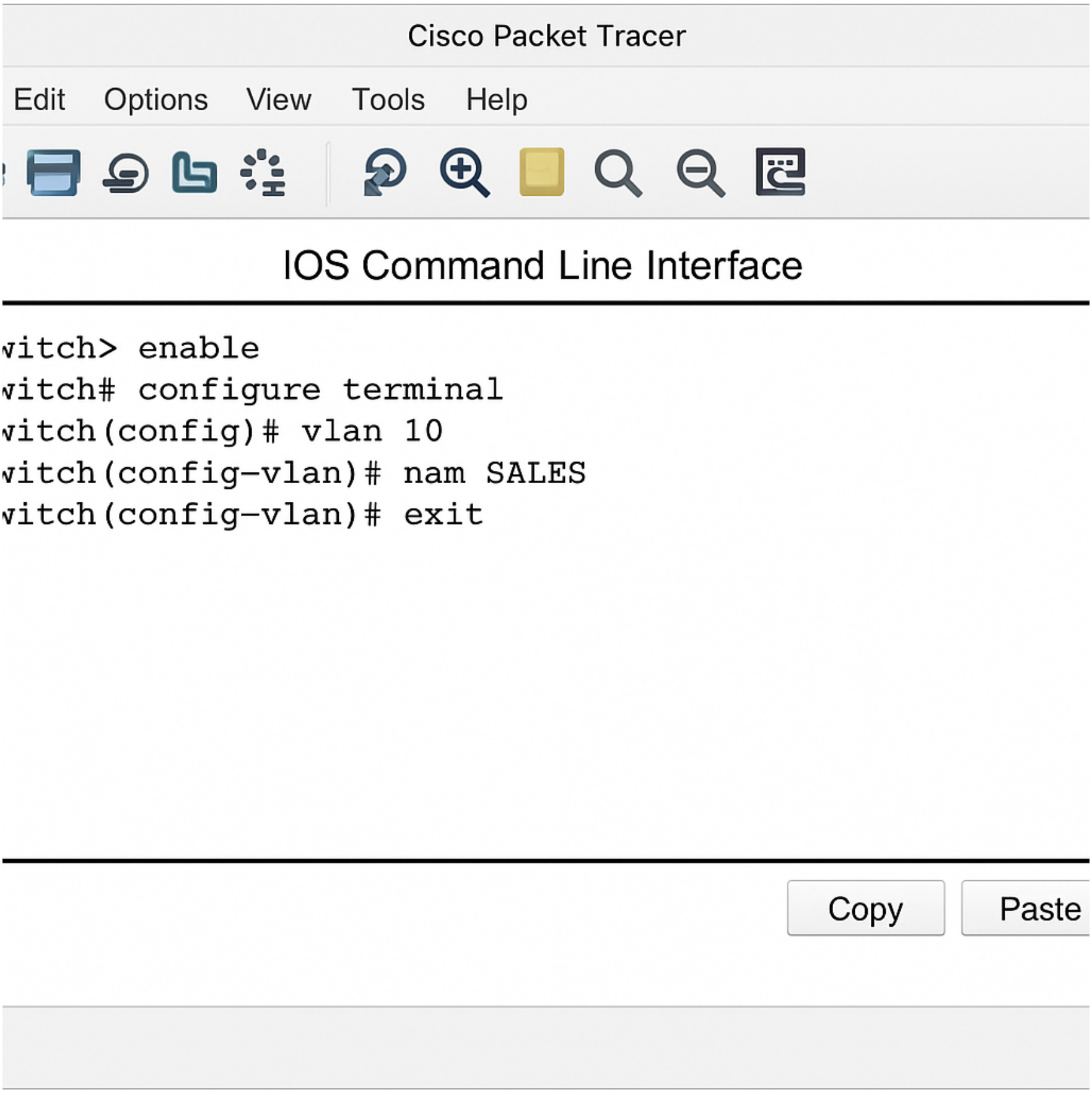
Emmanuel-Joyce NTSIA, Gauvain BOICHÉ, Joris STAVROULAKIS, Léo JARRY,

Nous jurons sur l'honneur que les commandes entre `` sont tapées à la main à partir de nos notes de cours. (Elles sont réfléchies par nous en notre âme et conscience, on boycott openAI)

Pour rigoler on a passé une instruction "Génère moi une capture d'écran de Cisco Packet Tracer en pleine configuration d'un VLAN par la CLI" et voilà le résultat :

