CHECKPOINT 2

Fichier réponses - CORRECTION

Exercice 1 :

1. Théorie

Q.1.1

Les raisons pour lesquelles le client ne reçoit pas de configuration IP du serveur sont :

* Au niveau du serveur :
  + Il est éteint
  + Le service DHCP est inactif ou non-démarré
  + Le pool DHCP est plein
* Au niveau du client :
  + La configuration IP est en statique
  + Il n’est pas dans le même réseau IP que le serveur DHCP
  + Le service DHCP est inactif ou non-démarré
  + En cas de présence de routeur, les trames broadcast en provenance du client sont bloquée

Q.1.2

Les 2 adresses de réseaux sont différente au niveau du 3ème octet, et le masque est en « /24 ». Cela indique que ce sont des réseaux différents (au niveau d’IP). En l’absence de passerelle, ils ne peuvent pas communiquer.

Q.1.3

Les raisons peuvent être les suivantes :

* Réutilisation d’une adresse déjà utilisée si le bail DHCP n’est pas terminé
* La première adresse disponible est peut-être déjà prise par une autre machine
* La première adresse disponible est peut-être sur une plage en exception
* Le client a peut-être une adresse réservée sur la plage DHCP qui n’est pas cette première adresse

Q.1.4

Oui c’est possible de forcer le client à avoir une adresse IP spécifique.

Sur le serveur on va créer une réservation d’adresse IP pour l’adresse MAC du client.

Le client doit être en DHCP, pas de configuration supplémentaire à faire.

Ensuite il faut redémarrer le client ou exécuter la commande « ipconfig /renew »

Q.1.5

Une adresse IPv6 qui commence par fe80 est une adresse de type unicast lien local (Link Local Address ou LLA).

C’est une adresse non-routable, qui sert à communiquer sur un même réseau. Son préfixe réseau est fe80 ::/10, mais en général on trouve fe80 ::/64. Elle est gérée dynamiquement par SLAAC.

Q.1.6

Il existe aussi en IPv6 :

* Les adresses unicast locales uniques (Unicast Local Address ou ULA), avec le préfixe fc00::/7 ou fd00::/8, avec une portée au sein d’un réseau interne, mais non-routable sur internet
* Les adresses unicast globales (Global Unicast Address ou GUA), avec le préfixe 2000::/3 ou 2001 ::/16, routable sur internet
* Les adresses de bouclage, qui sont ::1/128, qui correspond à la machine elle-même
* Les adresses multicast, avec le préfixe ff00::/8, pour envoyer des paquets à un groupe de machines

Q.1.7

Oui on peut configurer avec un DHCPv6 des plages d’adresses unicast locales uniques.

Sur le serveur, on peut prendre la configuration suivante :

* Préfixe ULA dans la plage fd00::/8, par exemple fd12 :3456 :789a ::/48
* Type d’étendue : Autre
* Durée de validité : mettre la durée du bail

Sur le client, il suffit que le service DHCPv6 soit activé.

Non cela ne suffit pas, car il faut aussi que les Router Advertisement (RA) soient activés pour donner différentes informations au client. Or Windows Server ne peut pas gérer les RA nativement. Donc à moins d’utiliser une solution tiers pour la gestion des RA (comme un routeur ou un système Linux avec radvd) cela ne fonctionnera pas.

Q.1.8

Le protocole qui permet cette résolution de nom est le DNS (Domain Name System).

Q.1.9

Par défaut on a une adresse IPv6 car le protocole ICMP priorise l’IPv6 sur l’IPv4.

On peut avoir le retour d’adresse en IPv4 avec l’option « -4 » de la commande ping.

Q.1.10

Méthode 1 : sans serveur DNS

On utilise le fichier hosts qui est sur les systèmes Microsoft Windows sous c :\Windows\System32\drivers\etc\hosts.

Dans ce fichier on met l’adresse IP associée au nom du client.

Par exemple si l’adresse IP du client CLIENT1 est 192.168.100.20, la ligne dans le fichier hosts sera :

« 192.168.100.20 CLIENT1 CLIENT\_TEST »

Méthode 2 : avec un serveur DNS

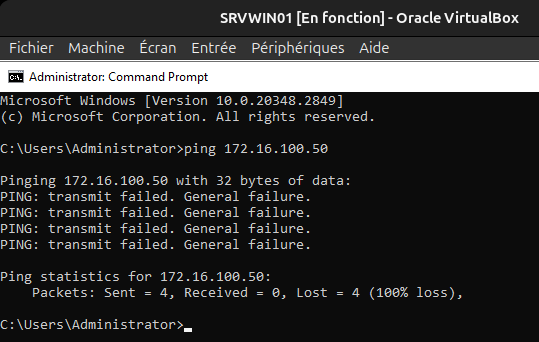
Sur le serveur qui a le rôle DNS, on créer un enregistrement A (en IPv4) ou AAAA (en IPv6) qui lie le nom du client à son adresse IP.

Ensuite on créer un enregistrement CNAME, c’est un alias) qui pointe vers le nom du client dans le DNS.

