

Table des matières

Introduction	1
I. Informations réseau.....	2
a) Débranchez le câble réseau. Quel message avez-vous ?	2
b) Rebranchez le câble réseau et affichez les connexions réseau (carte réseau).	2
c) Affichez le statut de la carte réseau et les détails.	2
d) Choisissez les propriétés IPv4.....	2
II. Tests de connexion.....	3
a) Ouvrez une console et testez la connexion avec votre voisin.	3
III. Suivi de connexion	3
a) Essayez cette commande avec www.nic.fr :.....	3
IV. Résolution DNS.....	3
a) Quelle est la commande qui permet d'interroger son serveur DNS ?.....	3
V. Adresses MAC	3
a) Combien de machines sont référencées dans votre table ARP ?	3
VI. Capture de trafic réseau.....	4
a) Avec Wireshark.....	4
b) Pendant la capture est en cours	4
c) Arrêtez la capture dans Wireshark.	4
d) Analysez le trafic capturé dans Wireshark.	4
e) Identifiez les paquets liés à votre requête vers le site web.	4
f) Relancez la capture de trafic.	4
g) Arrêtez la capture.	5
h) Comparez les résultats de la capture initiale avec ceux de la nouvelle capture.	5
VII. Table de routage.....	5
a) Affichez la table de routage de votre machine	5
Conclusion.....	5

Introduction

Le présent document constitue un guide détaillé pour la configuration et les tests de réseau sous l'environnement Windows. À travers une série de Travaux Pratiques (TP), nous explorerons les différentes étapes nécessaires pour comprendre, configurer et diagnostiquer les composants réseau d'un système Windows.

La connectivité réseau est un élément essentiel dans le fonctionnement de tout environnement informatique moderne. Qu'il s'agisse d'accéder à des ressources locales ou d'échanger des données sur Internet, la configuration correcte et la gestion efficace des paramètres réseau revêtent une importance capitale.

Ce TP est conçu pour offrir une expérience pratique et approfondie dans le domaine de la configuration réseau sous Windows. Nous aborderons divers aspects, allant de la collecte d'informations réseau de base à l'analyse avancée du trafic réseau en passant par la résolution de problèmes de connectivité.

Chaque section du document détaille les étapes à suivre, les commandes à exécuter et les résultats attendus pour accomplir les objectifs spécifiques du TP. Des explications claires et des exemples pratiques seront fournis pour faciliter la compréhension et l'exécution des tâches.

À la fin de ce TP, les participants devraient avoir acquis une compréhension approfondie des concepts clés liés à la configuration réseau sous Windows, ainsi que des compétences pratiques pour effectuer des tests de connectivité, diagnostiquer les problèmes réseau et analyser le trafic réseau à l'aide d'outils tels que Wireshark.

Sans plus tarder, plongeons dans les détails et commençons notre exploration des fondamentaux du réseau sous Windows.

I. Informations réseau

a) Débranchez le câble réseau. Quel message avez-vous ?

- ⑩ Notez le message affiché lors du débranchement du câble réseau.

b) Rebranchez le câble réseau et affichez les connexions réseau (carte réseau).

Par quel chemin passez-vous ?

- ⑩ Décrivez le chemin ou les étapes pour afficher les connexions réseau.

c) Affichez le statut de la carte réseau et les détails.

Notez :

- ⑩ La référence de la carte (fabricant) : Intel(R) Ethernet I210-T1 GbE NIC
- ⑩ Son adresse physique (MAC) : 68:05:ca:e3:41:1f
- ⑩ Son adresse IP : 169.254.227.37/16
- ⑩ Son masque : 255.255.255.0

d) Choisissez les propriétés IPv4.

Êtes-vous en adressage automatique ou manuel ?

- ⑩ Indiquez si l'adressage est automatique ou manuel.
- ⑩ Entourez votre machine et rajoutez son adresse IP.
- ⑩ Rajoutez l'adresse IP privée de la passerelle.
- ⑩ D'après le site mon-ip.com, rajoutez l'adresse IP publique de la passerelle.

II. Tests de connexion

a) Ouvrez une console et testez la connexion avec votre voisin.

Quelle commande tapez-vous ? Ping + adresse IP du voisin Quel est le résultat ?

- ⑩ Notez la commande utilisée et le résultat obtenu.

Pour cette étape, vous devriez ouvrir l'invite de commande Windows et utiliser la commande "ping" suivie de l'adresse IP de votre voisin. Par exemple : `ping 192.168.0.2`. Le résultat de cette commande devrait vous indiquer si la connexion avec votre voisin est réussie ou non, ainsi que des informations telles que le temps de réponse et les paquets perdus.

III. Suivi de connexion

a) Essayez cette commande avec www.nic.fr :

- ⑩ Par combien de passerelles passe la connexion ?
- ⑩ Pouvez-vous faire une hypothèse sur la localisation de la machine destinataire ?

Lorsque vous utilisez la commande "tracert" avec l'adresse du site web www.nic.fr, le résultat vous montrera le chemin parcouru par les paquets à travers les différentes passerelles. Comptez le nombre de passerelles pour déterminer le nombre d'étapes nécessaires pour atteindre la destination. Ensuite, utilisez ces informations pour faire une hypothèse sur la localisation de la machine destinataire en fonction des passerelles traversées.

IV. Résolution DNS

a) Quelle est la commande qui permet d'interroger son serveur DNS ?

