***DNS et DHCP***

***Questions***

Les ordinateurs utilisent le protocole **DHCP** pour obtenir automatiquement une adresse IP lorsqu'ils se connectent à un réseau. Lors de la connexion, le périphérique envoie une requête DHCP sur le réseau. Le serveur DHCP répond en attribuant dynamiquement une adresse IP disponible, un masque de sous-réseau, une passerelle par défaut et parfois même les adresses des serveurs DNS. Cela évite une configuration manuelle de chaque appareil sur le réseau.

Lorsque vous saisissez une adresse web (comme *www.google.fr*), votre ordinateur consulte un **serveur DNS** pour traduire ce nom de domaine en une adresse IP, par exemple *142.250.74.35*. Cette adresse IP est ensuite utilisée pour établir la connexion avec le serveur web correspondant et afficher le site demandé dans votre navigateur.

Les ordinateurs et les équipements réseau communiquent entre eux via des adresses IP, et non via des noms lisibles par les humains. Les noms de domaine comme *google.fr* sont donc des alias plus pratiques à retenir. Le **DNS** agit comme un annuaire mondial, traduisant ces noms en adresses IP afin que les ordinateurs puissent localiser et contacter les bons serveurs.

***Définitions***

**DHCP (Dynamic Host Configuration Protocol)** : un protocole réseau permettant **l’attribution automatique des paramètres IP** aux appareils d’un réseau. Cela inclut l’adresse IP, le masque de sous-réseau, la passerelle par défaut, et les serveurs DNS. Le DHCP simplifie la gestion réseau en évitant de configurer manuellement chaque poste, surtout dans les environnements d’entreprise où de nombreux équipements sont connectés.

**DNS (Domain Name System)** : un **service distribué** qui convertit les noms de domaine en adresses IP. Il fonctionne via une hiérarchie de serveurs DNS répartis dans le monde, depuis les serveurs racine jusqu’aux serveurs faisant autorité. Sans le DNS, les utilisateurs devraient retenir les adresses IP de chaque site web, ce qui serait très peu pratique.

***Questions inversées***

Si le serveur DHCP est hors service, les appareils ne pourront pas obtenir automatiquement une adresse IP. Cela entraînera des **déconnexions ou l'impossibilité d'accéder au réseau local ou à Internet**. Une solution temporaire consiste à configurer les adresses IP manuellement sur chaque poste, mais cela prend du temps et peut provoquer des conflits IP si mal géré.

Une résolution DNS rapide garantit un **chargement fluide et efficace des sites web**. Si le DNS est lent ou instable, les pages peuvent prendre du temps à s'afficher ou échouer complètement. Dans un environnement professionnel, une mauvaise résolution DNS peut impacter gravement la productivité et l’accès aux services en ligne.

Un indice classique est que **l’accès par adresse IP fonctionne**, mais **l’accès par nom de domaine échoue**. Par exemple, si *http://142.250.74.35* affiche Google mais *http://google.fr* ne fonctionne pas, cela signale un problème de résolution DNS. On peut aussi utiliser des commandes comme *nslookup*, *ping*, ou *dig* pour tester le fonctionnement des serveurs DNS.

***Pratique***

***Exercice 1 - Obtention automatique d’une adresse IP via DHCP***

Scénario : Vérifier le fonctionnement basique du DHCP sur un poste client.