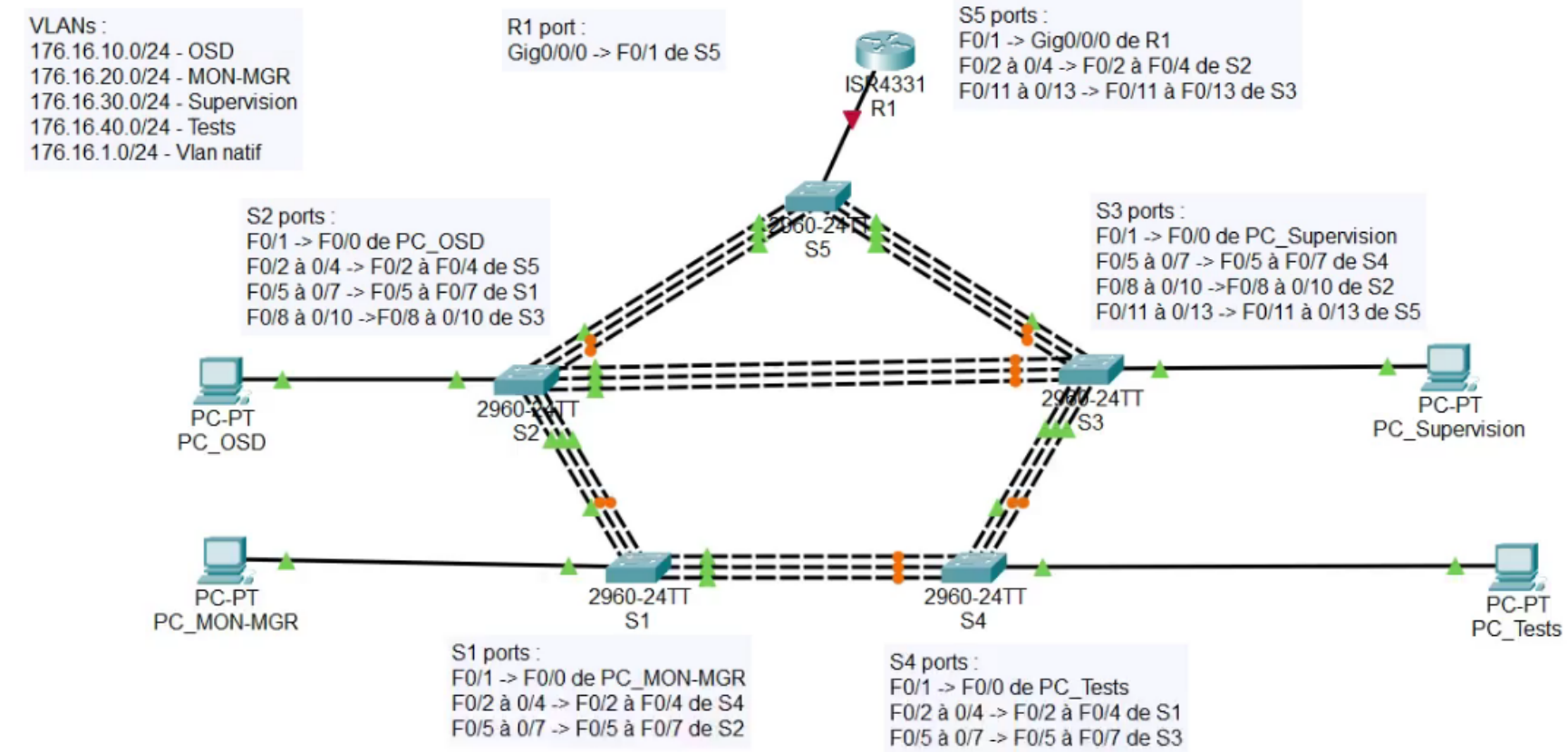


Pour ne pas rigoler, ça devrait être illégal de nous mettre du 176 quand on est habitué au 172 en adresse

