Travaux pratiques : Ethernet sur le LAN

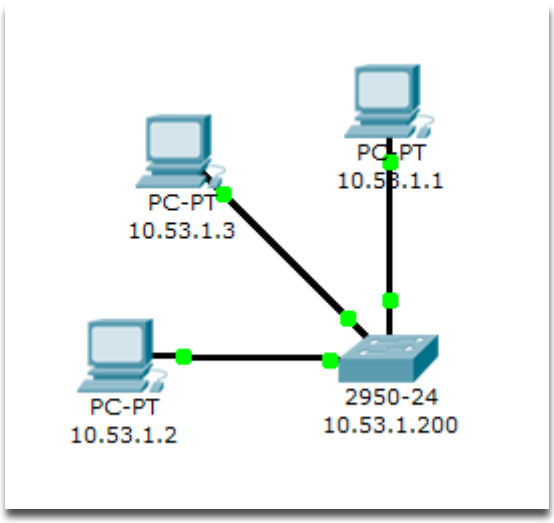
Lab 1.2.3&4

1: Configuration du switch Cisco 2960

Exemple de configuration de la vitesse d'un port sur l'interface fa0/1:

interface FastEthernet0/1
ip address 10.53.1.200 255.255.255.0
duplex auto
speed auto
end

Schéma du réseau



Commande flash_init , load_helper & del_flash

```
switch: flash_init
Initializing Flash...
...The flash is already initialized.
Setting console baud rate to 9600...

switch: load_helper

switch: del flash:config.text
Are you sure you want to delete "flash:config.text" (y/n)?y
File "flash:config.text" deleted

switch:
```

Commande dir flash

```
switch: dir flash:
Directory of flash:/

3    -rwx  5         <date>              private-config.text
4    -rwx  1543      <date>              enssat.cfg
5    -rwx  1480      <date>              ipv6.conf
6    drwx  192       <date>              c2960-lanbase-mz.122-25.SEE3
621  -rwx  1335      <date>              jfm.conf
622  -rwx  616       <date>              vlan.dat

24797696 bytes available (7716352 bytes used)

switch:
```

Configuration de base du switch

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password 0 lannion
Switch(config)#int vlan1
Switch(config-if)#ip address 10.53.1.200 255.255.255.0
Switch(config-if)#exit
Switch(config)#line vty 0
Switch(config-line)#password 0 lannion
Switch(config-line)#exit
Switch(config)#line vty 1
Switch(config-line)#password 0 lannion
Switch(config-line)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

2: Configuration du réseau

Après configuration du réseau et la modification de la vitesse de connexion sur une interface du switch, il s'est avéré que le réseau est tombé.

3 : Gestion des tables de commutation

Table de commutation :

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001a.9256.beba    DYNAMIC     Gi0/2
   1    001b.219c.86e5    DYNAMIC     Gi0/1
Total Mac Addresses for this criterion: 22
Switch#
```

Par défaut les ports sont « DYNAMIC » ce qui stipule qu'à chaque connexion le switch va relever l'adresse Mac de l'hôte ainsi que le numéro de port où il s'est branché.

Après changement de port, l'interface a été automatiquement changée