1. Vérifier que la carte réseau du poste est en mode auto :
   1. Windows

Centre réseau > Propriétés > Obtenir une adresse IP automatiquement

* 1. Linux

Bash  
CopierModifier  
sudo dhclient eth0

1. Commandes de vérification de l’adresse obtenue :
   1. Windows

Ipconfig/all

* 1. Linux

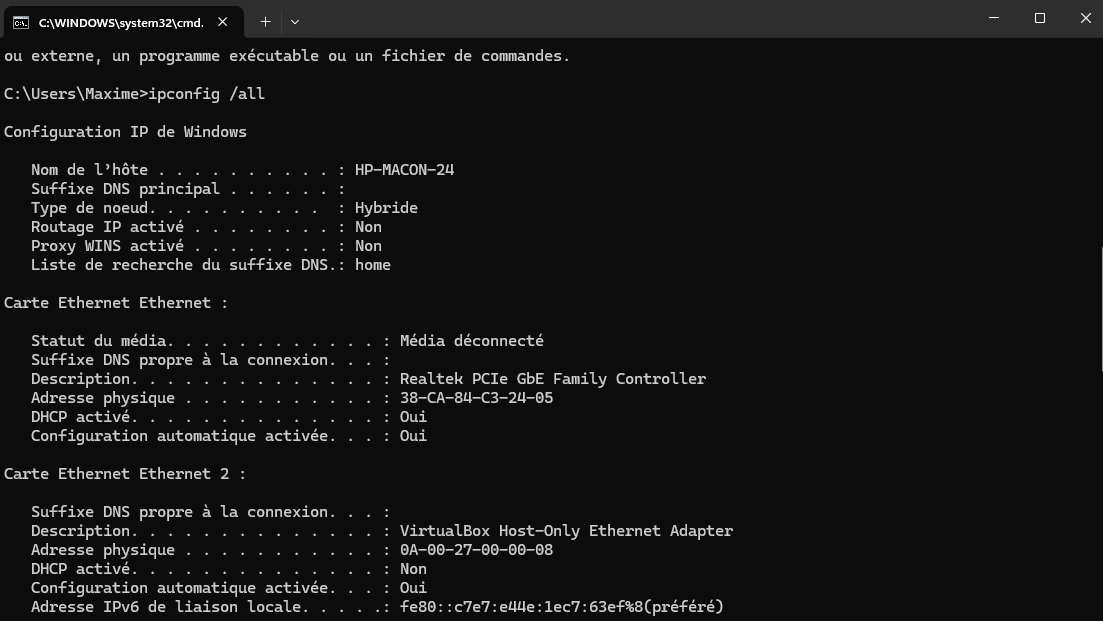
Ipconfig ou ip addr show

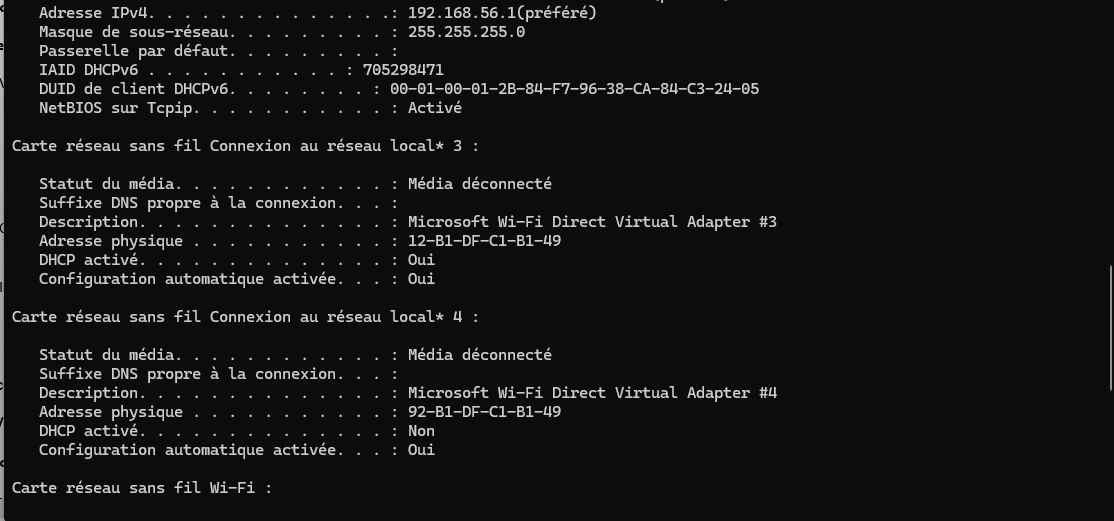
1. Identifier et noter clairement :
   * Adresse IP attribuée
   * Adresse de la passerelle par défaut (gateway)
   * Serveur DHCP utilisé
2. Vérifier si l’adresse IPv4 et IPv6 sont automatique

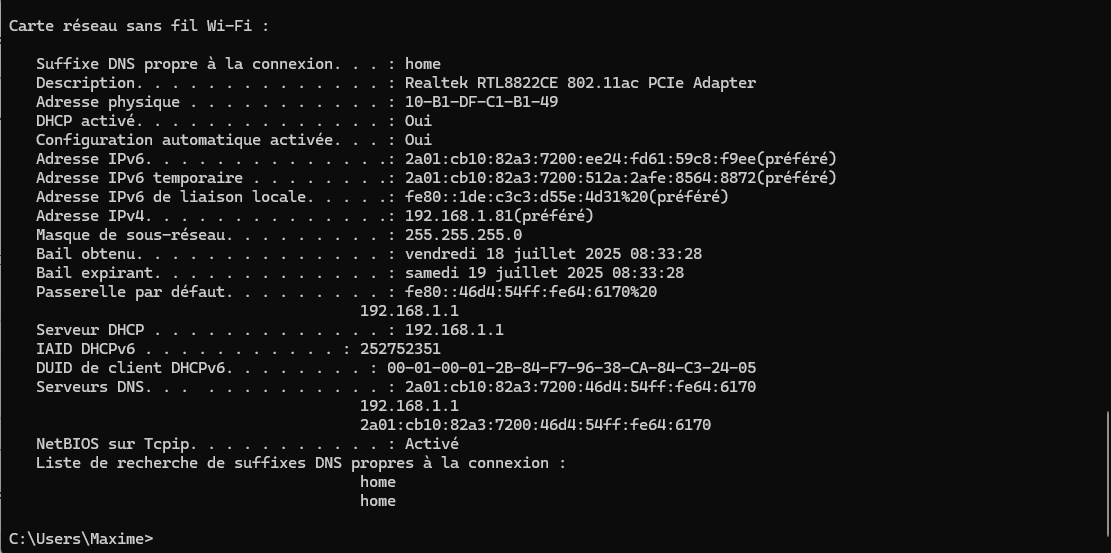
* **Ouvre le Panneau de configuration** (appuie sur Windows + S, tape “Panneau de configuration” et ouvre-le).
* Va dans **“Réseau et Internet”**, puis **“Centre Réseau et partage”**.
* Clique sur **“Modifier les paramètres de la carte”** à gauche.
* Fais un clic droit sur la **connexion réseau active** (Wi-Fi ou Ethernet), puis sélectionne **“Propriétés”**.
* Dans la liste, double-clique sur **“Protocole Internet version 4 (TCP/IPv4)” / “Protocole Internet version 6 (TCP/IPv6)”**.
* IPv4 est en auto, IPv6 l’est aussi.