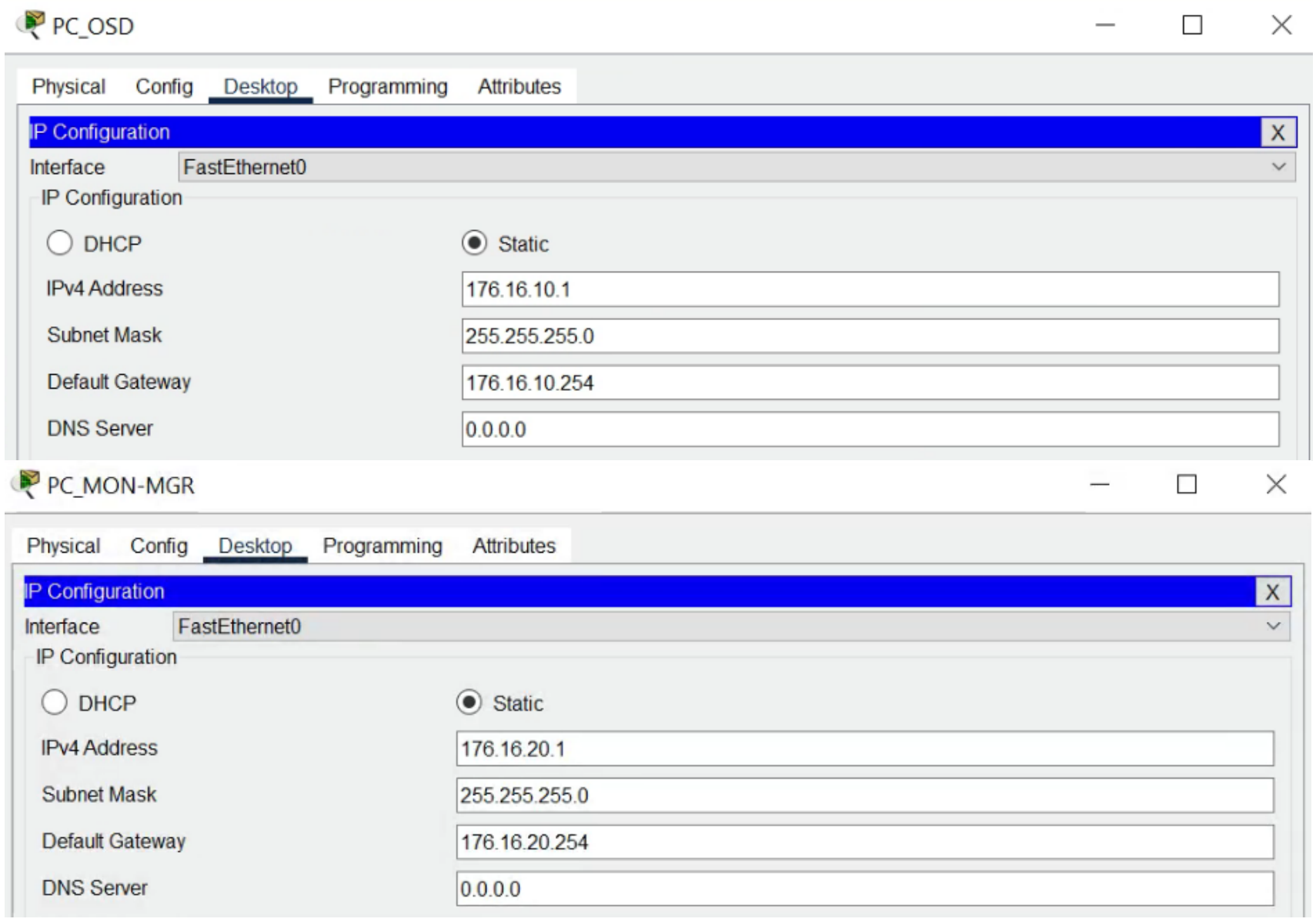
Mise en place de la Topologie physique:

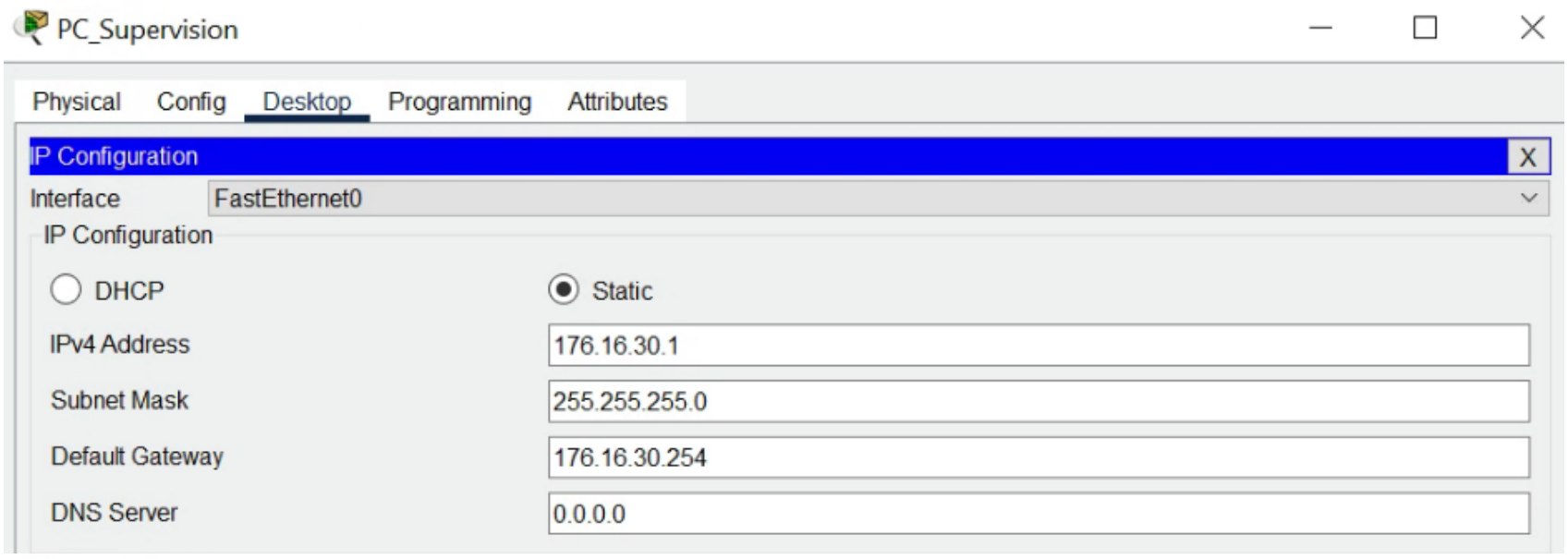
Le client a présenté une topologie précise avec des modèles précis, nous avons décidé de garder la topologie d'origine pour des questions de négociations facilitées.

