

MASTER 1 INFORMATIQUE - CYBERSÉCURITÉ ET
E-SANTÉ



TP1 : VIRTUAL LAN et Routage interVlans

10 mars 2024

Ivan KRIVOKUCA 22306432

Abdel-Malik FOFANA 22218511

Table des matières

1	Mise en place d'un réseau local commute	3
1.1	Combien de domaines de collisions existent et combien existe-t-il de domaines de diffusion?	3
1.2	Combien d'interfaces Fast Ethernet et de Gigabit Ethernet possède le switch? A quoi servent-elles?	3
1.3	Examinez le contenu actuel de la mémoire vive non volatile. Pourquoi le commutateur affiche cette réponse?	3
1.4	Quelles sont les caractéristiques de l'interface virtuelle VLAN1 : adresse IP, adresse MAC, activité, propriétés IP?	4
1.5	Quelles sont les propriétés par défaut de l'interface Fast Ethernet utilisée pour connecter votre PC. Adresse MAC, activité, vitesse, mode de transmission? Quel événement pourrait activer une interface?	5
1.6	Quelles sont les paramètres VLAN par défaut du commutateur : nom du VLAN 1, ports attribués à ce VLAN, type du VLAN par défaut?	6
2	Configuration de base du Commutateur	7
2.7	Configurer un nouveau VLAN, par exemple VLAN 99. Attribuer une adresse IP et un masque de sous-réseau à l'interface VLAN 99 (192.168.10.99/24). Affectez le port connectant votre machine au VLAN 99. Utiliser la commande show pour vérifier votre configuration.	7
2.8	Quelle est la bande passante définie sur cette interface VLAN99? Quelle est la stratégie de file d'attente?	10
2.9	Vérifier la connectivité du réseau ainsi formé, en envoyant des ping. Donner les étapes pour réaliser cette connectivité.	10
2.10	Mesurer le débit sur cette interface.	11
2.11	Vérifier la segmentation de votre LAN. Expliquer comment procéder à cette vérification et donner les résultats de chaque étape.	12

2.12	Maintenant, vérifier la segmentation de votre LAN en rajoutant des machines sur le switch.	12
2.13	13) Utilisez la commande <code>#show vlan brief</code> pour vérifier que ces deux VLANs sont bien créés.	14
2.14	14) Utilisez la commande <code>interface range</code> en mode de configuration globale pour simplifier la configuration.	15
2.15	15) Sur chaque commutateur, enregistrer la configuration courante.	16
2.16	16) Tester le fonctionnement de l'agrégation de VLANs en générant de ping. Observer les trames obtenues Maintenant, on souhaite faire communiquer les VLAN 10 et VLAN 20. Faire évoluer la topologie initiale (Fig 1), en précisant les équipements nécessaires à une telle solution. Justifier votre solution.	16
2.17	17) Expliquer les étapes de la configuration de votre solution. Justifier le résultat de chaque étape.	17
2.18	18) Tester le fonctionnement de votre solution.	18
2.19	19) Chercher et étudier les options permettant de définir la sécurité des ports sur l'interface <code>FastEthernet0/X</code> . <code>#switchport ?</code>	20
2.20	20) Configurez le port en question de sorte qu'il accepte un périphérique, acquière l'adresse MAC correspondante de façon dynamique et désactive le port en cas de violation.	21
2.21	21) Vérifier le résultat, en affichant les paramètres de sécurité des ports. <code>#show port-security</code> Combien d'adresses sécurisées sont autorisées sur <code>FastEthernet0/X</code> ? Quelle est la mesure de sécurité appliquée à ce port?	21
2.22	22) Vérifier la mesure de sécurité dans fichier de configuration en cours	22
2.23	23) Tester en branchant un deuxième PC sur le port sécurisé. Que constatez-vous? Afficher l'état de l'interface configurée.	23

1. Mise en place d'un réseau local commute

1.1 Combien de domaines de collisions existent et combien existe-t-il de domaines de diffusion ?

Avant la liaison avec les câbles :

Domaines de collision :

- o 2 pour les PCs connectés au *switch1*
- o 2 pour les PCs connectés au *switch2*
- o 1 entre le switch1 et le switch2 (ou vise versa)



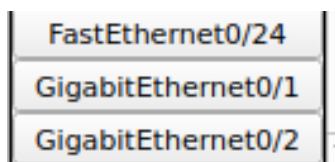
Domaines de diffusion :

2 (un pour chaque switch).

Après la liaison avec les câbles : Même nombres de domaines de collisions mais on aura que un domaine de diffusion (puisque les deux switches sont relié).

1.2 Combien d'interfaces Fast Ethernet et de Gigabit Ethernet possède le switch ? A quoi servent-elles ?

24 Fast Ethernet (100 Mbps) 2 Gigabit Ethernet (1000 Mbps)



Les interfaces *Fast Ethernet* sont utilisées pour connecter des périphériques comme des ordinateurs (et aussi d'autres switches) à un réseau local. Les interfaces *Gigabit Ethernet*, quant à elles, sont utilisées pour connecter des périphériques qui nécessitent une bande passante plus élevée (serveurs, routeurs, etc.) ou pour interconnecter des switches entre eux pour une communication plus rapide.

1.3 Examinez le contenu actuel de la mémoire vive non volatile. Pourquoi le commutateur affiche cette réponse ?

Pour examiner la NVRAM (mémoire vive non volatile), on exécute les commandes suivantes sur le CLI du commutateur/switch :

```
enable
show startup-config (ou show start)
```

On obtient *"startup-config is not present"*, ce qui signifie qu'aucune configuration n'est présente dans la NVRAM. C'est une réponse attendue car les branchements ne sont pas encore effectués et aucune configuration n'a été réalisée.

1.4 Quelles sont les caractéristiques de l'interface virtuelle VLAN1 : adresse IP, adresse MAC, activité, propriétés IP ?