```
 All    ffff.ffff.ffff    STATIC      CPU
   1    001a.9256.beba    DYNAMIC     Gi0/2
   1    001b.219c.86e5    DYNAMIC     Fa0/22
Total Mac Addresses for this criterion: 22
Switch#
```

Méthode pour identifier un port avec une adresse IP :

Afficher la table ARP (sh arp) qui va nous donner l'adresse Mac ainsi que le Vlan (si il y a lieu) dans lequel se trouve notre machine, puis afficher la table de commutation (sh mac-address-table) qui va nous donner le type du port (dynamic ou static) et surtout sur quel port la machine est connectée.

Protéger l'accès en verrouillant une adresse MAC sur un port :

Conf t
Int fa0/1
switchport mode access
switchport port-security
switchport port-security mac-address 001b.219c.86e5
switchport port-security violation shutdown
exit
exit

Switch#sh port-security interface fa0/1

Secure	Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Security Action
		(Count)	(Count)	(Count)	
	Fa0/1	1	1	0	Shutdown

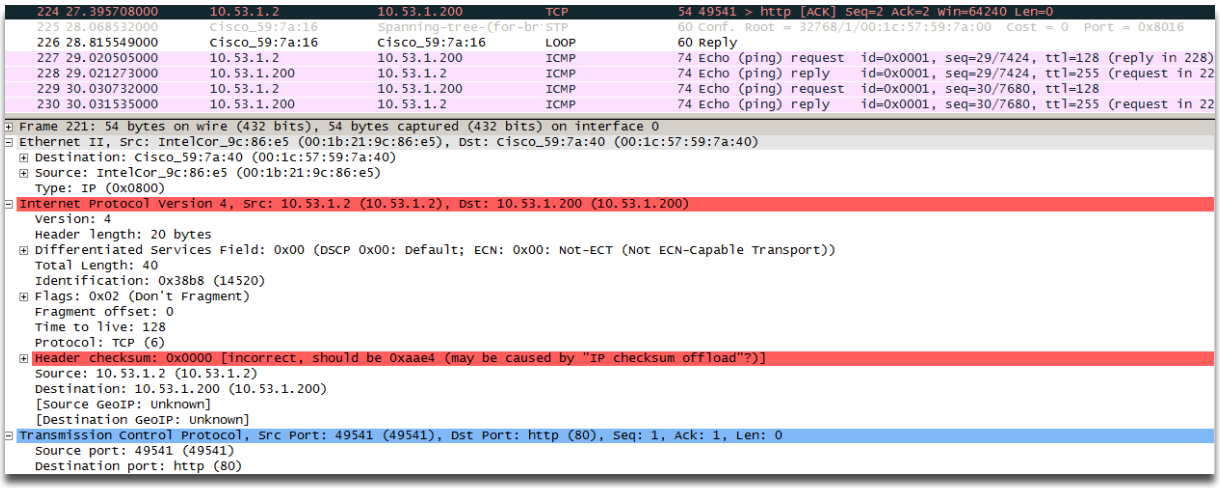
Switch#sh port-security interface fa0/1
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 001b.219c.86e5 :1
Security Violation Count : 0

Distinction entre table de commutation et table ARP

La table ARP est utilisée par les hôtes pour déterminer l'adresse MAC d'un autre ordinateur sur le même segment alors que table de commutation indique les données des routes stockées dans un commutateur, il indique la ligne de sortie en fonction de la référence transportée par le paquet.

4 : Analyse de trafic

Trame observée



En cas d'absence de trafic, aucunes trames ne circulent sur le réseau, dans notre cas nous avons des requêtes http (port 80) provoqué par ka page web du switch.

Cette fenêtre se décompose en trois sous-fenêtres. Celle du dessus indique la liste des trames capturées. Elle indique le numéro de capture, la date de capture (heure), l'adresse de l'émetteur, celle du récepteur, le protocole correspondant à l'information capturée et la sémantique de l'information transportée par la trame.
La seconde fenêtre indique l'encapsulation protocolaire. On peut y voir le paquet du plus haut niveau encapsulé, successivement dans des unités de données de plus bas niveau. Par exemple, un datagramme TCP, dans un paquet IP, lui-même dans une trame Ethernet. On peut sélectionner chaque paquet et y voir les divers champs.
Enfin, la sous-fenêtre en bas, affiche la même information, mais cette fois-ci sous forme hexadécimale.

Que ce passe t'il lors d'un trafic, sur un analyseur qui n'est pas sur la machine et un switch ?

Eh bien il ne se passe rien, la carte réseau ne lira que le trafic qui lui est destiné…
Si nous voulions observer tout le trafic sur une carte réseau, il faudrait par exemple activer le mode « promiscuous ».
Mais le mode promiscuous ne sert à rien si l'on est sur un switch en fonctionnement normal : il n'envoie que les broadcast et le trafic à destination des adresses mac connues sur ce port. Le mode promiscuous ne concerne que la carte réseau, en aucun cas le switch ou un hub (encore moins) pour lequel ça n'a aucune signification, puisqu'il fonctionne au niveau électrique et ne sélectionne pas les trames en fonction de la destination.

Pour qu'un port de switch puisse émettre le trafic destiné à un autre port, il faut le lui préciser par configuration (**monitor** chez Cisco) à la différence d'un hub qui retransmettra tout ce qu'il reçoit.

Redirection de trafic avec la commande « monitor »

```
Switch(config)#monitor session 1 source interface fa0/22
Switch(config)#monitor session 1 destination interface fa0/24
Switch(config)#end
Switch#
01:45:52: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh monitor
Session 1
---------
Type               : Local Session
Source Ports       :
    Both           : Fa0/22
Destination Ports  : Fa0/24
    Encapsulation  : Native
          Ingress  : Disabled
```

