Ingénieur Réseau Apprentissage ESIEE
2011/2012

Introduction Réseaux – Topologie des réseaux – Protocoles – Modèles OSI, IEEE, TCP/IP (RE3R11)

Travaux Pratiques

Présentation des TP du module Intro Réseau

- TP1 : Les outils de diagnostic réseau, Configuration commutateur Ethernet

Objectifs :

- Découvrir les principales commandes de test de connexion
- Analyser le trafic sur un réseau local
- Configurations de base d'un commutateur Ethernet : Port Mirorring, Spanning Tree, …

- TP2 : Installation et Configuration d'un serveur DNS

Objectifs :
L'objectif de ce TP est d'illustrer le concept et la configuration du service de nommage (DNS : Domain Name System). Dans ce TP, nous allons aborder :

- Les différents outils qui nous permettent d'interroger un serveur DNS
- La manière dont les informations de la structure DNS sont conservées
- La manière dont le serveur DNS sert des informations aux différents utilisateurs
- Le fonctionnement de la résolution de noms proprement dite

- Annexe :
  Commutation Ethernet – Configuration du commutateur Cisco Catalyst 2960

Ces deux TP donneront lieu à compte rendu par binôme à me rendre par mail (catherine.bernard@esigetel.fr.)

TP1 **avant le 28/09**
TP2 **avant le 05/10**

(merci d'indiquer dans l'objet du mail **TP ESIEE IR3**)

Rédaction du compte-rendu
Chaque TP réalisé donnera lieu à un compte rendu.

- Le compte-rendu est une synthèse du travail effectué pendant la séance.
- Il vous permet de retenir ce que vous avez appris en effectuant les manipulations. Un compte-rendu est avant tout un document de travail **pour votre usage personnel**.
- Structure du compte-rendu
  - Introduction, objectifs du TP – Conclusion, bilan des manipulations effectuées
  - Précisez votre environnement de travail : matériel, soft, OS utilisés
  - Description des manipulations effectuées, des tests
  - Attention à l'orthographe !

TP1 : Outils de diagnostic Réseau, Configuration commutateur Ethernet

Objectifs :

- Découvrir les principales commandes de test de connexion
- Analyser le trafic sur un réseau local
- Configurations de base d'un commutateur Ethernet
  - Thèmes abordés:
    - configuration de base (liaison série, via http);
    - configuration des ports : auto-négociation, débits, activation, désactivation…
    - analyse de trafic (*port monitoring* ou SPAN);
    - règles de base de sécurité
    - configuration du Spanning Tree
  - Thèmes non abordés: VLANs, Sécurisation avancée, administration SNMP, ...

Pré-Requis :

- Modèle OSI et équipements d'interconnexion
- Modèle TCP/IP
- Adresses MAC et IP

Matériel utilisé :

- Une station de travail en dual boot (Windows XP/Linux Mandriva)
- Commutateur Cisco (Catalyst 2960)
- L'analyseur de protocole Wireshark (outil opensource compatible Windows, Linux - http://www.wireshark.org/ - anciennement Ethereal)

Documents complémentaires :

- Annexe1 : Introduction Linux
- Annexe 2 : Commutation Ethernet, Configuration Commutateur Cisco Catalyst 2960
- Documentations Cisco : Catalyst 2960 Switch Software Configuration Guide Cisco IOS Release 12.2(25)FX (680 pages!!)
  http://www.cisco.com/en/US/products/hw/switches/
- Documents accessibles depuis le serveur de la salle de TP

Durée du TP : 4 heures

Remarques préliminaires :

- Vous effectuerez toutes les manipulations de configuration avec le **compte administrateur** (ce qui est nécessaire pour les changements d'adresse, etc…). Sous linux, passage en root par la commande **`su –`** si vous avez ouvert la session sous un autre compte.
  Attention, le compte administrateur n'est à utiliser que quand cela est nécessaire, travailler constamment avec ce compte administrateur est une véritable faille de sécurité !!! Inutile d'être administrateur pour faire du web ou de la bureautique !

- Sous linux
  - Les configurations se feront en mode ligne de commande.
  - Faites systématiquement une sauvegarde des fichiers initiaux avant de les modifier **(`cp fichier.conf fichier_old.conf`).**
  - La modification d'un fichier de configuration d'un serveur ou service impose de relancer ce service.
    `/etc/init.d/serviced start` ou `restart`
    `/etc/init.d/serviced stop`
    `/etc/init.d/serviced status`
    ou avec la commande :
    `service` *`nom_du_service`* `status|start|restart|stop` (touche de complétion qui fonctionne avec le nom du service, utile si vous avez oublié le nom exact du service)
  - Pensez à utiliser le **`man`** pour vous aider dans vos configurations.

1. Présentation de Wireshark

Il existe d'autres analyseurs de trames pouvant être lancé depuis un terminal sans interface graphique spécifiques : TCPDUMP et IPTRAF qui sont deux de ces analyseurs de trames très simples.
N'hésitez pas à les tester...

REMARQUE : Wireshark était connu dans les versions précédentes sous le nom de Ethereal, la dernière version a jouté notamment des fonctionnalités pour « l'écoute » de réseaux Wi-Fi.

Wireshark est aujourd'hui un outil largement utilisé aussi bien dans le cadre d'administration réseau (résolution de problèmes réseaux), dans l'examen de problèmes liés à la sécurité, dans le « débuggage » d'implémentation de protocoles, ou tout simplement comme outil permettant de comprendre le fonctionnement des réseaux. Jusqu'à 602 protocoles pouvant être analysés…
Projet démarré en 1998 (anciennement Ethereal), Wireshark intègre aussi des outils pour l'analyse VoIP, de réseaux sans fil....

Caractéristiques :

- Fonctionne sous Windows ou Unix (Linux)
- Capture des trames 'en live' depuis l'interface réseau
- Affichage des trames avec des infos sur les protocoles
- Import et export de captures de data venant d'autres programmes
- Possibilité de mettre en place des filtres selon différents critères
- Création de statistiques

….

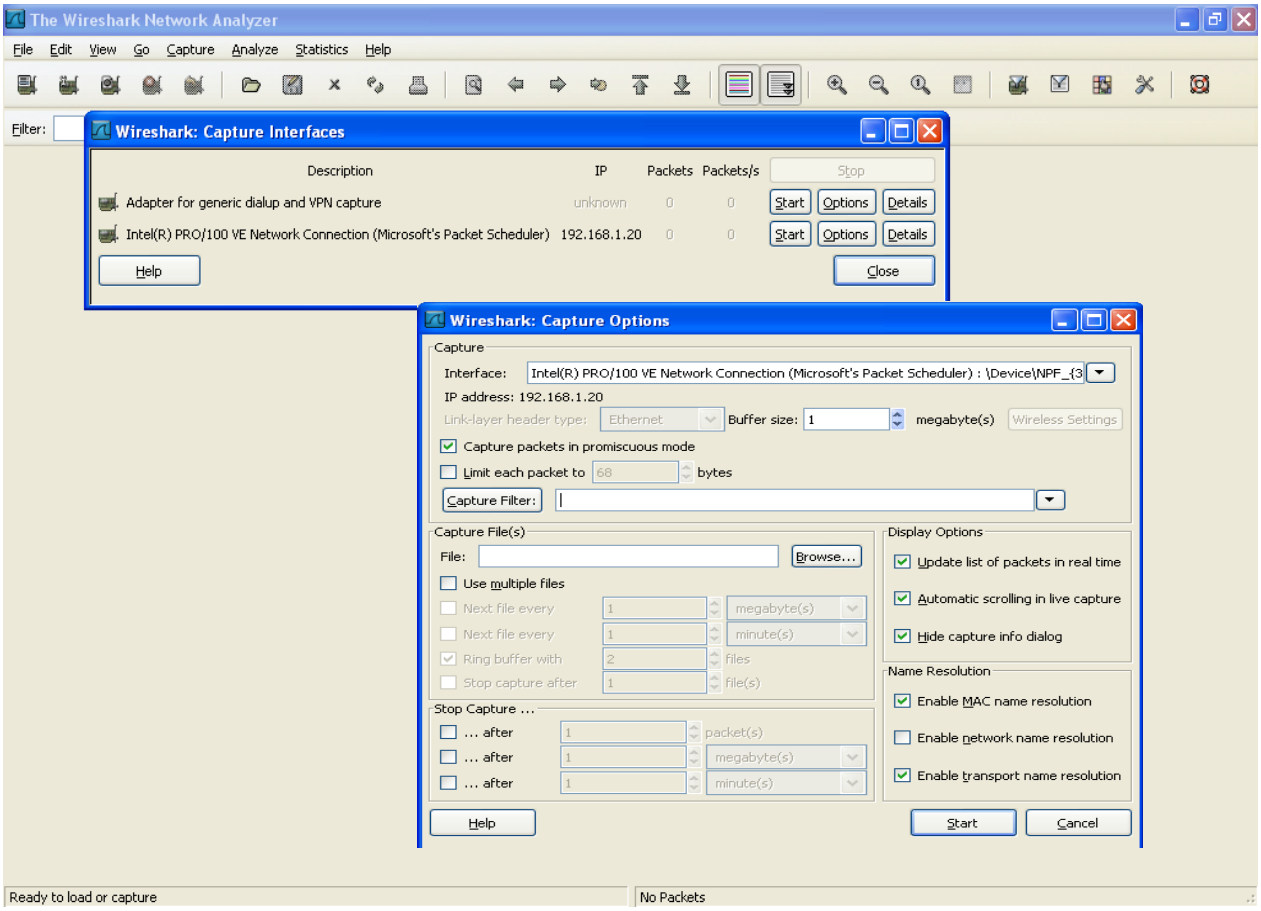


Figure 1 : Fenêtre de lancement de capture sous Wireshark

Le résultat d'une capture se présente sous la forme d'un fichier « découpé » en trois parties :

- Partie supérieure donnant la liste des trames capturées (indications temporelles par rapport aux émissions de trames, adresses source, destinataire, physique ou logique suivant le type de trame, protocole, infos sur le type de trame) ;
- Partie du milieu permettant d'avoir le détail des différents champs d'une trame (il suffit pour cela de se positionner sur la trame souhaitée) ;
- Partie inférieure donnant la trame en Hexa avec la correspondance ASCII.