Pour obtenir les informations de l'interface virtuelle VLAN1, on utilise la commande :

```
show interface vlan1
```

On obtient :

```
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0003.e435.b2ab (bia 0003.e435.b2ab)
  ...
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1682 packets input, 530955 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    563859 packets output, 0 bytes, 0 underruns
    0 output errors, 23 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Sur l'output (réduit pour gagner de la place), on remarque que l'adresse IP ainsi que les propriétés ne sont pas mentionnées car elle ne sont pas encore configurés.

- Adresse MAC : 0003.e435.b2ab
- Activité : administratively down

1.5 Quelles sont les propriétés par défaut de l'interface Fast Ethernet utilisée pour connecter votre PC. Adresse MAC, activité, vitesse, mode de transmission ? Quel événement pourrait activer une interface ?

```
Switch#show interface fa0/1

FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.cf38.5101 (bia 000c.cf38.5101)
  BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  ...
    956 packets input, 193351 bytes, 0 no buffer
    ...
    2357 packets output, 263570 bytes, 0 underruns
```

- Adresse MAC : 000c.cf38.5101
- Activité : up
- Vitesse : 100Mb/s
- Mode de transmission : Full-duplex (l'interface peut envoyer et recevoir des données simultanément)

Un événement qui pourrait activer une interface est la connexion d'un périphérique réseau (par exemple un PC) à l'interface. Lorsqu'un périphérique est connecté, l'interface détecte la connexion et active le lien réseau, ce qui permettra la communication entre les périphériques.

1.6 Quelles sont les paramètres VLAN par défaut du commutateur : nom du VLAN 1, ports attribués à ce VLAN, type du VLAN par défaut ?

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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 Gig0/1, Gig0/2

- Nom du VLAN 1 : 1
- Ports attribués à ce VLAN : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, 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, Gig0/1, Gig0/2
- Type du VLAN par défaut : default

2. Configuration de base du Commutateur

2.7 Configurer un nouveau VLAN, par exemple VLAN 99. Attribuer une adresse IP et un masque de sous-réseau à l'interface VLAN 99 (192.168.10.99/24). Affectez le port connectant votre machine au VLAN 99. Utiliser la commande show pour vérifier votre configuration.

Voici les commandes que l'on a fait pour configurer le vlan et le créer :

```
enable
configure terminal
vlan 99
name vlan99
interface fastEthernet 0/1
switchport mode access
switchport access vlan 99
```

Explication des commandes :

- Switch#*configure terminal* : Cette commande permet de passer en mode de configuration globale.
- Switch(config)#*vlan 99* : Cette commande crée un nouveau VLAN avec l'ID 99.
- Switch(config-vlan)#*name vlan99* : Cette commande donne un nom au VLAN créer qui sera "vlan99".
- Switch(config-vlan)#*interface fastEthernet 0/1* : : Cette commande permet de passer en mode de configuration de l'interface FastEthernet 0/1
- Switch(config)#*interface fastEthernet 0/1* : Cette commande nous place dans le mode de configuration de l'interface FastEthernet 0/1.
- Switch(config-if)#*switchport mode access* : Cette commande configure le port comme un port d'accès, ce qui signifie qu'il ne peut être connecté qu'à un seul appareil terminal, comme un PC ou un serveur.
- Switch(config-if)#*switchport access vlan 99* : Cette commande affecte l'interface FastEthernet 0/1 au VLAN 99. Cela signifie que tout le trafic entrant sur ce port sera associé au VLAN 99.


```
Switch>en
Switch>enable
Switch#configure te
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 99
Switch(config-vlan)#name vlan99
Switch(config-vlan)#interface fa
Switch(config-vlan)#exit
Switch(config)#interface f
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#
```

création du vlan99

configuration port ethernet 0/1 avec le vlan99

On a attribué une adresse IP et un masque de sous-réseau à l'interface *VLAN 99* (192.168.10.99/24) avec les commandes :

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.10.99 255.255.255.0
Switch(config-if)#no shutdown
```

Voici ce que la commande "*show*" nous donne :

```
show vlan
```

VLAN Name		Status	Ports
1 default		active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 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, Gig0/1 Gig0/2
99	vlan99	active	Fa0/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	1000001	1500	-	-	-	-	-	0	0
99	enet	1000999	1500	-	-	-	-	-	0	0
1002	fddi	1010002	1500	-	-	-	-	-	0	0
1003	tr	1010003	1500	-	-	-	-	-	0	0
--More--										

Vérification configuration des VLANs :

```
show vlan
```

```
Switch>show interface vlan 99
Vlan99 is up, line protocol is down
  Hardware is CPU Interface, address is 0001.9623.0801 (bia 0001.9623.0801)
  Internet address is 192.168.10.99/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1682 packets input, 530955 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    563859 packets output, 0 bytes, 0 underruns
    0 output errors, 23 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Vérification configuration de l'interface VLAN 99 :

```
show interface vlan 99
```

```
Switch>show interface FastEthernet0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 99 (vlan99)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
```

Vérification configuration du port connecté à notre machine :