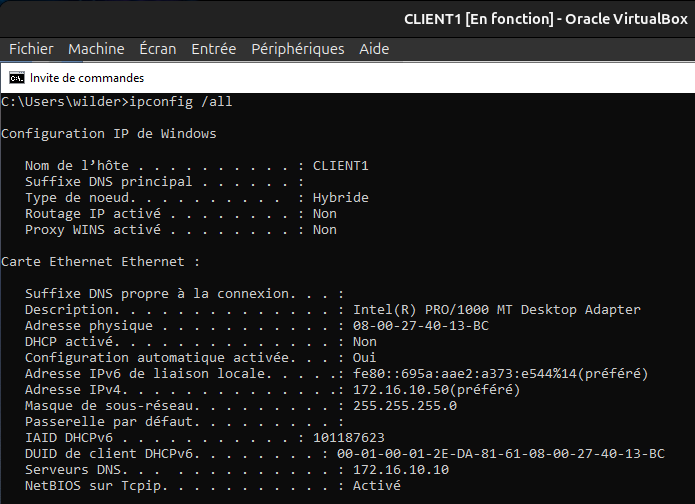
1. Mise en pratique

Q.1.11

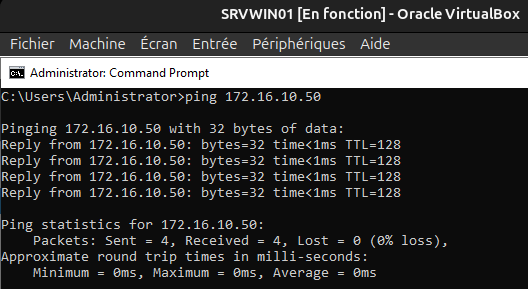
Copie d’écran d’un ping depuis le serveur vers le client en IPv4.



Copie d’écran du résultat de la commande ipconfig/all sur le client.

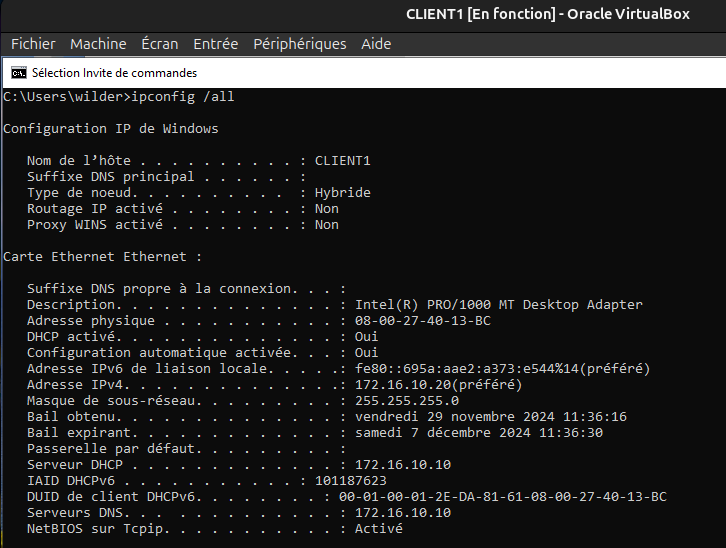
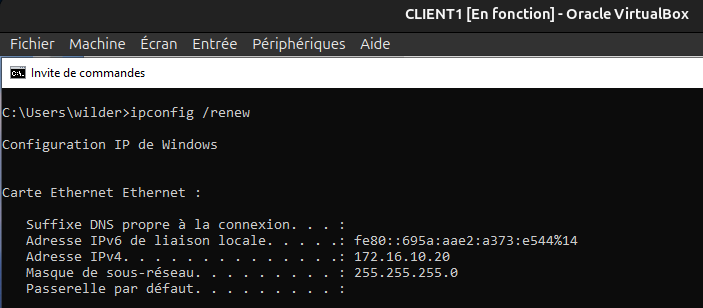


Copie d’écran d’un ping depuis le serveur vers le client en IPv4 (après modification).

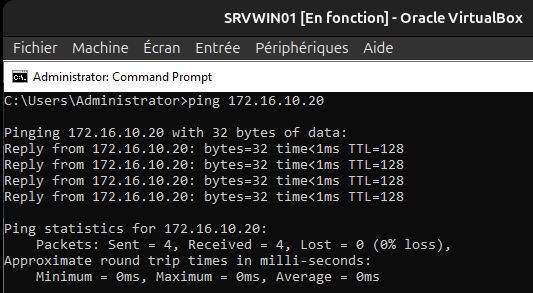


Q.1.12

Copie d’écran du résultat de la commande ipconfig/all sur le client.

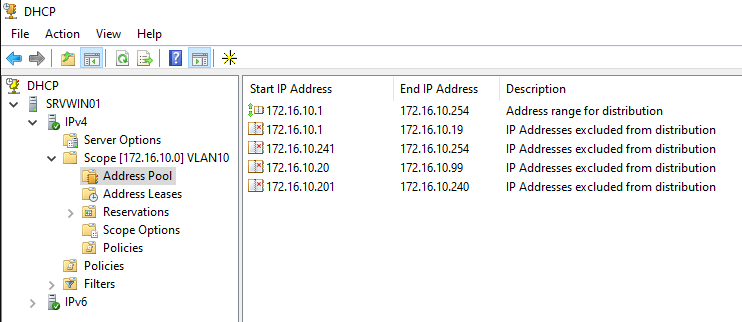


Copie d’écran d’un ping depuis le serveur vers le client en IPv4.