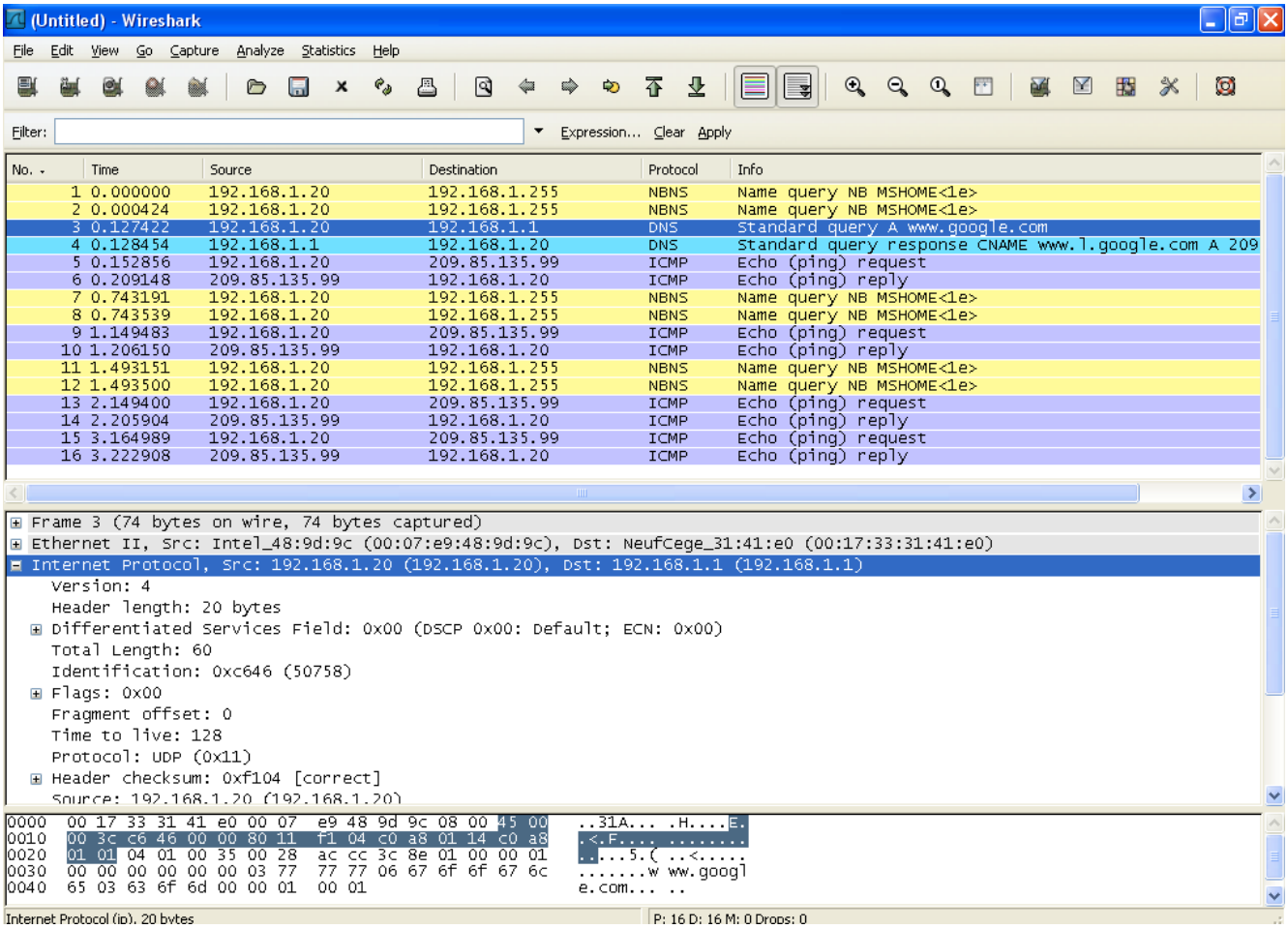
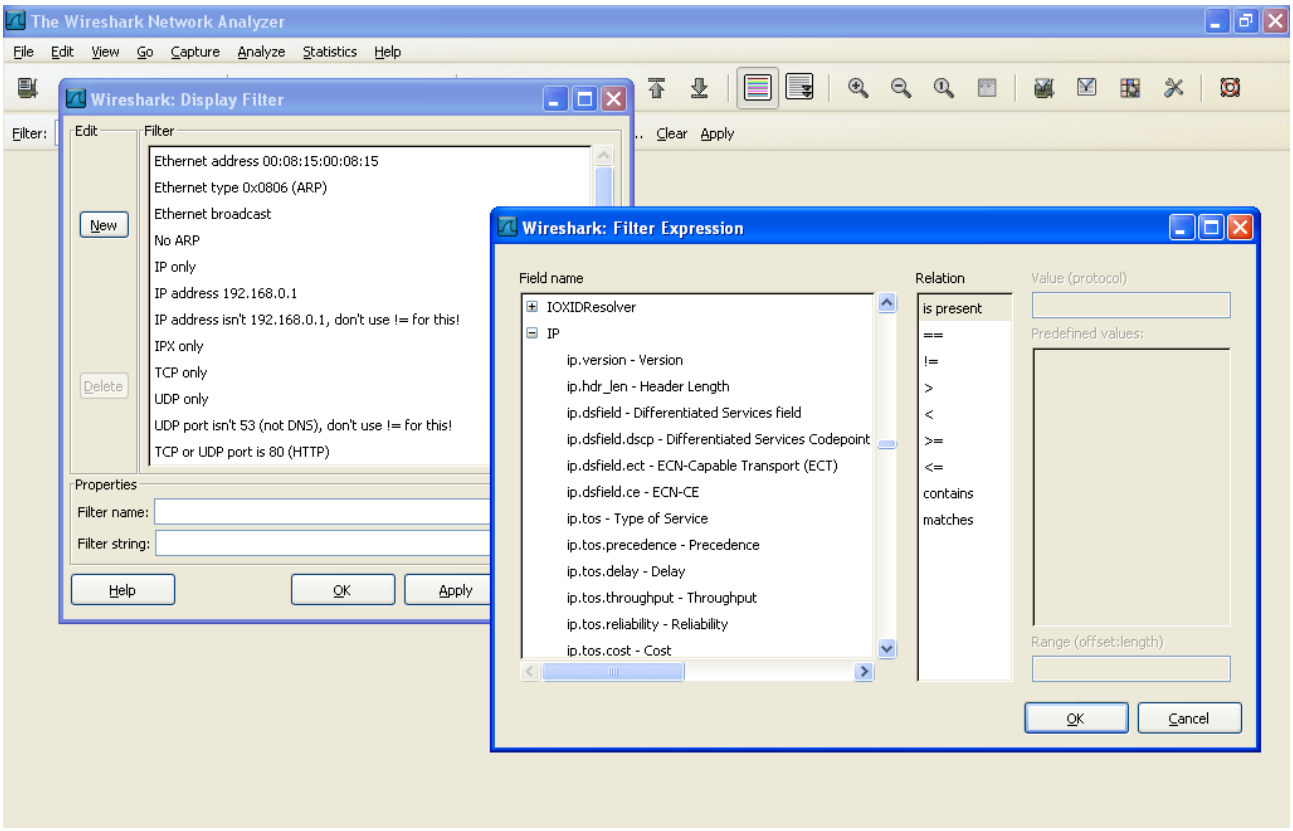


Figure 2 : Résultats de l'analyse de trame

Le menu statistiques permet d'avoir un certain nombre d'informations quant au fonctionnement de son réseau : quel type de trafic en majorité, « qui parle avec qui »…
N'hésitez pas à tester l'ensemble de ces fonctionnalités.

En outre, vous pouvez mettre en place des fonctions de filtrage. Par un clic sur le bouton appelé « filter » ou depuis le menu « Capture », vous accédez à la boîte de dialogue dédiée à la construction de filtres d'affichage (voir figure 3). Vous pouvez aussi composer un filtre directement en le tapant dans la fenêtre à droit de « filter », ou en choisir un prédéfini. Le filtre est activé en cliquant sur le bouton « apply ».