```
show interface FastEthernet0/1 switchport
```

2.8 Quelle est la bande passante définie sur cette interface VLAN99 ? Quelle est la stratégie de file d'attente ?

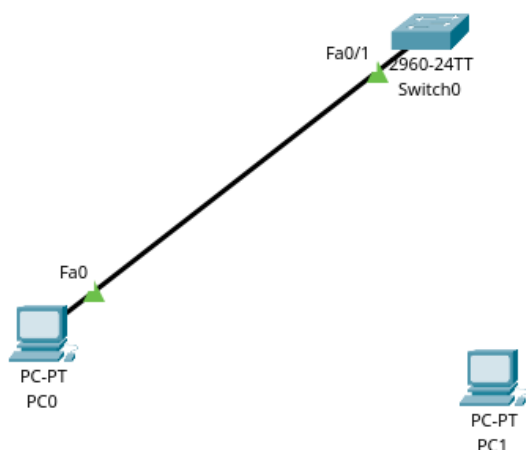
```
MTU 1500 bytes, BW 100000 Kbit,  
  reliability 255/255, txload  
Encapsulation ARPA, loopback no  
ARP type: ARPA, ARP Timeout 04:  
Last input 21:40:21, output nev  
Last clearing of "show interfac  
Input queue: 0/75/0/0 (size/max  
Queueing strategy: fifo
```

Dans la capture d'écran de la commande "*show interface vlan 99*", on voit que la bande passante est : 100000 kbit.

La stratégie de file d'attente est définie comme "fifo" (First In, First Out).

2.9 Vérifier la connectivité du réseau ainsi formé, en envoyant des ping. Donner les étapes pour réaliser cette connectivité.

Comme on peut voir j'ai ajouté les câbles et la connexion c'est bien effectuée :



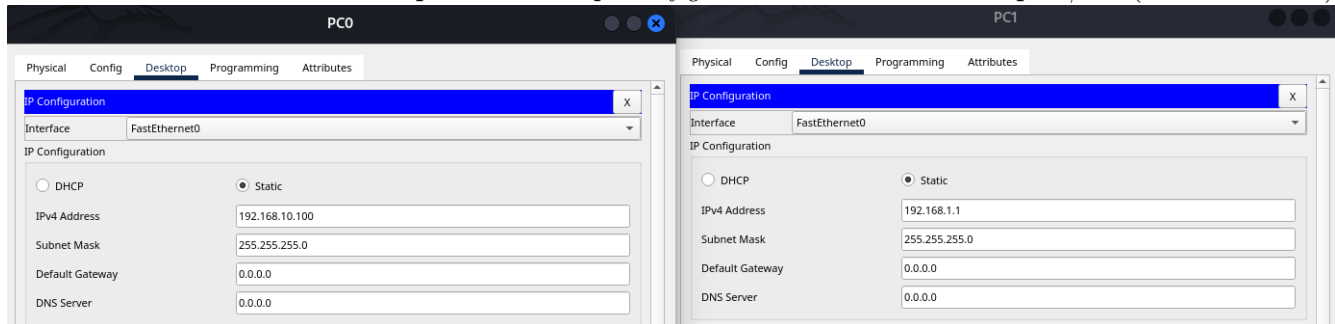
Le but est de pouvoir contrôler à distance le switch grâce au *vlan99*.

L'IP du *PC0* est 192.168.10.100 (donc dans le même sous-réseau que celui du câble Ethernet *vlan99*)

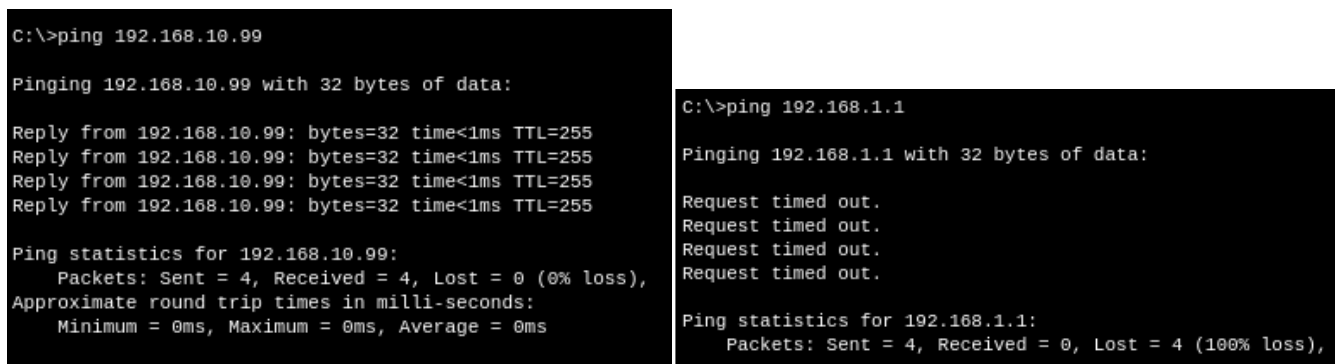
qui est *192.168.10.99*)

L'IP du *PC1* est 192.168.1.1.

On a modifié les IP dans le paramètre "*ip configuration*" avec les masque /24 (255.255.255.0)



Comme on peut le voir le ping du *PC0* vers le vlan switch (interface) réussit, mais on ne peut pas ping les PCs entre eux (ce qui est le but du vlan de plus les câbles sont pas branché au *PC1*).



2.10 Mesurer le débit sur cette interface.

Comme nous l'avons vu, sur le résultat de la commande "*show interfaces FastEthernet0/1*" la bande passante est de 'BW 100000 Kbit ', avec BW = bandwidth = bande passante.

Dans la sortie de la commande *show interface FastEthernet0/1*, les taux de débit sont indiqués dans les lignes suivantes :

- 5 minute input rate 0 bits/sec, 0 packets/sec : Cela indique le taux de débit d'entrée sur l'interface au cours des cinq dernières minutes. Ici, le débit d'entrée est de 0 bits par seconde et 0 paquets par seconde.
- 5 minute output rate 0 bits/sec, 0 packets/sec : Cela indique le taux de débit de sortie sur l'interface au cours des cinq dernières minutes. Ici, le débit de sortie est également de 0 bits par seconde et 0 paquets par seconde.

Ces valeurs indiquent qu'il n'y a pas eu de trafic sur l'interface *FastEthernet0/1* au cours des cinq dernières minutes, car les taux de débit sont tous deux à zéro.

2.11 Vérifier la segmentation de votre LAN. Expliquer comment procéder à cette vérification et donner les résultats de chaque étape.

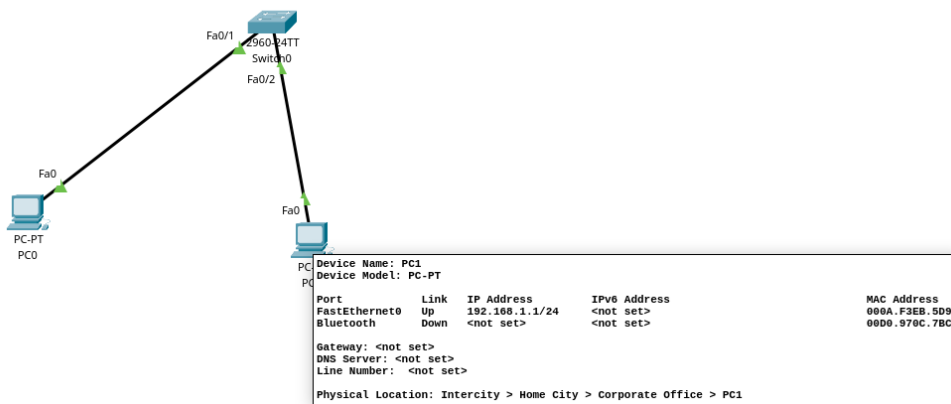
Voici comment vérifier la segmentation de notre LAN :

- Vérification de la connectivité entre les appareils
On a vu que l'interface du switch (192.168.10.99) et le PC0 (192.168.10.100) peuvent se pinguer entre eux, donc tout est ok (voir exo 9).
- Vérification de la configuration du VLAN
Toujours grâce à l'exo 9, on a vu que le *VLAN 99* était bien activé et configuré, comme le montre la commande "show vlan"
- L'interface *VLAN99* (192.168.10.99) est dans le même réseau que le PC.

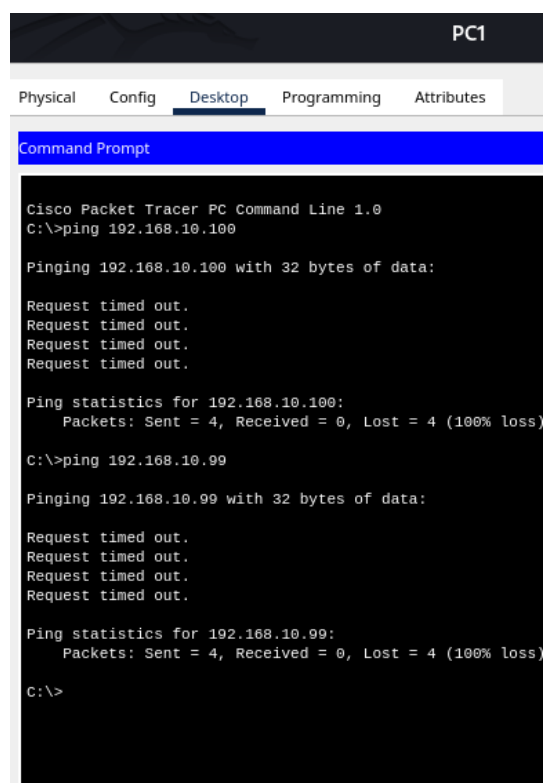
Ainsi on a pu voir que la segmentation de notre LAN était correcte et fonctionnait comme prévu (sous-réseau et VLAN).

2.12 Maintenant, vérifier la segmentation de votre LAN en rajoutant des machines sur le switch.

On a ajouté la machine PC1 au switch avec l'ip 192.168.1.1



On remarque que l'on peut pas pinguer la machine 192.168.10.100 ni l'interface FE 0/1 (192.168.10.99), en effet le pc1 n'est pas dans le meme vlan ce qui est donc normal



The screenshot shows the PC1 configuration window in Cisco Packet Tracer. The 'Desktop' tab is selected, and the 'Command Prompt' application is open. The command prompt displays the results of two ping commands. The first command is 'ping 192.168.10.100', which results in four 'Request timed out.' messages and a 100% loss of packets. The second command is 'ping 192.168.10.99', which also results in four 'Request timed out.' messages and a 100% loss of packets.

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\>ping 192.168.10.99

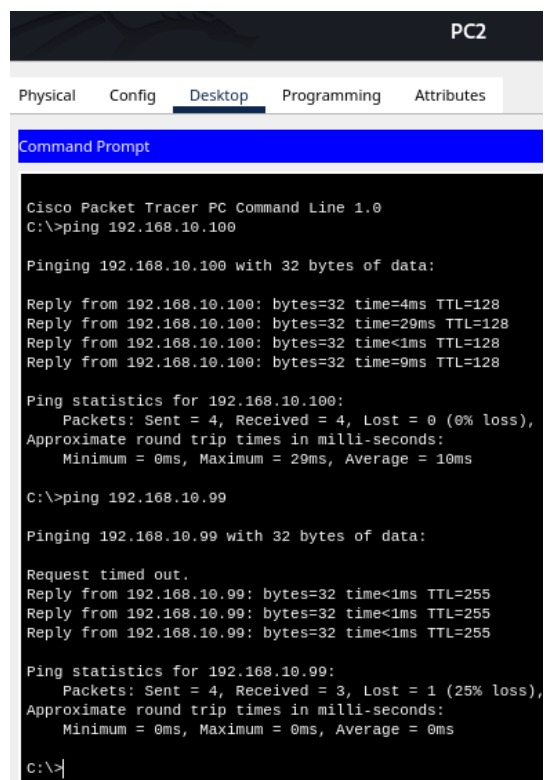
Pinging 192.168.10.99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)

C:\>
```

