

Simulación de red para una empresa mediana

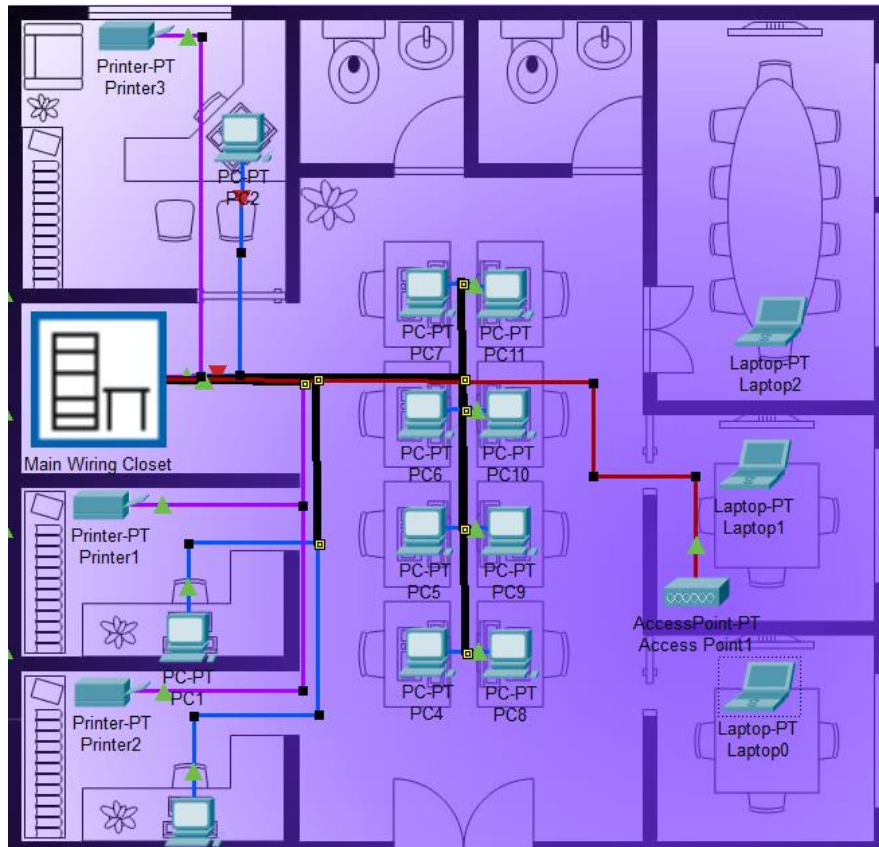
Nerea Fdez Fernández
Laboratorio Integral de
Redes de Datos
Junio de 2025



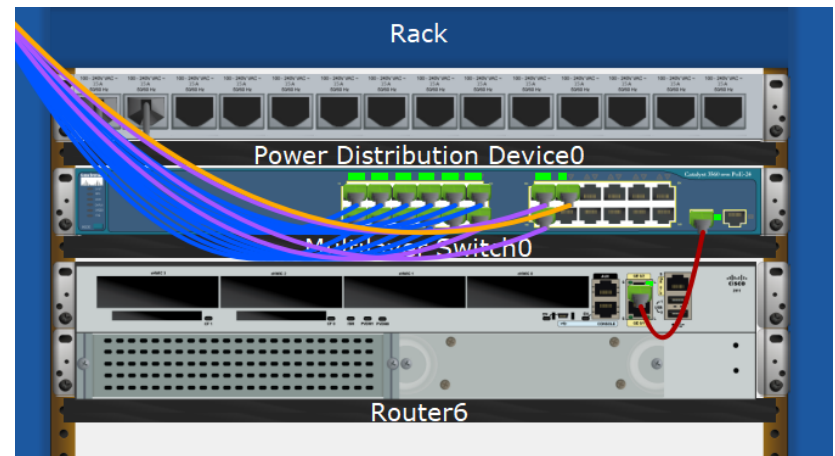
Topología lógica y física

Topología lógica:
Estrella con switch
de capa 3 central.

Topología física:
Rack centralizado
con conexiones
Ethernet.



La red se compone de: 11Hosts, 3 impresoras, 1 AP, 3 portátiles, 1 router y 1 Switch capa 3. Estas se conectan mediante cableado directo con conectores RJ45 y Wifi.



Creación de VLANs

- VLAN 10: Ordenadores (PC)
- VLAN 20: Impresoras (Printers)
- VLAN 30: WiFi (Portátiles, conectados al PA)
- VLAN 40: Router (router)

Esto se hará para segmentar la red, haciendo más fácil su gestión.