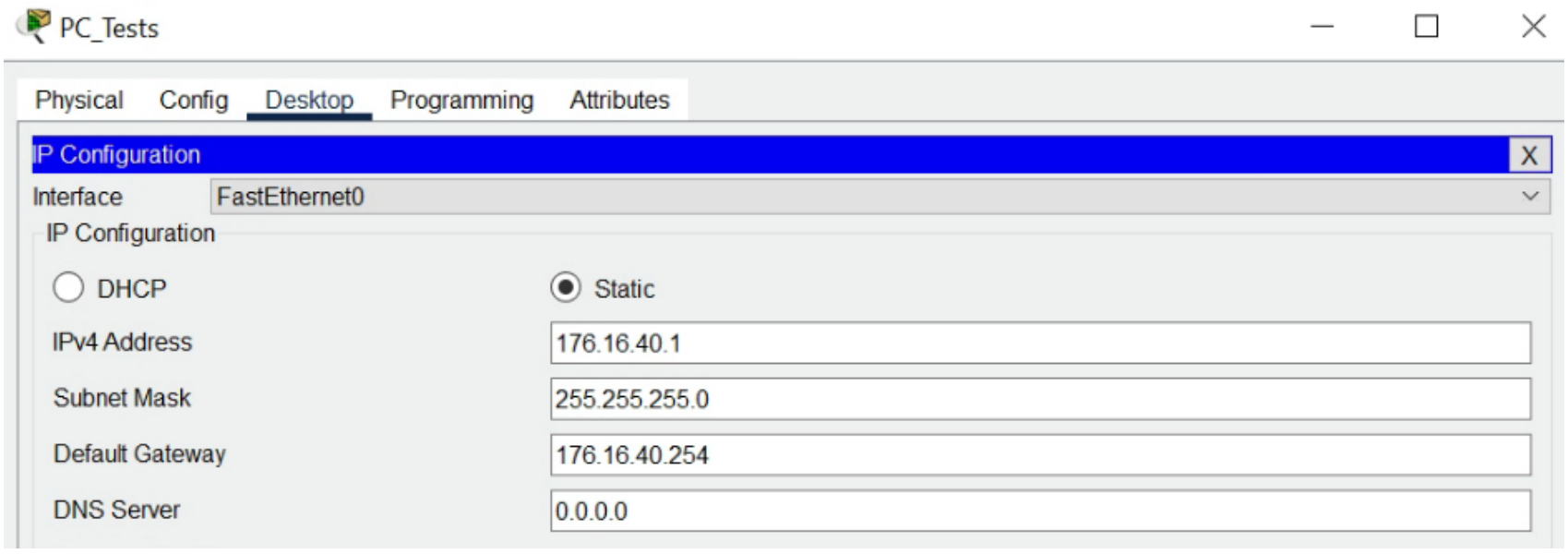
- Commutateurs 2960-24TT
- Routeur ISR4331
- Câbles droits pour liaisons routeurs & PC <-> commutateurs
- Câbles croisés pour liaisons inter-commutateurs



Mise en place des adresses IP pour les pc







Mise en place des VLAN

À noter qu'à partir de maintenant, des write memory sont fait après chaque étape pour s'assurer que la configuration soit bien sauvegardée

Création des VLANS dans les switch

À faire sur tous les Switchs

```
enable
  conf t
    vlan 10
      name OSD
      exit
    vlan 20
      name MON-MGR
      exit
    vlan 30
      name Supervision
      exit
    vlan 40
      name Tests
      exit
    interface vlan 1
      no shutdown
      exit
    interface vlan 10
      no shutdown
      exit
    interface vlan 20
      no shutdown
      exit
    interface vlan 30
      no shutdown
      exit
    interface vlan 40
      no shutdown
      end
  write memory
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#vlan 10
S1(config-vlan)#name OSD
S1(config-vlan)#vlan 20
S1(config-vlan)#name MON-MGR
S1(config-vlan)#vlan 30
S1(config-vlan)#name Supervision
S1(config-vlan)#vlan 40
S1(config-vlan)#name Tests
S1(config)#int vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#no shut
S1(config-if)#no shutdown
S1(config-if)#int vlan 20
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

S1(config-if)#no shu
S1(config-if)#no shutdown
S1(config-if)#int vlan 30
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

S1(config-if)#no shut
S1(config-if)#no shutdown
S1(config-if)#int vlan 40
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

S1(config-if)#no shutdow
S1(config-if)#no shutdown
```

```
S1(config-if)#int vlan 1
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

Vlan1	Up	1	<not set>	0030.F200.58D7
Vlan10	Up	10	<not set>	0030.F200.5801
Vlan20	Up	20	<not set>	0030.F200.5802
Vlan30	Up	30	<not set>	0030.F200.5803
Vlan40	Up	40	<not set>	0030.F200.5804

Mise en place des ports access Switch - PC

À faire sur tous les Switchs sauf S5 en adaptant le port et la vlan