Je me suis permis d'ajouter un pc2 avec l'ip 192.168.10.101 qui est là juste pour tester et temporairement, l'interface FE 0/3 qui relie le switch au pc2 est en vlan99 , et là on remarque que le ping fonction entre le pc2 et le pc1 , et le ping entre le pc2 et FE 0/1



The screenshot shows the PC2 configuration window in Cisco Packet Tracer. The 'Desktop' tab is selected, and the 'Command Prompt' application is open. The command prompt displays the results of two ping commands. The first command is 'ping 192.168.10.100', which results in four successful replies with round trip times of 4ms, 29ms, <1ms, and 9ms, and a 0% loss of packets. The second command is 'ping 192.168.10.99', which results in four successful replies with round trip times of <1ms, <1ms, <1ms, and <1ms, and a 25% loss of packets.

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time=4ms TTL=128
Reply from 192.168.10.100: bytes=32 time=29ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 10ms

C:\>ping 192.168.10.99

Pinging 192.168.10.99 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.99: bytes=32 time<1ms TTL=255
Reply from 192.168.10.99: bytes=32 time<1ms TTL=255
Reply from 192.168.10.99: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.99:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

2.13 13) Utilisez la commande `#show vlan brief` pour vérifier que ces deux VLANs sont bien créés.

On reutilise les mêmes commandes pour créer les vlan voici les commandes pour le vlan 10 (on a fait pareil pour vlan20)

```
Switch>enable
Switch#config terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Etudiant
```

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

Et voici ce que nous affiche `show vlan brief` :

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 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, Gig0/1 Gig0/2
10	Etudiant	active	
20	Enseignant	active	
99	vlan99	active	Fa0/1
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#
```

Les vlan 10 et 20 sont créés

Ensuite, nous allons configurer les ports selon les affectations données :

```
Switch(config)#interface range FastEthernet1/0/1 - 1/0/5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 99

Switch(config)#interface range FastEthernet1/0/6 - 1/0/10
```

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10

Switch(config)#interface range FastEthernet1/0/11 - 1/0/15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
```

et on peut voir après un show vlan brief que tout est configuré rapidement :

```
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/4, Fa0/5, Fa0/16, Fa0/17
                                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                           Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                           Gig0/2
10   Etudiant                active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10
20   Enseignant              active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15
99   vlan99                  active
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
```

Maintenant, concernant la différence entre un port agrégé et un port d'accès :

Port agrégé (Trunk) : Utilisé pour transporter plusieurs VLANs sur un seul lien entre commutateurs ou entre un commutateur et un routeur. Les trames sont marquées avec des tags VLAN (802.1Q) pour identifier à quel VLAN elles appartiennent. Les ports agrégés augmentent la bande passante entre les appareils et permettent le passage de plusieurs VLANs sur un même lien.

Port d'accès : Utilisé pour connecter un seul périphérique ou VLAN à un commutateur. Il transporte uniquement le trafic d'un seul VLAN et les trames ne sont pas marquées avec des tags VLAN. Les ports d'accès sont utilisés pour connecter des périphériques finaux comme des ordinateurs, des imprimantes ou des serveurs qui n'ont pas besoin d'accéder à plusieurs VLANs.

2.14 14) Utilisez la commande interface range en mode de configuration globale pour simplifier la configuration.

```
Switch(config)#interface range fa0/1-5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk native vlan 99
```

Voici la commande fait

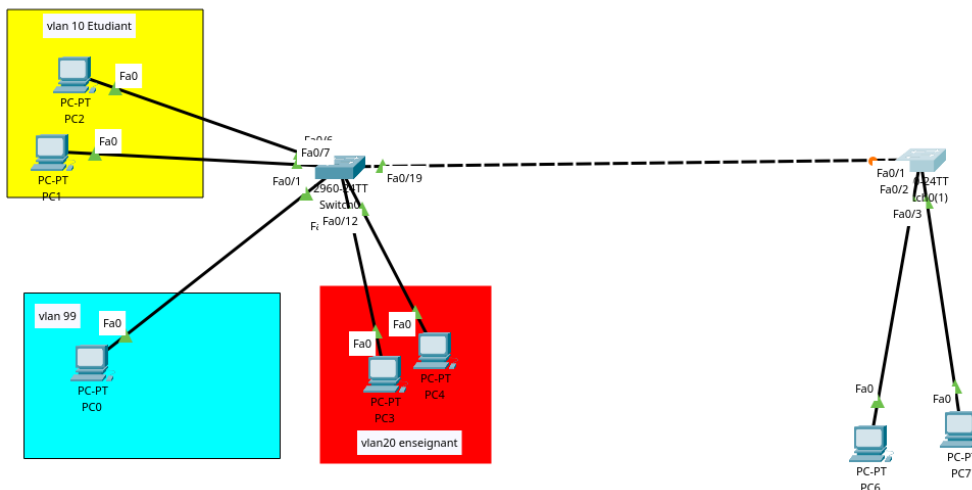
2.15 15) Sur chaque commutateur, enregistrer la configuration courante.