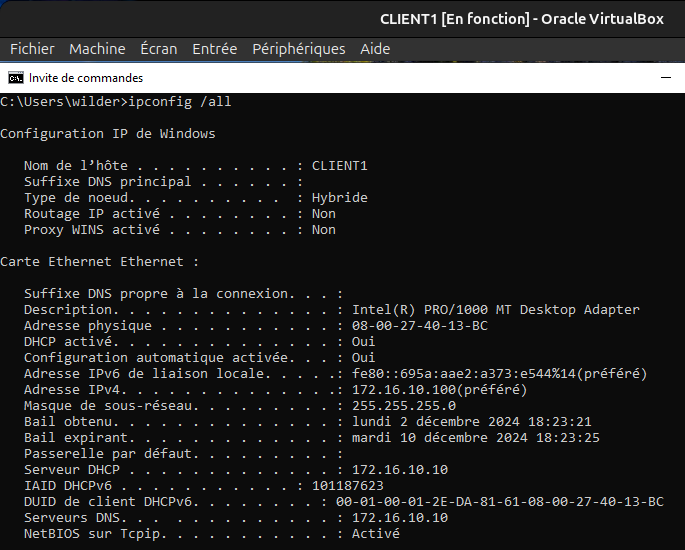
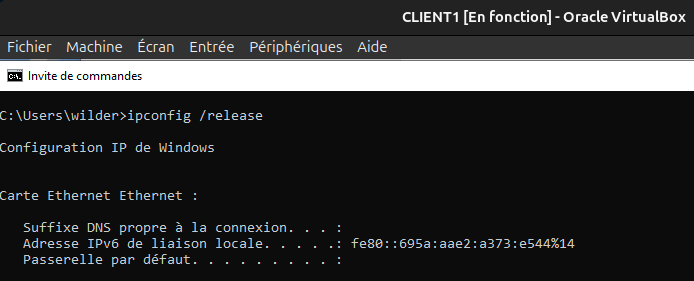


Q.1.13

Copie d’écran de la configuration DHCP sur le serveur.

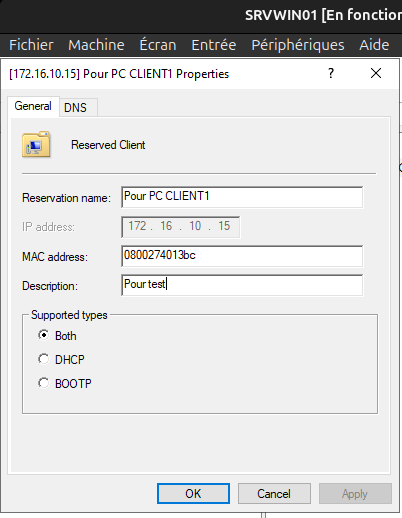


Copie d’écran du résultat de la commande ipconfig/all sur le client.

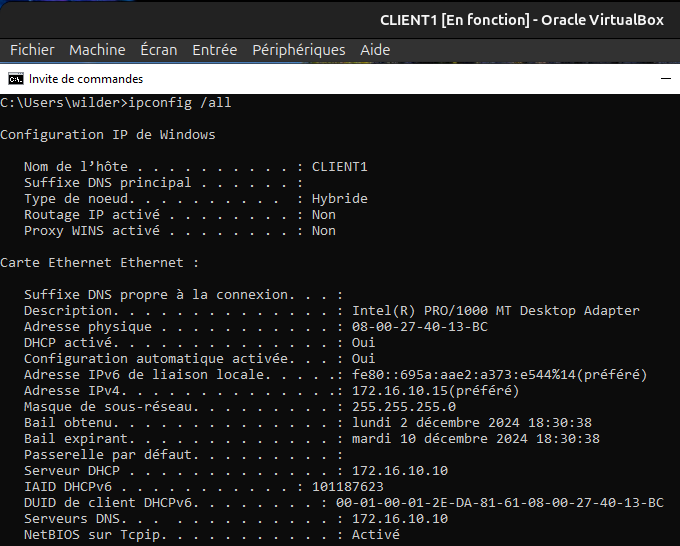


Q.1.14

Copie d’écran de la configuration modifiée sur le serveur.

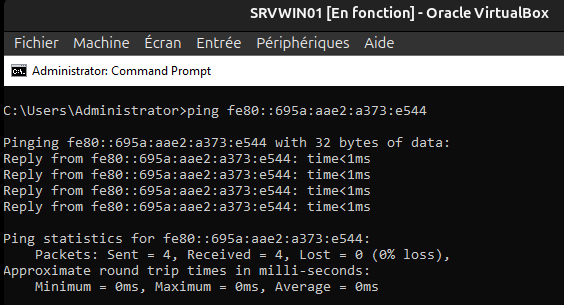


Copie d’écran du résultat de la commande ipconfig/all sur le client.