Pour lancer une capture, sélectionnez Start dans le menu Capture. La fenêtre Options de Capture s'affiche (figure 3). Elle vous permet de définir les options à utiliser lors de la capture : interface sur laquelle est réalisée la capture, utilisation d'un filtre de capture, limitation du nombre de paquets capturés, durée de la capture, résolution de nom à l'affichage.

N'hésitez pas à consulter la doc en ligne…

Mode opératoire :

- Vous travaillerez en tant qu'administrateur.
- Pour toutes les manipulations, sélectionnez l'option Update list of packets in real time afin que les paquets s'affichent en temps réel sur la fenêtre du haut.

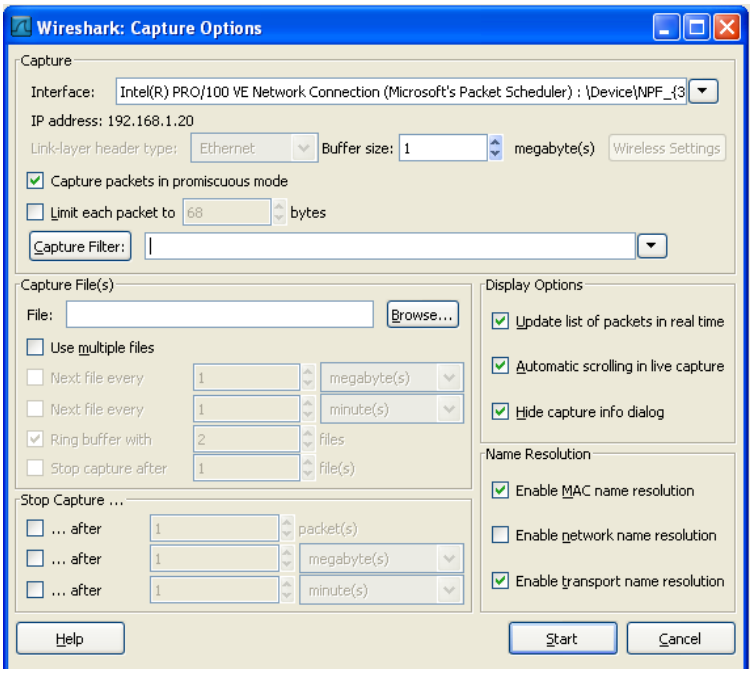


Figure 4 : Les options de capture

2. Etude des protocoles du LAN

Vous disposez de tout un ensemble de commandes qui permettent de tester la connectivité de votre machine. Certaines commandes sont spécifiques à Windows ou Linux (`ipconfig` pour Windows et `ifconfig` pour Linux), d'autres sont générales (`ping, arp`).

Ces commandes sous Windows sont accessibles depuis l'invite de commande ou depuis un terminal sous Linux. Pour obtenir de l'aide sur les commandes, sous Windows il suffit de taper dans l'invite `commande –h`, ou `help commande`, ou encore `commande /?`. Vous aurez notamment accès à la liste des options utilisables avec la commande. Sous Linux, utilisez les pages **`man`** (tapez depuis votre terminal `man « nom de la commande »`). Utiliser largement ces fonctions !

Pour l'utilisation de Wireshark, penser à utiliser les filtres facilitant la lecture des trames générées.

a) Paramètres IP de votre machine

Relever les paramètres Réseaux de votre machine :

- Adresse IP
- Adresse de la passerelle IP
- Adresse du DNS

Les configurations pour le DNS sont visibles dans le fichier `resolv.conf`. Que désigne la « passerelle par défaut » ? Donner l'adresse du réseau auquel appartient votre machine ?
Quelle commande utilisez-vous pour récupérer ces paramètres ?

La commande `netstat` permet de connaître les ports en écoute sur votre machine, sur quelles interfaces, avec quel protocole de transport (TCP ou UDP), les connexions actives et les routes.
Tester les différentes options vous permettant d'obtenir ces informations. Afficher la table de routage, les informations relatives à votre interface réseau. Quels sont les services « tournant » sur votre machine ?

b) La commande ping

La commande ping est une commande fondamentale du test de connectivité de votre station. Elle repose sur le protocole de niveau 3 ICMP (*Internet Control Message Protocol*), une norme TCP/IP définie dans la RFC 792.
Il permet aux hôtes et aux routeurs qui communiquent par le protocole IP de faire état des erreurs de connectivité et d'échanger des informations sur l'état du réseau. Par exemple, les messages ICMP sont généralement envoyés automatiquement lorsqu'un paquet IP ne peut pas atteindre sa destination (qui est déconnectée du réseau par exemple).
Les messages ICMP sont encapsulés et envoyés dans les datagrammes IP, comme le montre la figure suivante :

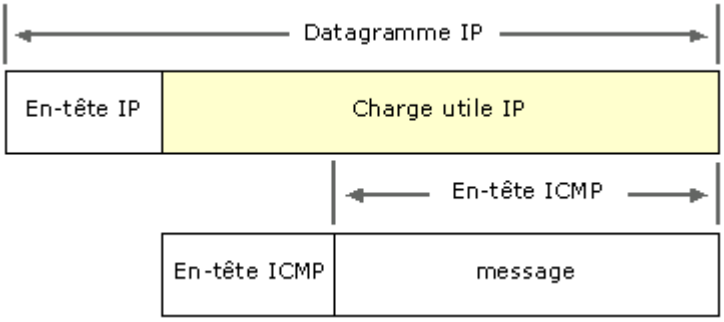


Figure 5 : Encapsulation des messages ICMP dans un paquet IP

Différents types de messages ICMP sont identifiés dans l'en-tête ICMP. Les messages ICMP les plus courants sont listés et décrits dans le tableau suivant.

Message ICMP	Description
Echo request (requête d'écho)	Détermine si un nœud IP (un hôte ou un routeur) est disponible sur le réseau.
Echo reply (réponse d'écho)	Répond à une requête d'écho ICMP.
Destination unreachable (destination inaccessible)	Informe l'hôte qu'un datagramme ne peut pas être livré.
Source quench (extension de source)	Informe l'hôte pour réduire la vitesse à laquelle il envoie les datagrammes (risque de congestion).
Redirect (redirection)	Informe l'hôte d'un itinéraire préféré.
Time exceeded (dépassement de la temporisation)	Indique que la durée de vie TTL (*Time-to-Live*) d'un datagramme IP a été dépassée.

La syntaxe de la commande `ping` est : `ping adresse_IP` ou `ping nom de machine` d'un domaine.

Tester le rebouclage local en tapant ping 127.0.0.1. A quoi peut servir le ping en bouclage local ?
Effectuer un ping local, sur la machine du binôme voisin. La réponse vous est présentée sous forme de colonnes. Que contient chaque colonne ?
Visualiser le cache ARP de votre machine. Qu'observer-vous ? Testez un second ping vers une autre machine, comment a évolué votre cache ? Pourquoi la sauvegarde est-elle temporaire ?

Configurez votre ping pour que la taille des paquets soit plus importante ? Dans quel cas est-il intéressant d'envoyer des paquets de taille plus importante ?

Vous allez maintenant vérifier votre connectivité avec l'extérieur. Tester un ping sur www.google.com
Quelle est l'adresse IP du serveur Google contacté ? Comment votre machine l'a-t-elle obtenue ?
Les valeurs de temps renvoyées sont-elles identiques pour chaque paquet ICMP Echo émis ? Pourquoi ?

Utiliser Wireshark pour observer les mécanismes d'encapsulation mis en jeu dans le cas de la commande ping ?
Observer les adresses MAC et IP utilisées dans le cas d'un ping vers une machine du réseau, puis un ping vers une adresse web.
Observer une trame ARP. Quelles sont les adresses source et destination ?

c) La commande traceroute

Tester la commande `traceroute -I www.yahoo.fr` par exemple.
Quel est le nombre de routeurs traversés par les paquets ? Auriez-vous pu prévoir ce résultat ?
Comment le système obtient-il les URL correspondant à ces adresses IP ?
Observer les temps de réponse obtenus successivement de chaque routeur sur le chemin. Commentez. Est-on sûr de retrouver le même chemin si l'on recommence l'expérience quelques minutes plus tard ?
Utiliser Wireshark pour comprendre le mécanisme utilisé par la commande traceroute.

d) La commande nslookup/dig

Tester la commande `nslookup` pour la résolution de nom de www.yahoo.fr par exemple. Quelles informations vous sont renvoyées ?
Tester la commande `dig`. Sans aucun argument à la commande dig, quelles infos vous sont néanmoins fournies ? Dans le cas de la résolution de nom de www.yahoo.fr, quelles informations supplémentaires vous apporte cette commande ?
Observer à partir de Wireshark une requête DNS. Quel protocole de niveau transport est utilisé ? Pourquoi ?

e) Test d'une connexion sur le web

Lancer une capture de trames.
Connecter-vous à un site de votre choix et donner l'ensemble des trames qui ont été générées par cette connexion. Représenter l'ensemble de ces trames, en précisant les adresses MAC et IP émetteur et destinataire. Analyser les différents champs de la connexion TCP.
Quel est le protocole de transport utilisé dans le cas d'une connexion web ? Le protocole de niveau transport utilisé par le protocole d'envoi des messages vous paraît-il bien choisi ? Pourquoi ?
Quel est le numéro de port pour accéder à une application web ?