On a fait la commande "write memory" pour enregistrer la configuration pour les routeurs (on pouvait faire aussi "copy running-config startup-config")

```
Switch#write memory
Building configuration...
[OK]
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.16 16) Tester le fonctionnement de l'agrégation de VLANs en générant de ping. Observer les trames obtenues. Maintenant, on souhaite faire communiquer les VLAN 10 et VLAN 20. Faire évoluer la topologie initiale (Fig 1), en précisant les équipements nécessaires à une telle solution. Justifier votre solution.

Pour tester les pings j'ai ajouté des ordinateurs dans chaque vlan (dans la bonne interface)

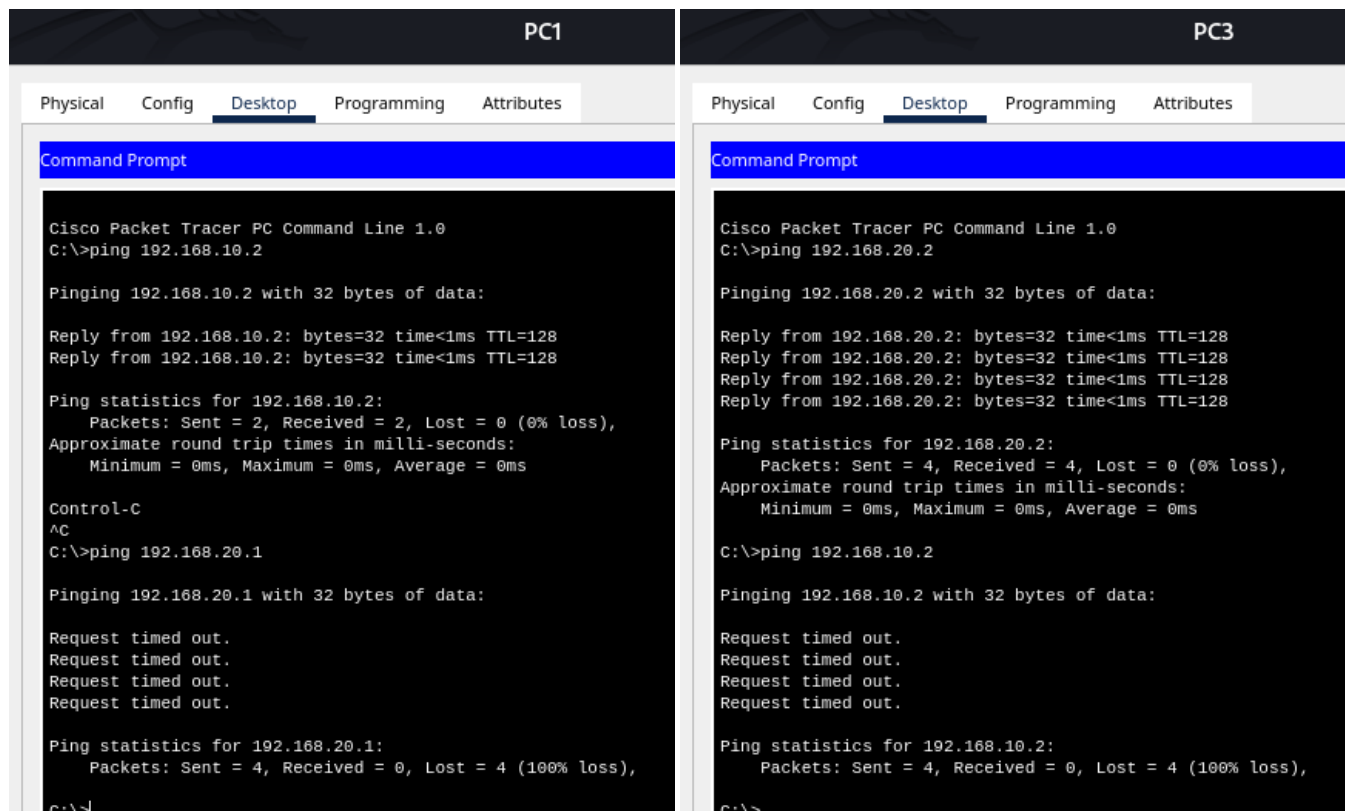


vlan 99 : pc0 = 192.168.10.100

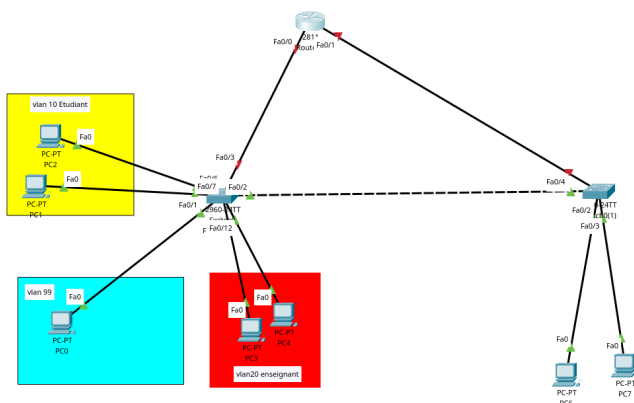
vlan 10 : pc1 = 192.168.10.1 ; pc2 = 192.168.10.2

vlan 20 : pc3=192.168.20.1 ; pc4= 192.168.20.2 ;

Le pc 1 du vlan 10 peut communiquer avec le pc2 car dans le même vlan mais il peut pas communiquer avec le vlan 20 car pas dans le même vlan , et vice verse le pc3 ne peut pas communiquer avec le vlan 10 mais peut communiquer avec le vlan 20 (voir ping suivant)



Pour faire évoluer la topologie initiale afin de permettre la communication entre les VLAN 10 et 20, on peut utiliser un routeur inter-VLAN. Un routeur inter-VLAN permet de faire passer le trafic entre différents VLANs en utilisant des sous-réseaux distincts. il faut donc ajouter un routeur a notre topologie



2.17 17) Expliquer les étapes de la configuration de votre solution. Justifier le résultat de chaque étape.

Pour configurer la communication entre les VLANs 10 et 20 en utilisant un routeur inter-VLAN, voici les étapes :

Connecter chaque switch au routeur à l'aide de câbles Ethernet.

Configurer des sous-réseaux distincts pour chaque VLAN sur le routeur.

Configurer les interfaces du routeur pour chaque VLAN et activer le routage inter-VLAN.

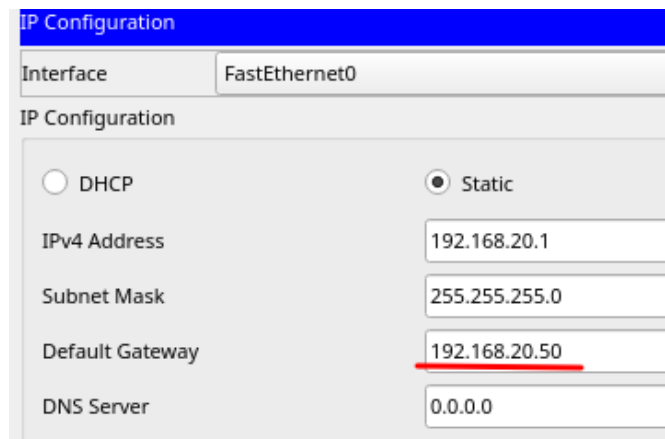
On va s'assurer que les appareils dans les VLANs 10 et 20 ont leurs passerelles par défaut configurées avec l'adresse IP de l'interface du routeur correspondant à leur VLAN.