```
S1(config-if)#
S1(config-if)#int f0/1
S1(config-if)#swi
S1(config-if)#switchport mode ac
S1(config-if)#switchport mode access
S1(config-if)#swi
S1(config-if)#switchport ac
S1(config-if)#switchport access vl
S1(config-if)#switchport access vlan 20
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

S1(config-if)#no shu
S1(config-if)#no shutdown
```

Mise en place du port trunk entre S5 et R1 (le routeur)

```
S5(config)#int f0/1
S5(config-if)#sw
S5(config-if)#switchport mode tr
S5(config-if)#switchport mode trunk
S5(config-if)#swi
S5(config-if)#switchport trunk n
S5(config-if)#switchport trunk native vl
S5(config-if)#switchport trunk native vlan 1
S5(config-if)#swi
S5(config-if)#switchport trunk a
S5(config-if)#switchport trunk allowed 1,10,20,30,40
                                       ^
% Invalid input detected at '^' marker.

S5(config-if)#switchport trunk allowed 1,10,20,30,40
S5(config-if)#switchport trunk allowed
S5(config-if)#switchport trunk allowed vlan 1,10,20,30,40
S5(config-if)#no shu
S5(config-if)#no shutdown
```

(Petit oubli) On rajoute le nonegotiate :

```
S5>en
S5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S5(config)#int f0/1
S5(config-if)#swi
S5(config-if)#switchport non
S5(config-if)#switchport nonegotiate
```

Mise en place des LAGs

Switch 1

```
enable
  conf t
    interface range Fa0/2 - 4
      channel-group 1 mode active
      exit
    interface range Fa0/5 - 7
      channel-group 2 mode active
      exit
    interface port-channel 1
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    interface port-channel 2
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    show interfaces Port-channel [1,2]    ! Pour contrôler
    show interfaces trunk                 ! Pour contrôler
    show etherchannel summary             ! Pour contrôler
    end
  write memory
```

Création du LAG en LACP actif

```
S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int range f0/2 - 4
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state
to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state
to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state
to up
```

Il faut faire pareil sur S4 (le switch de l'autre côté des ports concernés) du coup aussi pour que ça fonctionne

Configuration du trunk sur les LAGs

```
S1(config-if-range)#int port-channel 1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#switchport trunk allowed vlan 1,10,20,30,40
S1(config-if)#no shutdown
```

(Petit oubli) On rajoute le nonegotiate :

```
S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int port-channel 1
S1(config-if)#swi
S1(config-if)#switchport non
S1(config-if)#switchport nonegotiate
```

Ensuite il faut recommencer ces deux étapes (création du LAG et mise en place du trunk), sur tous les switchs en adaptant bien sûr les ports et en faisant bien attention de respecter les numéros de channel-group

Vérification du LAG et du trunk dessus

```
S1#show int Port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0006.2a7e.05ac (bia 0006.2a7e.05ac)
  MTU 1500 bytes, BW 300000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 300Mb/s
  input flow-control is off, output flow-control is off
  Members in this channel: Fa0/2 ,Fa0/3 ,Fa0/4 ,
  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
  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
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

S1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           LACP   Fa0/2(P) Fa0/3(P) Fa0/4(P)
2      Po2(SU)           LACP   Fa0/5(P) Fa0/6(P) Fa0/7(P)
S1#
```

```
S1>en
S1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Po1         on           802.1q         trunking      1
Po2         on           802.1q         trunking      1

Port        Vlans allowed on trunk
Po1         1,10,20,30,40
Po2         1,10,20,30,40

Port        Vlans allowed and active in management domain
Po1         1,10,20,30,40
Po2         1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Po1         1,10,20,30,40
Po2         1,10,20,30,40
```

Switch 2

```
enable
  conf t
    interface range Fa0/2 - 4
    channel-group 3 mode active
    exit
  interface range Fa0/5 - 7
    channel-group 2 mode active
    exit
  interface range Fa0/8 - 10
    channel-group 1 mode active
    exit
  interface port-channel 1
    switchport mode trunk
    switchport trunk native vlan 1
    switchport trunk allowed vlan 1,10,20,30,40
    no shutdown
    exit
  interface port-channel 2
    switchport mode trunk
    switchport trunk native vlan 1
    switchport trunk allowed vlan 1,10,20,30,40
    no shutdown
    exit
  interface port-channel 3
    switchport mode trunk
    switchport trunk native vlan 1
    switchport trunk allowed vlan 1,10,20,30,40
    no shutdown
    exit
  show interfaces Port-channel [1,2,3]
  show interfaces trunk
  show etherchannel summary
    end
  write memory
```

Switch 3

