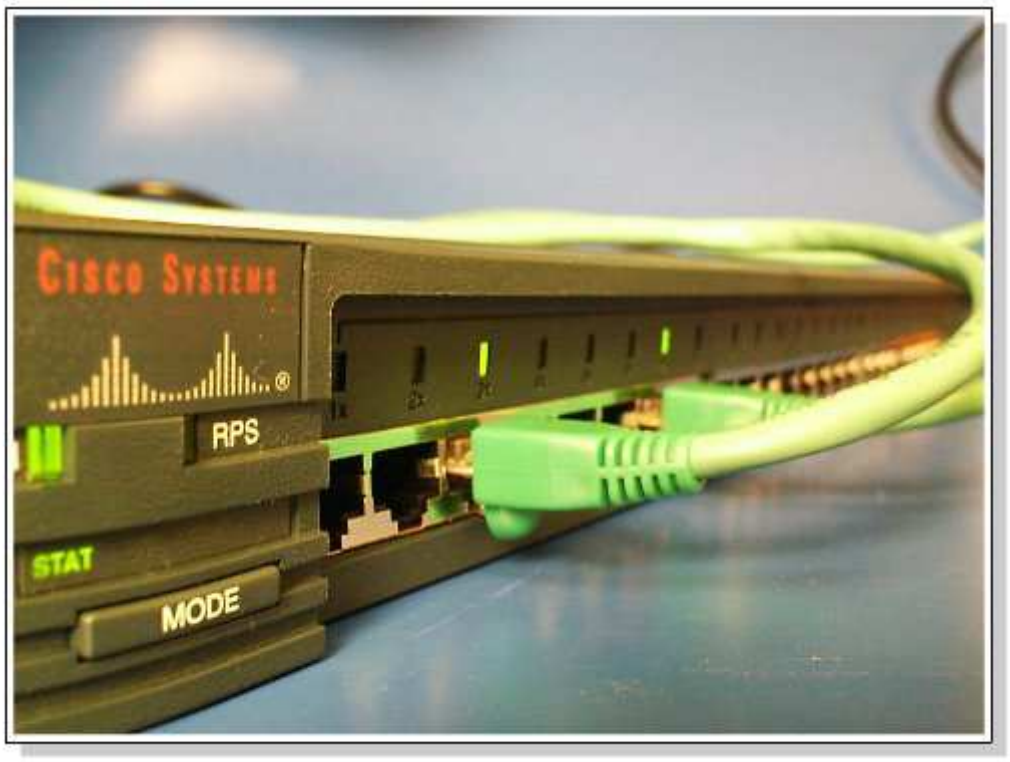
TP : Mise en place d'un LAN



TP Mise en place d'un LAN

1) Objectifs

L'étudiant devra être capable :

D'identifier les différents matériels dans le réseau (routeur, switch, hub, PC, etc....)

De câbler les différents matériels suivant une architecture réseau

De configurer les switches et les routeurs face aux exigences de sécurité et de configuration

- De vérifier par des tests élémentaires la conformité de l'architecture du réseau local

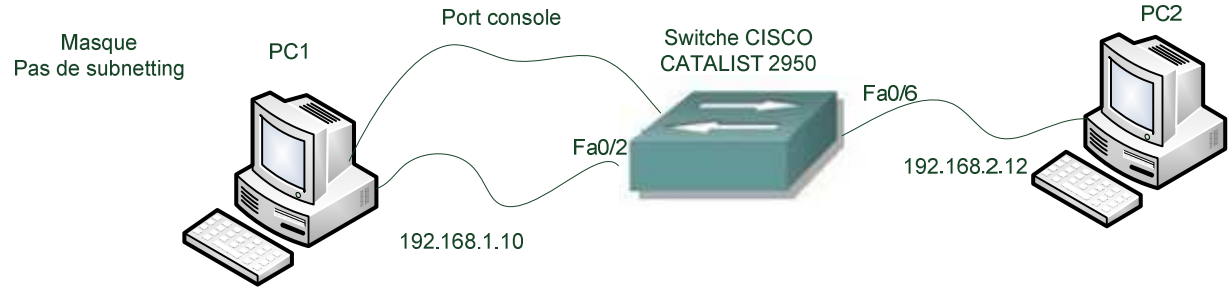
2) Pré-requis

Cours sur les réseaux à technologie TCP-IP.

3) Configuration d'un switch

3.1) Utilisation d'un switche sans paramétrage du switche

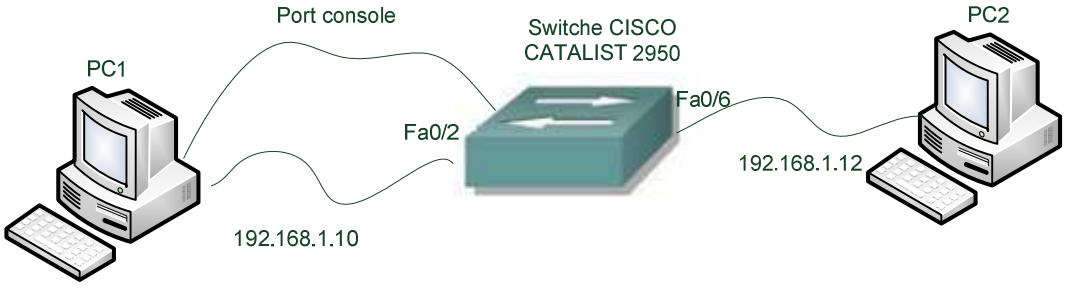
3.1.1) Réalisez le câblage suivant en configurant PC1 et PC2:



Pour la programmation du masque de sous –réseau on considérera pour tout le TP qu'il y aura un seul réseau (pas de subnetting)

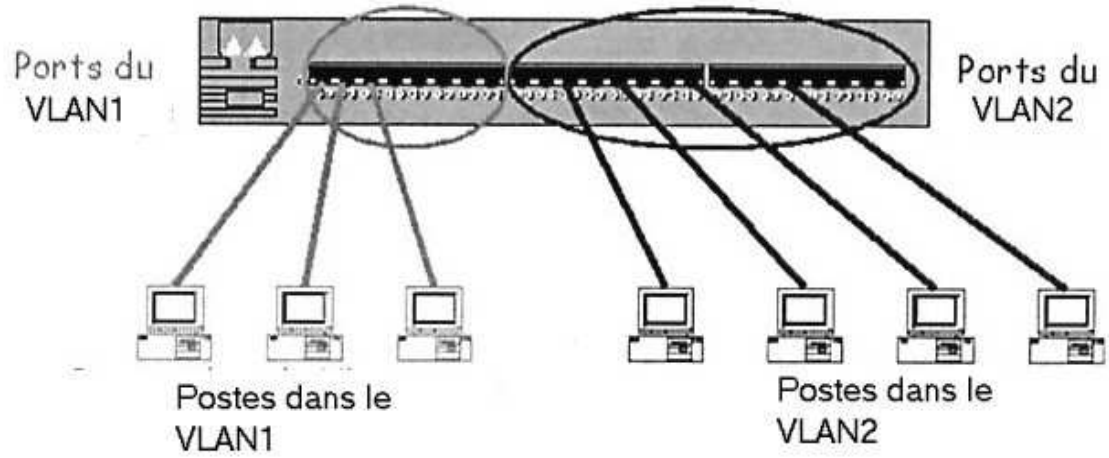
3.1.2) Pingez les 2 machines que constatez vous, interprétez les résultats.

3.1.3) modifiez la configuration de PC2 voir schéma ci-dessous :



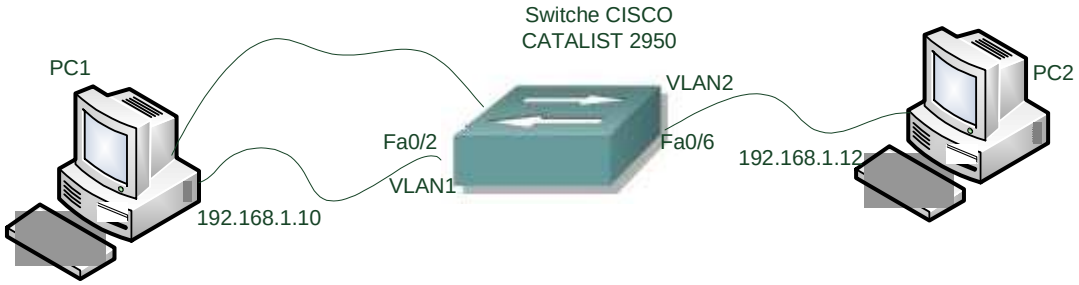
Pingez les 2 machines, conclure.

On souhaite créer 2 réseaux locaux virtuels VLAN1 et VLAN2 de niveau 1(voir dossier annexe) de la façon suivante :



3.2) Utilisation d'un switche avec VLAN

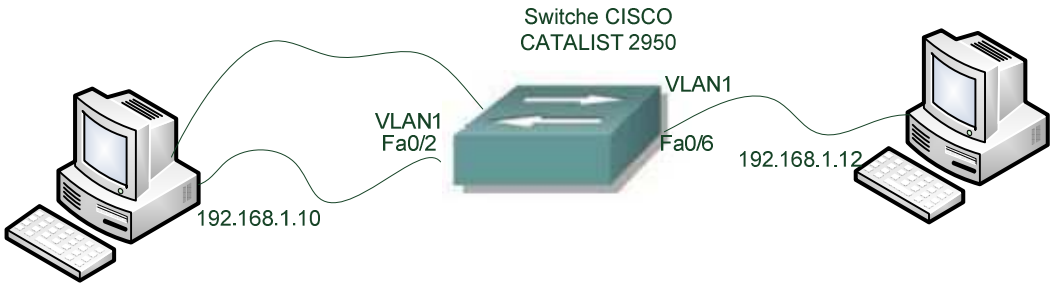
3.2.1) Configurez le switche CISC0 de la façon suivante:



On pourra s'aider du dossier annexe pour la configuration du switche

3.2.2) Pingez les 2 machines que constatez vous, interprétez les résultats.