The screenshot shows the configuration interface for a Multilayer Switch. The 'Config' tab is selected, and the 'VLAN Database' is open. The 'VLAN Configuration' section shows a form for adding a new VLAN. The 'VLAN Number' is set to 10, and the 'VLAN Name' is set to ORDENADORES. Below the form, there are 'Add' and 'Remove' buttons. A table lists the existing VLANs:

VLAN No	VLAN Name
1	default
10	ORDENADORES
20	Impresoras
30	WIFI
40	router
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Asignación de IPs a VLANs

```
SwitchPT>enable
SwitchPT#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchPT(config)#interface vlan 10
SwitchPT(config-if)#ip address 192.168.10.1 255.255.255.0
SwitchPT(config-if)#no shutdown
SwitchPT(config-if)#exit
SwitchPT(config)#
```

Copy

Paste

Vlan10	Up	10	192.168.10.1/24	<not set>	0040.0B90.9B01
Vlan20	Up	20	192.168.20.1/24	<not set>	0040.0B90.9B02
Vlan30	Up	30	192.168.30.1/24	<not set>	0040.0B90.9B03
Vlan40	Up	40	192.168.40.1/24	<not set>	0040.0B90.9B04

Esto nos permitirá crear interfaces con sus IPs en las VLANs, necesario para que puedan operar correctamente, todo se hace desde el apartado “CLI” del Switch. (haremos el mismo procedimiento con todas las VLANs).

Configuración del Router

IP asignada: 192.168.40.10 en GigabitEthernet0/1.
(irá en la VLAN 40).

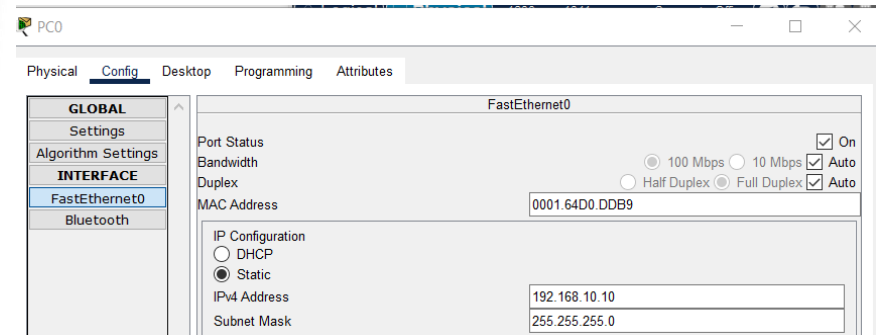
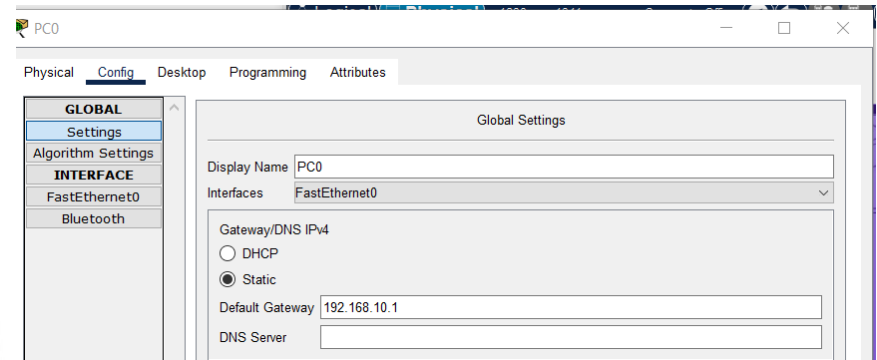
Physical Config CLI Attributes

GLOBAL	GigabitEthernet0/1	
Settings		
Algorithm Settings		
ROUTING		
Static		
RIP		
SWITCHING		
VLAN Database		
INTERFACE		
GigabitEthernet0/0		
GigabitEthernet0/1		
GigabitEthernet0/2		

Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input checked="" type="radio"/> 1000 Mbps <input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	0030.F2EE.6802
IP Configuration	
IPv4 Address	192.168.40.10
Subnet Mask	255.255.255.0
Tx Ring Limit	10