Pour interroger le serveur DNS, vous pouvez utiliser la commande "nslookup" suivie du nom de domaine que vous souhaitez interroger. Par exemple : `nslookup les-charmilles.fr`.

V. Adresses MAC

a) Combien de machines sont référencées dans votre table ARP ?

Après avoir exécuté la commande "`arp -a`" dans l'invite de commande Windows, vous comptez le nombre d'entrées pour déterminer le nombre de machines référencées dans la table ARP de votre ordinateur.

VI. Capture de trafic réseau

a) Avec Wireshark

Dans le menu Capture / Interface, sélectionnez votre carte réseau et cliquez sur Start.

- ⑩ Une fois que vous avez lancé Wireshark, vous devez choisir l'interface réseau à surveiller. Dans le menu Capture, sélectionnez "Interfaces". Une liste des interfaces réseau disponibles s'affichera. Choisissez celle qui correspond à votre carte réseau,

par exemple, "Ethernet0" ou "Wi-Fi". Cliquez ensuite sur le bouton "Start" pour commencer la capture.

b) Pendant la capture est en cours

Ouvrez un navigateur web et accédez à une page web.

- ⑩ Ouvrez votre navigateur web habituel et entrez une URL pour accéder à une page web. Par exemple, vous pouvez entrer "www.google.com".

c) Arrêtez la capture dans Wireshark.

- ⑩ Lorsque vous avez terminé de charger la page web ou que vous avez capturé suffisamment de trafic, retournez à l'interface de Wireshark. Arrêtez la capture en cliquant sur le bouton "Stop" ou en sélectionnant "Stop" dans le menu Capture.

d) Analysez le trafic capturé dans Wireshark.

- ⑩ Une fois la capture arrêtée, vous verrez une liste de paquets capturés dans la fenêtre principale de Wireshark. Vous pouvez explorer ces paquets pour examiner le trafic réseau qui a eu lieu pendant la capture. Vous pouvez filtrer les paquets, afficher des détails sur chaque paquet et analyser les échanges entre votre machine et d'autres appareils sur le réseau.

e) Identifiez les paquets liés à votre requête vers le site web.

- ⑩ Parcourez la liste de paquets capturés pour identifier ceux qui sont liés à votre requête vers le site web que vous avez visité. Vous pouvez généralement identifier ces paquets en examinant les adresses source et destination, ainsi que les ports utilisés dans la communication.

f) Relancez la capture de trafic.

Dans votre navigateur, ouvrez un nouvel onglet sur la même page.

- ⑩ Après avoir relancé la capture, ouvrez un nouvel onglet dans votre navigateur et accédez à la même page web que précédemment. Cela générera une nouvelle requête vers le site web, qui sera capturée par Wireshark.

g) Arrêtez la capture.

- ⑩ Une fois que vous avez capturé suffisamment de trafic après avoir ouvert le nouvel onglet, arrêtez la capture dans Wireshark comme précédemment.

h) Comparez les résultats de la capture initiale avec ceux de la nouvelle capture.

- ⑩ Comparez les paquets capturés lors de la première requête avec ceux capturés lors de la seconde requête. Vous devriez remarquer des différences dans les paquets, notamment des adresses source et destination différentes, ainsi que des ports différents. Cela montre que chaque requête est traitée comme une transaction distincte, même si elle est envoyée vers le même site web.

VII. Table de routage

a) Affichez la table de routage de votre machine

Tapez `route print`. Quelle est l'adresse de votre passerelle (gateway) ?

- ⑩ Lorsque vous exécutez la commande `route print` dans l'invite de commande Windows, vous verrez une liste des routes réseau configurées sur votre machine. Cherchez l'entrée marquée par défaut (Destination : 0.0.0.0) qui indique la passerelle par défaut ou la gateway. Notez l'adresse IP associée à cette entrée, car c'est l'adresse de votre passerelle.
- ⑩ Cette adresse représente la passerelle par défaut de votre machine, c'est-à-dire l'adresse IP à laquelle votre système envoie tout le trafic destiné à des réseaux pour lesquels il n'a pas d'entrée spécifique dans sa table de routage.

Conclusion

Dans ce TP, nous avons exploré divers aspects de la configuration et des tests de réseau sous Windows. Nous avons commencé par examiner les informations réseau telles que l'adresse IP, l'adresse MAC et les détails de la carte réseau. Ensuite, nous avons effectué des tests de connectivité à l'aide de commandes telles que `ping` pour vérifier la connectivité avec d'autres appareils sur le réseau local et sur Internet.

Nous avons également exploré des concepts tels que la résolution DNS pour convertir les noms de domaine en adresses IP, la consultation de la table ARP pour la correspondance entre les adresses MAC et les adresses IP, et l'analyse du trafic réseau avec Wireshark pour comprendre les échanges de données entre notre machine et d'autres appareils sur le réseau.

Enfin, nous avons examiné la table de routage pour comprendre comment notre machine détermine la route à prendre pour acheminer les paquets vers différentes destinations, en particulier vers la passerelle par défaut pour les réseaux inconnus.

Ce TP nous a permis d'acquérir une meilleure compréhension des principes fondamentaux du réseau et des outils disponibles sous Windows pour configurer, diagnostiquer et résoudre les problèmes de connectivité réseau. En maîtrisant ces concepts et en utilisant ces outils de manière appropriée, nous sommes mieux équipés pour gérer et optimiser les réseaux informatiques dans divers environnements.