1. Vérification de l’adresse

* Voici ce que j’obtiens :







1. Identifier et noter clairement

* Adresse IP attribuée
* Adresse IPv6 : 2a01:cb10:82a3:7200:ee24:fd61:59c8:f9ee
* Adresse IPv4 : 192.168.1.81
* Adresse de la passerelle par défaut (gateway)
  + Passerelle par défaut : fe80::46d4:54ff:fe64:6170%20 // 192.168.1.1
* Serveur DHCP utilisé
  + Serveur DHCP : 192.168.1.1

***Exercice 2 – Configuration manuelle du DNS et tests avec nslookup***

Scénario : Configuration d’un serveur DNS précis sur un poste client

1. Configurer manuellement un serveur DNS public (exemple Google : 8.8.8.8).
   * Windows : Propriétés IPv4, entrer manuellement DNS préféré.
   * Linux : éditer */etc/resolv.conf* (exemple : nameserver 8.8.8.8).
2. Tester la configuration DNS avec nslookup :

Bash  
CopierModifier  
nslookup www.google.fr

* + Identifier l’IP retournée et le serveur DNS interrogé.

1. Changer vers un DNS alternatif (ex : Cloudflare 1.1.1.1) et refaire le test :

Bash  
CopierModifier  
nslookup www.openai.com

1. Comparer les résultats, identifier la rapidité et fiabilité de la réponse DNS.

***Exercice 3 – Simulation et dépannage d’une panne DNS***

Scénario : Simuler une perte de DNS sur un poste

1. Volontairement configurer une adresse DNS incorrecte :
   * Windows/Linux : DNS primaire incorrect (exemple : 10.255.255.1).
2. Tester navigation Internet (constater l’échec).
3. Diagnostiquer avec commandes réseau simples :
   * Test IP direct (ping 8.8.8.8) – devrait fonctionner.
   * Test DNS (ping www.google.fr) – devrait échouer.
4. Correction :
   * Reconfigurer correctement le DNS (8.8.8.8) et retester.
   * Vérifier que le problème est résolu.

***Conclusion - Bilan***

Les symptômes typiques permettant d’identifier facilement une panne DHCP ou DNS :

|  |  |  |
| --- | --- | --- |
| Problème réseau | Symptômes observables | Cause probable |
| Panne DHCP | -L’appareil n’a pas d’adresse IP du type 192.168.x.x  -Entraine une perte de connectivité locale et internet. | Le serveur DHCP ne répond pas ou n’est pas accessible |
| Panne DNS | -Impossible d’accéder aux sites web par leur nom de domaine (google.fr ne fonctionne pas)  -Accès direct via une adresse IP fonctionne (<http://142.250.74.35> fonctionne)  -Messages d’erreur comme « DNS\_PROBE\_FINISHED\_NXDOMAIN » dans le navigateur | Le serveur DNS est mal configuré, inaccessible ou en panne. |

Les recommandations prioritaires à faire à un client :

**Vérifier la connectivité physique :**

* Câble Ethernet branché ?
* Wi-Fi activé et connecté au bon réseau ?

**Vérifier les paramètres IP :**

* Ouvrir Invite de commandes → entrer *ipconfig*
* Si l’adresse IP est en 169.254.x.x → Panne DHCP probable

**Tester le DNS :**

* Dans le navigateur, essayer d’accéder à une adresse IP directe (ex. http://142.250.74.35)
* Si ça fonctionne mais pas google.fr → Panne DNS probable