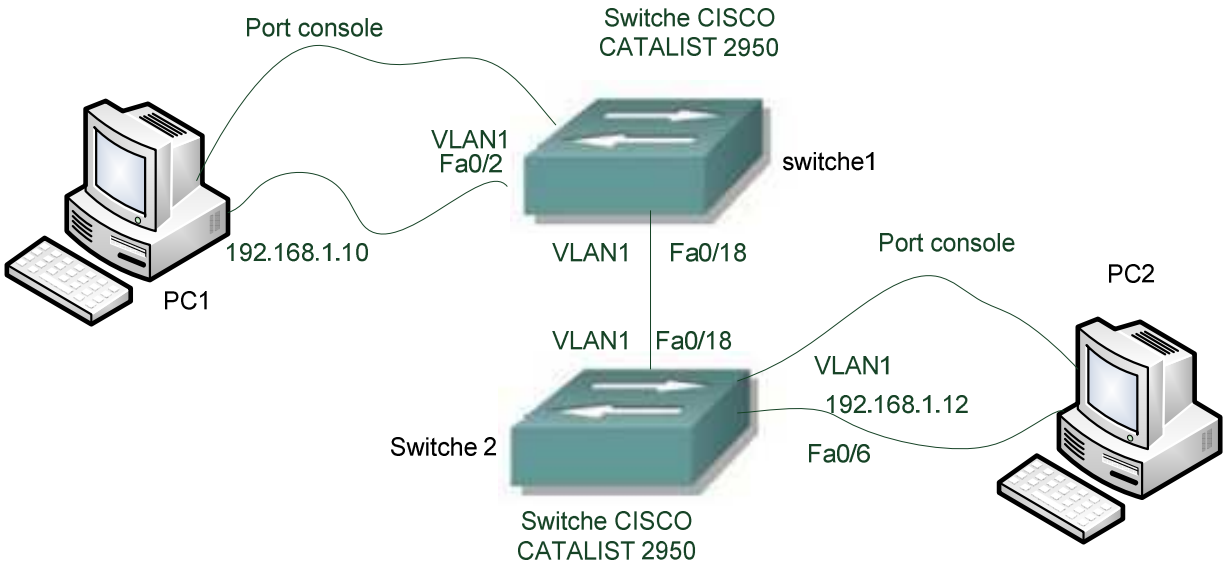
3.2.3) Modifiez la configuration du switche de la façon suivante :



Pingez les 2 machines, conclure.

3.3) Utilisation de 2 switches avec VLAN

3.3.1) Réalisez le câblage suivant en configurant les 2 switches.



3.3.2) Quelle est la nature du câble que vous avez choisi pour relier les 2 switches.

3.3.3) Pingez les 2 machines et vérifiez si celle-ci se voit

3.3.4) affectez les adresses IP suivantes :

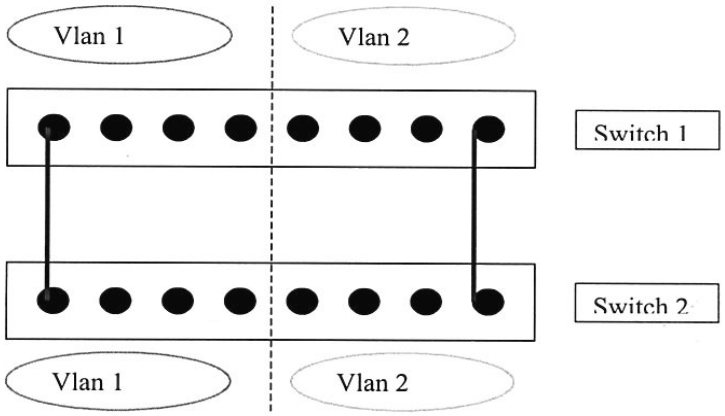
- 192.168.1.4 Aux VLAN1 du switche N°1.
- 192.168.1.5 Aux VLAN2 du switche N°2.

3.4) Remarque :

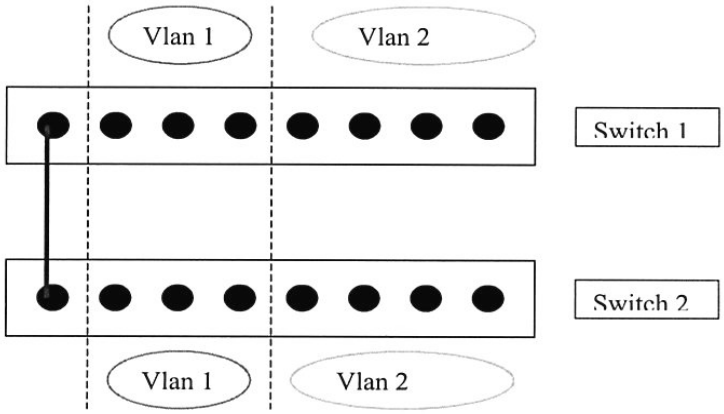
Propagation de VLAN

Si vous désirez propager plusieurs VLAN sur un même lien physique, il faut configurer un TRUNK et la norme établie est la 802.1Q. Pour cela il faudra que vos paquets soit taggués, c'est-à-dire qu'ils contiennent dans leurs en têtes le numéro du VLAN (VLAN ID) pour lequel ils sont destinés.

- **Propagation de VLAN :**



- On est obligé de tirer deux câbles pour relier les deux vlan ensemble .
- Pour éviter cela, on fait de la propagation de vlan ce qui permet de ne tirer qu'un seul câble .



Il existe trois types de définition d'appartenance d'un port à un VLAN

access	Place le port en mode access. Le port appartient à un seul VLAN et ne reconnaît que des trames non tagguées. C'est le mode normal pour les ports clients
Multi	Le port appartient à un ou plusieurs VLANS mais n'accepte que des trames non tagguées
Trunk	Place le port en mode trunk. Ce type de port est utilisé pour connecter des switchs entre eux ou le switch avec des routeurs. Le port émet et reçoit des trames tagguées

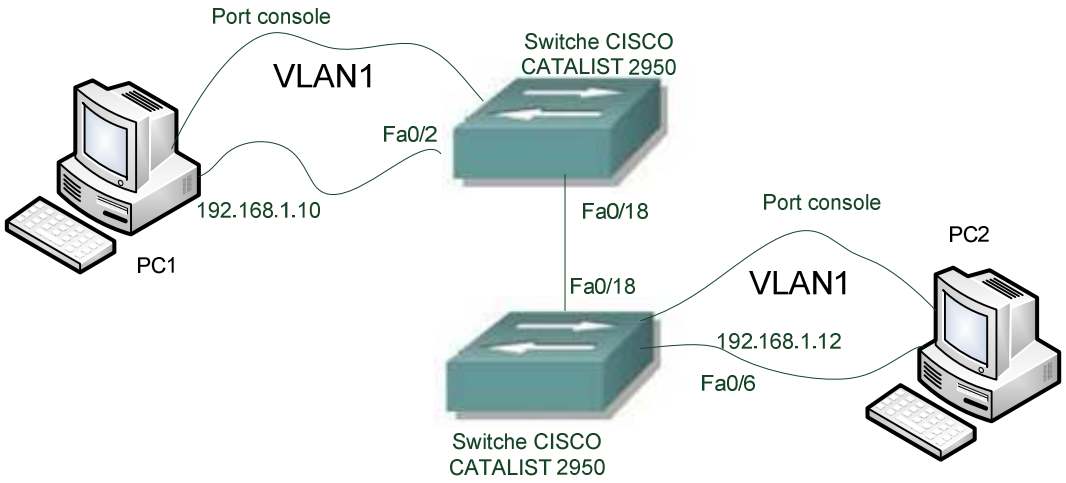
SwitchX # **conf t**

SwitchX(config)#**int** « *numéro de l'interface*»

SwitchX(config-if)#**switchport mode trunk**

SwitchX(config-if)#**switchport trunk allowed vlan except**« *numéro du vlan* »

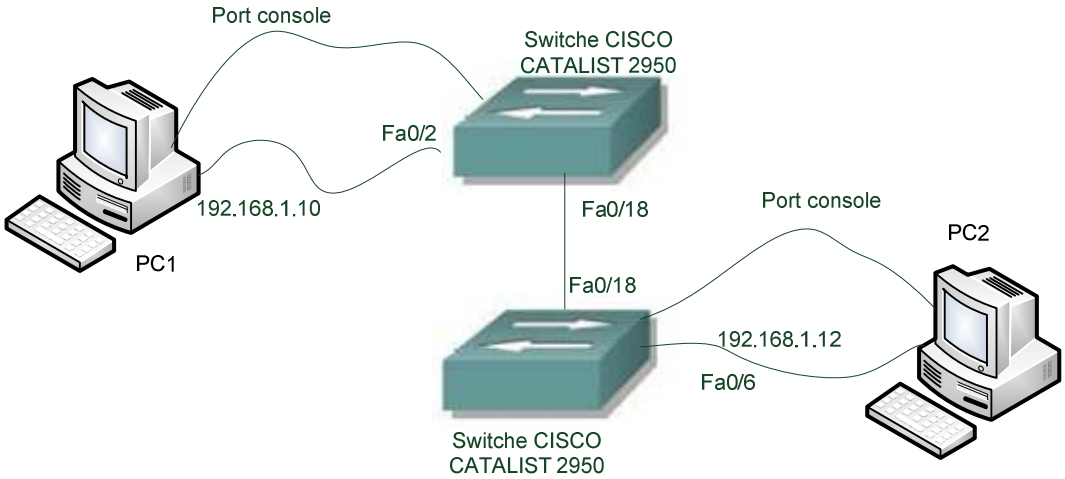
3.5) Propagation de VLAN



3.5.1) Configurez les switches de façon à créer un TRUNK entre le switche 1 et le switche 2
3.5.2) Pingez les 2 machines et vérifiez si celle-ci se voit

3.6) Utilisation de 2 switches sans VLAN

3.6.1) Configurez les switches de façon à supprimer les VLANs
3.6.2) Pingez les 2 machines et vérifiez si celle-ci se voit



3.6.3) Affectez respectivement le port fa0/2 et fa0/6 avec l'adresse Ethernet de PC1 et de PC2

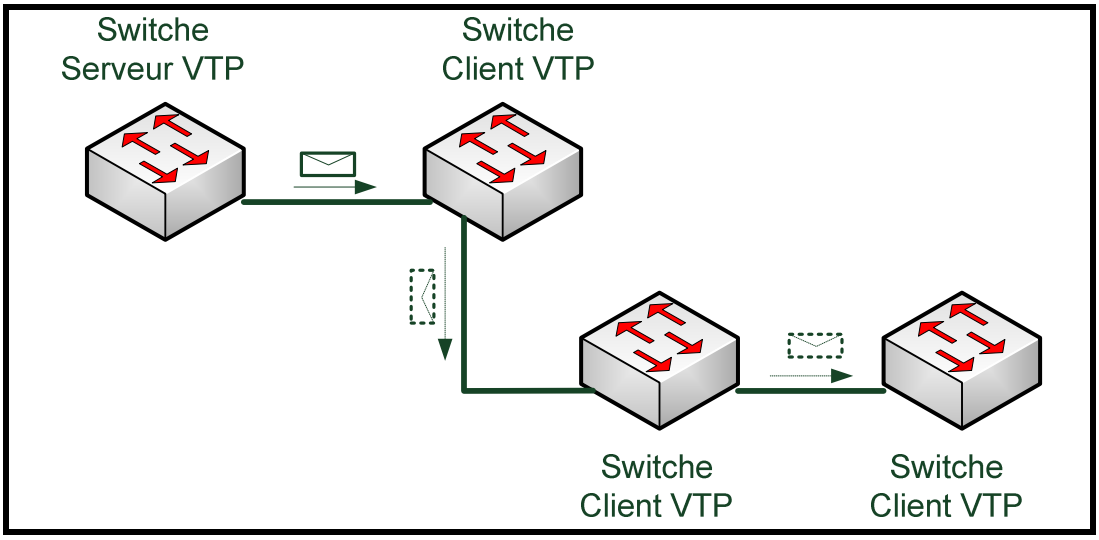
3.7) Le mode VTP (VLAN Trunking Protocol)