```
enable
  conf t
    interface range Fa0/5 - 7
      channel-group 2 mode active
      exit
    interface range Fa0/8 - 10
      channel-group 1 mode active
      exit
    interface range Fa0/11 - 13
      channel-group 4 mode active
      exit
    interface port-channel 1
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    interface port-channel 2
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    interface port-channel 3
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    show interfaces Port-channel [1,2,3]
    show interfaces trunk
    show etherchannel summary
    end
  write memory
```

Switch 4

```
enable
  conf t
    interface range Fa0/2 - 4
      channel-group 1 mode active
      exit
    interface range Fa0/5 - 7
      channel-group 2 mode active
      exit
    interface port-channel 1
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    interface port-channel 2
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    show interfaces Port-channel [1,2,3]
    show interfaces trunk
    show etherchannel summary
    end
  write memory
```

Switch 5

```
enable
  conf t
    interface range Fa0/2 - 4
      channel-group 3 mode active
      exit
    interface range Fa0/11 - 13
      channel-group 4 mode active
      exit
    interface port-channel 1
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    interface port-channel 2
      switchport mode trunk
      switchport trunk native vlan 1
      switchport trunk allowed vlan 1,10,20,30,40
      no shutdown
      exit
    show interfaces Port-channel [1,2,3]
    show interfaces trunk
    show etherchannel summary
    end
  write memory
```

Mise en place du routage inter-vlan

Routeur

```
enable
  conf t
    interface Gig0/0/0
      no shutdown
      exit
    interface Gig0/0/0.1
      encapsulation dot1Q 1 native
      ip address 176.16.1.254 255.255.255.0
      no shutdown
      exit
    interface Gig0/0/0.10
      encapsulation dot1Q 10
      ip address 176.16.10.254 255.255.255.0
      no shutdown
      exit
    interface Gig0/0/0.20
      encapsulation dot1Q 20
      ip address 176.16.20.254 255.255.255.0
      no shutdown
      exit
    interface Gig0/0/0.30
      encapsulation dot1Q 30
      ip address 176.16.30.254 255.255.255.0
      no shutdown
      exit
    interface Gig0/0/0.40
      encapsulation dot1Q 40
      ip address 176.16.40.254 255.255.255.0
      no shutdown
      end
  write memory
```

Interface physique

```
R1(config)#int gig0/0/0
R1(config-if)#no shut
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed
state to up

R1(config-if)#no ip add
```

Interfaces virtuelles

```
R1(config)#int gig0/0/0.1
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.1, changed
state to up

R1(config-subif)#encapsulation dot1q 1 native
R1(config-subif)#ip add 176.16.1.254 255.255.255.0
R1(config-subif)#no shutdown
R1(config)#int g0/0/0.10
R1(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.10, changed
state to up

R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip add 176.16.10.254 255.255.255.0
R1(config-subif)#no shutdown
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC_OSD	R1	ICMP		0.000	N	0	(edit)	

Depuis PC_OSD (vlan 10) :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 176.16.1.254

Pinging 176.16.1.254 with 32 bytes of data:

Reply from 176.16.1.254: bytes=32 time<1ms TTL=255
Reply from 176.16.1.254: bytes=32 time<1ms TTL=255
Reply from 176.16.1.254: bytes=32 time<1ms TTL=255
Reply from 176.16.1.254: bytes=32 time=8ms TTL=255

Ping statistics for 176.16.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>ping 176.16.40.1

Pinging 176.16.40.1 with 32 bytes of data:

Request timed out.
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127

Ping statistics for 176.16.40.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Puis on fait ça pour toutes les autres VLAN

```
Device Name: R1
Device Model: ISR4331
Hostname: R1

Port                    Link   VLAN   IP Address         IPv6 Address                              MAC Address
GigabitEthernet0/0/0    Up     --     <not set>          <not set>                                 0001.4383.D201
GigabitEthernet0/0/0.1  Up     --     176.16.1.254/24    <not set>                                 0001.4383.D201
GigabitEthernet0/0/0.10 Up     --     176.16.10.254/24   <not set>                                 0001.4383.D201
GigabitEthernet0/0/0.20 Up     --     176.16.20.254/24   <not set>                                 0001.4383.D201
GigabitEthernet0/0/0.30 Up     --     176.16.30.254/24   <not set>                                 0001.4383.D201
GigabitEthernet0/0/0.40 Up     --     176.16.40.254/24   <not set>                                 0001.4383.D201
GigabitEthernet0/0/1    Down   --     <not set>          <not set>                                 0001.4383.D202
GigabitEthernet0/0/2    Down   --     <not set>          <not set>                                 0001.4383.D203
Vlan1                   Down   1      <not set>          <not set>                                 0060.707E.CBA3

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > R1
```

