الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 Guelma

Faculté des Sciences et de la Technologie
Département d'électronique et Télécommunications

Support de TPs : Pour Master 1 Réseaux et Télécommunications
(Semestre 02 Unité d'enseignement UEM 1.2)

Série de TP de la Matière :
TP Administration des services réseaux

Chargé de TD de la Matière :
Dr. IKNI Samir

Version récente (2019/2020)

TP 01 : Environnement d'administration
- Mise en place du service DNS -

Matériel et Logiciels utilisés :

- Ordinateurs équipés de cartes réseaux avec TCP/IP bien installés sur windows.
- Câbles réseaux droits
- Switch (commutateur)
- Liaison Internet
- Logiciel sniffer (WireShark)

Objectif du TP :

Dans ce TP on va essayer de voir le fonctionnement du service DNS en passant par le protocole ARP (Address Resolution Protocole) par le biais des commandes MSDOS puis par le logiciel d'analyse de trame WireShark, afin de comprendre le fonctionnement du serveur de noms DNS et les différents trames échangées.

Partie théorique :

I. L'ARP (Address Resolution Protocol)

Le format de la trame Ethernet est le suivant : (entre parenthèses est indiqué le nombre d'octets des champs) :

Préambule (7) + marqueur début (1)	Destination @ (6)	Source @ (6)	Type (2)	**Data (46-1500)**	CRC (4)

Figure 1 : Structure d'une trame Ethernet

Après avoir installé le réseau la première fois, chaque machine doit savoir les adresses MAC des autres postes, donc elle lance une trame (requête) ARP par une adresse de diffusion afin de savoir leurs adresses MAC qui correspondent aux adresses IP.

Pour voir le fonctionnement du protocole ARP, vous pouvez lancez sur la fenêtre de commande DOS (cmd) : « **arp –a »** pour afficher le cache ARP.

Repérer la correspondance IP-MAC dans le tableau suivant :

N° : Poste	**Adresse IP**	**Adresse MAC**

Vider le cache ARP par la commande suivante (ouvrir la 'cmd' en tant qu'administrateur) :

- ✓ **arp –d**

Vérifier « rapidement » par **arp –a,** puis revérifier une deuxième fois, qu'est ce que vous constatez ? …….

……

Lancer la capture de trames sur le logiciel **wireshark**, vider le cache ARP puis faites arrêter la capture des trames.

1. Repérez la requête ARP diffusée, commenter la colonne 'info' de cette trame :

   ……

   ……
2. Combien de couche y a-t-il dans cette trame ? ……..
3. Dans quelle couche le protocole ARP est encapsulé ? ……
4. Est-ce qu'il dépend du protocole IP ou non ? …….
5. Relever les valeurs des champs suivants de cette trame ARP :
   - @MAC src : ……
   - @MAC dest :……
   - @IP src : …….
   - @IP dest :…….
6. Relever les valeurs des champs suivants d'une des réponses sur cette trame :
   - @MAC src : ……
   - @MAC dest :……
   - @IP src : …….
   - @IP dest :…….
7. Faites une conclusion.

II. Le DNS (Domain Name System)

Le DNS joue un rôle essentiel dans le succès d'Internet et du World Wide Web (w.w.w) puisqu'il sert de service de répertoire central pour les adresses réseau. Le réseau de serveurs DNS (également appelé serveurs de noms) **répartis dans le monde entier** garantit que les noms des différents utilisateurs du réseau et des applications réseau comme « ***example.org*** » soient détaillés dans les adresses IP qui se basent sur des chiffres lisibles par les ordinateurs et les routeurs. Ceci permet d'être toujours sûr d'atteindre le bon ordinateur ou le site Web désiré, même sans connaissance de l'IP réelle. Pour ce faire, un échange d'un certain nombre de trames est établi entre une machine cliente qui tente d'accéder sur un site web, et un serveur DNS, comme l'illustre la figure 2 :

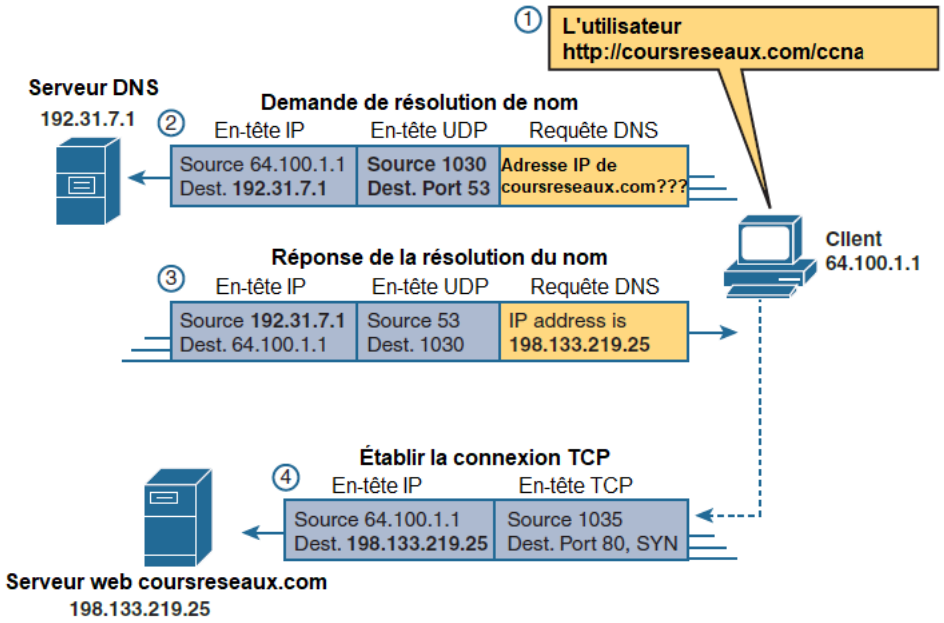


Figure 2 : Echange de trames entre un client et un serveur DNS

La commande « **nslookup** » (Name System Look Up) est un outil utile pour voir le fonctionnement du DNS. Suivez les étapes suivantes :

- Tapez : ***nslookup*** dans la fenêtre cmd.
- Notez l'adresse IP et le nom du serveur DNS de votre réseau :

  Serveur par défaut : ……..

  Adresse : …….
- Tapez maintenant : **ietf.org.**
  - Notez les adresses IPv4 et IPv6 de ce site.

  ……..

  ……..

- L'information est venue d'un serveur DNS d'autorité de ce site ou non ?

……

- Utilisez **« Ipconfig /flushdns »** pour vider le cache DNS de votre Hôte.
- Faire une requête **ping** vers le site web : **ietf.org** .
  - Interprétez le résultat.

    ……
  - Notez l'adresse IP de ce site web :……..
- Tapez maintenant **« Ipconfig /displaydns »** pour afficher le contenu de la cache DNS, qu'observez-vous ? ……
- Effacer de nouveau le contenu de la cache DNS.
- Ouvrez votre « browser » du navigateur et videz-le par « effacer les données de navigation ».
- Ouvrir le logiciel **Wireshark** et faites entrer (**host votre_@IP**) comme filtre pour ne pas capturer que du trafic vers ou de votre machine, lancer la capture.
- Avec votre navigateur, visitez le site : www.ietf.org , puis arrêtez la capture de paquets juste après l'ouverture de sa page.

Questions:

1. L'adresse du DNS est-t-elle modifiable ? comment ?
2. Localisez la trame "DNS query" et sa réponse "DNS query response". Sont-ils envoyés par UDP ou TCP ?
3. Où se situe le service DNS dans la pile du modèle TCP/IP ?
4. Quel est le port de destination pour le message "DNS query" ? quel est le port de source du message 'réponse DNS' ?
5. A quel adresse IP est envoyé le message "DNS query" ? utilisez « **ipconfig /all »**[(1)] pour déterminer l'adresse IP de votre serveur DNS local. Ces deux adresses IP sont-elles les mêmes ?
6. Localisez le paquet "DNS query", de quel type est-il ?
7. Localisez le paquet 'réponse DNS', combien de réponses sont fournit ?
8. Faites une conclusion générale.

(1) : Essayez de voir l'aide de cette commande en tapant : « ipconfig / ?