Wireshark propose un outil nommé, Follow TCP stream (menu Tools). Sélectionner un segment TCP et activer l'outil Follow TCP stream. Vous visualisez le contenu de la session TCP dans sa totalité. A l'aide des menus au bas de la fenêtre, pour pouvez afficher la totalité ou un seul sens du dialogue. Retenir cet outil bien pratique…

N'hésiter pas à tester l'ensemble des outils qui sont mis à disposition….

f) Nmap

Nmap ("Network Mapper") est un outil open source d'exploration réseau et d'audit de sécurité. Il a été conçu pour rapidement scanner de grands réseaux, mais il fonctionne aussi très bien sur une cible unique (source : http://www.insecure.org/nmap).

Informations fournies par Nmap :

- quels sont les hôtes actifs sur le réseau ?
- tables de ports intéressants
- noms DNS (reverse DNS)
- quels services (y compris le nom de l'application et la version) que ces hôtes offrent ?
- quels systèmes d'exploitation (et leurs versions) ils utilisent ?
- le type de matériel ou les adresses MAC
- quels types de dispositifs de filtrage/pare-feux sont utilisés ?
- ...

Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires de systèmes et réseaux l'apprécient pour des tâches de routine comme les inventaires de réseau, la gestion des mises à jour planifiées ou la surveillance des hôtes et des services actifs.

Nous allons utiliser ici cet outil pour tester les services de machines de la salle, ou de machines particulières.
Connecté sous Linux, vous pouvez déjà regarder les services et ports associés qui figurent dans /etc/services.

Effectuer les tests suivants et observez les trames générées par ces commandes :

- Affichage des hôtes en ligne sur la plage d'adresse du réseau auquel vous êtes connecté
- Affichage des services et OS pour ces hôtes
- Pour un de ces hôtes, affichage des services
- Scanne sur un port particulier sur la plage d'adresse de votre réseau

Options de la commande Nmap

Source : http://insecure.org/nmap/man/fr/man-briefoptions.html

Utilisation : nmap [Type(s) de scan] [Options] {spécifications des cibles}

SPÉCIFICATIONS DES CIBLES:
Les cibles peuvent être spécifiées par des noms d'hôtes, des adresses IP, des adresses de réseaux, etc.
Exemple: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0-255.0-255.1-254

DÉCOUVERTE DES HÔTES:
-sL: List Scan - Liste simplement les cibles à scanner
-sP: Ping Scan - Ne fait que déterminer si les hôtes sont en ligne
-PS/PA/PU [portlist]: Découverte TCP SYN/ACK ou UDP des ports en paramètre
-PE/PP/PM: Découverte de type requête ICMP echo, timestamp ou netmask
-n/-R: Ne jamais résoudre les noms DNS/Toujours résoudre [résout les cibles actives par défaut]

SPÉCIFICATIONS DES PORTS ET ORDRE DE SCAN:
-p <plage de ports>: Ne scanne que les ports spécifiés
Exemple: -p22; -p1-65535; -pU:53,111,137,T:21-25,80,139,8080

DÉTECTION DE SYSTÈME D'EXPLOITATION:
-O: Active la détection d'OS

-v: Rend Nmap plus verbeux

Exemples :

- nmap -v scanme.nmap.org

Cette option scanne tous les ports réservés TCP sur la machine scanme.nmap.org . L'option -v active le mode verbeux.

- nmap -sS -O scanme.nmap.org/24

Lance un scan furtif (stealth SYN scan) contre chaque machine active parmi les 255 machines du réseau de "classe C" sur lequel Scanme réside. Il essaie aussi de déterminer le système d'exploitation sur chaque hôte actif. Cette démarche nécessite les privilèges de root puisqu'on utilise un SYN scan et une détection d'OS.

- nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

Lance une recherche des hôtes et un scan TCP dans la première moitié de chacun des 255 sous-réseaux à 8 bits dans l'espace d'adressage de classe B 198.116 Cela permet de déterminer si les systèmes font tourner sshd, DNS, pop3d, imapd ou le port 4564. Pour chacun de ces ports qui sont ouverts, la détection de version est utilisée pour déterminer quelle application est actuellement lancée.

N'hésitez pas à consulter le man vous donnant l'ensemble des options possibles avec la fonction **nmap**.

3. Configuration d'un Commutateur Ethernet

Préambule

L'objectif de cette partie est donc d'étudier les différentes fonctionnalités d'un commutateur manageable, et aborder la configuration minimale de ce type d'équipement. Vous serez amené à tester des fonctions plus avancées sur ce commutateur pour d'autres cours.
Le management et donc la configuration de ce commutateur peut se faire à partir du port COM ou d'un port réseau, soit en ligne de commande soit à l'aide d'un logiciel de configuration fourni avec le commutateur (la plupart du temps utilisant une interface web).

L'étape de configuration par port COM est essentielle puisque cette étape permettra dans un premier temps de configurer votre commutateur pour permettre l'accès par le réseau.
Dans un premier temps, vous allez donc faire quelques configurations de base par port COM, puis accéder au menu de configuration en ligne de commande via le réseau. Pour ce TP, nous nous limiterons au menu par ligne de commande, vous pourrez pour d'autres TP tester l'outil graphique de management fourni par Cisco.

RQ : Le menu par ligne de commande est largement utilisé par les administrateurs, même si le menu de configuration par interface graphique est plus convivial, il est plus lourd et pas toujours utilisable dans votre environnement de travail (vous ne disposez pas d'un navigateur Internet « reconnu » par Cisco).

Configuration des paramètres réseau via port COM

Vous allez d'abord attribuer une adresse IP à ce commutateur. Quel est le rôle de cette adresse IP (**le commutateur reste un équipement de niveau 2**) ?
Comment choisissez-vous votre adresse IP ?

Vous allez configurer le commutateur comme s'il était neuf: Pour cela, suivre les étapes suivantes:

1. Connecter un PC au commutateur via un câble série (qui se branche sur la face arrière du commutateur);
2. Lancer un émulateur de terminal (HyperTerminal sous Windows, Minicom sous Linux...), le configurer en 9600 8N1. Que signifie ce paramétrage ?

   Brancher alors votre commutateur.
   Le système vous propose de lancer le dialogue de configuration initial:
   `Continue with the configuration dialog? [yes/no]: Y`
   Répondez oui.

3. Configurations à partir du menu de configuration initiale
   - entrer les mots de passes (utiliser toujours **cisco, cisco1**). Mettre ce mot de passe partout (le système va se plaindre car ce n'est bien sur pas recommandé pour la sécurité).

   RQ : le « `enable secret` » est le mot de passe du mode super-utilisateur (enable) qui est sauvé sous forme chiffrée, « `enable password` » est l'ancienne version du mot de passe sauvée sous forme non chiffrée qui ne sera utilisée que si l'on démarre le commutateur avec une veille version de l'IOS

   - indiquer "vlan1" pour que l'on puisse administrer le commutateur à partir du VLAN par défaut (désignant le switch).
   - spécifier une adresse IP à votre commutateur.

   ATTENTION : Ne pas sauvegarder cette configuration !!!!
   Cette première configuration vous donne les éléments clefs à configurer pour avoir le commutateur fonctionnel, mais nous allons revenir aux configurations de base du commutateur à partir du mode privilégié.

4. Configurations réseau à partir du mode privilégié (accès par port COM).

   Entrer dans le mode Privileged EXEC du commutateur.
   Donner un nom à votre commutateur et protègez son accès via un mot de passe (utilisez le pwd Cisco).
   Attribuer une adresse IP à votre commutateur.

A ce stade de la configuration, votre routeur dispose de deux configurations. La première, en mémoire vive (RAM) qui est la configuration courante peut être visualisée au moyen de :

```
Switch#show running-config.
```

La seconde est celle qui sera utilisée en cas de redémarrage qui peut être visualisée au moyen de :

```
Switch#show startup-config.
```

Pour afficher la configuration de démarrage, il est obligatoire d'être en mode privilégié.

Si les deux configurations ne sont pas les mêmes, copier la configuration de la RAM vers la NVRAM en tapant :

```
Switch#copy running-config startup-config.
```

Tester par un ping la communication entre votre poste de travail et le commutateur.

RQ : Passer les adresses IP de votre poste de travail en statique afin de garder vos adresses tout au long des configurations, puisque vous allez être déconnecté du réseau.

Déconnecter vous du mode d'accès par port COM pour accéder maintenant au menu de configuration de votre commutateur par le réseau.
Tester les fonctionnalités du serveur web de configuration présent sur le switch, mais revenir ensuite au mode de configuration en ligne de commande via la commande Telnet
Pour lancer un `telnet`, depuis un terminal sus Linux ou l'invite de commande de Windows, tapez **`telnet @IP`** de la machine sur laquelle vous souhaitez vous connecter.