Sécurisation et accès à distance sur chaque appareil

BPDU Guard

Sur les ports des switchs qui sont connectés aux pc/routeur on active le BPDU guard

```
enable
  conf t
    interface Fa0/1
      spanning-tree bpduguard enable
      end
  write memory

S1(config)#int f0/1
S1(config-if)#spanning-tree bpduguard enable
```

Sécurisation du port console

```
enable
  conf t
    line console 0
      password root
      login
      exit
    service password-encryption
    end
  write memory

S1(config)#line console 0
S1(config-line)#password root
S1(config-line)#login
S1(config-line)#exit
S1(config)#service pass
S1(config)#service password-encryption
```

Parce que c'est un exercice on va mettre le même mot de passe partout pour se simplifier la vie, bien sûr en vrai on mettrait des mots de passes forts et différents

Le service password-encryption servira à empêcher que le mot de passe soit accessible en clair dans la configuration

On fait la même chose sur tous les switch et routeur

Activation à distance (ssh)

```
enable
  conf t
    ip domain-name fuckssh.com
    username ssh secret root
    crypto key generate rsa general-keys modulus 2048
    line vty 0 15
      transport input ssh
      login local
      exit
    ip ssh version 2
    interface vlan 1
      ip address 176.16.1.1 255.255.255.0
      exit
    ip default-gateway 176.16.1.254
    end
  write memory
```

Le code est adapté pour chaque Switch, donc l'adresse IP sera 176.16.1.[1-5]

```
S1(config)#ip domain-name fuckssh.com
S1(config)#username ssh secret root
S1(config)#crypto key generate rsa modulus 2048
                                           ^
% Invalid input detected at '^' marker.

S1(config)#crypto key generate rsa?
rsa
S1(config)#crypto key generate rsa
The name for the keys will be: S1.fuckssh.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#line vty 0 15
*Mar 1 2:6:50.902: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#ip ssh version 2
```

On oublie bien sûr pas d'ajouter une ip au switch dans le vlan 1 pour pouvoir s'y connecter ainsi que l'ip default-gateway

```
S1(config)#ip default-gateway 176.16.1.254
```

```
S1(config)#int vlan 1
S1(config-if)#ip add 176.16.1.1 255.255.255.0
```

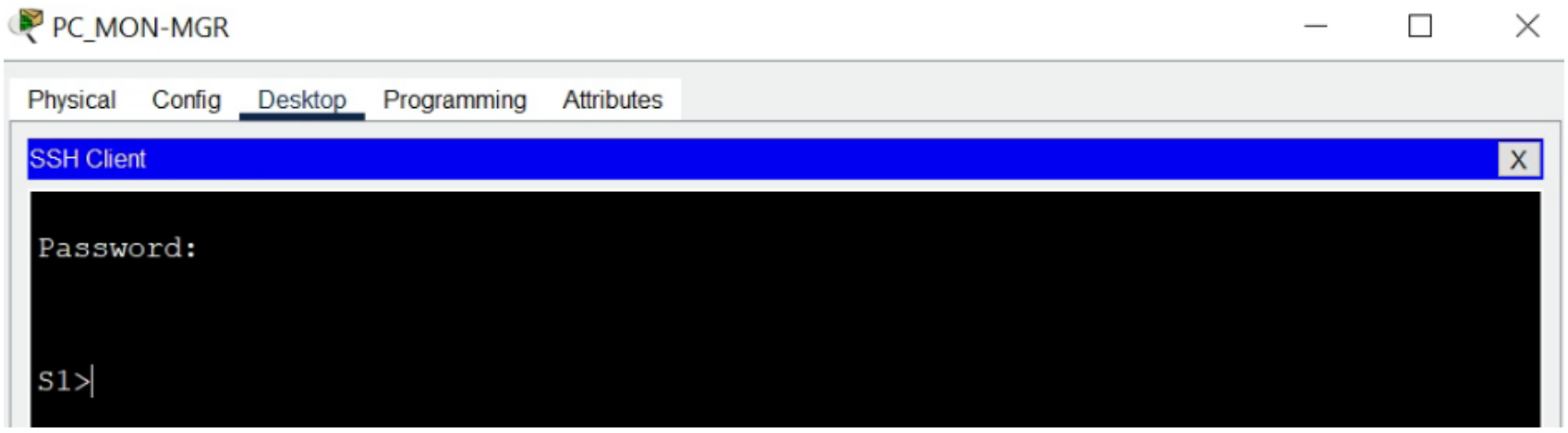
On fait la même chose sur tous les switch et routeur

Sécurisation du mode enable

```
enable
  conf t
    enable secret root
    end
  write memory
```

```
S1(config)#enable secret root
S1>en
Password:
```