TP2 : Service DHCP

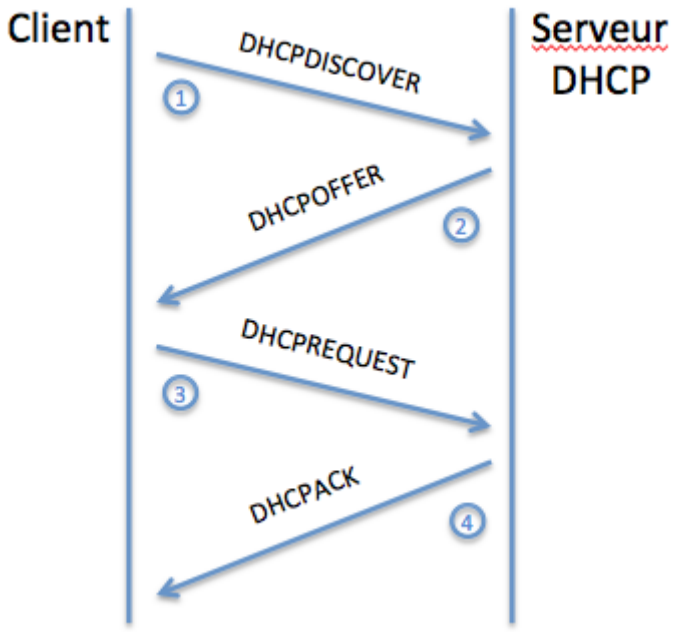
Partie Théorique :

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).

La trame permettant de trouver un serveur DHCP est une trame "DHCPDISCOVER", comme c'est un broadcast, elle est envoyée à l'adresse MAC ff:ff:ff:ff:ff:ff.

Une fois que notre serveur DHCP reçoit le DHCPDISCOVER, il va renvoyer une proposition, c'est un DHCPOFFER. Il va proposer une adresse IP, un masque ainsi qu'une passerelle par défaut et parfois un serveur DNS.

Le client (votre machine) répond par un DHCPREQUEST. Celui-ci est aussi envoyé en broadcast et sert à prévenir quelle offre est acceptée. Le serveur DHCP dont l'offre a été acceptée valide la demande et envoie un DHCPACK qui valide l'allocation du bail.



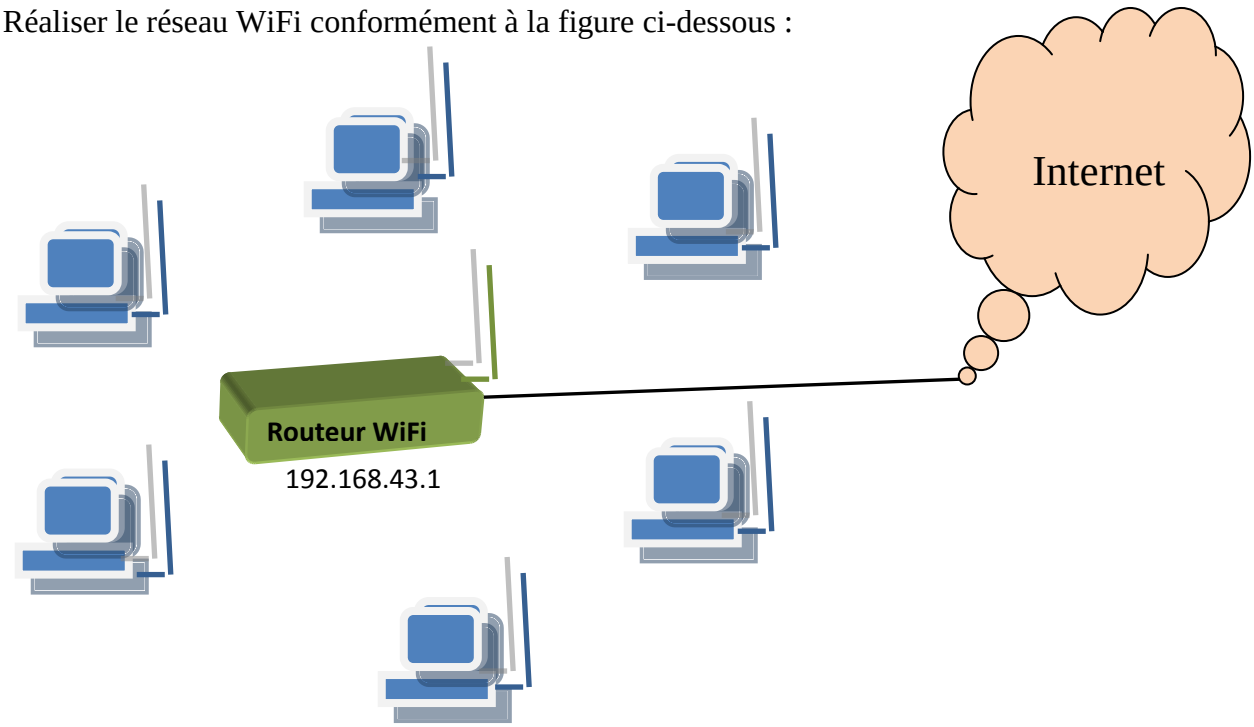
Toutefois, lors d'un renouvellement, notre machine ne va pas refaire toute la procédure en commençant par un DHCPDISCOVER. On repart directement du DHCPREQUEST. Les serveurs DHCP conservent en mémoire les adresses qu'ils ont distribuées, associées aux adresses MAC. Ainsi, vous constatez que vous conservez parfois très longtemps la même adresse IP, même si votre bail a sûrement été renouvelé plusieurs fois.

Il existe plusieurs autres types de paquets DHCP susceptibles d'être émis soit par le client pour le ou les serveurs, soit par le serveur vers un client :

- DHCPNAK (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
- DHCPDECLINE (le client annonce au serveur que l'adresse est déjà utilisée)
- DHCPRELEASE (le client libère son adresse IP)
- DHCPINFORM (le client demande des paramètres locaux, il a déjà son adresse IP

Partie Pratique :

Réaliser le réseau WiFi conformément à la figure ci-dessous :



Mettre les paramètres de la configuration réseau sur le mode automatique.

ARP :

Afficher le contenu de votre table ARP ?

Déterminer l'adresse MAC du routeur WiFi ?

Faire un ping vers www.yahoo.fr, afficher le contenu de la cache ARP, y a-t-il une entrée qui concerne l'adresse IP de yahoo.fr ? Expliquer ?

DHCP :

- ✓ **Commande ipconfig/all**

Quel est l'adresse IP attribuée par le serveur DHCP à votre machine ?

A partir des renseignements obtenus à l'aide de la commande ipconfig /all, renseignez les éléments ci-dessous :

Adresse physique : ……..

DHCP activé : ……..

Adresse IPv4 : …….

Masque de sous-réseau : …….

Bail obtenu : ……

Bail expirant : …….

Passerelle par défaut : ……..

Serveur DHCP : ……

Serveur DNS : ……

- ✓ **Commande ipconfig /release**

Commentez le résultat de cette commande ?

A partir des renseignements obtenus à l'aide de la commande ipconfig /release, renseignez les éléments ci-dessous :

Adresse IPv4 :……..

Masque de sous-réseau : ……..

Passerelle par défaut : ……..

- ✓ **Commande ipconfig /renew**

Commentez le résultat de cette commande ?

A partir des renseignements obtenus à l'aide de la commande ipconfig /renew, renseignez les éléments ci-dessous :

Adresse IPv4 :……..

Masque de sous-réseau : ……..

Passerelle par défaut : ……..

- ✓ **Commande netstat –an**

A partir des renseignements obtenus à l'aide de la commande « netstat –an », indiquez quel port UDP a été réservé par le client DHCP pendant l'échange client / serveur :

Quel est le socket identifiant le processus client ?

Etude de la trame DHCP DISCOVER :

Déconnectez-vous (en désactivant le WiFi), lancez une capture wireshark, activez le WiFi puis arrêtez la capture.

Sélectionnez la section Ethernet (entête de trame) correspondant à la trame DHCP et identifiez les adresses MAC source et destination :

Adresse mac source :……..

Adresse mac de destination :…….

Quel est le champ qui suit immédiatement les deux adresses MAC ?