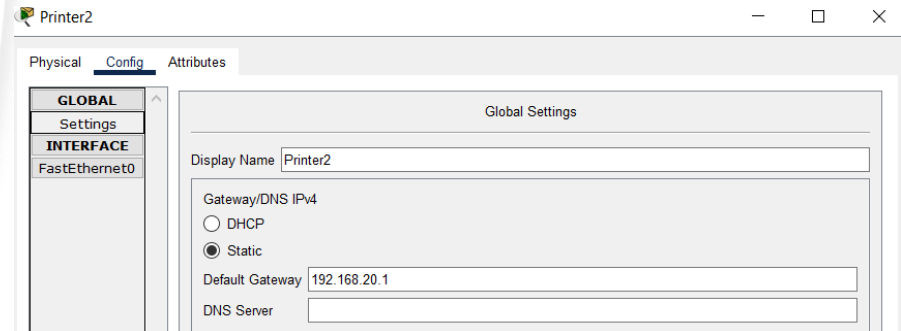
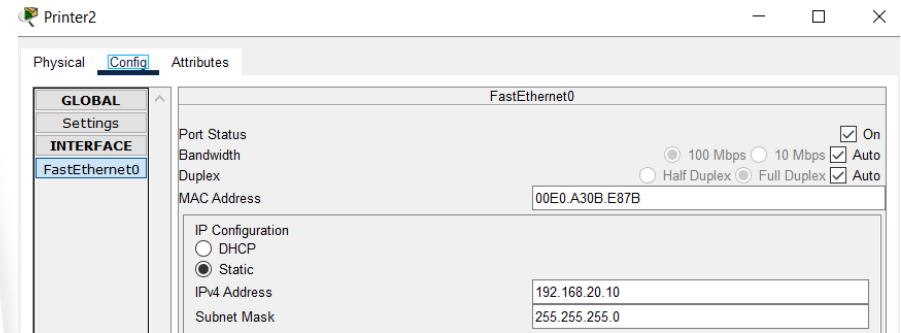
Configuración de PCs

- Gateway: 192.168.10.1 (VLAN 10).
- IP estática. (irán con el VLAN 10).
- Los 11 PCs, tendrán IPs a partir del 192.168.10.10-20. con máscara 255.255.255.0



Configuración de impresoras

- Gateway 192.168.20.1. (VLAN 20).
- IP estática (irán con la VLAN 20)
- Las 3 impresoras tendrán las Ips comprendidas en 192.168.20.10-12 con máscara 255.255.255.0



wifi

Physical **Config** Attributes

GLOBAL

Settings

INTERFACE

Port 0

Port 1

Port 1

Port Status ☒ On

SSID wifi

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase prueba1234

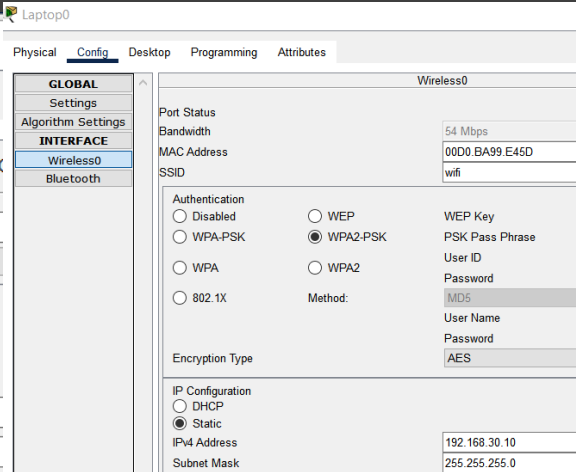
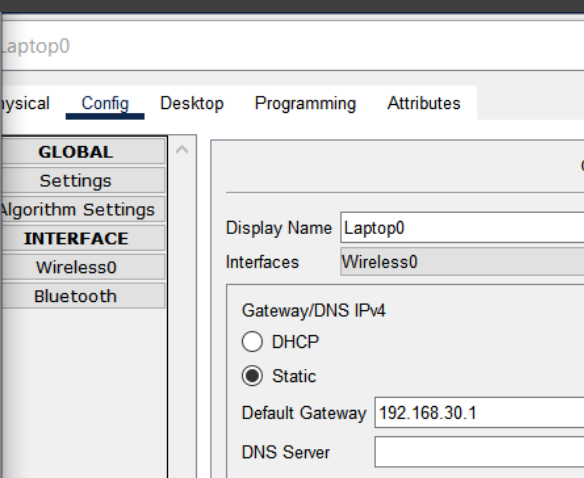
User ID

Password

Encryption Type AES

Configuración del AP

- Se configurará en el Puerto 1.
- SSID: wifi, Seguridad: WPA2-PSK, Pass: prueba1234. (Irà en la VLAN 30).



Configuración de portátiles



Open the

WPA2-Personal Needed for Connection

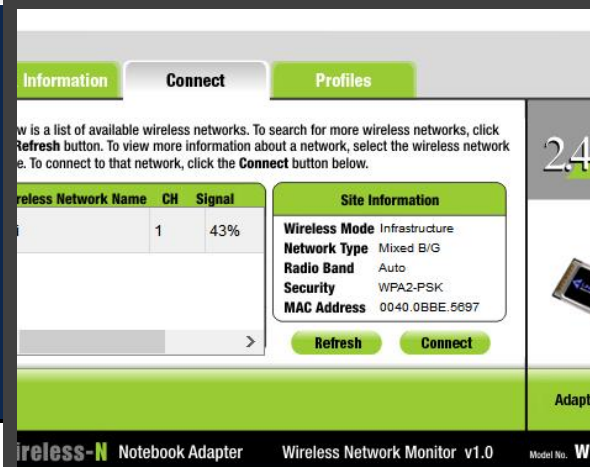
This wireless network has WPA2-Personal enabled. To connect to this network, enter the required prephrase in the appropriate field below. Then click the **Connect** button.