Chaque étape permet de mettre en place une infrastructure permettant la communication entre les VLANs. L'ajout du routeur et la configuration des interfaces permettent de relier les VLANs et d'acheminer le trafic entre eux. La configuration des sous-réseaux garantit que les appareils dans chaque VLAN sont sur des réseaux logiques distincts. La configuration des passerelles par défaut assure que les appareils dans les VLANs utilisent le routeur comme passerelle pour communiquer avec d'autres réseaux. Cette approche garantit une communication efficace et sécurisée entre les VLANs 10 et 20.

2.18 18) Tester le fonctionnement de votre solution.

on a déjà ajouté le routeur et connecté les switch au routeur ,

il faut également mettre à jour pour chaque ordinateur leurs default gateway :



IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.20.1

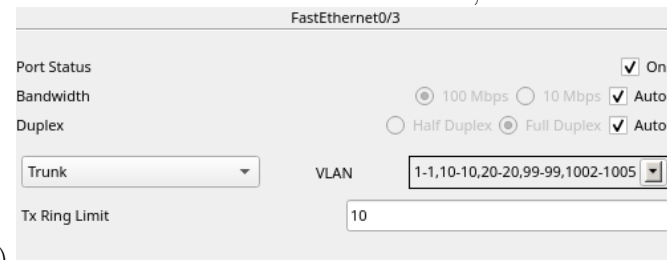
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.50

DNS Server: 0.0.0.0

pour les pc du vlan10 on a choisis 192.168.10.50 et les pc du vlan20 192.168.20.50 l'interface entre le routeur et le switch va être divisé grâce à ces 2 gateways

Il faut aussi autoriser les vlan 10 et 20 à être utilisés dans l'interface entre le routeur et switch 1 , et



FastEthernet0/3

Port Status: ☒ On

Bandwidth: ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☐ Half Duplex ☒ Full Duplex ☒ Auto

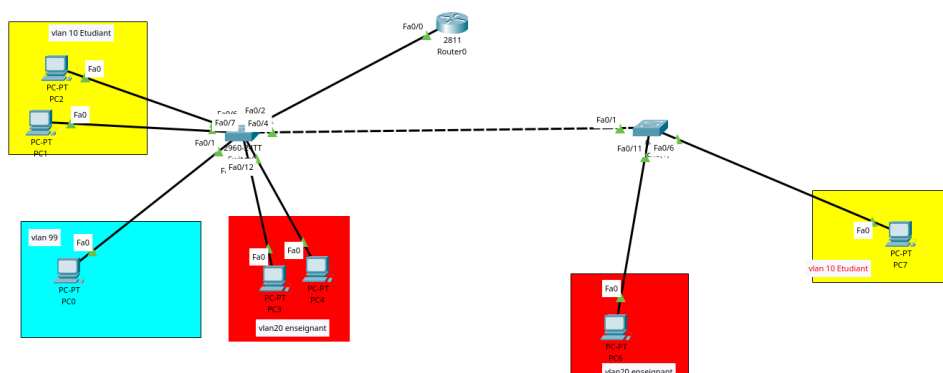
Trunk:

VLAN: 1-1,10-10,20-20,99-99,1002-1005

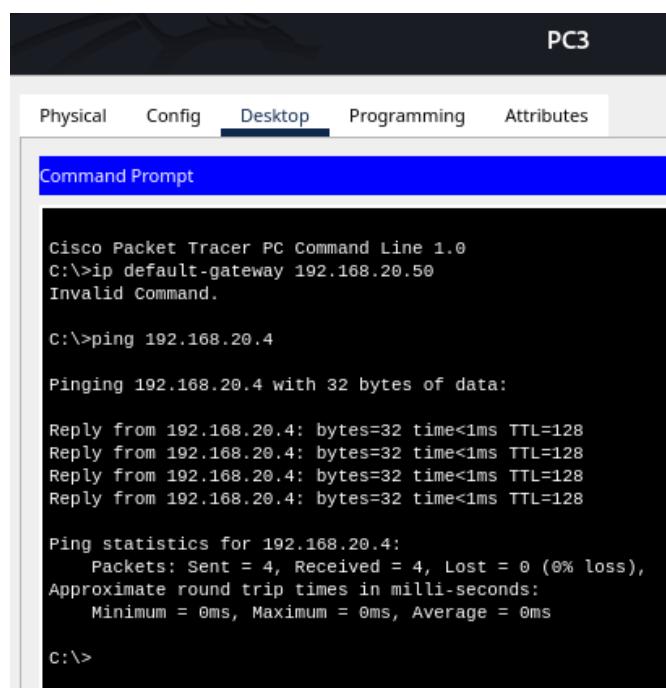
Tx Ring Limit: 10

l'interface entre les 2 switch (Fa0/2 et Fa 0/3) (screen suivant)

Voici à quoi ressemble le réseau pour l'instant :



Maintenant on devrait pouvoir pinger les ordinateurs du même vlan meme si ils sont sur l'autre switch



le pc3 du vlan 20 dans le switch à gauche peut communiquer avec le pc6 du switch2 à droite.

on va donc maintenant configurer le routage intervlan pour permettre la communication entre les 2 vlan via une seule interface physique , voici les commandes à faire sur le routeur