Quelle valeur contient-il ? Que signifie-t-elle ?

Quels sont les protocoles inclus dans cette trame ?

Quel est le champ de l'en-tête IP permettant de connaître le protocole de transport des messages DHCP ?

Quel est le protocole utiliser dans la couche 3 et le numéro de port ?

Quel est le port UDP utilisé par le client DHCP ?

Quel est le port UDP utilisé par le serveur DHCP pour écouter et recevoir la requête du client?

Commentez les deux trames ARP : requête et sa réponse.

Faites une conclusion du TP.

TP3 : Service DNS

Partie Théorique :

Le DNS permet de retrouver l'adresse d'un serveur à partir de son nom, càd qu'il fait la conversion des adresses URL taper par l'utilisateur sur le navigateur web, en des adresses IP utilisables par les routeurs.

Supposons que vous voulez consulter un site web résident su une machine dont l'FQDN (Fully Qualified Domain Name) est www.monsiteweb.com .

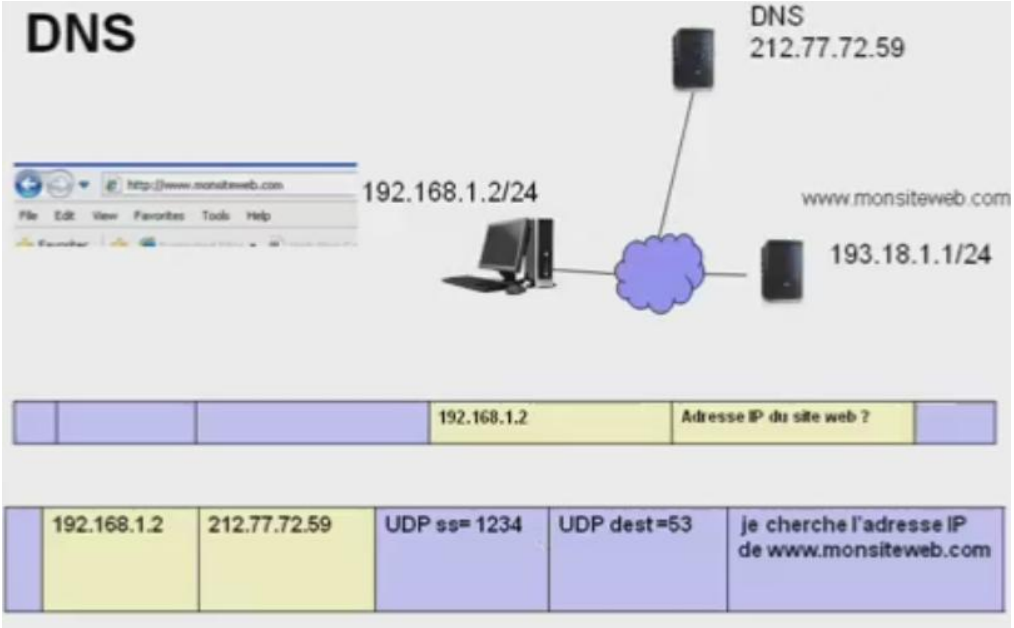


Figure : Requête DNS

Pour cela il faut interroger le DNS local qui est déjà affecté à votre carte réseau que ce soit manuellement ou à partir d'un serveur DHCP. Donc un paquet UDP sera formé qui va prendre le port DNS de destination = 53 et l'adresse IP de destination du DNS qui est bien 212.77.72.59 (voir la figure ci-dessus).

Le serveur DNS local vous renvoie donc l'adresse IP du serveur ou du site web que vous cherchez qui est donc : 193.18.1.1/24 (voir la figure ci-dessus).

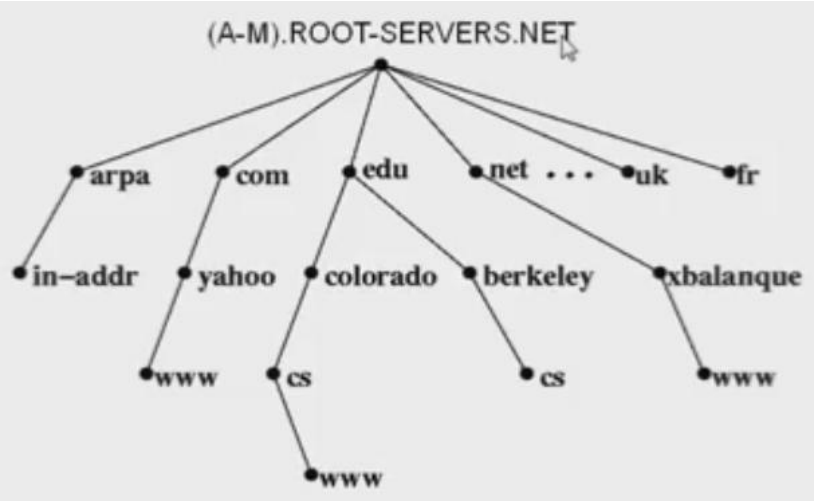
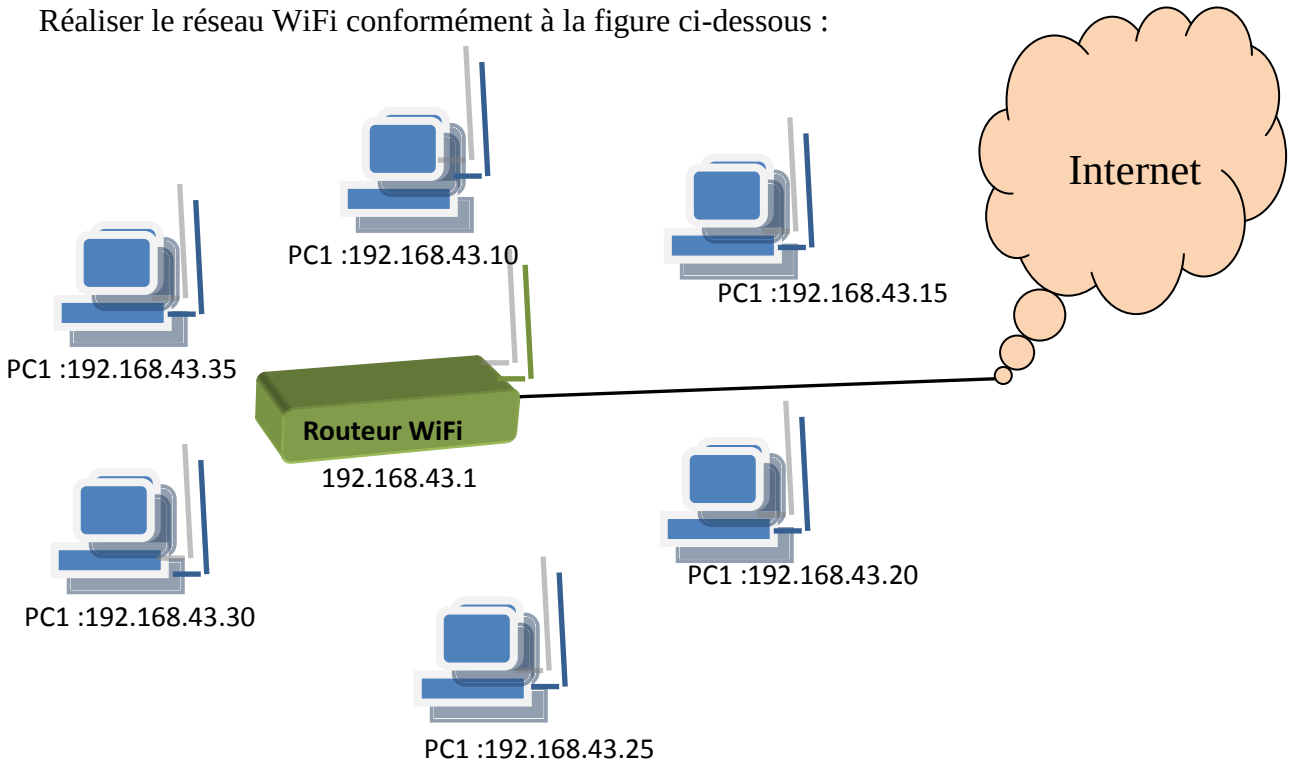


Figure : Architecture DNS

Si le serveur DNS local ne dispose pas de cette adresse demandé, il doit interroger le serveur DNS de la racine, (ils sont au nombre de 13 trouvés dans la page ftp://ftp.rs.internic.net/domain/named.root) qui va à son tour le diriger vers un serveur DNS TLD responsable du ***domaine*** voulu, qui à son tour va lui diriger vers un serveur autoritaire approprié qui va lui fournir l'adresse IP de la machine ou site web voulu (voir figure ci-dessus).