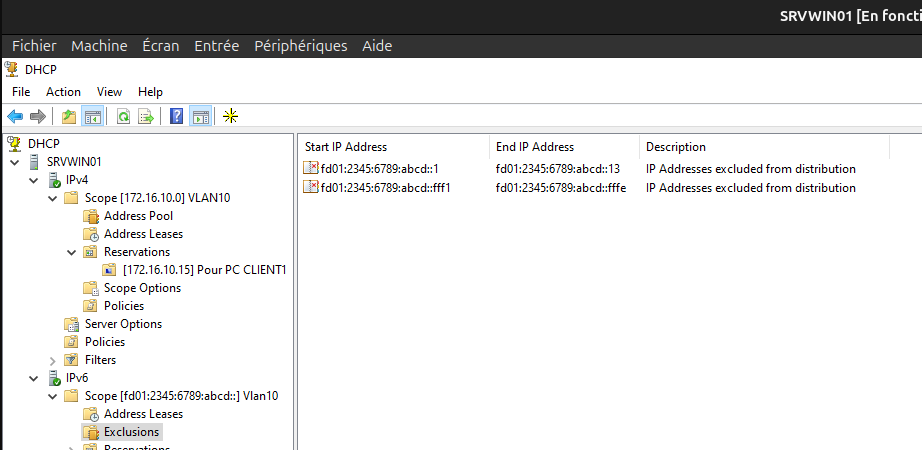
Q.1.15

Copie d’écran d’un ping depuis le serveur vers le client en IPv6.



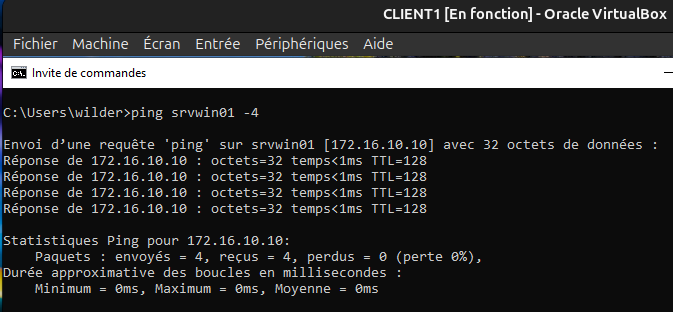
Q.1.16

Copie d’écran de la configuration DHCPv6 sur le serveur.



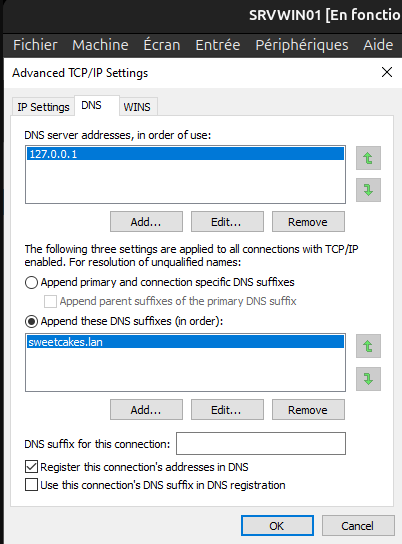
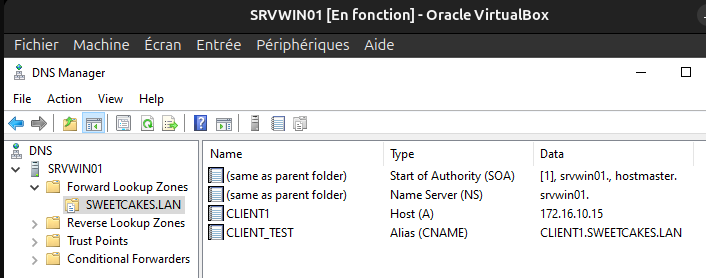
Q.1.17

Copie d’écran d’un ping depuis le client vers le serveur avec le nom du serveur (IP de sortie en v4).

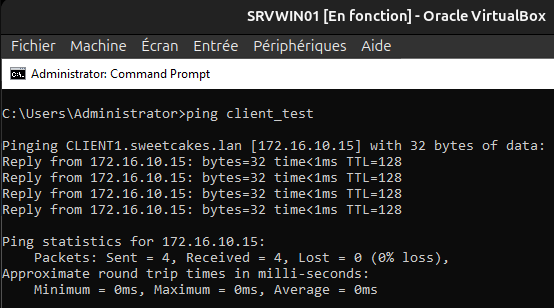


Q.1.18

Copie d’écran de la modification de la configuration sur le serveur.



Copie d’écran d’un ping depuis le serveur vers la machine CLIENT\_TEST avec le nom CLIENT\_TEST.