```
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.50 255.255.255.0

Router(config)#interface GigabitEthernet0/0.20
```

```
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.50 255.255.255.0

#ne pas oublier d'activer l'interface avec no shutdown comme d'habitude
```

Et maintenant le pc2 (192.168.10.10) du vlan 10 étudiant peut communiquer avec le pc6 du vlan 20 enseignant

```
C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Tout les pc peuvent communiquer entre eux maintenant peu importe le vlan ou dans quel switch il est

2.19 19) Chercher et étudier les options permettant de définir la sécurité des ports sur l'interface FastEthernet0/X.#switchport ?

La commande switchport port-security est utilisée pour définir la sécurité des ports sur une interface FastEthernet sur un commutateur Cisco. Voici les options disponibles avec cette commande :

```
Switch(config-if)#switchport ?
  access      Set access mode characteristics of the interface
  mode        Set trunking mode of the interface
  nonegotiate  Device will not engage in negotiation protocol on this
               interface
  port-security Security related command
  priority     Set appliance 802.1p priority
  protected   Configure an interface to be a protected port
  trunk       Set trunking characteristics of the interface
  voice       Voice appliance attributes
```

Pour définir la sécurité des ports sur l'interface FastEthernet0/X, on peut utiliser la commande

switchport port-security. Cela permet de configurer des restrictions sur le nombre d'adresses MAC autorisées sur le port, de limiter les adresses MAC autorisées, et de configurer des actions en cas de violation de sécurité, telles que la mise en place d'une alerte ou la désactivation du port.

2.20 20) Configurez le port en question de sorte qu'il accepte un périphérique, acquière l'adresse MAC correspondante de façon dynamique et désactive le port en cas de violation.

Voici les commande pour faire cela que j'ai fait :

```
Switch(config)#interface fastEthernet 0/12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
```

2.21 21) Vérifier le résultat, en affichant les paramètres de sécurité des ports. #show port-security Combien d'adresses sécurisées sont autorisées sur FastEthernet0/X? Quelle est la mesure de sécurité appliquée à ce port?