Partie Pratique :

Réaliser le réseau WiFi conformément à la figure ci-dessous :



Questions

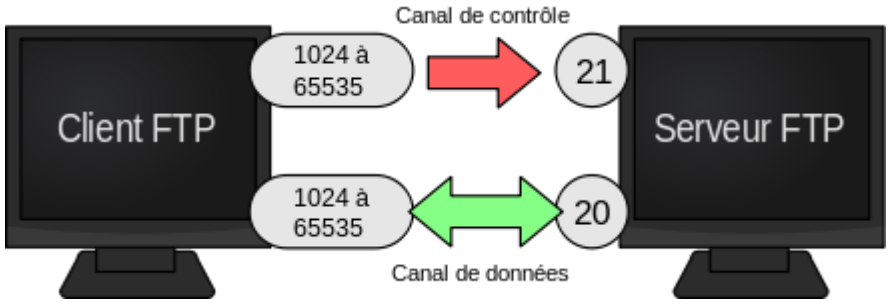
1. Trouver l'adresse IP du serveur DNS local de votre carte réseau ?
2. Afficher le contenu de la cache DNS de votre PC ? Interpréter le résultat ?
3. Faire ping sur www.univ-guelma.dz, interpréter le résultat. Noter l'adresse IP du site de l'université de guelma.
4. Effacer le contenu de la cache DNS de votre machine ? confirmer ?
5. Effacer l'adresse IP du serveur DNS au niveau de la carte réseau. Refaire un « ipconfig /all » puis un « ping » sur www.univ-guelma.dz et expliquer le résultat ?
6. Ouvrir le fichier « hosts » et ajouter l'enregistrement de www.univ-guelma.dz avec l'adresse IP trouvé précédemment. Refaire un ping et interpréter le résultat.
7. Comment fait-on pour afficher la page de www.yahoo.com en utilisant le URL : www.univ-guelma.dz
8. Effacer l'enregistrement www.univ-guelma.dz du fichier « Hosts », effacer le contenu de la cache DNS de votre machine, et reconfigure l'adresse DNS au niveau de votre carte réseau. Utiliser la commande « nslookup » pour trouver l'adresse IP de www.univ-guelma.dz. Est-ce que la réponse est autoritaire ?
9. Trouver l'adresse IP d'un serveur DNS root (voir la figure : Architecture DNS). Configurer cette adresse en tant que DNS de votre carte réseau. Faire « nslookup » sur le site www.yahoo.fr Interpréter ?
10. Faites une conclusion du TP.

TP 03 : Création, configuration et fonctionnement d'un serveur FTP

Partie Théorique :

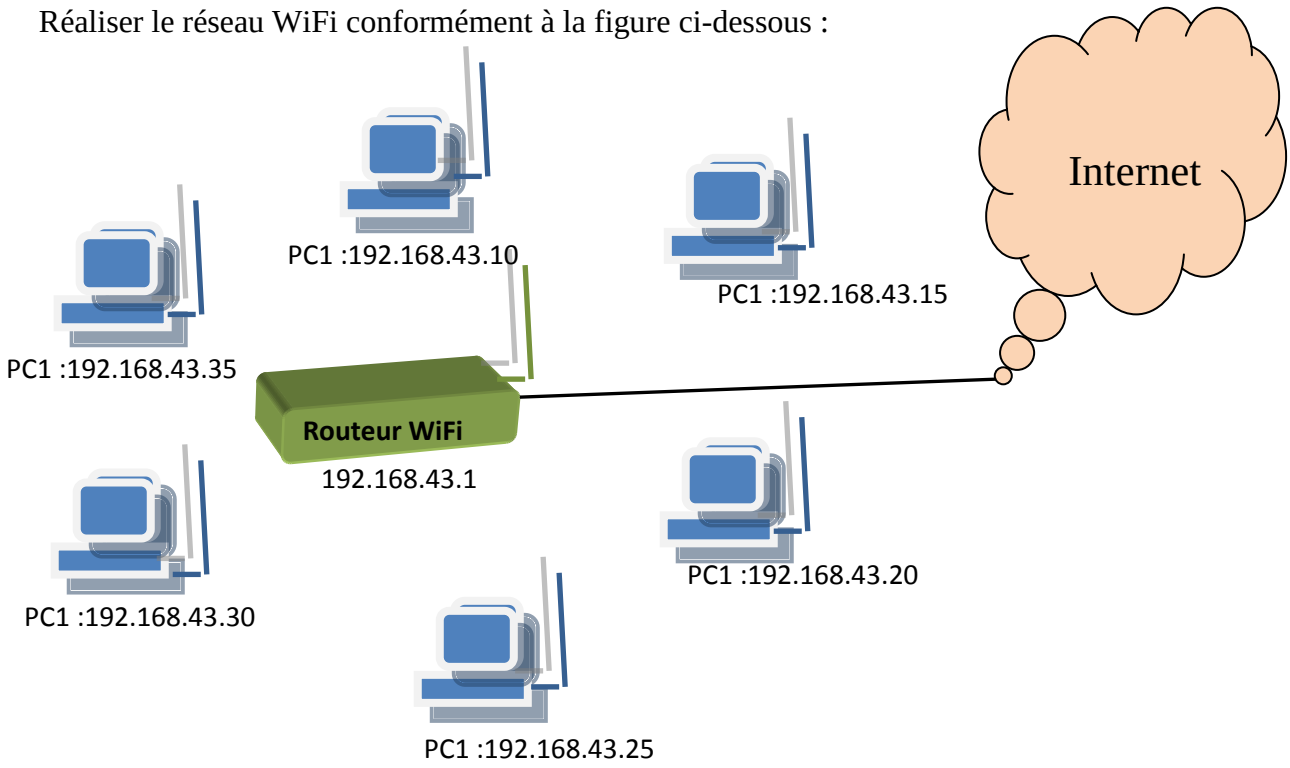
Le serveur FTP (File Transfer Protocol) permet, comme son nom l'indique, de transférer des fichiers par Internet ou par le biais d'un réseau informatique local (intranet).

Toute personne en ayant l'autorisation, peut télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur. Le port par défaut et le plus souvent utilisé est le port 21.



Partie Pratique :

Réaliser le réseau WiFi conformément à la figure ci-dessous :



1- Activation du service FTP sur windows :

Sur votre poste allez-vous au panneau de configuration/Programmes/Activer ou désactiver des fonctionnalités Windows.

Pour activer des serveurs FTP il faut cocher : Internet Information Services (IIs). Vérifiez que : Extensibilité FTP et Service FTP sont tout les deux bien cochés, ainsi que les Services World Wide Web.

Une fois le service FTP est activer, allez-vous sur : panneau de configuration/Système et sécurité/Outils d'administration et double-cliquez sur : Gestionnaire des services Internet (IIS).

A gauche : vous pouvez visualisez toutes les sites FTP que vous avez, pour le moment on ne voit qu'un site Web par défaut, à lequel on peut ajouter un site FTP.

Question : quelle est la relation entre les deux protocoles FTP et WWW ?

2- Création du dossier FTP et des utilisateurs authentiques :

Tout d'abord il faut créer un dossier (sur la partition D par exemple et vous l'appelez FTPdataX avec X=1,2,…6 selon votre poste) dans le quel on met les données FTP à partager. Pour tester créez un fichier texte dedans par exemple Bonjour.txt qui contient : Bonjour !.

Ainsi qu'il faut créer des utilisateurs pour leur donner accès à ce dossier lorsqu'ils se connectent à notre serveur FTP, ils peuvent donc voir les données partagées. Pour cela faites un clique droit sur « Computer » et vous choisissez « gérer »/utilisateurs et groupes locaux/utilisateurs. Créer un nouvel utilisateur (clic droit) et vous donnez un nom : FTPUserX (X=1,2,…6 selon votre poste).