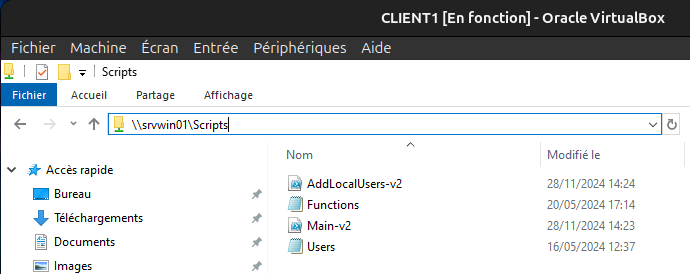
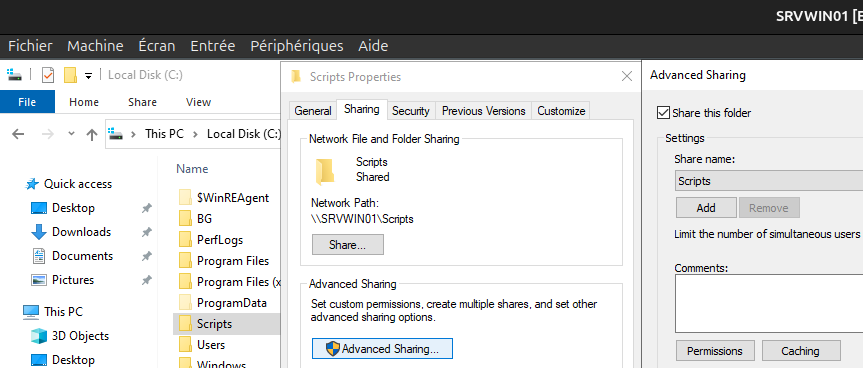
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Exercice 2 :

1. Théorie

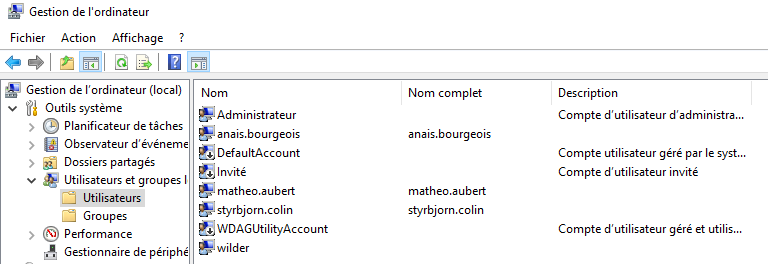
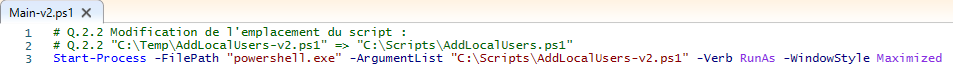
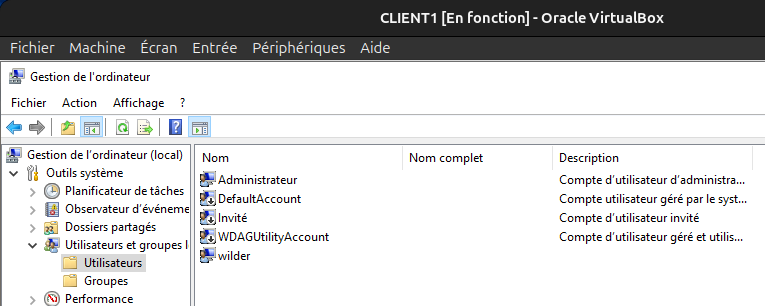
Q.2.1

Copie d’écran de la configuration pour le partage de dossier.



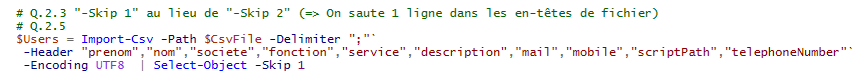
Q.2.2

Copie d’écran de la modification du code pour que AddLocalUsers.ps1 s’exécute correctement.

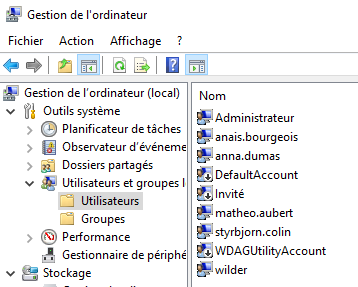
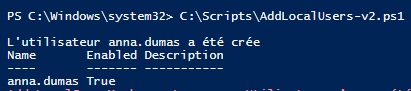


Q.2.3

Copie d’écran de la modification du code pour que le 1er utilisateur soit crée.

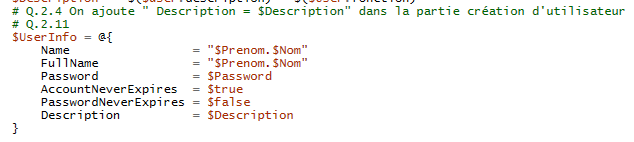


Copie d’écran montrant que le 1er utilisateur est créer.

