez dhcp ou bootp pour filtrer et ne visualiser que les paquets DHCP.
- **Ports utilisés par DHCP** : DHCP utilise les ports UDP **67** (serveur) et **68** (client).

Vous devriez observer les échanges de paquets suivants :

The screenshot shows the Wireshark interface with the following details:

- Filter Bar:** The filter is set to "bootp".
- List View:** Shows 34 entries in a table with columns: No., Time, Source, Destination, Protocol, and Info. The entries are mostly DHCP messages (Discover, Offer, Request, ACK) and one BootP request.
- Details View:** The selected entry is a BootP request (Message type: Boot Request (1)). The details pane shows:
 - Hardware type: Ethernet
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0xe220d8c3
 - Seconds elapsed: 0
 - Boot flags: 0x0000 (unicast)
 - Client IP address: 0.0.0.0 (0.0.0.0)
 - Your (client) IP address: 0.0.0.0 (0.0.0.0)
 - Next server IP address: 0.0.0.0 (0.0.0.0)
 - Relay agent IP address: 0.0.0.0 (0.0.0.0)
 - Client MAC address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - option: (t=53, l=1) DHCP Message Type = DHCP Discover
 - option: (t=116, l=1) DHCP Auto-Configuration
 - option: (t=61, l=7) Client identifier
 - option: (t=50, l=4) Requested IP Address = 192.168.2.145
 - option: (t=12, l=10) Host Name = "wingamajig"
 - option: (t=60, l=8) Vendor class identifier = "MSFT 5.0"
 - option: (t=55, l=11) Parameter Request List
 - End option
 - Padding
- Hex View:** Shows the raw hex and ASCII data for the selected BootP request. The ASCII dump shows the string "...D.C.4 y. [a.m.]".
- Statistics:** At the bottom, it shows "Bootstrap Protocol (bootp), 300 bytes" and "P: 50 D: 11 M: 0 Drops: 0".

Faites une capture d'écran et répondez aux questions suivantes :

1. DHCP utilise-t-il UDP ou TCP ?

- Réponse : Dhcpc utilise UDP

2. Diagramme des quatre premiers paquets (Discover/Offer/Request/ACK)

1. DHCP Discover :

- **Source :** 0.0.0.0
- **Destination :** 255.255.255.255
- **But :**

2. DHCP Offer :

- **Source :** 192.168.28.253
- **Destination :** 192.168.28.85
- **But :**

3. DHCP Request :

- **Source :** 0.0.0.0
- **Destination :** 255.255.255.255
- **But :**

4. DHCP ACK :

- **Source :** 192.168.28.253
- **Destination :** 192.168.28.85
- **But :**

3. Quelle est l'adresse Ethernet de votre hôte ?

- Réponse : 255.255.255.255

4. Différence entre le message DHCP Discover et le message DHCP Request

- Le message **DHCP Discover** : demande
- Le message **DHCP Request** : accept

5. Valeur du Transaction-ID dans les quatre premiers paquets DHCP

- **Transaction-ID** : 0x49b4e6f0

6. Valeur IP dans les datagrammes IP pendant l'échange (avant l'attribution de l'adresse IP)

- Réponse : 0xa1d6

7. Quelle est l'adresse de votre serveur DHCP ?

- Réponse : 192.168.18.253

8. Quelle adresse IP vous est proposée dans le message DHCP Offer ?

- Réponse ("Yours DHCPOFFER" ou "Your IP address") :

9. Y a-t-il un relais entre l'hôte et le serveur DHCP ?

- Réponse (Gateway IP address) : 255.255.255.0

10. Objectif du masque dans le message DHCP Offer

- Réponse :

11. Intérêt du « lease time »

- Réponse : c'est le temps d'on l'offre du dhcp reste actif cela permet au dhcp de pouvoir attribuer l'adresse a un autre poste si il y a trop de client par rapport aux ip
- Sa valeur : 51 2 hours

12. Objectif du message DHCP Release

- Réponse : cela permet au dhcp de revoquer un adresse pour la reattribuer

13. Désactivez le filtre bootp. A-t-il eu des échanges ARP pendant l'échange DHCP ?

- Réponse : oui

178 1.610424	VMware_01:d3:37	Broadcast	ARP	60 Who has 192.168.28.9
183 1.645781	Cisco_6e:96:1e	Broadcast	ARP	60 Who has 192.168.28.1
188 1.685855	Cisco_6e:96:1e	Broadcast	ARP	60 Who has 192.168.28.1
191 1.705779	Cisco_6e:96:1e	Broadcast	ARP	60 Who has 192.168.28.1
228 2.046771	HewlettPacka_4c:2c:...	Broadcast	ARP	60 Who has 192.168.28.2
573 5.257281	HewlettPacka_4c:2c:...	Broadcast	ARP	60 Who has 192.168.28.2
738 6.629005	Dell_9f:fb:58	Broadcast	ARP	42 Who has 192.168.28.2
745 6.631131	VMware_01:d3:37	Dell_9f:fb:58	ARP	60 192.168.28.253 is at
752 6.642793	Dell_9f:fb:58	Broadcast	ARP	42 Who has 192.168.28.8
807 6.726200	Cisco_6e:96:1e	Broadcast	ARP	60 Who has 192.168.28.1
826 6.746210	Cisco_6e:96:1e	Broadcast	ARP	60 Who has 192.168.28.1
884 6.877002	Dell_9f:fb:58	Broadcast	ARP	42 Who has 192.168.28.2
885 6.877141	VMware_01:d3:37	Dell_9f:fb:58	ARP	60 192.168.28.253 is at
921 7.143115	SunnrichTechn_1f:00:	Broadcast	ARP	60 Who has 192.168.28.8