Vous donnez et confirmer un mot de passe : 12345678 par exemple.

Il est recommander que vous cochez « L'utilisateur ne peut pas changer le mot de passe ».

Faites : « Créer » et « Fermer ».

Vous allez visualiser l'utilisateur ainsi créé.

Cet utilisateur doit avoir la permission de voir le dossier que nous venons de créer. Faites un clic droit sur le dossier/propriétes/sécurité/modifier/ajouter.

Dans « emplacement » choisissez votre ordinateur puisque c'est un utilisateur local. Puis entrez le nom de l'utilisateur que vous avez créez (FTPUserX) et cliquez sur « vérifier les noms », s'il le détecte cliquez sur « Ok ».

Autorisez l'utilisateur de faire :

- Lecture et exécution
- Affichage du contenu du dossier
- Lecture

Cliquez sur « appliquer », « Ok » et « Ok » de l'autre fenêtre.

Question : pourquoi doit-on créer des comptes utilisateurs authentique ?

3- Création du serveur FTP :

Maintenant nous somme prêts à créer notre site FTP, sur « IIS » double-cliquez par le bouton droit sur « Sites » et ajouter un site FTP, vous lui donnez un nom : FTPTLCX (X=1,2,…6 selon votre poste).

Sur chemin d'accès physique, indiquez le chemin de votre dossier (FTPdataX avec X=1,2,…6 selon votre poste).

Vous faites « suivant » et vous allez voir que le port FTP par défaut et « 21 », et pour l'adresse IP vous choisissez la votre (192.168.43.X : avec X=1,2,…6 selon votre poste).

Pour « SSL » (Secure Socket Layer) vous choisissez « pas de » : pas sécurité juste une démonstration pour faire le TP rapidement.

Pour l'authentification vaut mieux de choisir « de base » pour que les utilisateurs doivent s'authentifier par un mot de passe. Vous faites « suivant ».

Pour les utilisateurs vous choisissez « utilisateurs définis » et vous mettez le nom de l'utilisateur que vous avez créez. Pour l'autorisation choisissez « lecture » et vous faites « terminer ».

Vérifier que le site FTP a été créé et vérifiez aussi l'authentification et l'autorisation à droite. Ainsi que sur « liaison » (tout à fait à droite) vous pouvez modifier la configuration du site FTP

Une fois le serveur est créé il est recommander de le redémarrer (bouton à droite) pour ne pas avoir des problèmes.

Question : peut-on modifier le port 21 ? si oui pourquoi faire ?

4- Test de notre site FTP :

Allez vous sur le navigateur web (google chrome par exemple) et mettre l'adresse URL suivante : ftp://192.168.43.X:21

Vous rentrez « nom utilisateur » et « mot de passe » pour vous authentifier.

Pouvez-vous voir le fichier partagé « Bonjour.txt » et le lire ?

Test supplémentaire facultatif :

On peut également utiliser « cmd » pour tester les fonctionnalités FTP comme suit :

Tapez : telnet 192.168.43.X 21

Que constatez-vous ?

Autoriser le service FTP et son port sur firewall :

Allez vous sur : firewall de Windows/Paramètres avancés/Règles de trafic entrant et en bas vous activez toutes les règles du FTP.

(si vous modifiez le port 21 vous devez ajouter une nouvelle règle pour l'autoriser).

Sur cmd, tapez « ftp » ensuite : Open 192.168.43.X 21

Commentez le résultat ?

Faites entrer le user-name et le pass-word

Tapez : ls

Commentez le résultat ?

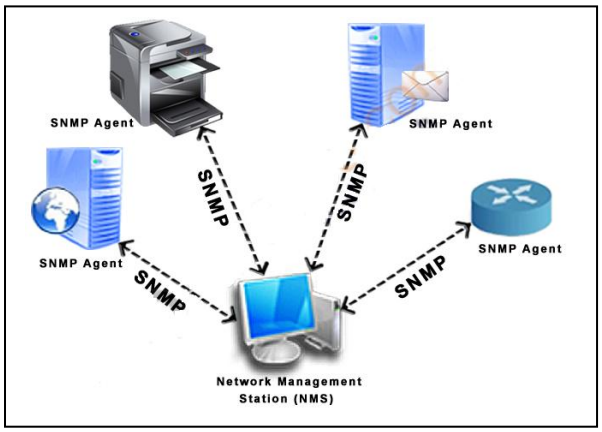
Faites des conclusions sur les 4 étapes de ce TP

TP5 : Administration à distance

(Protocole SNMP)

I. Introduction :

Simple Network Management Protocol (abrégé SNMP), en français « protocole simple de gestion de réseau », est un protocole de communication de la couche application, qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels ***<u>à distance</u>***. Il s'agit d'un protocole permettant de **collecter** et **d'organiser**, dans une base d'informations de gestion (**MIB**), des informations sur les périphériques gérés sur les réseaux IP *(Bp, température cpu, marche, arrêt ...etc)* et de manipuler ces informations à distance pour gérer les applications et le comportement des périphériques. Les périphériques qui prennent généralement en charge SNMP incluent les modems, les routeurs, les commutateurs, les serveurs (physiques ou virtuels), les stations de travail, les imprimantes, etc.

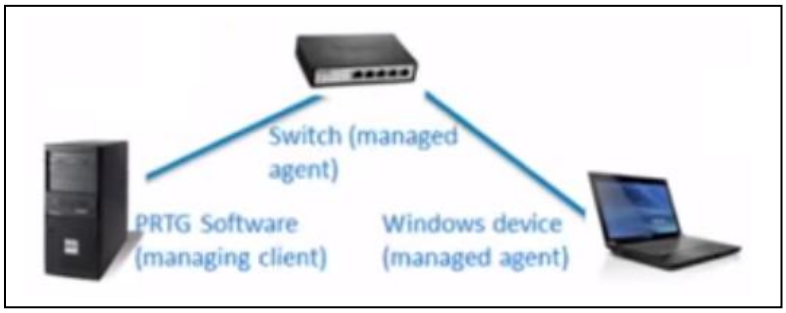


II. Principe du SNMP

Le système SNMP est basé sur trois éléments principaux : superviseur « manager », des agents et une base de données MIB. Dans la terminologie SNMP, le terme « manager » est plus souvent employé que superviseur. Le Manager est le serveur qui permet à l'administrateur réseau d'exécuter des requêtes de gestion (get request). Les agents sont des entités qui se trouvent au niveau de chaque interface, connectant au réseau l'équipement géré et permettant de récupérer des informations sur différents objets. SNMP permet le dialogue entre le manager et les agents afin de recueillir les informations souhaitées et les stocker dans une base de données MIB bien organisée.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc fondée sur quatre principaux éléments :

- les équipements gérés (managed devices) sont des éléments du réseau (commutateurs, routeurs ou serveurs), contenant des « objets de gestion » (managed objects) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- les agents, c'est-à-dire les applications SNMP de gestion de réseau installées sur un périphérique, sont chargés de transmettre les données locales de gestion du périphérique au format SNMP vers le Manager ;
- les systèmes de gestion de réseau (network management systems notés NMS), c'est-à-dire les consoles à travers lesquelles les administrateurs peuvent réaliser des tâches d'administration à partir du Manager. Dans la pratique, pour qu'un serveur devienne « Manager », il doit disposer d'un programme (exemple MRTG (Multi Router Traffic Grapher), PRTG (Paessler Router Traffic Grapher)).
- La base d'informations MIB dans laquelle les données sont structurées et organisées par un identificateur OID (Object ID). Les messages envoyés par un manager SNMP sont de type : Get, Get next, Set, Response, Inform, sur des paquet UDP avec numéro de port 161 ; et Trap (Interruption ou Alertes): avec numéro de port 162.