Vérification accès à distance



MOTD + Sécurisation des interfaces inactives

```
enable
  conf t
    banner motd # Personnel autorise seulement #
    end
  write memory
```

On fait la même chose sur tous les switch et routeur

Puis on fait la sécurisation des interfaces inactives en les éteignant et en les mettant sur un vlan 44 créé exprès pour ça

```
S1(config)#vlan 44
S1(config-vlan)#int range f0/8 - 24
S1(config-if-range)#swi
S1(config-if-range)#switchport mode a
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access
S1(config-if-range)#switchport access vlan 44
S1(config-if-range)#shut
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down
S1(config)#int range gig0/1 - 2
S1(config-if-range)#swi
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 44
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively
down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively
down
S1(config-if-range)#
```

```
S1(config)#banner motd # Personnel autorise seulement #
```

```
Personnel autorise seulement

User Access Verification

Password:
```

Switch 1

```
enable
  conf t
    interface range Gig0/1 - 2
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/8 - 24
      switchport mode access
      switchport access vlan 44
      shutdown
      end
  write memory
```

Switch 2

```
enable
  conf t
    interface range Gig0/1 - 2
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/11 - 24
      switchport mode access
      switchport access vlan 44
      shutdown
      end
  write memory
```

Switch 3

```
enable
  conf t
    interface range Gig0/1 - 2
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/2 - 4
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/14 - 24
      switchport mode access
      switchport access vlan 44
      shutdown
      end
  write memory
```

Switch 4

```
enable
  conf t
    interface range Gig0/1 - 2
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/8 - 24
      switchport mode access
      switchport access vlan 44
      shutdown
      end
  write memory
```

Switch 5

```
enable
  conf t
    interface range Gig0/1 - 2
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/5 - 10
      switchport mode access
      switchport access vlan 44
      shutdown
      exit
    interface range Fa0/14 - 24
      switchport mode access
      switchport access vlan 44
      shutdown
      end
  write memory
```

Router

```
enable
  conf t
    interface range Gig0/0/1 - 2
      shutdown
      end
  write memory
```

Mise en place des ACLs

Pour les ACLs on a décidé deux faire deux listes, une spécifiquement à l'entrée de la gateway du vlan 10 sur le routeur qui bloque uniquement les ports utilisés par les OSD avec les protocoles CEPH

Et une deuxième à l'entrée de la gateway du vlan 20 sur le routeur pour bloquer les ports utilisés par le monitor / manager de la même façon

On bloque donc les paquets qui viennent de ces deux vlan sur les ports utilisés par CEPH et qui sont en destination du réseau Tests (vlan 40)

Tout le reste du traffic est permis entre tous les vlans définis (icmp / ip, etc...)

```
R1(config)#ip access
R1(config)#ip access-list extended CEPH_EXCLUDE_TESTS_VLAN10
R1(config-ext-nacl)#deny tcp 176.16.10.0 0.0.0.255 176.16.40.0 0.0.0.255 range
6800 7300
R1(config-ext-nacl)#permit icmp any any
R1(config-ext-nacl)#permit ip any any
R1(config)#ip access-list extended CEPH_EXCLUDE_TESTS_VLAN20
R1(config-ext-nacl)#deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 range
6800 7300
R1(config-ext-nacl)#deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 eq 3300
R1(config-ext-nacl)#deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 eq 6789
R1(config-ext-nacl)#permit icmp any any
R1(config-ext-nacl)#permit ip any any
R1(config-ext-nacl)#exit
R1(config)#int g0/0/0.10
R1(config-subif)#ip access-group CEPH_EXCLUDE_TESTS_VLAN10 in
R1(config)#int g0/0/0.20
R1(config-subif)#ip access-group CEPH_EXCLUDE_TESTS_VLAN20 in
```

```
Pinging 176.16.40.1 with 32 bytes of data:

Reply from 176.16.40.1: bytes=32 time<1ms TTL=127
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127
Reply from 176.16.40.1: bytes=32 time<1ms TTL=127

Ping statistics for 176.16.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
enable
  conf t
    ip access-list extended CEPH_EXCLUDE_TESTS_VLAN10
      deny tcp 176.16.10.0 0.0.0.255 176.16.40.0 0.0.0.255 range 6800 7300
      permit icmp any any
      permit ip any any
      exit
    ip access-list extended CEPH_EXCLUDE_TESTS_VLAN20
      deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 range 6800 7300
      deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 eq 3300
      deny tcp 176.16.20.0 0.0.0.255 176.16.40.0 0.0.0.255 eq 6789
      permit icmp any any
      permit ip any any
      exit
    interface Gig0/0/0.10
      ip access-group CEPH_EXCLUDE_TESTS_VLAN10 in
      exit
    interface Gig0/0/0.20
      ip access-group CEPH_EXCLUDE_TESTS_VLAN20 in
      end
  write memory
```

FIN

Ps : moins de 20/20 on débarque chez toi Cédric (dans minecraft)