Test de la sécurité du protocole Telnet

Observez les trames générées lors la connexion par Telnet à votre commutateur notamment au moment de la connexion et de la saisie du login et mot de passe.

Que pouvez vous conclure (pensez à utiliser la fonction Follow TCP stream) ?

Visualisation de la table de commutation

Quelle commande permet de visualiser votre table de commutation ? Quel paramètre détermine la durée de vie des entrées dans la table de commutation, comment modifier ce paramètre ?

Etat des ports

Changer les options de vitesse, mode de transmission (full-duplex, half duplex) pour un port. Quelle commande permet d'activer/désactiver un port ?
Quelle commande utiliser pour appliquer ces modifications à plusieurs ports à la fois ?
Trouver les options vous permettant de récupérer des statistiques sur le trafic de chaque port.

Sécurisation d'un port

Configurer de manière statique une entrée de votre table de commutation en associant une adresse MAC à un port. Que se passe-t-il si cette machine est connectée à un autre port ? Vérifier à l'aide de Wireshark les messages ICMP échangés au moment des tests.

Port Mirorring

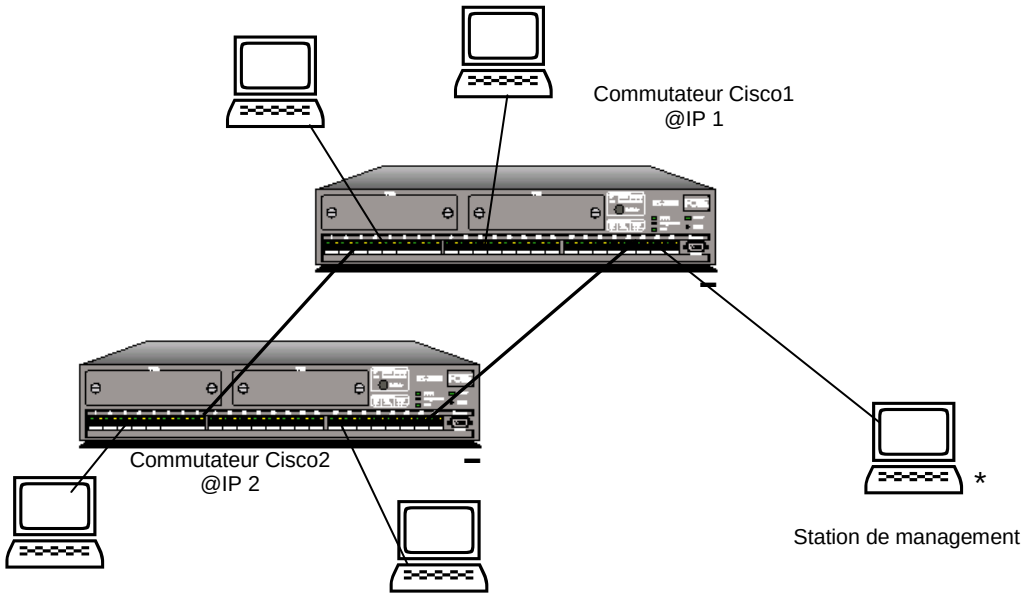
Mettre en place d'une fonction de port mirroring (SPAN pour les commutateurs Cisco).
Quel est l'intérêt de cette fonction et dans quel cas l'utilise-t-on ? Tester cette fonctionnalité et vérifier grâce à votre analyseur de trames son fonctionnement. Expliquer votre mode opératoire.

Mécanismes de filtrage

Configurer votre commutateur de manière à bloquer le trafic venant d'une machine (tester avec la machine de vos voisins).
Si vous avez le temps, poussez cette politique de filtrage en bloquant par exemple le trafic HTTP.

Configuration des paramètres de Spanning Tree

Pour mettre en œuvre le Spanning Tree, on met en place l'architecture suivante.



Exemple d'architecture pour la configuration du Spanning Tree

* Chaque machine de ce schéma est en réalité une des cartes réseau de votre poste de travail.

Quel est l'intérêt de cette architecture ? Justifier la nécessité de configurer le Spanning Tree.

Configurer le Spanning Tree sur votre réseau de sorte que le commutateur Cisco1 soit le commutateur racine.
Tester votre configuration de Spanning Tree en lançant un ping "en continu" et en testant les différents liens.
A partir de Wireshark, observer le fonctionnement de l'algorithme en fonctionnement normal pour l'élection du pont racine, puis en créant une défaillance et en observant le comportement de l'algorithme (observation des statistiques, des trames BPDU envoyées par chaque station, etc....)

Utiliser la configuration permettant à la station de management d'observer le trafic passant sur un des liens entre les deux commutateurs

COMMUTATION ETHERNET
CONFIGURATION DU COMMUTATEUR CISCO CATALYST 2960

Préambule :

Ce document a pour objectif de vous rappeler les principes clefs de la commutation Ethernet et donner les concepts et commandes de base permettant la configuration du commutateur Cisco Catalyst 2960

Plan :

Sommaire

Glossaire :

ACL : Access List
CLI : Command Line Interface
IOS : “l’OS” des équipements mangeables de Cisco (commutateur, routeur)
SNMP : Simple Network Mangement Protocol
VLAN : Virtual Local Area Network

1. Commutation Ethernet : Rappels de base

Un commutateur Ethernet est un équipement de niveau 2 : il manie des trames Ethernet (**adresses MAC**) sans regarder leur contenu (par exemple un datagramme IP).

Un commutateur Ethernet (switch) s'installe comme un hub. Un hub répète les trames qu'il reçoit sur tous ses ports. Un commutateur essaie de minimiser les envois inutiles qui gaspillent de la bande passante et génèrent des collisions. Pour cela, il utilise une table de commutation qui associe à chaque adresse MAC connue le port par lequel on peut l'atteindre.

Afin de simplifier la mise en place du commutateur et son administration, cette table est apprise automatiquement durant le fonctionnement. Lorsque l'adresse de destination d'une trame n'est pas dans la table, le commutateur l'envoie sur tous ses ports, sauf celui par lequel elle est arrivée (il se comporte alors comme un hub). Cependant, il note au passage l'adresse source de la trame dans sa table. De cette façon, les futurs envois vers cette station pourront être optimisés.

Un mécanisme de mise à jour dynamiquement de la table de commutation permet de résoudre le problème des déplacements de station d'un port à l'autre (notion de *ageing-time* pour les entrées de la table de commutation).

Débits, modes de fonctionnement (full-duplex, half duplex) et autonégociation :

Les réseaux Ethernet filaires offrent différents débits et différents modes: half duplex, full duplex.
Le support utilisé est soit des paires torsadées (TX) soit de la fibre optique (FX) (historiquement du coax).

La configuration la plus commune est de 100Mbit/s sur paires torsadées (100BaseTX).

Deux équipements connectés ne peuvent communiquer que s'ils utilisent le même mode. Certaines erreurs de configuration se traduisent par une communication possible mais avec de forts taux d'erreurs ou de collisions (exemple: carte half-duplex connectée à commutateur full-duplex).

En général, on peut soit fixer le mode (débit et duplex) sur chaque équipement, soit utiliser un mécanisme d'**autonégociation** (dans ce cas, il faut le spécifier aux deux extrémités). Dans le doute, il est en général conseillé d'utiliser l'autonégociation.

Les commutateurs les plus répandus offrent en général tous les modes 10 et 100, et parfois des ports 1000 sur paires torsadées ou des logements pour interfaces fibres optiques 100 ou 1000 Mbit/s.

Les commutateurs Ethernet disposent de nombreuses autres fonctionnalités qui sont abordées ici rapidement :

- Agrégation de lien
  Cette fonction permet de regrouper logiquement plusieurs ports afin d'augmenter la bande passante. Si un des liens est défaillant, le trafic est réparti alors sur les liens restants.

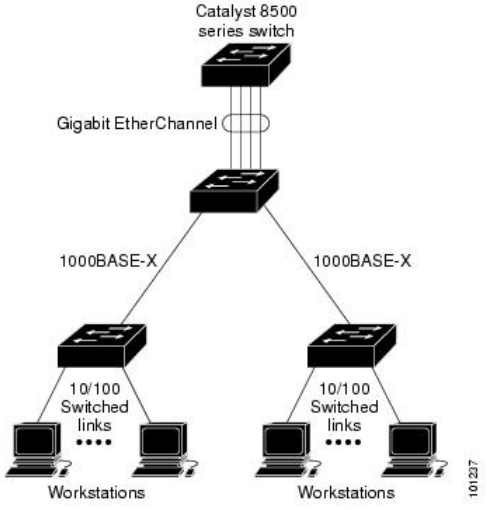
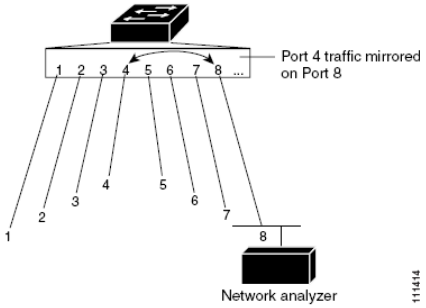


Figure 1 : Agrégation de liens

- Miroir de ports



Cette fonction permet de recopier le trafic d'un port sur un autre port afin de pouvoir analyser le trafic sur un port du commutateur.