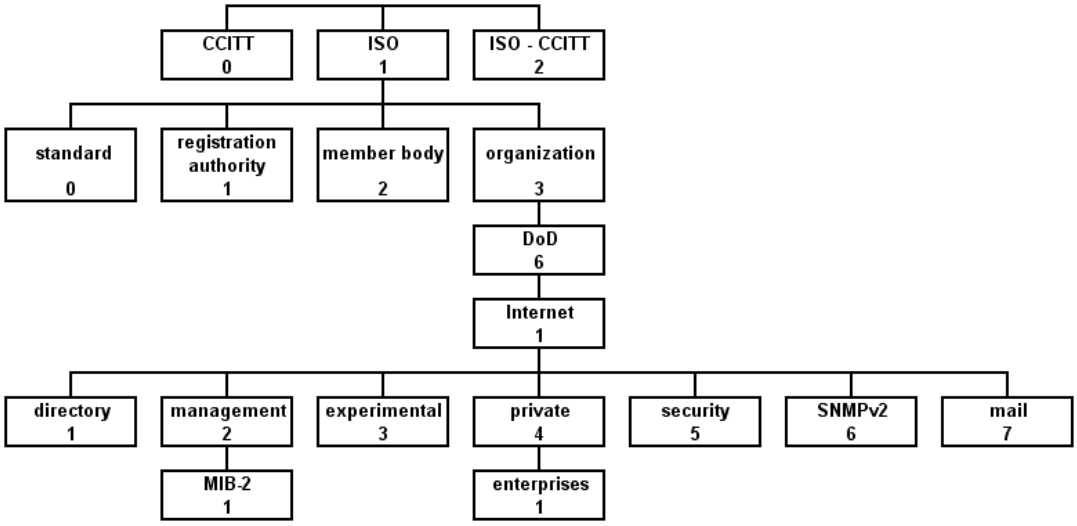
III. La base d'information de gestion MIB

Une MIB (management information base, base d'information pour la gestion du réseau) est un ensemble d'informations structuré sur une entité réseau, par exemple un routeur, un commutateur ou un serveur. Ces informations peuvent être récupérées, ou parfois modifiées, par un protocole comme SNMP.

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre. Chaque information a un Object IDentifier, une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

Par exemple, 1.3.6.1.2.1.2.2.1.2 est l'object identifier ***ifDescr*** qui est la chaîne de caractères décrivant une interface réseau (Ethernet0 sur un routeur Cisco).

Une des MIB les plus connues est MIB-II, décrite dans le RFC 1213, et qui est mise en œuvre dans quasiment tous les équipements TCP/IP. Elle compte dix groupes, "system", "interfaces" (dont fait partie ifDescr, citée plus haut), "Address Translation", "IP", "ICMP", "TCP", "UDP", "EGP", "transmission" et "SNMP". Chaque nœud est associé d'un numéro d'identification appelé OID (voir la figure ci-dessous).



ASN.1 (Abstract Syntax Notation One) est un standard international spécifiant une notation destinée à décrire des structures de données dans le secteur des télécommunications et des réseaux informatiques. Les MIB sont décrites en utilisant ASN.1.

Une MIB se présente comme une base de données normalisée, qui permettra de lire et d'écrire sur les équipements distants, de façon également normalisée. Ce sera à l'agent lui-même de faire l'interface entre les informations récupérables sur la plateforme où il est installé et le Manager SNMP.

Travail demandé
Répondre aux questions suivantes :

1. Quel est l'intérêt d'avoir un arbre de référence qui soit unique ?
2. Tous les objets de l'arbre de référence doivent ils être implémentés dans une MIB?
3. Quels sont les éléments qui définissent un objet géré ?
4. Le type ASN.1 de la valeur d'un objet géré a-t-il un rapport avec la référence de l'objet ?
5. Arbres et MIB : grâce aux arbres donnés en annexe,
    a. donner le nom des nœuds correspondant aux OID suivants
        i. 1.3.6.1.6

ii. 1.3.6.1.2.1.4.22.1.3

b. donner les OID des nœuds suivants :

i. ipAdEntBcastAddr

ii. CiscoIgrp

6. Quelle est l'information demandée par le manager au travers de la trame suivante ?

```
SNMP: len: 38 version: int(1) 0x00 comm: string(6) «public» type: GET-NEXT
req-id: int(2) 0x5e31 error: int(1) 0x00 error-index: int(1) 0x00
var: obj(8) 1 3 6 1 2 1 2 1 val: empty(0)
```

7. Quelle est la réponse transmise par l'agent ?

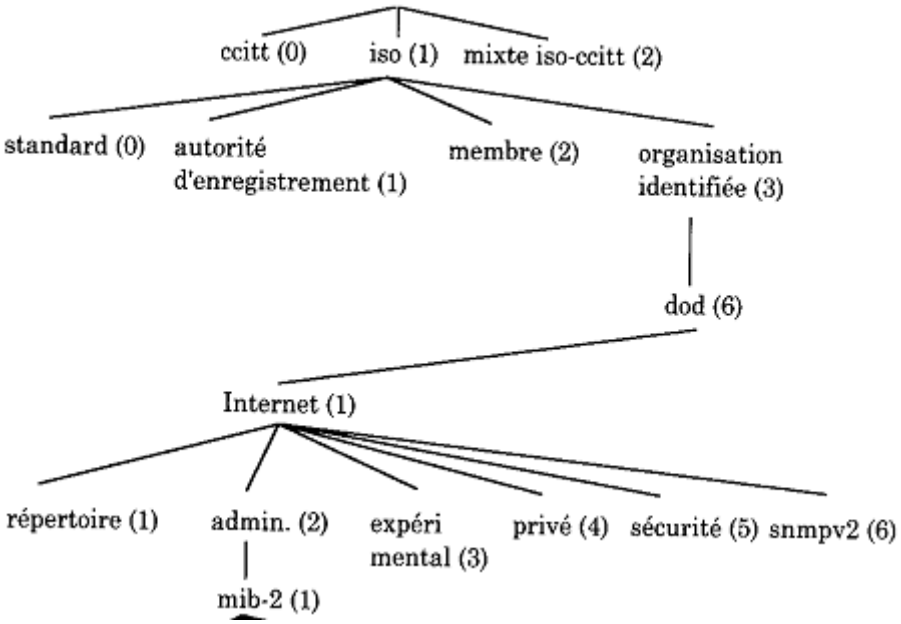
```
SNMP: len: 40 version: int(1) 0x00 comm: string(6) «public» type: RESPONSE
req-id: int(2) 0x5e31 error: int(1) 0x00 error-index: int(1) 0x00
var: obj(7) 1 3 6 1 2 1 2 1 0 val: 0x06
```

8. Même question pour cet échange :

```
SNMP: len: 178 version: int(1) 0x00 comm: string(6) «public» type: GET-NEXT
req-id: int(2) 0x00a2a2 error: int(1) 0x00 error-index: int(1) 0x00
var: obj(9) 1 3 6 1 2 1 2 2 1 1 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 2 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 3 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 4 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 5 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 6 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 7 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 8 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 9 val: empty(0)
var: obj(9) 1 3 6 1 2 1 2 2 1 10 val: empty(0)

SNMP: len: 219 version: int(1) 0x00 comm: string(6) «public» type: RESPONSE
req-id: int(2) 0x00a2a2 error: int(1) 0x00 error-index: int(1) 0x00
var: obj(10) 1 3 6 1 2 1 2 2 1 1 1 val: int(1) 0x01
var: obj(10) 1 3 6 1 2 1 2 2 1 2 1 val: string(9) «Ethernet0»
var: obj(10) 1 3 6 1 2 1 2 2 1 3 1 val: int(1) 0x06
var: obj(10) 1 3 6 1 2 1 2 2 1 4 1 val: int(2) 0x05dc
var: obj(10) 1 3 6 1 2 1 2 2 1 5 1 val: gauge(4) 0x00989680
var: obj(10) 1 3 6 1 2 1 2 2 1 6 1 val: string(6) ******
var: obj(10) 1 3 6 1 2 1 2 2 1 7 1 val: int(1) 0x01
var: obj(10) 1 3 6 1 2 1 2 2 1 8 1 val: int(1) 0x01
var: obj(10) 1 3 6 1 2 1 2 2 1 9 1 val: time(2) 0x0420
var: obj(10) 1 3 6 1 2 1 2 2 1 10 1 val: counter(4) 0x6b055aa0
```

