Labo 4 : Internetworking (90 min)

1	**Objectifs**

Connaître les indicateurs utiles (LEDs, valeur de paramètre) d'une interface Ethernet sous Vista
Etudier la gestion d'un commutateur ethernet Cisco 2950
Analyser des échanges (ping et traceroute) avec Wireshark
Etudier les outils TCPView, netstat et nslookup

2	**Poste de travail**

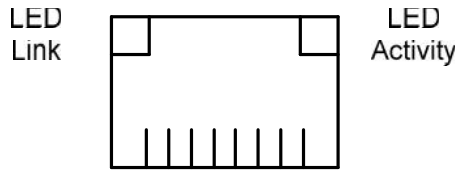
Objectif Ouvrir une session utilisateur Username=**ursula** password=**user**

Remarques Votre PC (Vista Enterprise), désigné par Dx (D1-D16), est situé dans l'intranet

Action *Start – Run…* - **`\\10.1.1.1\FilesTD\Labo409\Labo4`**
S'authentifier sur le serveur Username=**rpi** password=**rpi**
Conserver cette fenêtre de partage

3	**Interface ethernet**	**10'**

Objectif Comprendre les LEDs *(Light-Emitting Diode)* présentes sur le connecteur RJ45 du PC

Action	Observer ces 2 LEDs • Celle de gauche indique l'état de la liaison *(link)* • Celle de droite renseigne sur l'activité (émission réception)	

Objectif Utiliser les outils de configuration réseau de Vista

Remarque **Ne pas modifier la configuration réseau de votre PC afin de conserver une connexion réseau pour ce travail de labo**

Action Start – Settings - Networks Connections
Cliquer sur l'objet Local Area Network

Question 3a Quels sont les paramètres utiles ?

Action Cliquer sur Details

Question 3b Quels sont les 4 paramètres IP ?

Question 3c Quels sont les paramètres relatif au protocole DHCP ?

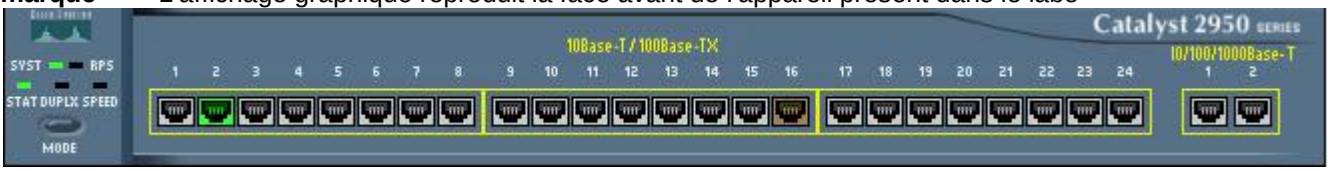
Question 3d Quelle est l'adresse ethernet ?

4	**Catalyst 2950**	10’

Objectif Bien qu’il soit possible d’administrer ce commutateur via le port Console avec Hyper Terminal, nous vous proposons de le faire d’abord depuis votre navigateur.

Action Lancer IE avec URL = http://10.1.0.55/
Username=**cisco** password=**labo**
Continue

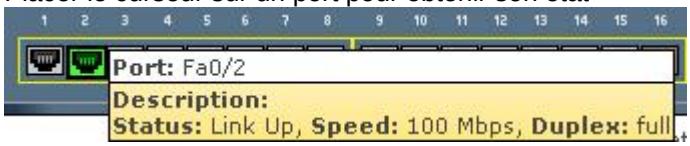
Remarque L’affichage graphique reproduit la face avant de l’appareil présent dans le labo



Cet équipement dispose de 24 ports compatibles 10/100Base-T et de 2 ports 10/100/1000 Base-T.

Objectif Visualiser l’état d’un port

Action Placer le curseur sur un port pour obtenir son état



Remarque Vous obtenez le même résultat depuis **Monitor – Port Status**

Question 4a Utiliser l’aide (**Help**) puis **Legend** pour préciser les paramètres d’un port ainsi que les valeurs possibles.

Action Fermer la fenêtre d’aide.