RQ : Le port mirorring correspond à la configuration SPAN pour les commutateurs Cisco

Figure 2 : Exemple de Port mirorring

- Sécurisation des ports
  Deux méthodes :
  - associer à un port une liste d'adresses MAC autorisées (méthode qui peut devenir lourde par rapport à la gestion des adresses MAC)
  - authentification avec la mise en place de serveur RADIUS (méthode plus complexe, mais qui peut être combinée avec les services d'annuaires utilisés dans l'entreprise (LDAP pour les environnements Linux ou Active Directory pour Windows), se développe avec l'intégration de plus en plus importante des utilisateurs nomades)

- VLAN (*Virtual Local Area Network*)
  Les VLAN est une segmentation logique du réseau commuté. Cela permet de sécuriser les échanges et augmenter les performances (broadcasts qui restent dans le VLAN). Les VLAN peuvent être définis par port ou par adresse MAC. Pour communiquer entre deux VLAN doivent être reliés par un routeur (niveau 3).

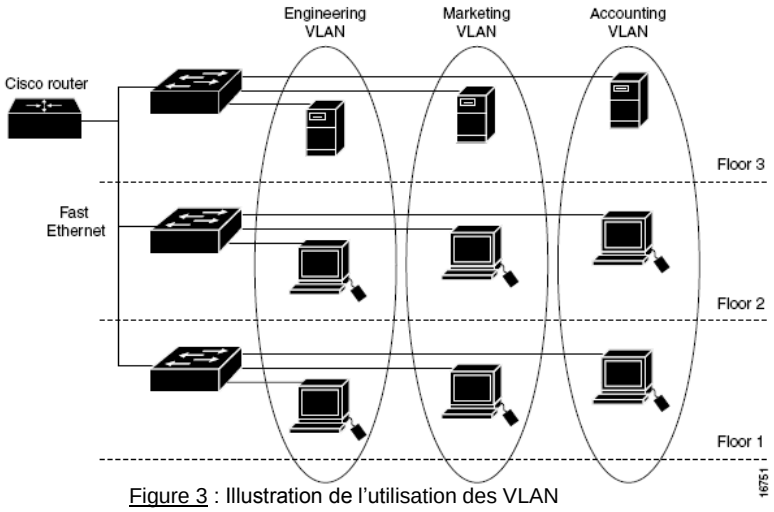


Figure 3 : Illustration de l'utilisation des VLAN

- Fonctions de supervision du trafic et des dysfonctionnements (via SNMP, *Simple Network Management Protocol*)

- Contrôle de flux : mécanisme permettant d'éviter la congestion au niveau d'un port

- Spanning Tree : Ce protocole (STP) est utilisé si l'on choisit de créer des boucles dans le réseau commuté (ces boucles permettent par exemple d'avoir un lien de backup). Le protocole de Spanning Tree a pour objectif d'éviter la recopie multiple de trames (désactive le lien secondaire et en cas de problème sur le lien principal, commutation vers le lien secondaire alors activé).

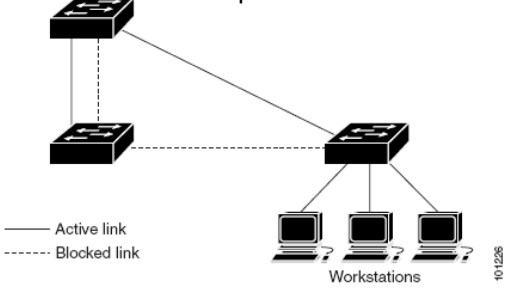


Figure 4 : Connexions redondantes et Spanning Tree

- Configuration et administration d'un commutateur

La configuration d'un commutateur manageable (il existe des modèles meilleur marché offrant moins de fonctionnalités) peut s'effectuer de différentes façons :

- Mode console sur liaison série RS232 (Il faut utiliser un câble null modem et utiliser une console ou un émulateur de terminal – hyperterminal sous Windows, Minicom sous Linux)
- Mode console via `telnet` ou `ssh` (avant de pouvoir administrer par le réseau, il faut d'abord se connecter sur le port série pour configurer l'adresse IP du commutateur)
- Serveur HTTP embarqué (interface graphique)
- Protocole SNMP (dispositif de management permetant d'administrer le commutateur)

RQ : Même si les outils graphiques sont plus conviviaux, la configuration en ligne de commande est largement utilisée dans le cadre de l'administration de réseau (permet d'être indépendant de l'environnement réseau utilisé, Windows, Linux, du navigateur web utilisé...).

2. Présentation et Configuration des commutateurs Cisco Catalyst 2960

2.1. Préambule

Cette partie présente les principaux concepts et commandes base pour la configuration des commutateurs CISCO CATALYST 2960.
Un certain nombre de commandes courantes sont donné dans ce document, ce qui est loin de couvrir l'ensemble des possibilités du commutateur, elles permettent d'accéder aux configurations courantes, pour aller plus loin se référer aux documentations Cisco.

Documents complémentaires :

- Documentations Cisco : Catalyst 2960 Switch Software Configuration Guide Cisco IOS Release 12.2(25)FX (680 pages!!)
  http://www.cisco.com/en/US/products/hw/switches/
- Préparation à la Certification Cisco CCNA (CISCO, Installation, configuration et maintenance de réseaux) – Examen CCNA 640-801 – Editions ENI

Référence du commutateur :

- WS-C2960-24TT-L, version d'IOS 12.2 (25)FX, 24 ports 10/100 Mbit/s + 2 ports Gbit/s

2.2. Présentation du commutateur Catalyst 2960

La gamme Catalyst® 2960 de Cisco est destinée à la commutation d'étage dédiée Ethernet 10/100/1000 Mbits/s. Ces commutateurs disposent d'une interface de gestion Web fournissant des fonctions d'administration faciles à utiliser via la suite CMS (Cisco Cluster Management Suite) et le logiciel Cisco IOS intégré.
La gamme de commutateur Catalyst 2960 est composée de différents modèles permettant de combiner tous les besoins en nombre de ports paires torsadées 10/100 de 12 à 48 ports, et les besoins en ports fibres 100FX, Gigabit cuivre, et Gigabit fibre.

Remarque : Différences entre les logiciels Cisco IOS Standard (SI) et Enhanced (EI) Image
Les commutateurs Catalyst 2960 existent avec deux versions différentes de logiciel Cisco IOS, permettant ainsi de couvrir les besoins en fonctionnalités des petites, moyennes et grandes entreprises à l'extrémité de leur réseau (commutateurs de bureau). La version SI offre les fonctionnalités Cisco IOS basiques pour des données, de la vidéo et des services voix sur un réseau, soit les fonctionnalités nécessaires pour la plupart des petites et moyennes entreprises. Pour une sécurité encore plus avancée, de la qualité de service encore plus précise et efficace, et de la haute disponibilité du réseau, la version EI offre des services de réseaux intelligents comme la gestion sophistiquée du trafic, l'optimisation de la bande passante et le filtrage des utilisateurs et de la sécurité des accès au réseau. Toutes les fonctionnalités présentes dans la version SI le sont également dans

la version EI. Se référer aux documentations Cisco pour connaître précisément les différences entre ces deux versions d'IOS.

Conventions pour les commutateurs Cisco Catalyst 2960 :

Une adresse MAC est présentée sous la forme xxxx.xxxx.xxxx (x, valeur en héxa).
Un port (interface) est désigné de la manière suivante : FastEthernet 0/x (slot/numéro de ports, slot toujours à 0 pour la gamme 2960).
Menu de configuration par ligne de commande appelé CLI (*Command-Line Interface*).
vlan 1 : vlan par défaut, désigne le commutateur.
Le mot de passe par défaut est vide.

2.3. Structure matérielle des équipements Cisco

Un point important porte sur le type de mémoire utilisée. Le tableau suivant donne les caractéristiques principales et l'utilisation des différents types d mémoires des équipements Cisco.

Type de mémoire	Caractéristiques	Contenu
RAM/DRAM	Utilisée par le système d'exploitation pour maintenir le informations durant les fonctionnement	Le système IOS actif, la configuration active, les tables de routage, le cache ARP, les commandes exécutives
NVRAM (RAM Non Volatile)	Pallie le problème de la RAM avec la volatilité des données. Données dans al NVRAM conservées même après une coupure électrique.	Fichier de configuration de démarrage.
ROM (Read Only Memory)	Contient le code pour réaliser les diagnostics de démarrage (POST : Power on Self Test) ; permet le démarrage et le chargement du système d'exploitation contenu sur la mémoire Flash.	POST, bootsrap, les outils de mise en route et de démarrage et le système Cisco IOS
Flash (EPROM, Erasable Programmable Read Only Memory)	Mémoire effaçable et programmable. Utilisée pour maintenir une image et le micro code d'un ou plusieurs systèmes d'exploitation.	Cisco IOS

Tab.1 : Différents types de mémoire dans les équipements Cisco

Les fichiers de configuration :
Il existe différents types de fichiers de configuration. Il y a un fichier de configuration dans la NVRAM (**`startup-config`**), lu au démarrage de l'équipement et copié en mémoire RAM/DRAM. Il existe un autre fichier de configuration dans la mémoire vive (**`running-config`**).