Annexes


ccitt (0)
iso (1)
mixte iso-ccitt (2)
standard (0)
autorité d'enregistrement (1)
membre (2)
organisation identifiée (3)
dod (6)
Internet (1)
répertoire (1)
admin. (2)
expéri mental (3)
privé (4)
sécurité (5)
snmpv2 (6)
mib-2 (1)

MIB II (1)	Système (1)				
	Interface (2)				
	Ip (4)	ipForwarding (1)	Forwarding (1)		
			Not-forwarding (2)		
		IpDefaultTTL (2)			
		ipInReceives (3)			
		IpInHdrErrors (4)			
		ipInAddrErrors (5)			
		ipForwDatagrams (6)			
		ipInUnknownProtos (7)			
		ipInDiscards (8)			
		ipInDelivers (9)			
		ipOutRequests (10)			
		ipOutDiscards (11)			
		ipOutNoRoutes (12)			
		ipReasmTimeout (13)			
		ipReasmReqds (14)			
		ipReasmOKs (15)			
		ipReasmFails (16)			
		ipFragOKs (17)			
		IpFragFails (18)			
		ipFragCreates (19)	IpAddrEntry (1)	IpAdEntAddr (1)	
				IpAdEntIfIndex (2)	
				IpAdEntNetMask (3)	
				ipAdEntBcastAddr (4)	
				IpAdEntReasmMaxSize (5)	
		ipAddrTable (20)			
		IpRoutingTable (21)	ipRouteEntry (1)	IpRouteDest (1)	
				IpRouteIfIndex (2)	
				ipRouteMetric1(3)	
				ipRouteMetric2 (4)	
				ipRouteMetric3 (5)	
				ipRouteMetric4 (6)	
				ipRouteNextHop (7)	
				ipRouteType (8)	Other (1)
					Invalid (2)
					Direct (3)
					Remote (4)
				ipRouteProto (9)	Other (1)
					Local (2)
					Netmgmt (3)
					Icmp (4)
					Egp (5)
					Ggp (6)
					Hello (7)
					Rip (8)
					Is-is (9)
					Es-is (10)
					CiscoIgrp (11)
					BbnSpfIgp (12)
					Ospf (13)
					Bgp (14)
				ipRouteAge (10)	
				ipRouteMask (11)	
		IpNetToMediaTable (22)	IpNetToMediaEntry (1)	IpNetToMediaIfIndex (1)	
				IpNetToMediaPhysAddress (2)	
				IpNetToMediaNetAddress (3)	
				IpNetToMediaType (4)	

	Icmp (5)
	Tcp (6)
	Udp (7)
	Egp (8)
	Transmission (10)
	Exemple (11)

TP7 : Service de messagerie
(Protocole SMTP)

Objectif du TP :

- Comprendre le fonctionnement d'un serveur de messagerie ;
- Etudier les protocoles SMTP, POP et IMAP.

Pré-requis :

- Architecture client/serveur de messagerie ;
- TCP-IP, protocoles SMTP, POP et IMAP.

A. Installation de postfix :

Le logiciel libre ***Postfix*** est un gestionnaire de messagerie simple à configurer et conçu pour une sécurité optimale. De plus il est peu gourmand en ressources système et constitue donc une véritable alternative à Sendmail. Postfix est un logiciel de messagerie au standard SMTP. Il est modulaire et préconfiguré pour une utilisation classique.

*Il existe de la documentation sur **postfix** en français : http://x.guimard.free.fr/postfix*

1. Installez le paquetage ***postfix*** et ses dépendances. Choisir "Site Internet" lors de l'installation et valider les options par
défaut.

2. Relever les derniers messages de l'installation : identifiez le fichier de configuration du service, la commande pour afficher les options de configuration et le script de démarrage.

3. Quelle sont les valeurs et les significations des variables ***mydestination, mynetworks***, ***inet_interfaces*** et ***relayhost*** ?

B. Test de la configuration du serveur SMTP :

1. Créez sur la machine Linux deux comptes utilisateur pour les tests, ***user1*** et ***user2*** par exemple, avec un répertoire de travail et un mot de passe pour chacun des utilisateurs.

2. Ouvrez dans un deuxième terminal une session sous le compte ***user1 (su user1)*** afin de réaliser un envoi de mail pour ***user2***.

La commande ***mail*** permet de gérer en ligne de commande votre courrier. Envoyer un courrier à user2 : ***mail user2@localhost.localdomain***, terminer le message en tapant "ctrl D " ou un point sur une nouvelle ligne.

3. Ouvrez dans un troisième terminal une session sous le compte ***user2*** et **v**érifiez que user2 à bien reçu le message : Pour lire son courrier : ***mail*** pour entrer dans le gestionnaire de courrier (***quit*** pour en sortir), puis le numéro du message.

Autres commandes dans le manuel : ***man mail*** *ou http://www.chez.com/bsdlibre/man1/mail.1.html*

4. Où le message est-il stocké avant et après sa lecture par ***user2*** ? Le message est-il effacé du serveur après lecture ?

5. Commentez les différents champs de l'en-tête du message.

6. Quel protocole a été utilisé pour relever le courrier. Nécessite-t-il une authentification ?

7. Relever la trace du transfert dans les fichiers de logs qui se situent dans ***/var/log***/. On y trouve les erreurs (***mail.err***), des informations (***mail.info***) et des avertissements (***mail.warn***). Commentez les traces correspondant au dernier mail.

C. Etude du protocole SMTP :

On utilisera la commande *netcat(nc)* pour faire des requêtes via une socket (on pourrait également utiliser *Telnet* sur le port 25).

1. A partir d'un client en ligne de commande sous le compte ***user1***, connectez-vous au serveur :

nc localhost 25

2. Vous devez ensuite taper la succession de commandes SMTP permettant d'identifier votre machine (**EHLO**), de fournir l'email de l'expéditeur (**MAIL from**), celui du destinataire (**RCPT to**), le sujet et le corps du message (**DATA**).

3. Donnez en les commentant la succession de commandes et de codes de retour pour envoyer un message de ***user1*** vers ***user2***.

4. Quels sont les programmes client (MUA) et serveur (MTA) locaux entre lesquels sont échangées ces commandes et ces réponses ?

D. Installation du serveur POP3 :

1. Pour relever sa boite aux lettres sur une machine autre que le serveur de courrier il faut installer un serveur POP. Installez le package ***courier-pop***.

2. La commande ***netstat –at*** permet de visualiser les ports ouverts. Vérifier la présence du *daemon* POP3.

3. Pour l'utilisation de POP il faut que les messages de l'utilisateur soient stockés dans son répertoire de travail. Ajouter la variable ***home_mailbox = Maildir/*** dans le fichier de configuration ***/etc/postfix/main.cf*** et relancer le daemon (pour des distributions Debian, il est nécessaire de désactiver ***mailbox_command = procmail -a "$EXTENSION"*** dans ***main.cf***).

4. Créer pour ***user1*** et ***user2*** un dossier ***Maildir*** dans leurs répertoires de travail avec la commande ***maildirmake Maildir***

E. Etude du protocole IMAP

1. Pour relever sa boite aux lettres sur une machine autre que le serveur de courrier avec des fonctionnalités avancées, il faut installer sur le serveur un serveur IMAP. Installez le package ***courier-imap***.

2. Vérifier la présence du démon IMAP avec ***netstat.***

3. Envoyez un nouveau mail de ***user1*** vers ***user2***.

4. A partir d'un client en ligne de commande sous le compte ***user2***, connectez-vous au serveur IMAP à l'aide de ***netcat***. Quel numéro de port devez-vous utiliser ?

5. Vous devez ensuite taper la succession de commandes IMAP permettant d'effectuer les mêmes opérations que pour POP3. Rappelons que chaque commande IMAP doit être précédée d'un identifiant unique (id1, id2…) au cas où plusieurs commandes arrivent en même temps. Quelques rappels sur les commandes IMAP sur : http://cri.univ-lyon2.fr/doc/ImapMaisCEstTresSimple.html

6. Donnez en les commentant la succession de commandes et de messages de retour pour les opérations de réception de courrier décrites précédemment.

7. IMAP permet de gérer des boites sur le serveur, quelle est la commande pour créer une boite ? Pour lister les boites ? Pour vider une boite ?