Lorsqu'il y a beaucoup de switches sur un réseau dans une topologie arbre il devient très fastidieux de configurer chaque switche pour propager les VLANs. Il existe un protocole qui permet à un switche serveur de propager les VLANs vers plusieurs switche client. Ce protocole est appelé VTP.
Le serveur VTP envoit des messages entre les differents switches pour maintenir ces VLANS sur ces differents switches .
Les messages VTP sont échangés entre les switches à l'intérieur d'un domaine VTP Commun.
Les switches peuvent dont opérer suivant 3 modes VTPs :

- Serveur
- Client
- Transparent (ne participe pas au mode VTP)

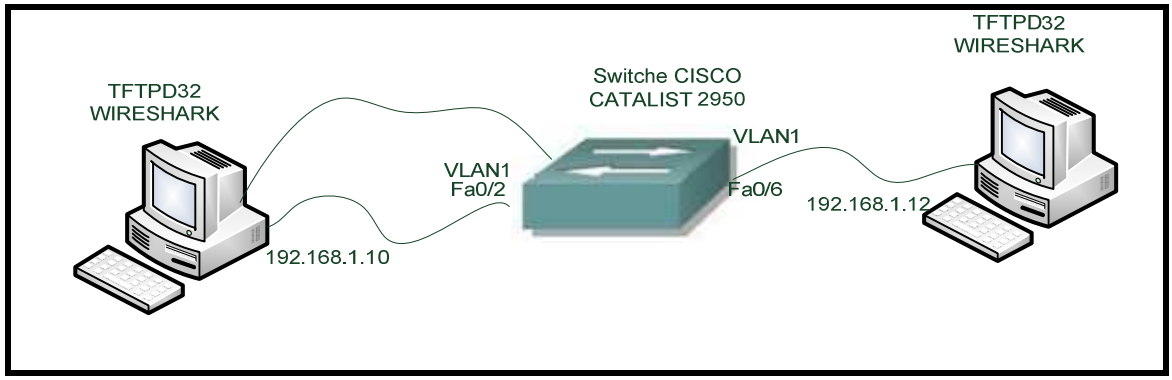
	Task	Command
Step 0	Define the VTP mode (server/client/transparent)	**vtp mode** *mode*
Step 1	Define the VTP domain name (Case sensitive)	**vtp domain** *name*
Step 2	Set which VTP version to run	**vtp version** #
Step 3	(Optional) Set a password for the VTP domain.	**vtp password** *password*
Step 4	Verify the VTP configuration.	**show vtp status**

Cisco1912# delete vtp (pour effacer le mode VTP)



3.8) Etude du protocole applicatif TFTP (trivial file transfert protocol)

3.8.1) Schéma de câblage



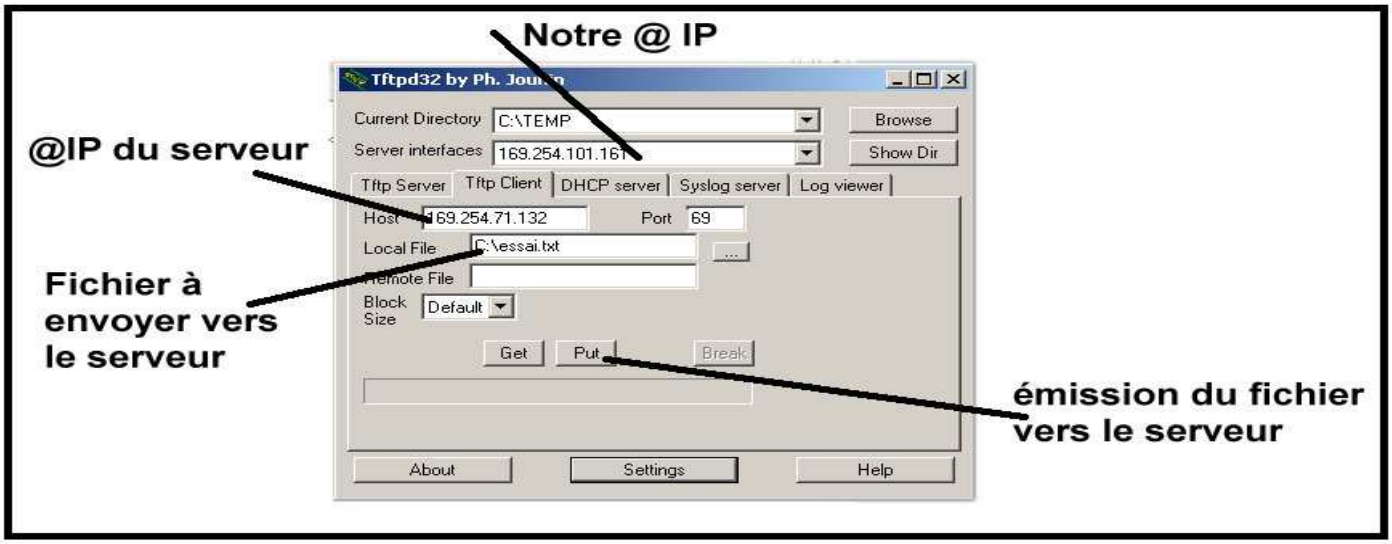
3.8.2) Préliminaire

- installer wireshark et tftpd32 sur les 2 machines
- créez sur les 2 machines un répertoire c:\temp
- créer un fichier texte essai.txt en mettant une centaine de ligne de texte et enregistrez-le sur c:\temp
- lancez tftpd32.exe sur les 2 machines
- cliquez sur setting et choisir comme directory de base c:\temp
- lancez une capture avec wireshark

3.8.3) Questionnaire

3.8.3.1) Emission d'un fichier texte

Paramétrez le logiciel (voir figure ci-dessous) et cliquez sur put



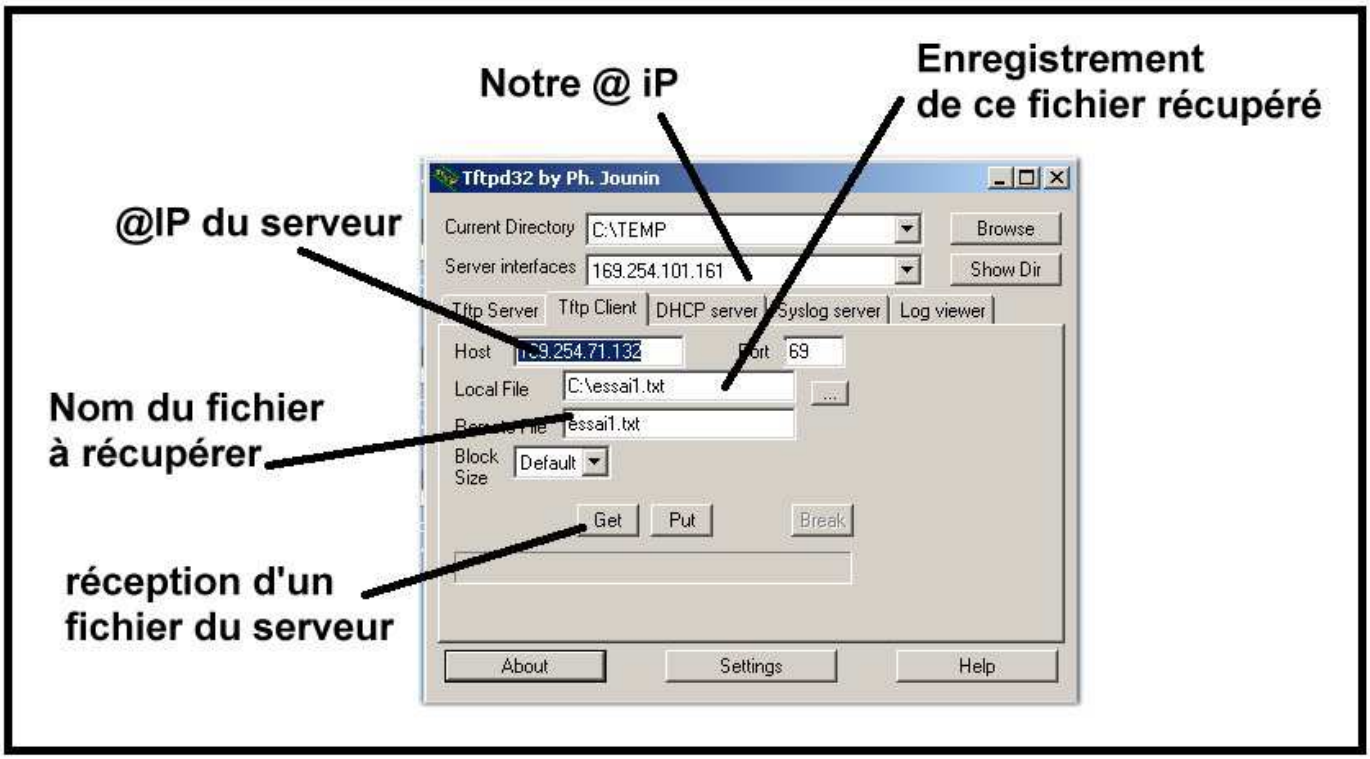
a) Pourquoi avoir choisi le port 69

b) Relevez dans la couche application les trames sur wireshark, relevez et identifiez les trames suivantes

- La demande d'écriture du fichier essai.txt, Sur quel protocole de la couche transport travaille t'on ?
- L'acquittement de la demande d'écriture
- L'émission du premier bloc de données
- L'acquittement du premier bloc de données

3.8.3.2) La réception d'un fichier texte

Paramétrez le logiciel (voir figure ci-dessous) et cliquez sur get



c) Relevez dans la couche application les trames sur wireshark, Identifiez et interprétez les trames suivantes