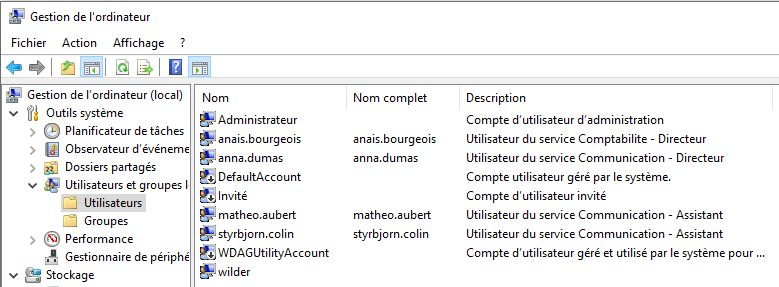


Q.2.4

Copie d’écran de la modification du code pour importation correcte du fichier CSV.



Copie d’écran montrant que le champ « Description » est bien importé.



Q.2.5

Copie d’écran de la modification du code pour bonne utilisation des champs du fichier CSV.



Q.2.6

Copie d’écran de la modification du code pour avoir l’affichage d’un message lorsque l’utilisateur est crée.



Q.2.7

Copie d’écran de la modification du code pour l’intégration de la fonction « Log ».



Q.2.8

Copie d’écran N°1 d’un exemple de journalisation du code en utilisant la fonction « Log ».

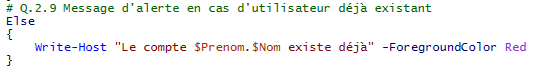


Copie d’écran N°2 d’un exemple de journalisation du code en utilisant la fonction « Log ».



Q.2.9

Copie d’écran de la modification du code pour avoir l’affichage d’un message lorsque l’utilisateur existe déjà.



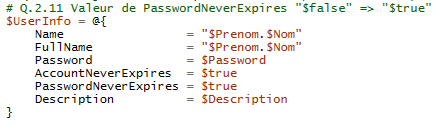
Q.2.10

Copie d’écran de la modification du code pour que l’ajout des utilisateurs au groupe local fonctionne correctement.



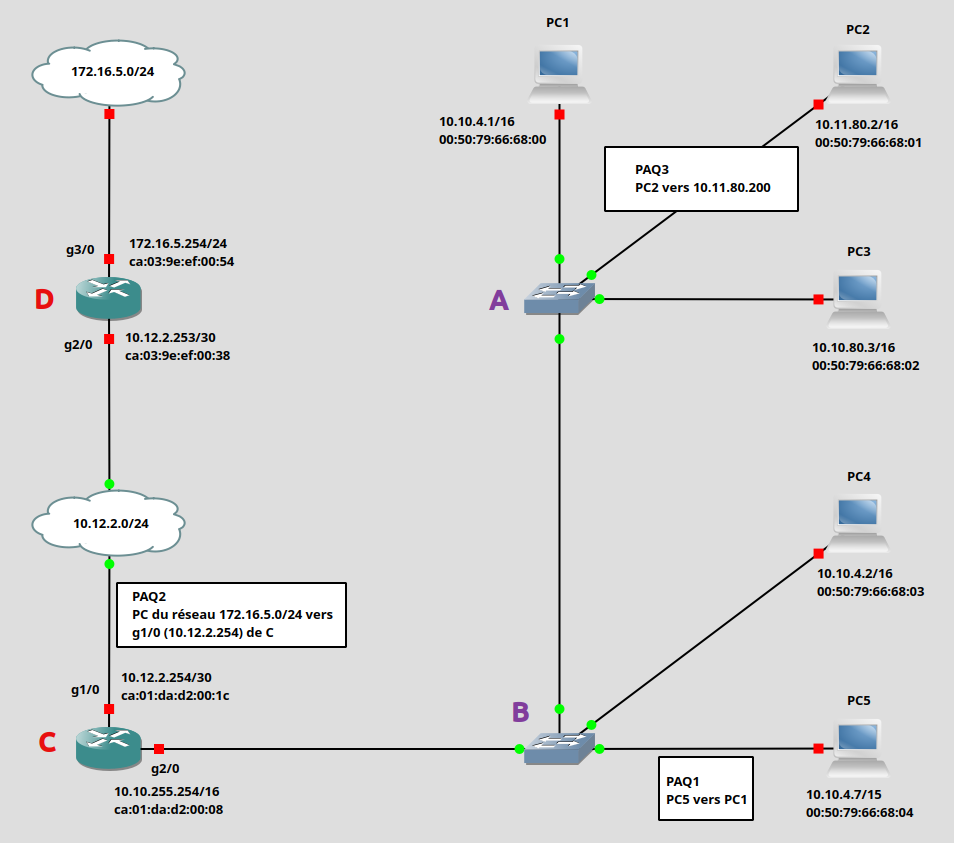
Q.2.11

Copie d’écran de la modification du code pour que le mot de passe des utilisateurs n’expirent plus.



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Exercice 3 :



1. Théorie

Q.3.1

Matériel A (type, rôle sur un réseau, couche du modèle OSI) ?

Le matériel réseau A est un commutateur, communément appelé switch.

Son rôle est de connecter les ordinateurs entre-eux et de faciliter leur

communication avec les adresses MAC.

Il intervient au niveau de la couche 2 du modèle OSI.