F. Analyse des messages

En utilisant vos comptes personnels de l'université ou privés, réalisez à l'aide de wireshark une capture lors de l'envoi de messages SMTP, lors de la réception de messages POP3 et lors de la réception de messages IMAP. Vous devrez pour cela configurer un client de messagerie ou utiliser votre client habituel (outlook, thunderbird…).

1. Comment sont encapsulés les messages ?

2. Quel sont les tailles des messages de contrôle ?

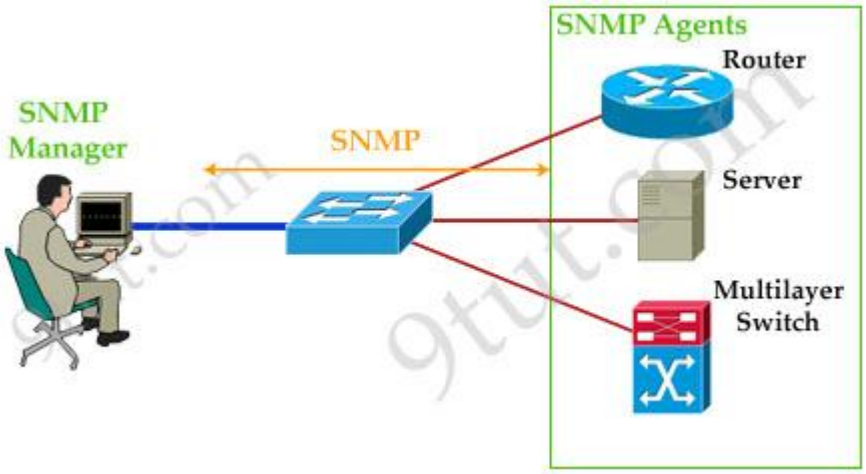
3. Quels sont les avantages d'IMAP sur POP ?

4. Qu'est-ce que le SMTP authentifié ? A quoi sert-il ?

TP N° : 04 : Fonctionnement du serveur SNMP

Partie théorique :

SNMP (Simple Network Management Protocol) est un protocole réseau permettant de gérer les réseaux TCP/IP. Sur Windows, le service SNMP (aussi appelé agent SNMP) fournit des informations d'état relatives à un hôte SNMP sur un réseau TCP/IP.



Les systèmes de gestion SNMP peuvent demander la personne à contacter, l'emplacement du système et les services réseau de cet ordinateur en envoyant une requête SNMP.

Une interruption SNMP est un message de notification d'événement envoyé par le Service d'interruption SNMP qui s'exécute sur un hôte SNMP. L'interruption SNMP est envoyée à d'autres hôtes SNMP ou à un système de gestion SNMP (Manager), aussi appelés destinations des interruptions. Les destinations des interruptions peuvent être spécifiées sous forme de noms d'hôtes ou d'adresses IP.

Partie pratique :

Activation des services SNMP sous Windows 7 :

De la même façon que FTP (TP 03), activez SNMP sous windows. Allez-vous sur :

Panneau de configuration\Système et sécurité\Outils d'administration\services.

Double-cliquez sur service SNMP, sur l'onglet « Agent » cochez toutes les cases de « service ».

Vérifier l'autorisation au niveau « Firewall ».

On va utiliser un logiciel qui s'appelle « SNMPb » qui nous permet de lancer de requêtes GET/SET SNMP, d'afficher la MIB d'un agent et pas mal de tâches suivant

le protocole SNMP. C'est un logiciel libre est gratuit. Il supporte à la fois le protocole SNMP dans ses versions 1, 2c et 3. Il permet de réaliser des requêtes SNMP GET/WALK/SET/TABLE. Il affiche la description des OIDs, peut importer des MIBs efficacement et effectuer des recherches dans des OIDs.

Tout d'abord, nous allons voir où le récupérer, puis l'installer et enfin son utilisation.

1. **Téléchargement de SNMPb**

SNMPB est disponible sur le site web de SourceForge. Pour le trouver, il suffit de faire une recherche avec le mot clé « SNMPb ».

2. **Description et utilisation du logiciel SNMPb**

Lancez le logiciel SNMPb.

SNMPb répartit les fonctionnalités principales en différents parties. La première partie et le menu standard. La deuxième partie correspond à l'agent qui sera interrogé. Ensuite, nous avons l'arbre des MIBs. On peut dérouler cette MIB en cliquant sur les différents OID. En faisant un clic droit sur un OID, on accède aux actions telles que le WALK ou le GET. En cliquant sur un OID, la vue du bas donne des informations sur celui-ci : le nom, l'oid complet, le type et surtout la description. En faisant un clic droit puis l'opération désirée, on obtient le résultat dans la vue de droite.

3. **Configuration de l'agent**

Pour paramétrer l'hôte à interroger, on clique sur le bouton en haut au milieu  . On rentre les paramètres généraux: **on laisse la configuration par défaut**.

- nom de l'équipement : localhost càd votre poste.
- adresse IP : 127.0.0.1,
- port SNMP : 161,
- les versions SNMP gérées : version 1 et 2.

Ensuite, en cliquant sur la gauche, on peut configurer :

- la communauté SNMP en lecture : public.
- la communauté SNMP en écriture : private.
- Confirmer avec « ok » et l'agent est configuré.

Remarque 1 : Il faut noter que pour configurer une version de SNMP, il faut avoir coché la case dans les paramètres généraux.

Requêtes simples avec SNMPb

Une fois l'agent configuré et les MIBs chargées, il est possible de dérouler l'arbre des MIBs et de faire des requêtes sur des OIDs. Pour cela, il vous suffit de cliquer sur

chaque noeud jusqu'à l'OID souhaité. Pour interroger un OID, il vous suffit de faire un click droit sur celui-ci et de choisir l'opération GET ou WALK.

Activité 1 :

1. En faisant un clic droit sur l'élément « system » de la MIB-2, lancez une requête de type « Walk ».
2. Notez les informations qui s'affichent sur le volet droit. Utilisez « Description » pour interpréter certaines informations.
3. Lancez une requête de type « Get » sur « sysName », Utilisez « Description » pour interpréter cette information.
4. Lancez une requête de type « Table view » sur « ipRoutTable », que vous constatez ?

Remarque 2 **:** vous pouvez lancer des recherches de mots clés par « find » pour rechercher une information qui vous intéresse.

4. Configuration des modules

Une fois l'agent SNMP à interroger correctement configuré, il est nécessaire d'indiquer à SNMPb quelles sont les MIBs à charger. SNMPb inclut quelques MIBs par défaut. Toutes ne sont pas chargées et toutes les MIBs existantes ne sont pas référencées.

Ensuite, il faut se rendre dans l'onglet « Modules » et sélectionner quelles sont les MIBs à charger en les faisant passer de la partie de gauche à la partie de droite.

Cliquer sur une MIB (à droite) pour obtenir des informations détaillées sur celle-ci.

Activité 2 :

1. Ajouter la MIB des imprimantes.
2. Vérifiez qu'elle est affichée sur l'arbre.
3. Notez quelques informations sur les imprimantes connectées ?
4. Lisez la description de l'OID et en faire sortir des informations et les notez.

Remarque 3 **:** éviter de charger touts les modules en même temps et de lancer des requêtes sur la racine. En effet, vous risquez de saturer l'agent ou le serveur SNMP et le réseau ou votre poste de travail.

Activité 3 : *Taux d'*occupation de la mémoire RAM

1. Le taux d'occupation d'une partition se trouve sur l'OID host/hrStorage. (Si la MIB de « host » n'existe pas ajoutez-la sur « Modules »)

2. Interprétez les différents OIDs qui se trouvent sous cette rubrique en lisant leurs « Description ».
3. Faites un clic droit sur l'OID « hrStorage Table » et lancez une requête « table View ». Commentez le résultat ?

Faites des conclusions sur les 2 activités précédentes

Remarque 4 : Si une MIB n'est pas disponible sur votre système vous pouvez la télécharger sur le site du constructeur ou sur un repository de MIBs.

http://www.snmplink.org

SNMP Ressouce/MIB puis MIB Repository : une série de sites qui vous proposent des MIB de différents constructeurs à télécherger et à stocker dans un répertoire qu'on doit indiquer dans **Options/Preferences**.