Depuis la machine connecté au fastEthernet 0/12 on envoie un ping vers n'importe quel machine pour mettre à jour

Pour afficher les parametres de securités il faut faire la commande "show port-security interface FastEthernet0/12" :

```
Switch#show port-security interface fastEthernet 0/12
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
```

```
Configured MAC Addresses      : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : 0090.2B10.CCC3:20
Security Violation Count     : 0
```

On peut voir qu'il y a qu'une seule mac address sécurisée autorisée ("Maximum MAC Addresses : 1") qui est 0090.2B10.CCC3 :20 et lorsque que l'on va sur la machine attachée on voit que l'adresse mac est bien celle-là avec la commande `ipconfig /all`

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0090.2B10.CCC3
    Link-local IPv6 Address.....: FE80::290:2BFF:FE10:CCC3
    IPv6 Address.....: ::
```

La mesure de sécurité appliquée à ce port est la violation de sécurité en mode "Shutdown", ce qui signifie que si une violation de sécurité se produit (par exemple, si plus d'une adresse MAC est détectée sur ce port), le port sera désactivé (Shutdown).

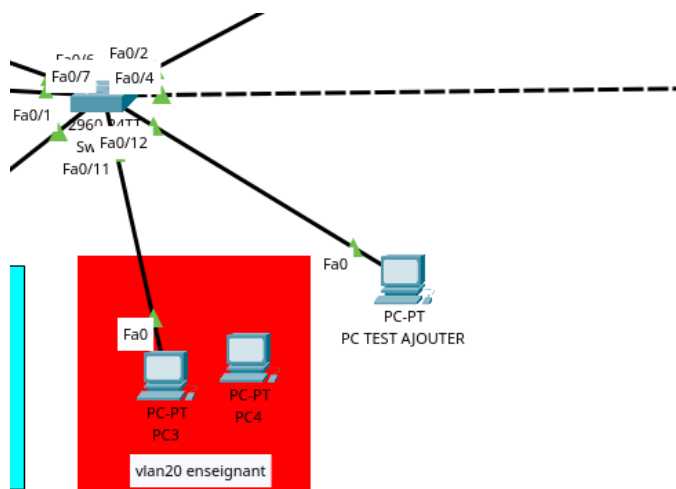
2.22 22) Vérifier la mesure de sécurité dans fichier de configuration en cours

En faisant la commande "show running-config", on peut voir la config actuelle du switch

```
Switch#show running-config
...
interface FastEthernet0/12
  switchport access vlan 20
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security violation restrict
  switchport port-security mac-address sticky 0090.2B10.CCC3
...
```

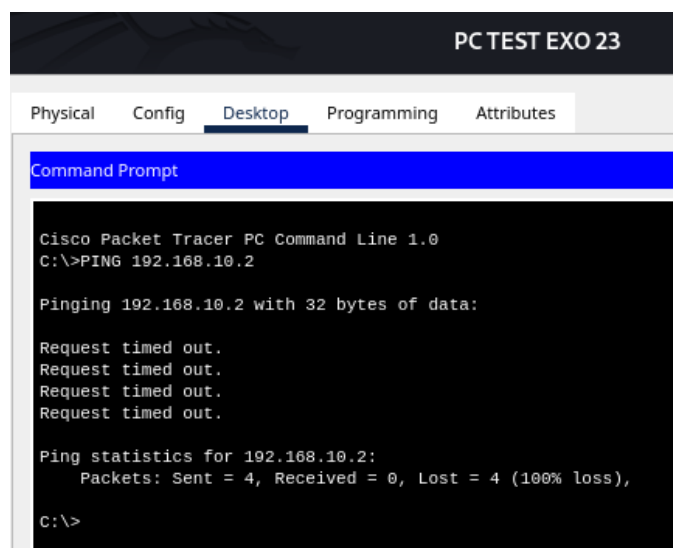
On remarque que `switchport port-security` est bien activé pour l'interface Fa0/12 et la seule mac address autorisée est : 0090.2B10.CCC3 Tout est ok

2.23 23) Tester en branchant un deuxième PC sur le port sécurisé. Que constatez-vous ? Afficher l'état de l'interface configurée.



On a débranché le pc connecté avec l'interface fa0/12 et on a branché le pc test tout nouveau (il a donc une autre adresse mac)

Et on remarque que l'on peut plus ping



Port Security	: Enabled
Port Status	: Secure-up
Violation Mode	: Restrict
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1

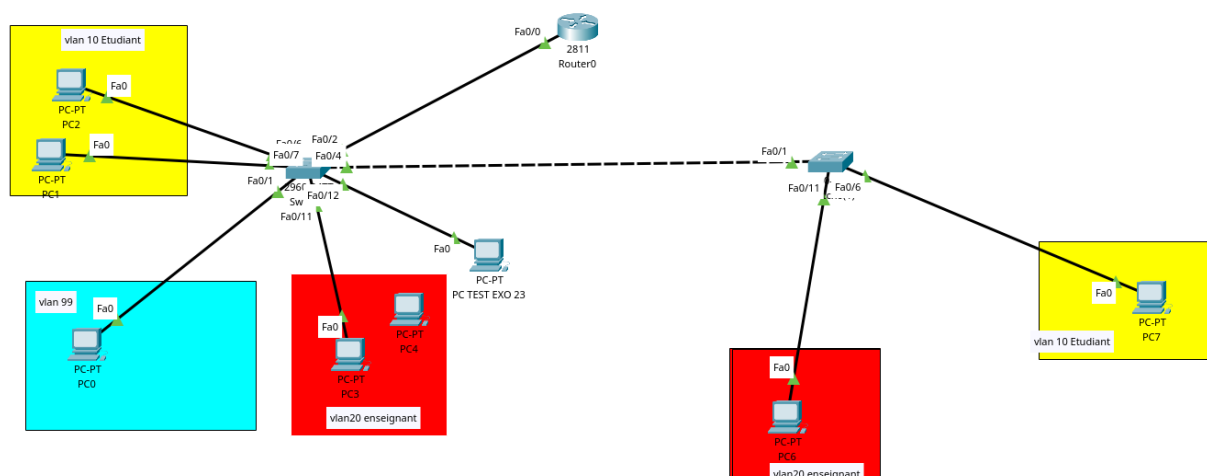

```
Total MAC Addresses      : 1
Configured MAC Addresses : 0
Sticky MAC Addresses     : 1
Last Source Address:Vlan : 0060.5C0D.6AC2:20
Security Violation Count  : 4
```

On remarque également que le switch nous signal 4 violation "Security Violation Count : 4" après que l'on est effectué un ping avec la machine suspect vers d'autre machine et que l'adresse mac n'est pas la même que celle souhaiter : 0060.5C0D.6AC2 :20 au lieu de 0090.2B10.CCC3

```
Switch#show port-security interface fastEthernet 0/12
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Restrict
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 0060.5C0D.6AC2:20
Security Violation Count : 4

Switch#
```

Voici à la fin à quoi ressemble notre réseau :



Tout fonctionne