Remarque Sélectionner **Configuration – Port Settings** pour accéder à la configuration de chaque interface.
Ne jamais appuyer sur Submit afin de conserver la configuration originale nécessaire aux 14 participants !

Question 4b Sélectionner **Monitor – Port Statistics** pour afficher l’activité (total / émission / réception) par port.

Remarque L’onglet **Receive Detail** affiche les compteurs suivants :

- Unicast Trame ethernet point à point
- Multicast Trame ethernet point à plusieurs points (pas étudié en théorie)
- Broadcast Trame ethernet point à tous les points
- FCS Errors Erreur de CRC
- Alignment Longueur de trame non multiple de 8 bits
- Oversize Longueur de trame > 1518 bytes
- Undersize Longueur de trame < 64 bytes
- Collision Collision CSMA/CollisionDetect

Objectif Il est également possible d’administrer cet équipement avec une session telnet.

Action

```
telnet 10.1.0.55
Password:labo
Switch>ena                      mode privilégié
Password:labo
Switch#sh int status            show interface status
       sh int counter           show interface counter
       sh int F0/16             show interface 16
       sh mac-address-table     show table (port - MAC)
       sh arp                   show ARP cache
```

Remarque Il est possible de travailler efficacement avec les caractères <TAB> et ?

`Switch#`**`sh mac?`**	Je sais que la commande commence par mac
`mac  mac-address-table`	Il existe 2 commande
`Switch#`**`sh mac-<TAB>`**	Le système propose **`sh mac-address-table`**

Question 4c Comment configurez-vous Wireshark pour afficher la phase d'authentification de la session telnet

5 Commande ping 10'

Objectif Analyser l'acquisition **ping_www.unine.ch**

Action Lancer cette acquisition présente dans le partage réseau

Question 5a Quelle est l'adresse IP du poste client ?

Question 5b Quelle est l'adresse IP du serveur www.unine.ch ?

Question 5c Quelle est son adresse physique ?

Question 5d Quelles sont les valeurs du champ TTL ?

Question 5e Votre poste client répond-il aux commandes Ping reçues ?

6 Commande traceroute 15'

Objectif Analyser l'acquisition **tracert_www.unine.ch** produite avec Cyberkit

Action Lancer cette acquisition présente dans le partage réseau

Remarque Observer que certains paquets sont mis en noir par Wireshark

Question 6a Quelle est la valeur du champ TTL (protocole IP) pour le paquet 5 ?

Question 6b Quelle est la valeur du champ TTL (protocole IP) pour le paquet 7 ?

Question 6c Quelle est la valeur du champ TTL (protocole IP) pour le paquet 33 ?

Question 6d Pourquoi le poste client 192.168.1.43 n'envoie pas de paquet 37 avec un champ TTL = 17 ?

Question 6e Pouvez-vous connaître la valeur du masque de sous-réseau utilisé par www.unine.ch ?

7	**Outils TCPView et netstat**	**15'**

Objectif Se familiariser avec l'outil GUI TCPView de www.sysinternals.com

Action Lancer TCPView.exe situé dans le dossier C:\tools
Contrôler avec <CTRL U> que les connexions en attente ne sont pas affichées

Lancer Internet Explorer
Observer les connexions (vert = établissement, rouge = libération)
Sélectionner avec <CTRL R> le mode d'affichage préféré des sockets
Attendre la déconnexion

Objectif Se familiariser avec l'outil CLI netstat *(network statistics)* qui donne le même type d'information

Action Ouvrir l'interface de commande **Command Prompt** situé sur le bureau avec les droits admin
Sélectionner le raccourci puis clic droit puis *Run as administrator*
Typer **`c:\..>netstat –an`** pour connaître les connexions en attente (identiques à celles affichées précédemment par TCPView avec <CTRL U>)

Typer **`c:\..>netstat –bn`** pour connaître les connexions en attente

Typer **`c:\..>netstat –e`** pour connaître les statistiques de la couche ethernet

Question 7a Que signifie *unicast packet* ?