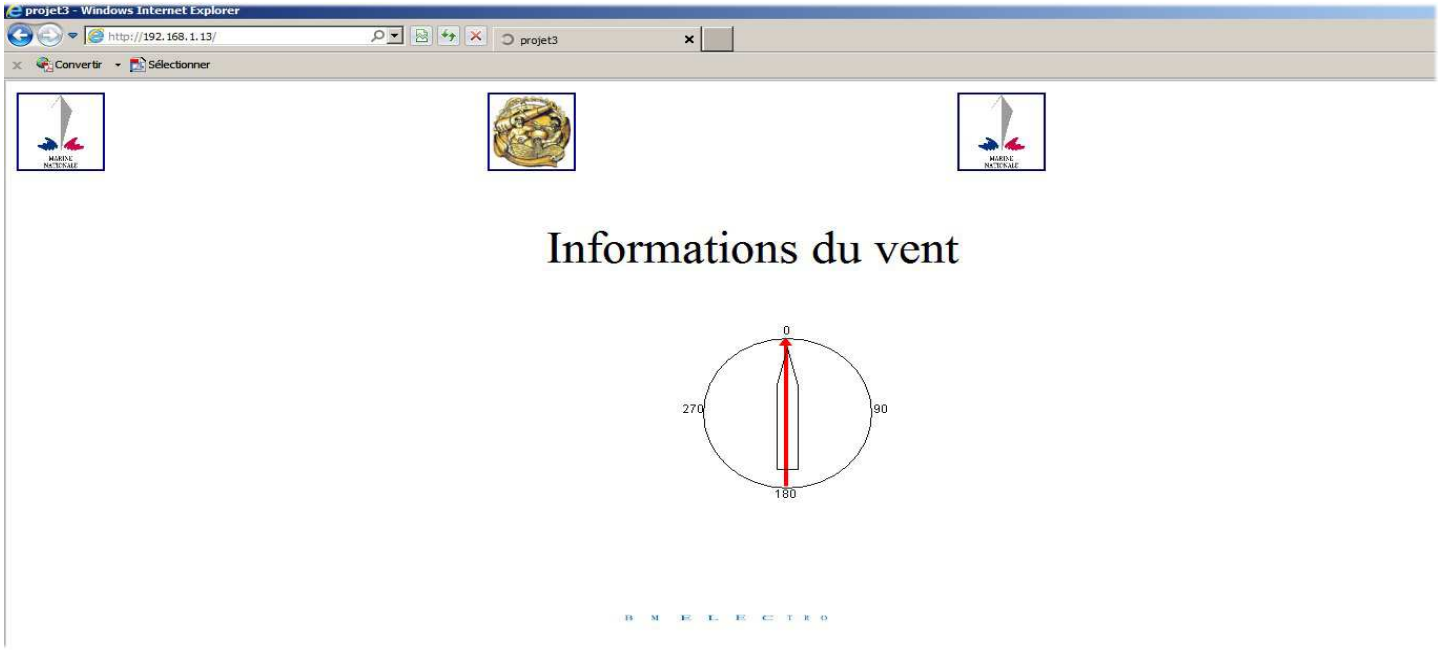
- La demande de lecture du fichier essai1.txt.
- L'acquittement de la demande de lecture
- La réception du premier bloc de données
- L'acquittement du premier bloc de données

3.9) Etude du protocole applicatif HTTP (hypertext transport protocol)

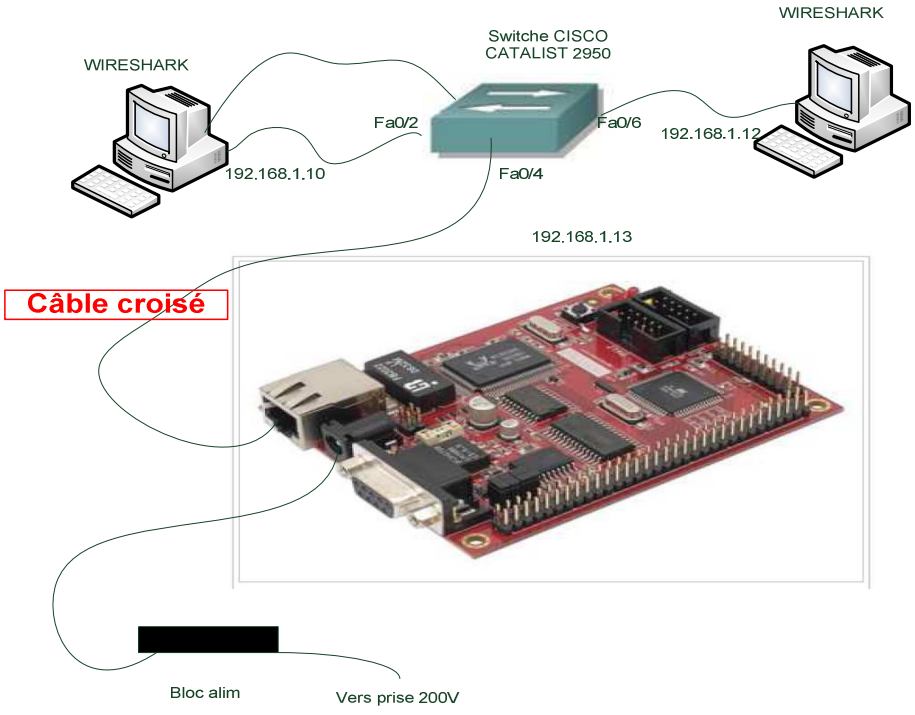
On souhaite relever le dialogue entre un client web (internet explorer) et un serveur WEB. Le serveur Web est un serveur embarqué sur une carte de la société ATMEL (ETHERNUT 1.3H). Les pages WEBs sont implantées dans la carte. Pour accéder à ce serveur web, il faut ouvrir internet exploreur et tapez l'adresse suivante :

http://192.168.1.13/

La page de démarrage suivante se lance :



3.9.1) Schéma de câblage



3.9.2) Questionnaire

a) On donne les schémas structurels partiels de la carte ETHERNUT 1.3H page N°12 et 13. Quel type de microcontrôleur et de contrôleur Ethernet a-t-on utilisé ?

b) A quoi sert le circuit ST3222CD ?

Fermez Internet explorer, Lancez une capture sous wireshark , relancez Internet explorer et connectez vous sur le serveur web.

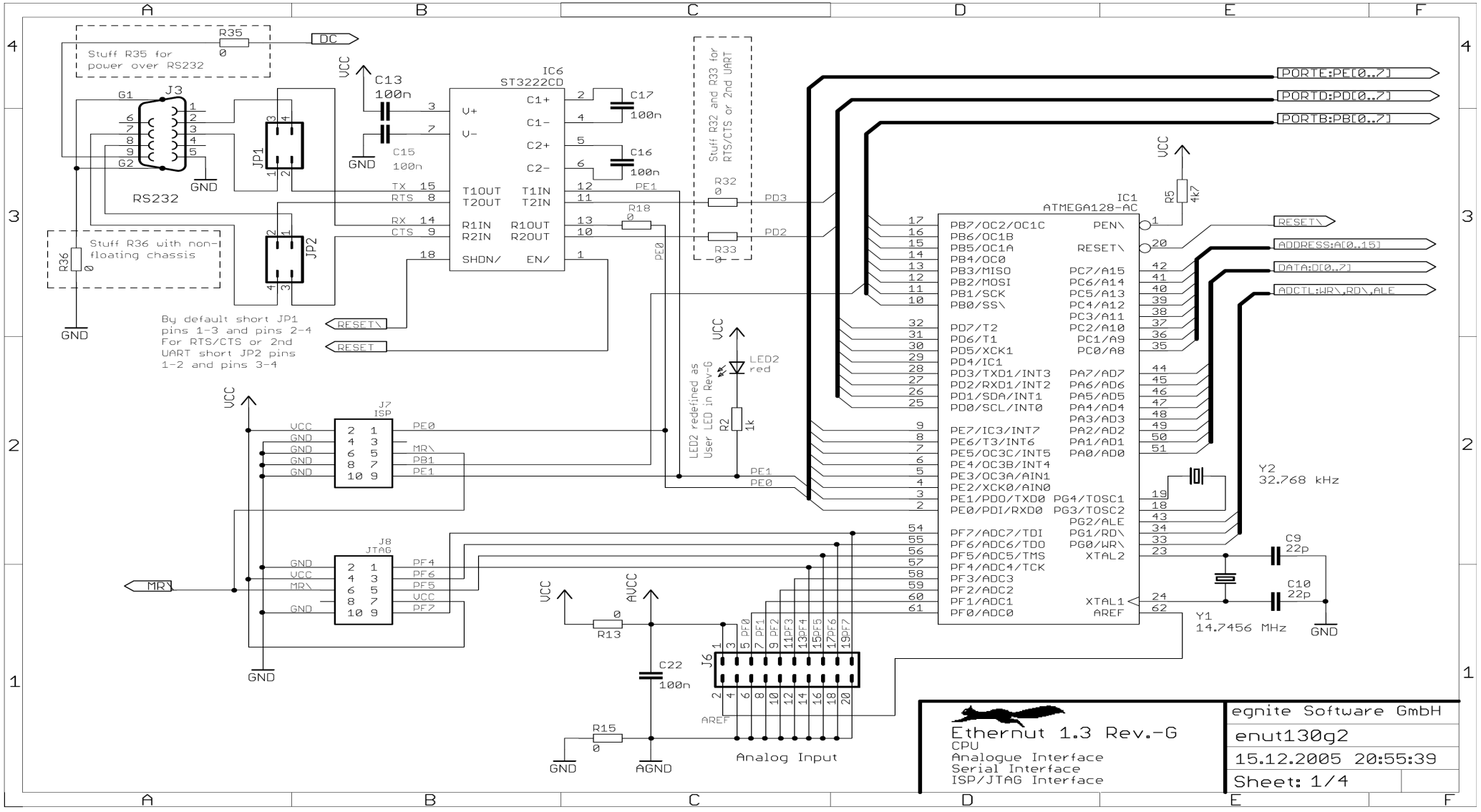
c) Stoppez la capture, Quel est le rôle des trois premières trames TCP observées ?

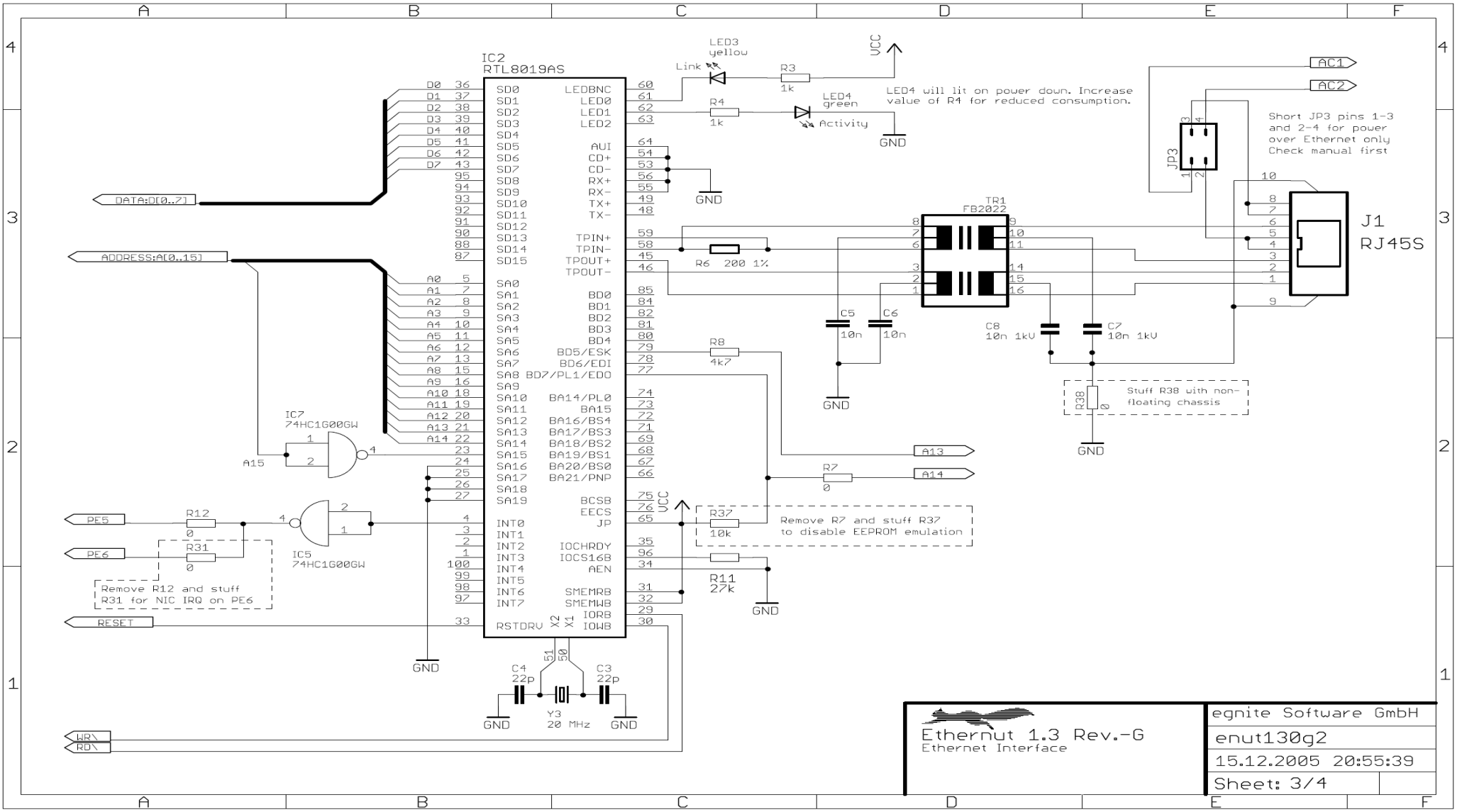
d) Décodez la première et la deuxième trame TCP.