Matériel B (type, rôle sur un réseau, couche du modèle OSI) ?

Même matériel que A.

Q.3.2

Tableau à remplir :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC | Adresse Réseau | 1ère @IP | Dernière @IP | @IP Diffusion |
| PC1 | 10.10.0.0/16 | 10.10.0.1 | 10.10.255.254 | 10.10.255.255 |
| PC2 | 10.11.0.0/16 | 10.11.0.1 | 10.11.255.254 | 10.11.255.255 |
| PC3 | 10.10.0.0/16 | 10.10.0.1 | 10.10.255.254 | 10.10.255.255 |
| PC4 | 10.10.0.0/16 | 10.10.0.1 | 10.10.255.254 | 10.10.255.255 |
| PC5 | 10.10.0.0/15 | 10.10.0.1 | 10.11.255.254 | 10.11.255.255 |

Q.3.3

Rôle de A pour un ping de PC1 vers PC3

* PC1 construit un paquet ICMP "echo request" et l'encapsule dans une trame Ethernet. L'adresse MAC destination de cette trame est l'adresse MAC de PC3, et l'adresse MAC source est celle de PC1
* Le switch A reçoit la trame sur l'un de ses ports. Il consulte sa table MAC pour trouver l'adresse MAC de PC3 (cette table associe les adresses MAC des appareils aux ports du switch sur lesquels ils sont connectés)
* Si le switch A trouve l'adresse MAC de PC3 dans sa table, il transmet la trame uniquement sur le port auquel PC3 est connecté. Sinon, il diffuse la trame sur tous les ports sauf celui d'origine.
* PC3 reçoit la trame, la désencapsule, traite la requête ping et envoie une réponse "echo reply" à PC1 en suivant le même chemin inverse.

Communication réussie ?

PC1 et PC3 ont la même adresse de réseau 10.10.0.0/16, ils sont donc sur le même réseau IP. Le matériel A va transmettre les trames d’un matériel vers un autre car un seul vlan 10.10.0.0/16 est configuré sur A, donc la communication a réussi.

Q.3.4

Rôle de B pour un ping de PC2 vers PC4

PC2 a l’adresse de réseau 10.11.0.0/16 et PC4 a l’adresse 10.10.0.0/16. Ils ne sont donc pas sur le même réseau. B est un commutateur (ou switch) et ne peut pas transmettre des paquets IP entre des hôtes de réseaux différents.

Donc B n’a aucun rôle dans cette communication.

Communication réussi ?

Non la communication échoue parce que les 2 machines ne sont pas sous le même réseau.

Q.3.5

Explication du résultat du ping de PC5 vers PC2

Pour PC5 (10.10.4.7) :

Adresse de réseau : 10.10.0.0/16

1ère adresse disponible : 10.10.0.1

Dernière adresse disponible : 10.11.255.254

Adresse de diffusion : 10.11.255.255

Pour PC2 (10.11.80.2) :

Adresse de réseau : 10.11.0.0/16

1ère adresse disponible : 10.11.0.1

Dernière adresse disponible : 10.11.255.254

Adresse de diffusion : 10.11.255.255

L’adresse IP de PC2 (10.11.80.2) fait partie de la plage d'adresse du réseau de PC5 (10.10.0.1 - 10.11.255.254). Donc les paquets « request » de PC5 parviennent au PC2 (même si le CIDR est différent).

L'adresse IP de PC5 (10.10.4.7) ne fait pas partie des adresses de la plage du réseau de PC2 (10.11.0.1 - 10.11.255.254). Donc pour PC2 l’adresse de PC5 ne fait pas partie de son réseau, d’où les paquets « reply » qui ne sont pas envoyé et le resultat : « icmp\_seq=1 timeout ».

Explication du résultat du ping de PC2 vers PC5

L'adresse IP de PC5 (10.10.4.7) ne fait pas partie des adresses de la plage du réseau de PC2 (10.11.0.1 - 10.11.255.254). Donc pour PC2 l’adresse de PC5 ne fait pas partie de son réseau.

Si aucune passerelle n’a été configurée sur PC2, le ping retourn « No gateway found ».

Q.3.6

Matériel C et D (type, rôle sur un réseau, couche du modèle OSI) ?

Ce sont des routeurs.

Le rôle d’un routeur est de faire communiquer des réseaux différents entre-eux. Les PC du réseaux 10.10.0.0/16 peuvent communiquer avec les machines des autres réseaux. Il se sert des adresses IP et intervient au niveau de la couche 3 du modèle OSI.

Q.3.7

Moyen de PC3 pour sortir du réseau ?

PC3 va utiliser sa passerelle par défaut.

Matériel du réseau servant à cette tâche ?

Le routeur C, et plus spécifiquement l’interface g2/0 qui a l’adresse IP 10.10.255.254.

Q.3.8

Le matériel servant à PC3 sert aussi pour tous les autres PC du réseau ?

Tout les PC sauf PC2 qui a l’adresse IP 10.11.80.2 avec l’adresse de réseau 10.11.0.0/16, et donc qui n’est pas dans le même réseau que celui de l’interface g2/0 du routeur C.