La **`startup-config`** est conservée dans la NVRAM sous forme ASCII. Tandis que la **`Running-config`** apparaît dans la RAM sous forme binaire.

2.4. Les modes de commande du CLI

Il existe plusieurs modes de commandes principaux :

- Accès au mode de configuration en utilisateur (User EXEC)
  Mode utilisé pour changer les paramètres pour l'accès en mode terminal, faires des tests basiques, connaître des informations système
- Accès au mode de configuration en utilisateur privilégié (Privileged EXEC)
  Permet d'accéder à toutes les configurations du commutateur. A protéger par un mot de passe.
- Configuration globale
- Configuration des interfaces
- Configuration des VLAN
  Pour la configuration de VLAN, il existe deux modes de configuration (cf. pour plus de détails la documentation Cisco)
- Configuration des accès ligne de commande

Command Mode	Méthode d'accès	Prompt	Sortir ou accéder au mode suivant
User EXEC	Premier niveau d'accès (accès avec mot de passe)	`Switch>`	**logout** ou **quit** pour sortir **enable** pour accéder au mode EXEC privileged
Privileged EXEC	Du mode User EXEC, entrez **enable**	`Switch#`	**disable** pour sortir **configure** pour entrer dans le mode Global configuration
Global configuration	Du mode Privileged EXEC, entrez la commande **configure**	`Switch(config)#`	**exit** ou **end** ou **ctrl-Z** pour sortir (retour au mode Privileged EXEC) **interface** pour entrer dans le mode Interface configuration
Interface configuration	Du mode Global configuration, entrez la commande **interface**	`Switch(config-if)#`	**end** ou **ctrl-Z** pour sortir (retour au mode Privileged EXEC) **exit** pour sortir (retour au mode Global configuration) **interface** *nom_de_l'interface* pour configurer une interface spécifique
Config-vlan	Du mode Global configuration, entrez la commande **vlan** *vlan-id*	`Switch(config-vlan)#`	**end** ou **ctrl-Z** pour sortir (retour au mode Privileged EXEC) **exit** pour sortir (retour au mode Global configuration)
VLAN configuration	Du mode Privileged EXEC, entrez la commande **vlan database**	`Switch(vlan)#`	**exit** pour sortir (retour au mode Global configuration)
Line configuration	Du mode Global configuration, spécifiez la commande en ligne utilisée (telnet, console..) et entrez la commande **line vty** ou **line console**	`Switch(config-line)#`	**end** ou **ctrl-Z** pour sortir (retour au mode Privileged EXEC) **exit** pour sortir (retour au mode Global configuration)

Tab. 2 : Les différents modes de commande

Les commandes d'aide :

Commande	Rôle
help	Donne un bref descriptif sur l'utilisation d'une commande.
abbreviated-command-entry?	Liste les commandes commençant par une chaîne de caractères Ex : `Switch# di?` `dir disable disconnect`
abbreviated-command-entry<**Tab**>	Complete une commande partielle Ex : `Switch# sh conf`<**tab**> `Switch# show configuration`
?	Liste toutes les commandes d'un mode donné Ex : `Switch> ?`
command ?	Liste les mots clefs pour une commande Ex : `Switch> show ?`
command keyword ?	Liste les arguments d'une commande Ex : `Switch(config)# cdp holdtime ?` `<10-255> Length of time (in sec) that receiver must keep this packet`
↑↓	Rappel des commandes

Tab. 3 : Les commandes d'aides

2.4. Commandes générales

configure terminal : pour entrer dans le mode de configuration
Pour accéder à une fonction de menu il suffit de taper le nom de cette fonction
Pour activer une configuration, **command** pour désactiver cette configuration **no command**

Commandes du mode EXEC user

ping 1.2.3.4 : pingue une machine
traceroute : trouve le chemin vers une destination (adresse IP ou nom)
show history : affiche l'historique des commandes entrées
show mac-address-table : affiche la table de commutation (correspondance numéros de ports, adresse MAC)

show vlan : affiche les vlan (`show vlan id 1`, pour avoir les infos du vlan par défaut, le commutateur si aucun autre vlan n'a été configuré)
show users : affiche les utilisateurs connectés
show snmp : affiche les informations snmp
show flash : affiche les informations système
show clock : affiche l'heure

Commandes du mode EXEC Privileged

clear : pour effacer diverses fonctions configurées (cache arp, mac address-table, port-security...)

copy running-config startup-config : pour sauvegarder ses entrées dans le fichier de configuration

Exemples de commandes d'affichage (`show`) :

show running-config : affiche les configurations courantes fonctionnant
ex : `show running-config vlan` (affiche les vlan en fonction sur le commutateur)

show access-lists : affiche les listes d'accès (ACL, access list) configurées (ACL définie par un numéro ou un nom)

show arp : affiche la table arp des hôtes connectés sur le commutateur

show controllers : affiche les informations sur un port ou tous les ports
ex1 : affiche pour une interface les paquets envoyés et reçus (paquets erronés, collision...)
`switch# show controllers ethernet-controller FastEthernet0/2`

ex2 : affiche l'utilisation de la bande passante sur le commutateur ou un port
show controllers [interface-id] **utilization**
`switch> show controllers utilization` (affiche l'utilisation de la bande passante pour tous les ports)

show interfaces [interface-id|vlan vlan-id] | **accounting** | **capabilities** [module module-number] |**cpe**[port port-id] | **description** | **etherchannel** | **flowcontrol** | **media** [interface-id] | **pruning** | **stats** | **status**[err-disabled] | **switchport** | **trunk** | **transceiver properties** [|{**begin|exclude|include**}expression]
ex : `show interfaces fastethernet0/1` (affiche les informations de l'interface 1 du commutateur)

Options :

- **accounting** : type de protocole + nbre de paquets
  ex : `switch# show interfaces accounting`
- **capabilities** : affiche les capacités d'une ou toutes les interfaces du commutateur (numéro module toujours à 0)
  ex : `switch# show interfaces fastethernet0/1 capabilities` (affiche les différents paramétrages au niveau de l'interface 1 du commutateur)
- **description** : affiche le statut et état de l'interface
  ex : `switch# show interfaces fastethernet0/1 description`
- **stats** : affiche les statistique sur chaque port du commutateur
  ex : `switch# show interfaces stats`

- **status** : affiche le statut, le mode de connexion (connecté - non connecté), l'appartenance à un vlan ou un trunk, le mode duplex, la vitesse, le type d'une interface ou de toutes les interfaces du commutateur
  ex : `switch# show interfaces status`

- **trunk** : affiche les informations sur le trunk (si interface non précisée, informations sur le trunk actif)
  ex : `switch# show interfaces trunk (show interfaces festethernet0/1 trunk)`

- **transceiver properties** : affiche vitesse et mode duplex pour une interface
  ex : `switch# show interfaces transceiver properties`

show ip interface `vlan 1` : affiche les informations IP du vlan par défaut (donc du commutateur)

show ip traffic : affiche le trafic par protocole sur le commutateur

show mac address-table : affiche la table de commutation du commutateur

Commandes du mode Global configuration

mac address-table ageing-time : permet de fixer la durée de vie d'une adresse dynamique dans la table de commutation

mac address-table static : permet d'avoir une entrée statique dans la table de commutation
mac address-table static `@mac` **vlan** `vlan-id` **interface** `interface-id`
no mac address-table static `@mac` **vlan** `vlan-id` **interface** `interface-id`
ex : `switch(config)#mac address-table static 0004.5236.bc45 vlan 1 interface fastethernet 0/2`

Configuration de **fonction de monitoring** (**monitor**)
Il est possible d'analyser le trafic d'un port en recopiant ce trafic sur un autre port, on parle de miroir de port, Cisco utilise le terme de technologie SPAN. Les miroirs SPAN reçoivent ou envoient (ou les deux) le trafic d'un ou plusieurs port(s) source vers un port destination pour permettre l'analyse.

monitor session `number-session` **source interface** `interface-id` [**both|tx|rx**]
- session number à mettre à 1
- possibilité de monitorer le trafic entrant et sortant (both) ou entrant (rx) ou sortant (tx)

ex : Dans un premier temps toutes les configurations SPAN sont effacées, et ensuite tout le trafic du port 1 est recopié sur le port 8