e) Sous internet explorer, affichez la source de la page web, conclure avec le résultat obtenu sur les deux premières trames http.

f) Dans les trames qui suivent au niveau du protocole HTTP, que demande le client auprès du serveur ?

g) Trouvez la trame que renvoie le serveur au client en lui fournissant le pseudo code java de l'applet appletbpc.class

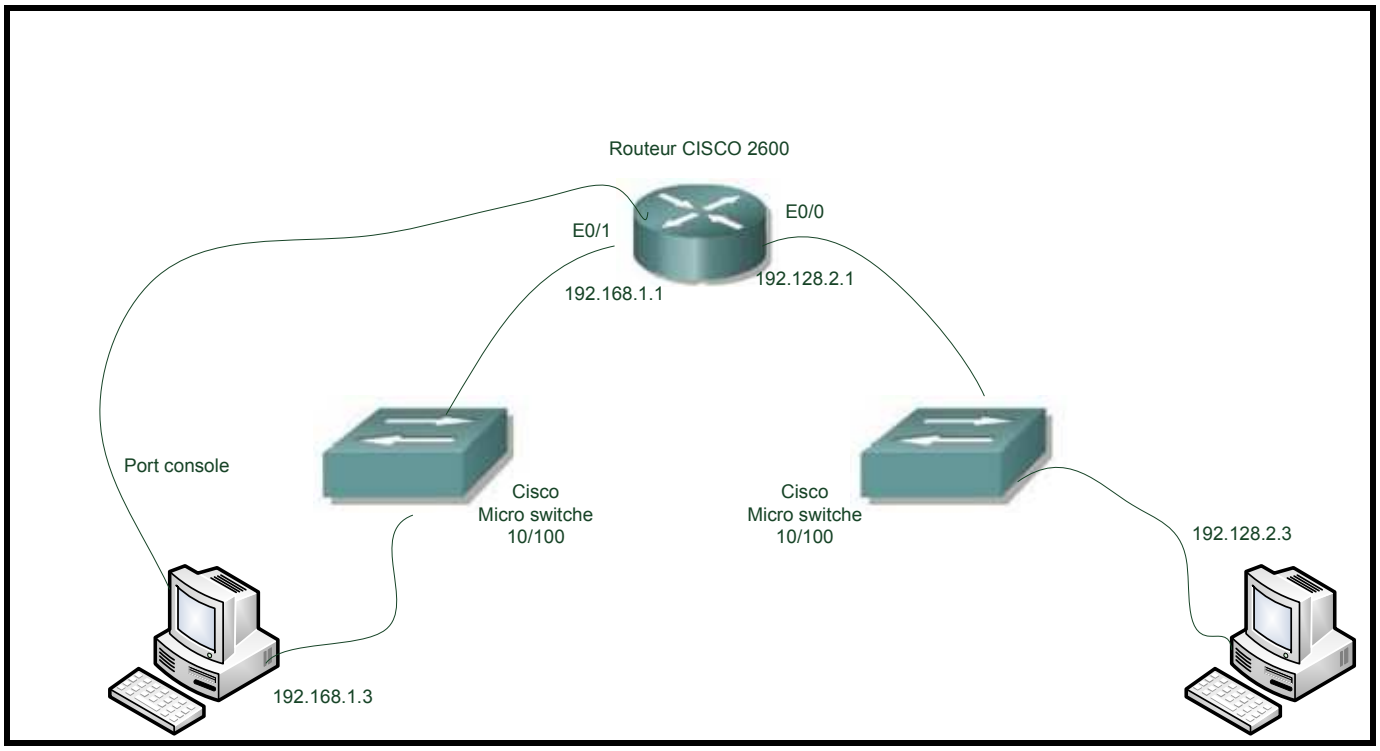

Stuff R35 for power over RS232
R35
DC
J3
RS232
JP1
JP2
C13 100n
C15 100n
C16 100n
C17 100n
IC6 ST3222CD
C1+
C1-
C2+
C2-
V+
V-
T1OUT
T2OUT
T1IN
T2IN
R1IN
R2IN
R1OUT
R2OUT
SHDN/
EN/
TX
RTS
RX
CTS
Stuff R32 and R33 for RTS/CTS or 2nd UART
R32
R33
R18
PE1
PE0
PD3
PD2
R36
Stuff R36 with non-floating chassis
By default short JP1 pins 1-3 and pins 2-4 For RTS/CTS or 2nd UART short JP2 pins 1-2 and pins 3-4
RESET\
RESET
IC1 ATMEGA128-AC
PB7/OC2/OC1C
PB6/OC1B
PB5/OC1A
PB4/OC0
PB3/MISO
PB2/MOSI
PB1/SCK
PB0/SS\
PD7/T2
PD6/T1
PD5/XCK1
PD4/IC1
PD3/TXD1/INT3
PD2/RXD1/INT2
PD1/SDA/INT1
PD0/SCL/INT0
PE7/IC3/INT7
PE6/T3/INT6
PE5/OC3C/INT5
PE4/OC3B/INT4
PE3/OC3A/AIN1
PE2/XCK0/AIN0
PE1/PDO/TXD0
PE0/PDI/RXD0
PF7/ADC7/TDI
PF6/ADC6/TDO
PF5/ADC5/TMS
PF4/ADC4/TCK
PF3/ADC3
PF2/ADC2
PF1/ADC1
PF0/ADC0
PEN\
RESET\
PC7/A15
PC6/A14
PC5/A13
PC4/A12
PC3/A11
PC2/A10
PC1/A9
PC0/A8
PA7/AD7
PA6/AD6
PA5/AD5
PA4/AD4
PA3/AD3
PA2/AD2
PA1/AD1
PA0/AD0
PG4/TOSC1
PG3/TOSC2
PG2/ALE
PG1/RD\
PG0/WR\
XTAL2
XTAL1
AREF
R5 4k7
PORTE:PE[0..7]
PORTD:PD[0..7]
PORTB:PB[0..7]
ADDRESS:A[0..15]
DATA:D[0..7]
ADCTL:WR\,RD\,ALE
Y2 32.768 kHz
Y1 14.7456 MHz
C9 22p
C10 22p
LED2 red
R2 1k
LED2 redefined as User LED in Rev-G
J7 ISP
J8 JTAG
MR\
PB1
R13
C22 100n
R15
J6
AVCC
AREF
Analog Input
GND
AGND
Ethernut 1.3 Rev.-G
CPU
Analogue Interface
Serial Interface
ISP/JTAG Interface
egnite Software GmbH
enut130g2
15.12.2005 20:55:39
Sheet: 1/4


IC2
RTL8019AS
LED3
yellow
Link
R3
1k
VCC
R4
1k
LED4
green
Activity
LED4 will lit on power down. Increase value of R4 for reduced consumption.
GND
AC1
AC2
JP3
Short JP3 pins 1-3 and 2-4 for power over Ethernet only Check manual first
TR1
FB2022
J1
RJ45S
DATA:D[0..7]
ADDRESS:A[0..15]
R6 200 1%
C5 10n
C6 10n
C8 10n 1kV
C7 10n 1kV
R38
Stuff R38 with non-floating chassis
R8 4k7
A13
A14
R7
IC7
74HC1G00GW
A15
PE5
PE6
R12
R31
IC5
74HC1G00GW
Remove R12 and stuff R31 for NIC IRQ on PE6
R37 10k
Remove R7 and stuff R37 to disable EEPROM emulation
R11 27k
RESET
C4 22p
C3 22p
Y3
20 MHz
WR\
RD\
egnite Software GmbH
Ethernut 1.3 Rev.-G
Ethernet Interface
enut130g2
15.12.2005 20:55:39
Sheet: 3/4

4) Les routeurs

4.1) Configuration d'un routeur

4.1.1) Réalisez le montage suivant

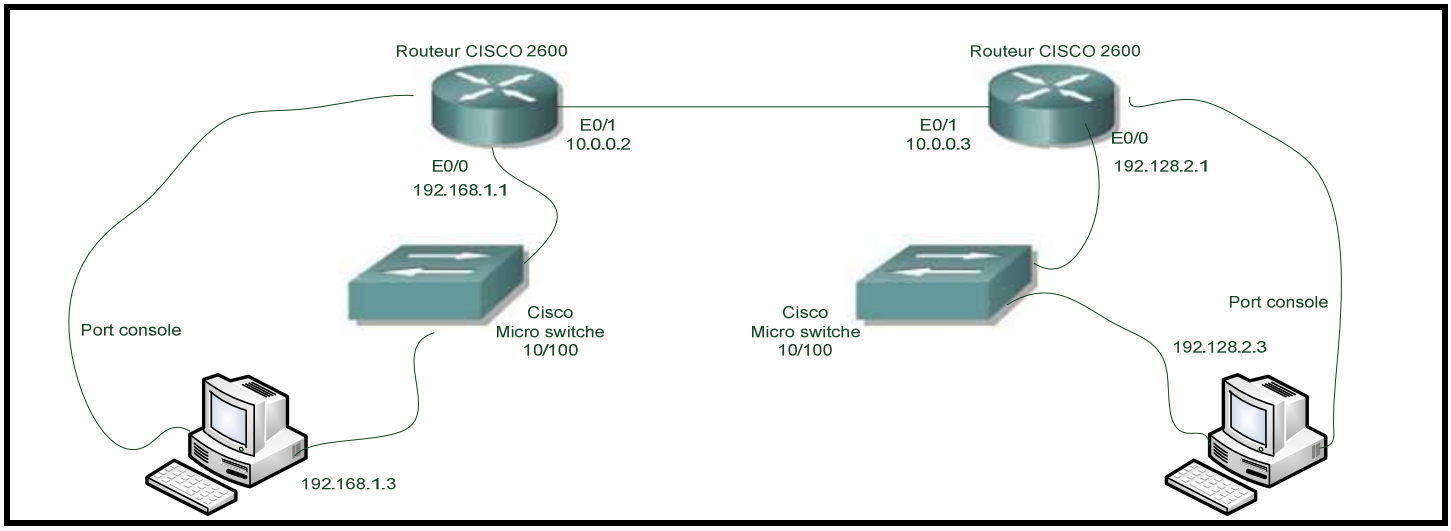


4.1.2) En vous aidant du dossier annexe, configurez les routeurs afin de respecter l'architecture réseau précédente.