```
Switch(config)#do sh int fa0/24
FastEthernet0/24 is up, line protocol is down (monitoring)
  Hardware is Fast Ethernet, address is 001c.5759.7a18 (bia 001c.5759.7a18)
```

Lab 5

5 : Différence entre un HUB et un SWITCH

Quel câble utiliser pour raccorder un switch à un hub ? : Le câble droit.

Le trafic du hub sélectionne tout ce qui passe sur le réseau, il est donc inutile de faire une redirection.

Les performances du hub sont significativement moins bonnes que le switch (collisions…).

Une redirection s'opère sur le lien « switch-hub » (comportement réseau) lorsqu'un pc émet vers un autre pc.

Le **hub** est le matériel réseau le plus basique. Il est utilisé pour un réseau local avec un nombre très limité de machines. Il n'est ni plus ni moins qu'une 'multiprise RJ45' qui amplifie le signal réseau (base 10/100). Dans ce cas, une requête destinée à un ordinateur X du réseau sera envoyée à la totalité des ordinateurs du réseau. Cela réduit considérablement la bande passante et pose des problèmes d'écoute du réseau.

Le **switch** (ou commutateur) travaille lui sur les deux premières couches du modèle OSI, c'est-à-dire qu'il distribue les données à chaque machine destinataire, alors que le hub envoie toutes les données à toutes machines qui répondent. Conçu pour travailler sur des réseaux, avec un nombre de machines légèrement plus élevé que le hub, il élimine les collisions de paquets éventuelles *(une collision apparaît lorsqu'une machine tente de communiquer avec une seconde alors qu'une autre est déjà en communication avec celle-ci..., la première réessaiera quelques temps plus tard)*.

Lab 6

6 : Mise en place des Vlans

Placer les switchs en mode VTP Transparent :

Conf t
vtp mode transparent

Création des vlans

Conf t
Vlan 1,2,3

Que se passe t'il lorsque l'on place un port dans un vlan non configuré ?

Le switch va créer automatiquement le vlan

Contenu de la « database »

Commande : Sh vlan

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
2    VLAN0002                          active
3    VLAN0003                          active    Fa0/1
4    VLAN0004                          active    Fa0/3
5    VLAN0005                          active    Fa0/5
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Attribuer un port, ou plusieurs à un vlan

Un seul port

2960-switch(config)#interface fa0/1
2960-switch(config-if)#switchport mode access
2960-switch(config-if)#switchport access vlan 1
2960-switch(config-if)#end

Plusieurs ports

2960-switch(config)#interface range fastEthernet 0/5-8
2960-switch(config-if-range)#switchport mode access
2960-switch(config-if-range)#switchport access vlan 4
2960-switch(config-if-range)#end

Les machines ne peuvent se « pinguer » puisqu'elles n'appartiennent pas au même vlan.

En changeant tous les ports dans le même vlan, seules les machines du même réseau pourront communiquer.

Le broadcast est une diffusion de données à un ensemble de machines connectées à un réseau, les vlans (réseau virtuel) quant à eux n'existent que sur les switchs (bien que l'on puisse en configurer en mode trunk, donc multiplexés, sur les routeurs et les serveurs). Cela consiste à diviser le switch (comme si on le coupait en morceaux) en différents switchs virtuels de façon à isoler le trafic entre ces différentes parties. Le but étant essentiellement de réduire le pourcentage de trafic broadcast (diffusé sur tous les ports d'un même vlan) sur un réseau.

Un switch à par défaut un vlan (en général vlan1), il consiste à y intégrer tous les ports non attribués manuellement, ce qui permettra la communication entre eux.

Lab 7, 8

7 : Construction d'un trunk entre 2 switchs

Après avoir placé les ports 1 des switchs dans le vlan 3 et les ports 2 dans le vlan 4, nous avons paramétré un trunk sur les ports 24 des switchs :

Conf t
Int fa0/24
switchport mode trunk

La continuité des vlans 3 est établie tout comme celle des vlans 4 mais les deux réseaux, 10.53.1.x et 10.53.2.x ne se pinguent pas.

Activer le mode trunk revient à activer un protocole d'encapsulation (généralement dot1q) dont le but est de marquer les trames qui transitent entre deux équipements afin qu'elles puissent être attribuées au bon VLAN de l'autre côté.

Pour interdire un vlan de passer par le lien trunk (dans l'exemple, le vlan3)

switchport trunk allowed vlan remove 3

8 : Utilisation du protocole VTP

Le switch possède 3 modes VTP: client, transparent ou server (actif par défaut), mais cela ne change pas la connectivité entre switchs :

- VTP Server: switch qui crée les annonces VTP
- VTP Client: switch qui reçoit, se synchronise et propage les annonces VTP
- VTP Transparent: switch qui ne traite pas les annonces VTP

Switch en mode VTP Server

Le switch en mode **Server** permet à l'administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les switchs du réseau.

Le VTP Server :
- Crée des VLANs
- Supprime des VLANs
- Modifie des VLANs (par exemple son nom : name xxxx)
- Envoi et transmet des messages VTP
- Se synchronise avec d'autres switchs VTP

Switch en mode VTP Client

Le switch en mode ***Client*** **ne permet pas** à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN.

Le VTP Client:
- Ne peut pas créer des VLANs
- Ne peut pas supprime des VLANs
- Ne peut pas modifier des VLANs
- Traite les messages reçus et les transmets aux voisins
- Se synchronise avec d'autres switchs VTP

Switch en mode VTP Transparent

Le switch en mode ***Transparent*** permet à l'administrateur de faire toute modification sur les VLANs en **local uniquement** et donc **ne propage pas** ses modifications vers tous les switchs du réseau. Très pratique pour des maquettes!

Le VTP Transparent :
- Crée des VLANs
- Supprime des VLANs
- Modifie des VLANs
- Ne traite pas les messages VTP reçus mais les transmets aux voisins
- Ne se synchronise pas avec d'autres switchs VTP

9 : Mise en place de liens redondants et activation du spanning-tree


```
Switch#sh spanning-tree int fa
04:31:34: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state t
o up0/24

Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Altn BLK 19        128.24   P2p
VLAN0002         Desg FWD 19        128.24   P2p
VLAN0003         Altn BLK 19        128.24   P2p
VLAN0004         Altn BLK 19        128.24   P2p
VLAN0005         Desg FWD 19        128.24   P2p
Switch#
```