Q.3.9

Pour le matériel C, pour le label « g1/0 », Que signifie le « g » ?

Le « g » indique que l’interface réseau est en Gigabit, ou Gigabit Ethernet.

Le « 1 » ?

Dans « g1/0 » le « 1 » correspond au numéro du module (ou slot). La numérotation commence à 0, donc « g1/0 » indique que l’on est sur le 2ème module.

Le « 0 » ?

Dans « g1/0 » le « 0 » correspond au numéro de l’interface réseau du module correspondant, soit le port. La numérotation commence à 0, donc « g1/0 » indique que l’on est sur le 1er port.

Q.3.10

Ligne de commande ?

Il faut configurer une règle de routage, soit sur le routeur C : « ip route 172.16.5.0 255.255.255.0 10.12.2.253 ». Cela indique au routeur que les paquets à destination du réseau 172.16.5.0/24 doivent passer par la passerelle 10.12.2.253.

Périmètre de la commande ?

Cette commande est effective au niveau du routeur C et pas d’une interface réseau en particulier.

Q.3.11

Tableau à remplir :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Emplacement sur le réseau | Adresse MAC destination | Adresse MAC source | @IP Source | @IP Destination |
| Entre PC1 et A | CA:01:DA:D2:00:08 | 00:50:79:66:68:00 | 10.10.4.1 | 172.16.5.x |
| Entre B et C | CA:01:DA:D2:00:08 | 00:50:79:66:68:00 | 10.10.4.1 | 172.16.5.x |
| Entre C et D | CA:03:9E:EF:00:38 | CA:01:DA:D2:00:1C | 10.10.4.1 | 172.16.5.x |
| Après D | xx:xx:xx:xx:xx:xx | CA:03:9E:EF:00:54 | 10.10.4.1 | 172.16.5.x |

1. Mise en pratique

FICHIER FILE1

Q.3.12

Ethertype du protocole encapsulé ?

L’Ethertype du protocole encapsulé dans le paquet N°1 est 0x806.

Nom et rôle du protocole encapsulé ?

Ce code correspond au protocole ARP (Address Resolution Protocol).

Il est utilisé pour résoudre les adresses IP en adresses MAC.

Lorsqu’un appareil souhaite communiquer avec un autre appareil sur le même réseau local, il connait l’adresse IP de destination, mais pas son adresse MAC. ARP permet de découvrir cette adresse MAC.

Q.3.13

Utilité de la communication ?

Elle sert à résoudre les adresses IP en adresses MAC.

Q.3.14

Nom du matériel répondant ?

Le matériel qui répond est PC1.

Justification ?

Sur la paquet N°1, Le matériel qui a l’adresse MAC 00:50:79:66:68:04, soit PC5, envoie une trame broadcast pour demander qui a l’adresse IP 10.10.4.1.

Sur le paquet N°2, le matériel qui a l’adresse MAC 00 :50 :79 :66 :68 :00 indique que c’est lui, donc ici PC1.

Q.3.15

Emplacement de la capture ?

Entre PC1 et PC5.

Justification ?

On voit les adresses IP des 2 PC dans les paquets avec le protocole ICMP. On n’a pas assez d’information sur la capture pour être plus précis.

FICHIER FILE2

Q.3.16

Protocoles encapsulés ?

Les protocoles encapsulés sont l’IPv4 et l’ICMP.

Q.3.17

Matériel source ?

Sur le paquet N°1, le « ping request », la source a l’adresse IP 172.16.5.253 et on voit une adresse MAC CA:03:9E:EF:00:38.

L’adresse IP correspond à un matériel du réseau 172.16.5.0/24. Donc le ping a été fait d’une machine du réseau 172.16.5.0/24.

Matériel Destination ?

Sur le paquet N°1, le « ping request », la destination a l’adresse IP 10.12.2.254 et on voit une adresse MAC CA:01:DA:D2:00:1C.

L’adresse IP correspond à l’interface g1/0 du routeur C. Donc le ping est à destination de cette interface.

Réussite de la communication (justification) ?

Il y a un « ping reply » donc la communication a réussi.

Q.3.18

Emplacement de la capture ?

La capture a été faite entre les routeurs C et D.

Justification ?

L’adresse MAC source est CA:03:9E:EF:00:38, qui est l’interface g2/0 du routeur D, et l’adresse MAC destination est CA:01:DA:D2:00:1C qui est celle de l’interface g1/0 du routeur C.

FICHIER FILE3

Q.3.19

Détails de la capture.

Le matériel qui a l’adresse MAC 00:50:79:66:68:01, soit PC2, envoie une trame ARP broadcast pour demander qui a l’adresse IP 10.11.80.200.

Q.3.20

Réussite de la communication (justification) ?

Non car aucun matériel n’a l’adresse IP 10.11.80.200 sur le réseau.

Q.3.21

Emplacement de la capture ?

Non, la capture n’a pas été faite entre C et D mais entre PC2 et C.

Justification ?

La source est PC2 et les trames vont s’arrêter à la passerelle, donc à l’interface g2/0 de C.