4.1.3) Vérifiez si les 2 machines se voient et interprétez le paramètre TTL

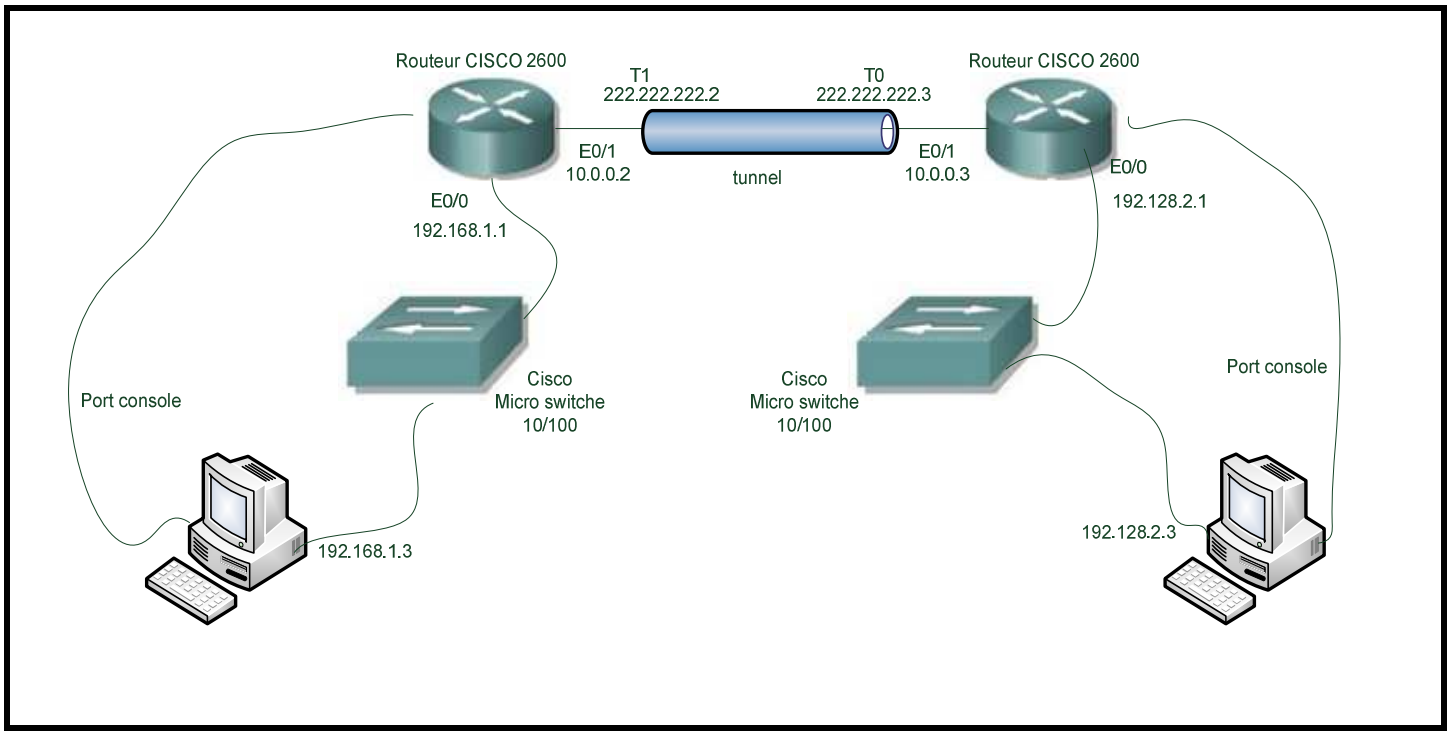
4.2) Configuration de deux routeurs

4.2.1) Réalisez le montage suivant :



4.2.2) En vous aidant du dossier annexe, configurez les routeurs afin de respecter l'architecture réseau précédente (on utilisera un routage statique).
4.2.3) Vérifiez si les 2 machines se voient et interprétez le paramètre TTL
4.2.4) Supprimez le routage statique et mettez en place un routage dynamique du type RIP.
4.2.5) Vérifiez si les 2 machines se voient et interprétez le paramètre TTL
4.2.6) Si le routeur dispose d'une interface série, vérifiez le type de protocole série par défaut utilisé par le routeur.
Router# conf t
Router(config)# int S0
Router(config-if)#encap ? → type de protocole utilisé
Router(config-if)#encap hdlc -→ utilisation du protocole hDLC
Router(config-if)#ctrl z
Router#sh int S0

Afin de sécuriser l'information qui circule entre les 2 routeurs on souhaite mettre en place un tunnel.



4.3) Mise en place d'un tunnel

4.3.1) en vous aidant du dossier annexe, configurez les routeurs afin de réaliser le tunnel précédent entre les 2 routeurs.
4.3.2) Vérifiez si les 2 machines se voient.

Dossier annexe

1) Les commandes CISCO pour un switche

- Démarrer +programme+accessoire +Communication + Hyperterminal:

o Nom = nom du switch +OK
  o Port Com = l + OK
  o Vitesse = 9600 bauds + Appliquer + OK

- Après Password

  o SwitchX> **en** ou **enable**
  o SwitchX#

- Création de VLAN (Virtual Local Area Network) :

  o SwitchX#**vlan database**
  o SwitchX(VLAN)#**vlan** «*numéro du vlan*» **name** «*nom du vlan n* >>
  o SwitehX(VLAN)#**apply**
  o SwitehX(VLAN)#**exit**
  o SwitchX#**sh vlan**

- Suppression un VLAN :

  o SwitchX#**vlan database**

  o SWitehX(VLAN)#**no vlan** «*numéro du vlan* »

  o SwitchX(VLAN)#**apply**

  o SwitchX(VLAN)#**exit**

- Affectation des interfaces aux vlan :

  o SwitchX#**conf t**
  o SwitchX(config)#**int** « *numéro de l'interface*»
  o SwitchX(config-if)#**speed 100**
  o SwitchX(config-if)#**duplex half**

  o SwitchX(config-if)#**switchport access vlan** « *numéro du vlan n*>>

· Affectation **d'un port avec une adresse MAC** :

On peut spécifier une @Mac par port pour le bloquer si une autre adresse Mac est connectée

- SwitchX#**conf t**
- SwitchX(config)#**int** « *numéro de l'interface* »
- SwitchX(config-if)#**switchport mode access**
- SwitchX(config-if)#**switchport port-security**

- SwitchX(config-if)#**switchport port-security mac-address** «*@mac*»
- Pour trouver l'@ mac d'un PC : sous msdos : ipconfig -all

- Affectation d'une adresse IP à un VLAN pour administration à distance :

Pour l'administration à distance d'un switch, il faut l'emploi de telnet.

- SwitchX#**conf t**
- SwitchX(config)#**int vlan 1**
- SwitchX(config-if)#**ip add** « *adresse IP du vlan 1* » « *masque par défaut*»
- SwitchX(config-if)#**no shut**

Pour avoir accès au switch, il faut faire la commande suivante sous DOS :

telnet « *adresse IP du vlan1*»

- Sécurisation de l'accès du switch à distance :

Pour cela, il faut créer un access-list. II faut créer une règle et l'appliquer à une interface.

- Création de la règle :
- SwitchX#**conf t**

- SwitchX(config)#**ip access-list standard** « *numéro de la règle de l à 99*»
- SwitchX(config-std-nacl)#**permit host** « *@IP du poste qui peul administrer à distance* »
- SwitchX(config-std-nacl)#**deny any**
- SwitchX(config-std-nacl)#**exit**
- Application de la règle à une interface :
- SwitchX(config)#**int** vlan 1
- SwitchX(config-if)#**ip access-group** « *numéro de la règle n*»

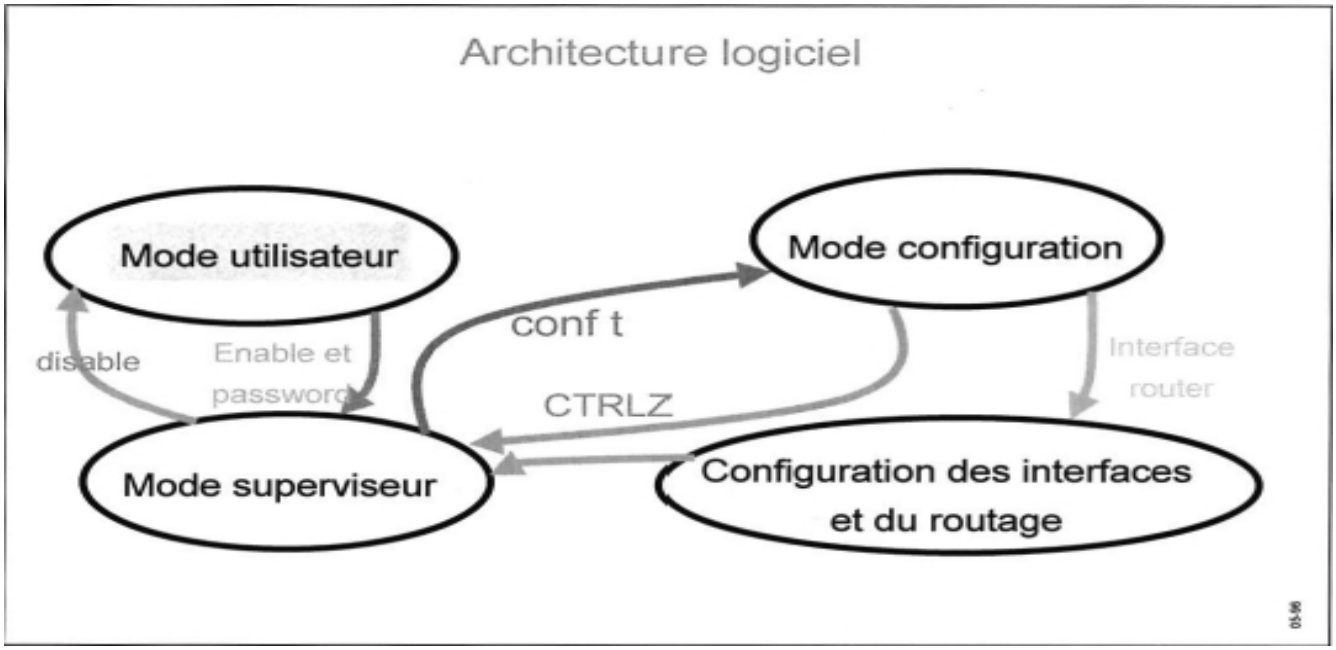
Pour supprimer cet access-list, il faut taper les lignes de commandes suivantes :