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/1
Switch(config)# monitor session 1 destination interface fastethernet0/8
```

Configuration des **access-list** (ACL)

access-list : pour configurer des listes d'accès (ACL, Access list) sur le commutateur ou une interface (filtrage par adresses MAC ou IP, par protocoles, par numéros de ports...)
no access-list : pour supprimer l'ACL
access-group : pour appliquer une ACL à une interface particulière (depuis le menu interface en spécifiant l'interface sur laquelle on désire appliquer l'ACL, dans le sous-menu `ip`)

`switch(config)#`**`access-list`** `access-list-number {`**`deny|permit|remark`**`} {source source-wildcard | `**`host`** `source | `**`any`**`}`

- numéro de ACL : entre 1 et 99 pour des ACL IP standard (filtrage utilisant les adresses sources) et entre 100 et 199 pour des ACL IP étendues (filtrage utilisant les adresses sources et destinations, et optionnellement des informations sur les types de protocoles permettant un filtrage plus "fin")
- `source` : adresse de l'émetteur du paquet, donnée en décimal pointée (adresse qui sera rejetée –`deny`- ou autorisée –`permit`)
- `source-wildcard` : netmask inversé (par défaut 0.0.0.0)
- `any` équivalent à la source 0.0.0.0 et la source-wildcard 255.255.255.255
- le mot `host` est une abréviation pour une adresse source avec comme la valeur par défaut pour la source-wildcard (0.0.0.0)

Remarques :

- `wildcard address` désigne l'adresse de netmask inversée (exemple pour un netmask d'un réseau de classe C en 255.255.255.0, la notation à adopter pour l'ACL est 0.0.0.255 ; pour désigner une machine spécifique, la valeur pour l'`address wildcard` sera 0.0.0.0)
- si le masque est omis, la valeur par défaut est 0.0.0.0 qui sera associée à l'adresse IP
- en créant une ACL, il existe implicitement une règle par défaut à la fin de la liste des différentes règles contenant l'état **`deny`** pour tous les paquets qui ne sont pas traités dans les règles définies par l'ACL. Il faut alors ajouter à la fin une règle autorisant tout le reste.
  De manière générale, pour définir les règles de sécurité, il existe deux approches selon la politique de sécurité appliquée :
  - Autoriser uniquement les communications ayant été explicitement autorisées et tout ce qui n'est pas explicitement autorisé est interdit
  - Empêcher les échanges explicitement interdits.

ex1 : Exemple d'ACL rejetant l'adresse IP 171.69.192.68, et autorisant toutes les autres

```
switch(config)# access-list 2 deny 171.69.192.68
switch(config)# access-list 2 permit any
switch(config)# end
switch# show access-list
Standard IP access list 2
        deny 171.69.192.68
        permit any
```

Pour appliquer cette ACL au commutateur (soit le vlan par défaut)

```
switch#configure
switch(config)# interface vlan 1
switch(config-if)#ip access-group 2 in
```

Pour l'appliquer à un port particulier

```
switch#configure
switch(config)# interface FastEthernet 0/1
switch(config-if)#ip access-group 2 in
```

ex2 : Exemple d'ACL étendue pour rejeter le trafic du port 80, et autoriser tous les autres trafics sur le port gigabit numéro1 (port en gigabit)

```
switch(config)# access-list 106 deny tcp any any eq 80
switch(config)# access-list 106 permit ip any any
switch(config)# interface GigabitEthernet 0/1
switch(config-if)#ip access-group 106 in
```

ex3 : Exemple d'ACL appliquée au commutateur acceptant les paquets du réseau 36.0.0.0/8 et refusant les paquets du réseau 56.0.0.0/8

```
switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
switch(config)# access-list 2 deny 56.0.0.0 0.255.255.255
switch(config)# interface vlan 1
switch(config-if)#ip access-group 2 in
```

ex4 : Exemple d'ACL autorisant un hôte connecté à Internet de pouvoir accéder à telnet et à sa messagerie

```
switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
switch(config)# interface vlan 1
switch(config-if)#ip access-group 2 in
```

Commandes du mode Interface configuration

Préambule : Qu'appelle-t-on interface sur les commutateurs Cisco Catalyst 2960 ?

Types d'interface définis sur les commutateurs Cisco Catalyst 2960
- **`access port`** : port faisant transiter du trafic d'un seul vlan
- **`trunk port`** : port faisant transiter du trafic de plusieurs vlan (nécessité de marquer les trames pour identifier leur appartenance à un vlan donné – vlan tagging, norme 802.1Q)
- **`vlan`** : réseau commuté logiquement segmenté (par port ou adresse mac) - identifiant vlan-id
- **`EtherChannel port groups`** : possibilité de traiter plusieurs ports comme un seul port

Paramètres d'une interface physique (port)
- Type : Fast Ethernet (**`FastEthernet`** ou `fa`) pour Ethernet 10/100, Gigabit Ethernet (`gigabitethernet` ou `gi`), ou LRE (`longreachethernet` ou `lo`).
- Slot : numéro de slots toujours à 0 sur ces commutateurs
- Numéro de port

ex1 : `switch(config)# interface FastEthernet 0/x` (accès au menu de configuration du port numéro x, possibilité de paramétrer le mode de fonctionnement -`duplex`- la vitesse -`speed`-, fixer une adresse mac -`mac-address`- désactiver ce port -`shutdown`...)

ex2 : `switch(config)# interface vlan 1`
`switch(config-if)# ip address x.x.x.x` (x, nombre décimal)
Fixe l'adresse IP du commutateur. Configuration du vlan vue comme une interface permettant de donner une adresse IP, une adresse mac, fixer la bande passante, le désactiver...

`shutdown` (**`no shutdown`**) : pour activer ou désactiver un port ou un vlan (choix du vlan pour le management, par défaut le vlan1)

ex3 : Exemple de désactivation/réactivation d'un port

```
Switch# configure terminal
Switch(config)# interface fastethernet0/5
Switch(config-if)# shutdown
Switch(config-if)#
*Sep 30 08:33:47: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to a
administratively down

Switch# configure terminal
Switch(config)# interface fastethernet0/5
Switch(config-if)# no shutdown
Switch(config-if)#
*Sep 30 08:36:00: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
```

ex4 : Procédure pour changer le vlan par défaut (vlan3 devenant le vlan par défaut)

```
switch(config)# interface vlan 3
switch(config-if)# ip address 172.10.1.1 255.255.255.0
switch(config-if)# no shutdown
switch(config-if)# exit
```

`range` : permet de configurer plusieurs ports avec les mêmes paramètres de configuration

ex5 : Configuration de la vitesse pour plusieurs ports

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 5
Switch(config-if-range)# speed 100
```

ex6 : Activation d'une gamme de ports (utilisation de la virgule pour séparer les différents arguments)

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 - 3, gigabitethernet0/1 - 2
Switch(config-if-range)# no shutdown
```

Configuration **d'EtherChannel**

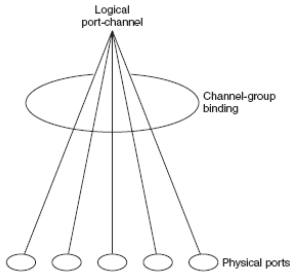


Figure 5 : Relation entre Port Physique, Channel Group, et le port logique agrégé

Plusieurs protocoles d'agrégation de ports : propriétaires Cisco (PAgP) ou LACP (norme IEEE 802.3ad)

Ex : Configuration d'un lien EtherChannel ayant 2 ports physiques du Vlan 10 sur le channel 5 en mode automatique (choix du mode qui permet de choisir le protocole d'agrégation de ports)

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode auto
Switch(config-if-range)# end
```

Commandes du mode config-vlan

mtu : configuration du la taille maximum de trame sur le réseau
state : activer ou suspendre un vlan
shutdown vlan vlan-id (**no shutdwon vlan** vlan-id) : pour suspendre le trafic local sur un vlan

Commandes du mode Line configuration

vty 0 15 : permet de configurer jusqu'à 16 sessions telnet
password : pour donner un mot de passe pour les accès au menu de configuration

ex : Configuration d'un mot de passe pour un accès par Telnet (jusqu'à 10 sessions telnet en parallèle)

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
Switch(config-line)# login
```

Commandes de configuration du Spanning Tree

BID : <priority> : <MAC@> -- priority dftl to 32768
Lowest priotity bridge gets elected root bridge

Specify root bridge per VLAN	`Switch(config)# spanning-tree <VLANn> root`
Set priority (dflt 32768)	`Switch(config)# spanning-tree <VLANn> [priority <p>]`
Set STP cost of If	`Switch(config-if)# spanning-tree cost <c>`
	`Switch# show spanning-tree [interface|vlan]`

Procédure de sauvegarde sur serveur TFTP

Downloading the Configuration File By Using TFTP

To configure the switch by using a configuration file downloaded from a TFTP server, follow these steps:

Step 1 Copy the configuration file to the appropriate TFTP directory on the workstation.

Step 2 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page B-10.

Step 3 Log into the switch through the console port or a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the switch.

Specify the IP address or hostname of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

```
Switch# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File By Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

Step 1 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File By Using TFTP" section on page B-10.

Step 2 Log into the switch through the console port or a Telnet session.

Step 3 Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

Procédure de récupération de mot de passe

Passwd Recovery : enter ROMmon	Hold MODE at power up, release when STAT turns off

load flash	`flash_init`
	`load_helper`
	`dir flash:`

rename config file	`rename flash:config.text flash:config.old`
boot switch	`boot`
exit setup	`Ctrl-C / N`
	`Switch# rename flash:config.old flash:config.text`
	`Switch# copy flash:config.text system:running-config`
	`Switch# config t`
	`Switch(config)# no enable secret`
	`Switch(config)# enable passwd <passwd>`
Reset console/vty passwd as well	`Switch(config)# exit`
	`Switch# copy run start`
	`Switch# reload`