Action Typer **`c:\...>netstat -s`**

Remarque Cette commande complète la précédente en affichant les valeurs pour les protocoles IP, ICMP, TCP et UDP.
Ces mêmes valeurs peuvent être lues à distance, grâce au protocole SNMP *(Simple Network Management Protocol)*, par un outil de gestion réseau du type HP Openview.

Remarque Utiliser au besoin l'aide **`c:\..>netstat -?`**

8	**nslookup**	**30'**

Objectif Etudier l'outil d'administration en ligne de commande Nslookup.exe qui permet de tester et de dépanner des serveurs DNS.

Remarque Les actions qui suivent concernent nslookup.exe de Windows XP, celui de Vista étant un peu différent. C'est pourquoi il faut d'abord copier l'exécutable de XP (disponible sur la fenêtre de partage) en local.

Action Copier nslookup.exe sur le bureau
Ouvrir un *Command Prompt* puis typer **`c:\Users\ursula\Desktop\nslookup`**

```
Default Server: dc1.tdeig
Address:  10.1.1.10
>
```

Aide en ligne Au besoin, pensez à utiliser l'aide en ligne
> **`help`**

Action 8a Entrer

```
> root
Default Server:  A.ROOT-SERVERS.NET
Address:  198.41.0.4
```

> **`ch.`** Ne pas oublier le point final

Question 8a Expliquer le résultat obtenu

Remarque Le site http://www.root-servers.org énumère les 13 (A – M) serveurs DNS *root*
Le 21 oct 2002, 7 serveurs étaient indisponibles suite à une attaque de type *Distributed Denial of Service*

Action 8b Entrer
```
> set root=b.root-servers.net
> root
...
> ch.
```

Question 8b Bien que le résultat soit identique au précédent, quelle est la principale différence ?

Action 8c Entrer
```
> server domreg.nic.ch
...
> set type=soa
> ch.
```

Question 8c Expliquer commandes et résultats

Remarque Utiliser ce lien http://www.robtex.com/dns/ch.html pour connaître dans quels pays se situent ces serveurs

Action 8d Entrer
```
> set type=ns
> unige.ch.
```
Ne pas oublier le point final

Question 8d Expliquer commandes et résultats

Action 8e Entrer
```
> server dns93.unige.ch
...
> set type=soa
> unige.ch.
```

Question 8e Expliquer commandes et résultats

Action 8f Utiliser la commande **`> set type=mx`** pour connaître l'adresse IP du serveur de messagerie de la zone **cern.ch**

Question 8f Préciser les commandes entrées

Question 8g Quelle est la valeur de l'adresse IP recherchée ?

Action 8h Entrer
```
> server 129.194.184.212
> ls –d td.unige.ch
```

Question 8h A quoi sert la commande > **`ls –d td.unige.ch`** ?

Question 8i Expliquer le résultat obtenu

Objectif Utiliser l'option d2 de la commande nslookup (voir help) pour connaître les données DNS échangées dans les paquets

Lien Utiliser le lien http://www.frameip.com/dns/ pour comprendre le rôle des divers champs

RFC Utiliserer au besoin les rfc relatives au DNS
RFC1034 DOMAIN NAMES - CONCEPTS AND FACILITIES
RFC1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

9 En réserve

9A Quelques liens relatifs à ce cours :

- http://fr.wikipedia.org/wiki/Ethernet
- http://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau
- http://en.wikipedia.org/wiki/Router

9B Le produit Nagios qui supervise les principales ressources du labo http://nagios.tdeig/nagios/
Username=chat Password=noir
Site officiel http://www.nagios.org/

9C Divers documents Cisco sur le commutateur 2950 qui équipe le labo :

- 2950_Config_Guide.pdf (volumineux document qui démontre qu'un commutateur offre beaucoup de fonctions !)
- VLAN.pdf (comment configurer un Virtual LAN → module 3)
- Switch_Port_Analyzer.pdf (où brancher un analyseur pour voir tout le trafic du réseau ?)
- Port-Based_Traffic_Control.pdf (sécurisation du commutateur → module 3)

9D Analyse de protocole DHCP à partir de l'acquisition **dhcp.cap** et du document **dhcp.pdf**