SwitchX(config)#**no ip access-list standard** « *numéro de la règle n*»

SwitchX(config-it)**#no ip access-group** « *numéro de la règle*›› in

2) <u>Les commandes CISCO pour un routeur</u>

<u>Les différents modes :</u>



- <u>Démarrer + **programme** + accessoire + Communication + Hyperterminal :</u>
  - o Nom = nom du routeur +OK
  - oPort Com l + OK
  - oVitesse = 9600 bauds + Appliquer + 0K

- <u>Après Password</u> :

  Router1› **en** ou **enable** -->passage en mode superviseur
  Router1 # **sh run** --› visualise la configuration
  Router1 # **sh ip route** -->pour voir les tables de routages

  <u>Configuration des interfaces :</u>

o Routeur1# **conf t** Configuration du terminal
o Routeur1 (config)**#int** « nom de l'interface » *ex : int.ea0/0*
o Routeur1 (config-if)**#ip add** « @IP de l'interface » « Masque du réseau de l'interface» *ex: ip add 192.168.2.202 255.255.255.0*

- Pour les interfaces Séries DTE :
  - o Routeur1(config-if)**#encap lapb**
- . Pour les interfaces Séries DCE :
  - o Routeur1(config-if)**#encap lapb DCE**
  - o Routeur1(config-if)**#clock rate 1300000**

- Routeur1(config-if)#**no shut** => pour activer l'interface (l'interface est montée)

- Si l'interface tombe :
  - Routeur1(config-if)#**shutdown**

- **Configuration du Routage:**

- Routage statique :

- Routeur1 #**conf t**
- Routeur1(config)#**ip routing** => Validation du routage
- Routeur1 (config)#**ip route** « @IP du réseau à atteindre » « Masque » « @IP de l'interface d'en face par ou l'on veut passer »
  Ex : ip route 192.168.2.0 255.255.255.0 192.168.20.201

- Supprimer le routage statique :

- Routeur1(config)#**no ip route** « ligne de routage à supprimer » => supprime une ligne de routage
  Ex :no ip route 192.168.1.0 255.155.255.0 192.168.20.201
- Routeur1(config)#**no ip routing** => supprime toutes les lignes de routage

- Routage dynamique :

- Routeur1 #**conf t**
- Routeur1(config)#**router rip**
- Routeur1 (config-router)#**net** « @IP du LAN »
- Routeur1(config-router)#**net** «@IP du WAN1 » => si elle existe
- Routeur1 (config-router)#**net** « @IP du WAN2 » => si elle existe

- Supprimer un routage dynamique :

- Routeur1(config-router)#**no net** « @IP de RLE »
- Routeur1(config-router)#**no net** « @IP du WANI »
- Routeur1(config-router)#**no net** « @IP du WAN2 »

- **Tunneling :** (sert à protéger les infos par encapsulation)

- Montage d'un tunnel

- Routeur1 #**conf t**
- Routeur1(config)#**int** «t0 (nom de l'interface virtuelle) »
- Rouleur1(config-if)#**ip add** « @ IP de l'interface virtuelle » « Masque »
- Routeur1 (config-if)#**tun source** « nom de l'interface physique réelle »
- Routeur1(config-if)#**tun dest** << @IP de l'interface physique réelle d'en Face»
- Routeur1 (config-if)#**tun key** «chiffre(ex :1234) »

- On force les infos à passer par le tunnel :

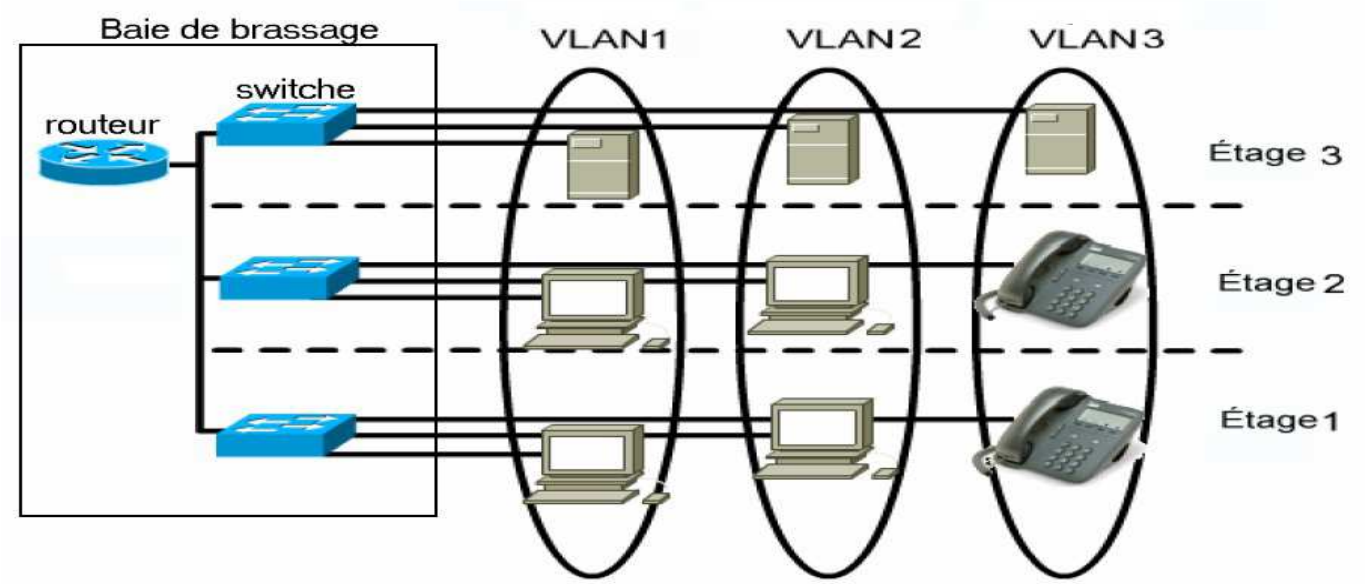
- Routeur1#**conf t**

- Routeur1 (config)**#router rip**
- Routeur1 (config-router)**#no net** « @IP du réseau ou l'on à placer le tunnel »
- Routeur1 (config-router)**#net** « @IP du réseau du tunnel »

5) Les réseaux virtuels locaux (VLAN)

5.1) Présentation

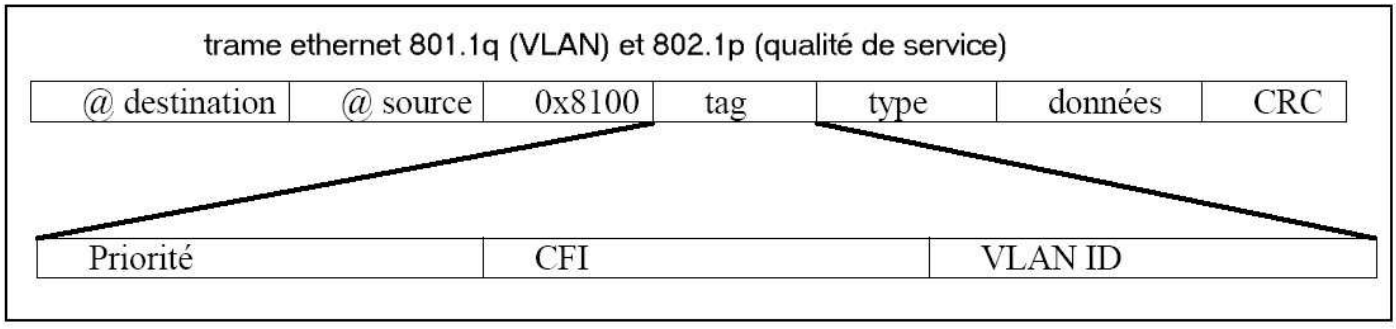
Le VLAN (Virtual Local Area Network) Permet de créer plusieurs LAN sur les mêmes équipements de commutation de trames, Le Vlan Permet de séparer des groupes de machines



5.2) Les différents types de VLAN

On retrouve 3 types de VLAN

Les VLAN de niveau physique 1(couche physique) ou par port, c'est à dire que chaque VLAN se verra attribuer un ou plusieurs ports physiques du commutateur.
La configuration des VLAN se fait au niveau du switche. Ce sont des VLAN statiques car il faut modifier la configuration du commutateur pour déplacer logiquement une machine d'un réseau virtuel à un autre. Afin de pouvoir étendre les VLAN au delà d'un seul commutateur, il a été définit un protocole le 802.1q permettant de faire transiter l'information concernant les VLAN sur les liens entre commutateurs.



Priorité a une longueur de 3 bits et permet de définir 8 niveaux de priorité dans les flux. La façon dont est gérée cette qualité de service est définie dans la norme 802.1p.

CFI a une longueur de 1 bit et n'est pas utilisé pour Ethernet (il l'est pour Token Ring). Nous n'entrerons donc pas en détail sur sa signification.
VLAN ID a une longueur de 12 bits et représente le numéro de VLAN de 1 à 40953. 0 indiquant l'absence de VLAN.
Une autre façon de considérer ce nouveau format de trame est de le faire comme une trame Ethernet classique dont le type est 0x8100 et les données sont constituées de la séquence suivante :

tag + type + anciennes données

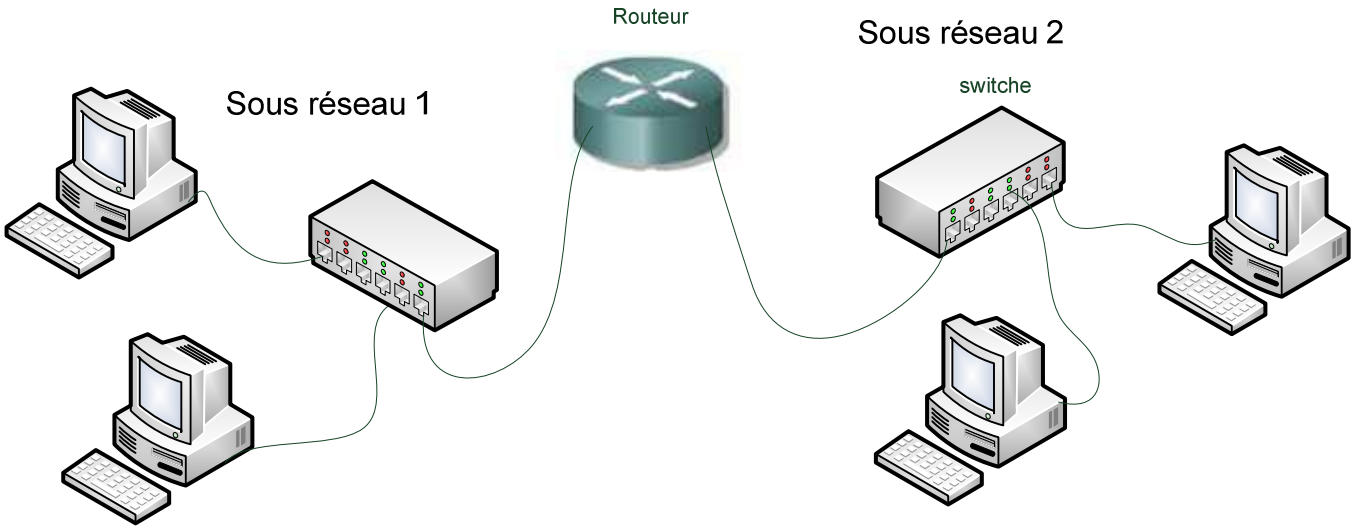
Cela permet de comprendre comment un matériel ignorant l'extension à la norme4 est capable de transmettre les trames étendues (sans en exploiter évidemment les informations de VLAN ou de qualité de service).

La conversion entre trames classiques et trames étendues se fait au niveau d'un commutateur. Celui ci ajoute ou supprime selon le cas l'étiquette (« tag ») et recalcule le CRC.
Nous pouvons dire qu'un VLAN est un VPN. Le marquage 802.1q des trames circulant entre 2 matériels permet de réaliser un tunnel.
Si les trames marquées (802.1q ou et 802.1p) ont d'abord été prévues pour assurer le transport de VLAN sur les liaisons entre commutateur, elles peuvent aussi être utilisées pour la connexion d'une machine à un commutateur. Il suffit que celle-ci sache gérer les protocoles correspondants. Dans ce cas le commutateur n'a plus à ajouter ou supprimer un en-tête, lorsqu'il reçoit ou envoie une trame. Par contre, il est alors impératif que le commutateur s'assure que la politique de sécurité et de qualité de service est bien respectée. Il doit vérifier le numéro de VLAN et la priorité fournis par la machine et le cas échéant refuser la trame ou modifier son en-tête pour imposer le respect des règles.

VLAN de niveau 2 par adresse MAC, VMPS

Dans un VLAN par adresse, on définit dans un simple fichier la correspondance entre machines et numéros de VLAN. Il existe une réalisation possible sur du matériel Cisco à l'aide d'un protocole propriétaire VQP (VLAN Query Protocol). Ce protocole assure les échanges entre le commutateur et un serveur VMPS (VLAN Management Policy Server). Le principe en est le suivant :
- La machine est connectée au commutateur, elle est mise sous tension, son interface Ethernet est activée.
- Différents paramètres comme le débit, half ou full duplex, sont négociés entre le commutateur et la machine.
- Une fois la liaison établie (link) le commutateur attend une trame provenant de la machine.
- Il récupère l'adresse source de la trame Ethernet.
- Il envoie cette adresse ainsi que le numéro du port à un serveur VMPS qui soit lui retourne le numéro de VLAN à utiliser, soit lui demande de refuser de connexion.
- Il affecte ce numéro au port considéré.

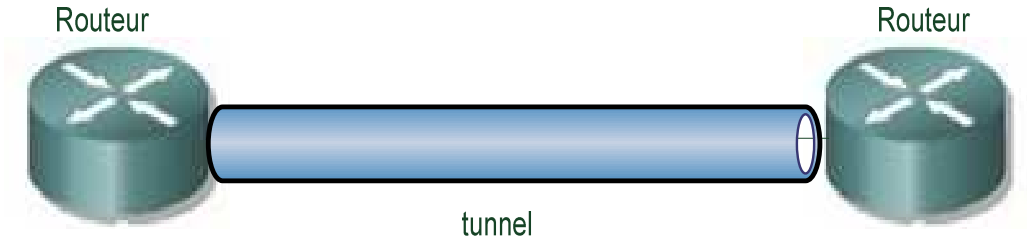
Le VLAN de niveau 3 ou VLAN d'adresse réseaux c'est le subnetting par exemple.



Avantages VLAN	Inconvénients VLAN
séparer des groupes d'ordinateurs, calculateurs téléphonie IP sans qu'ils ne puissent communiquer Meilleure sécurité	Compléxité dans la configuration des switches
partager les mêmes liens d'interconnections réseaux entre les placards	Des informations pour les protocoles (VQP) doivent circuler entre commutateur
Utiliser les mêmes équipements donc diminuer les coûts	Certaines trames sont taggées
Améliorer la gestion des flux et la bande passante car on confine au sein d'un VLAN le trafic entre quelques machines.	Dans le cas du VLAN 3 l'attribution d'adresse IP par DHCP est problématique

6) Le tunneling

Le tunneling est une méthode qui permet de transporter un protocole (et ses données) dans un autre protocole. Lorsque le protocole d'encapsulation permet de protéger les données qu'il transporte (d'une manière ou d'une autre, sans parler forcément de chiffrement), on préfèrera employer le terme de tunnel.



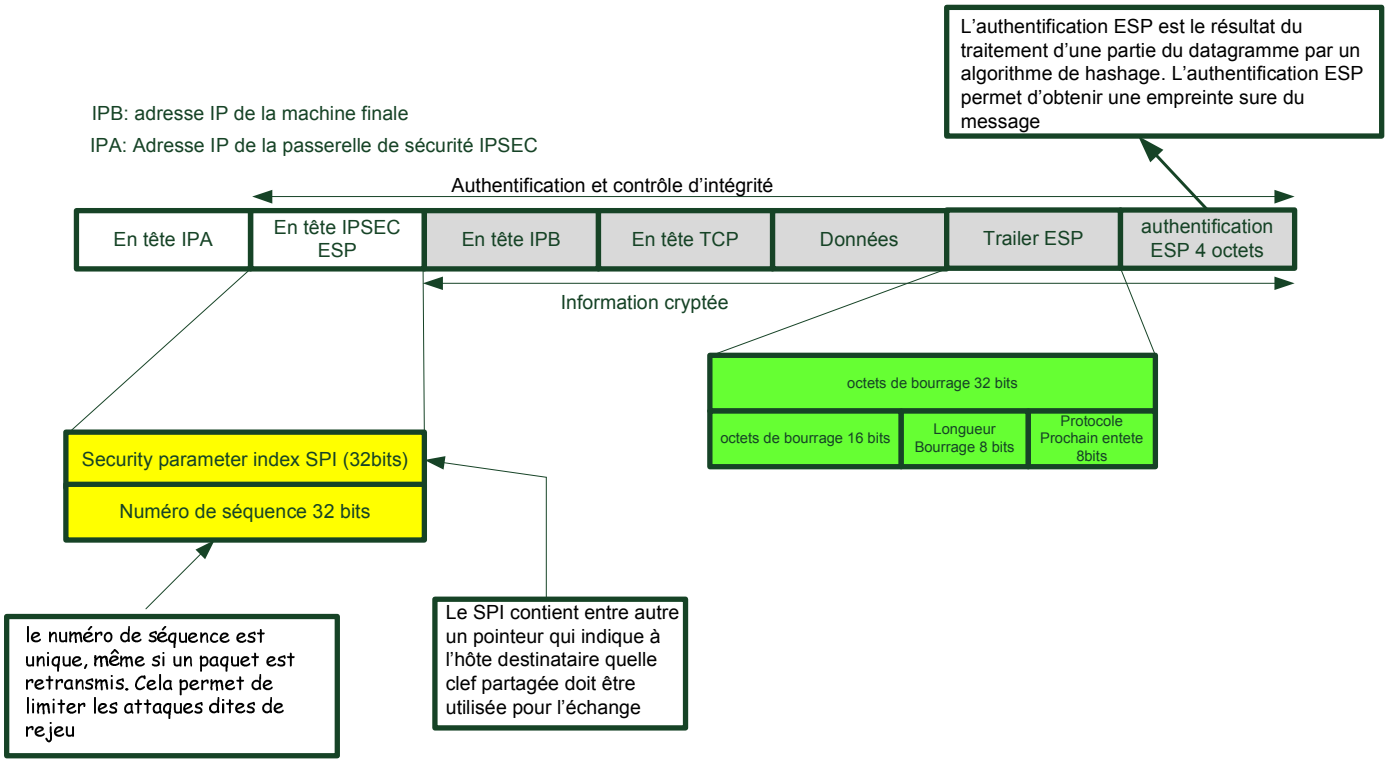
Le protocole le plus utilisé pour sécuriser TCP/IP au niveau de la couche 3 est le protocole IPSEC contrairement à SSL/TLS ou SSH qui sécurisent respectivement les couches 6 et 7 (ce qui évite de rattacher IPSec à un port donné 22 pour SSH ou 443 pour HTTPs).

Le mode ESP (Encapsulating Security Payload) du protocole IPSEC fournit les services de sécurité suivants :

- **Confidentialité des données** : IPSec permet si on le désire de chiffrer le contenu de chaque paquet IP pour éviter la lecture de ceux-ci par quiconque. Elle est assurée par un chiffrement symétrique des données.
- **Intégrité des données** : IPSec permet de s'assurer qu'aucun paquet n'a subit de modification quelconque durant son trajet en rajoutant à chaque paquet IP le résultat d'un calcul de hachage (SHA-1 ou MD5) portant sur tout ou partie du datagramme.
- **Protection contre les écoutes et analyses de trafic** : IPsec permet de chiffrer les adresses IP réelles de la source et de la destination, ainsi que toute l'en-tête IP correspondant.
- **Protection contre le rejeu** : IPSec permet de se prémunir des attaques consistant à capturer un ou plusieurs paquets dans le but de les envoyer à nouveau pour bénéficier des mêmes avantages que l'envoyeur initial. Elle est assurée par la numérotation des paquets IP et la vérification de la séquence d'arrivée des paquets.

Puisque IPSEC est embarqué par défaut dans IPv6, c'est forcément un protocole d'avenir et déjà du présent.

On donne page suivante un bref aperçu de ce protocole IPSEC en mode tunnel mode ESP (Encapsulated Security Payload)



7) PRESENTATION DE TELNET

Telnet est un protocole permettant d'émuler une console de commande à distance. Pour fonctionner il faut un serveur telnet , un client telnet et un login et mot de passe sur le serveur. Le but de telnet est de pouvoir travailler en mode console sur une machine distante. Ce protocole a plutôt été utilisé sous Unix ou Linux qui est plus dédié OS en mode console.
Telnet a par contre un énorme avantage, c'est qu'il envoie des caractères directement au dessus de la couche 4 tcp et donc peut permettre comme nous l'avons déjà vu de tester les autres protocoles ftp, smtp, http, pop. Le port utiliser pour la communication en telnet est le port 23.
Connexion vers le serveur telnet à l'adresse 10.23.254.2 (port 23 par défaut).
telnet 10.23.254.2
Connexion vers le serveur http à l'adresse 10.23.254.2
telnet 10.23.254.2 80