Security WPA2-Personal Please select the wireless security method used by your existing wireless network.

Pre-shared Key prueba1234 Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel Connect

Wireless-N Notebook Adapter Wireless Network Monitor v1.0 Model No.



- Conexión WiFi (se conectará al PA, mencionado anteriormente).
- IP estática (irá con la VLAN 30) 3 portátiles con Ips desde el 192.168.30.10-12 con máscara 255.255.255.0
- Gateway: 192.168.30.1 (VLAN 30)
- Como se muestra en la imagen, colocamos los datos del PA en el apartado Wireless0 del Portátil, y luego nos vamos a Desktop y a "PC Wireless", una vez dentro daremos Refresh y nos saldrá el PA, ponemos la contraseña y ya lo tendríamos conectado.

Integración por VLAN

- Una vez, configuradas las IPs en todos los dispositivos, lo siguiente que haremos será comprobar cuáles son los puertos que usa cada uno de ellos.

Para ello, dejaremos el ratón encima del Switch utilizado, y saldrá está lista en la que podemos comprobar que puertos se están utilizando.

En este caso:

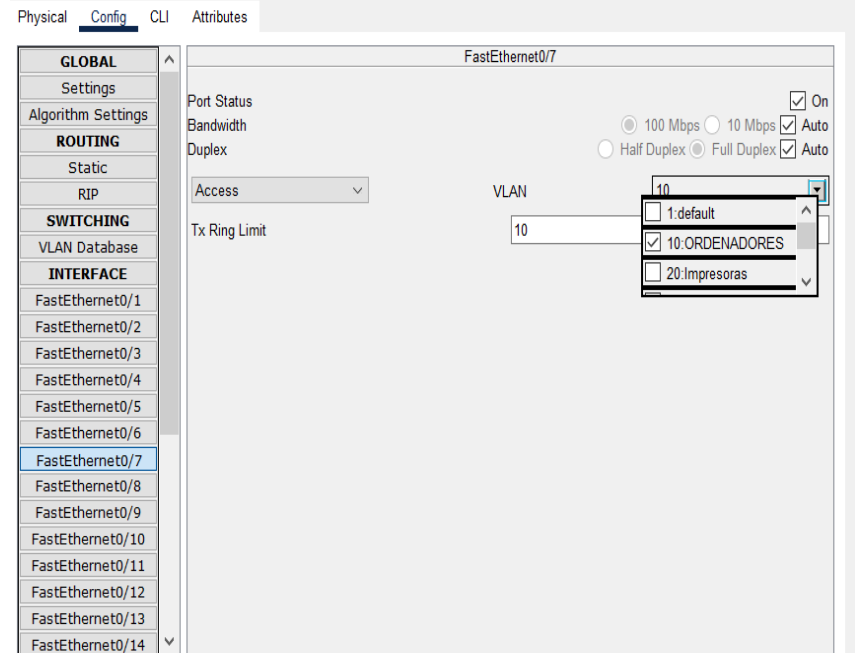
Fa01/ - Fa0/11: Son los PCs VLAN 10.

Fa0/12 – Fa0/14: Son las impresoras VLAN 20.

Fa0/15: Es el PA VLAN 30, luego los portátiles se conectarán a el.

Gig0/1: Router VLAN 40.

Que como se muestra en la 1ª imagen añadiremos su respectiva VLAN.



Device Name: Multilayer Switch0
Device Model: 3560-24PS
Hostname: SwitchPT

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/1	Up	10	<not set>	<not set>	000B.BE8D.3001
FastEthernet0/2	Up	10	<not set>	<not set>	000B.BE8D.3002
FastEthernet0/3	Up	10	<not set>	<not set>	000B.BE8D.3003
FastEthernet0/4	Up	10	<not set>	<not set>	000B.BE8D.3004
FastEthernet0/5	Up	10	<not set>	<not set>	000B.BE8D.3005
FastEthernet0/6	Up	10	<not set>	<not set>	000B.BE8D.3006
FastEthernet0/7	Up	10	<not set>	<not set>	000B.BE8D.3007
FastEthernet0/8	Up	10	<not set>	<not set>	000B.BE8D.3008
FastEthernet0/9	Up	10	<not set>	<not set>	000B.BE8D.3009
FastEthernet0/10	Up	10	<not set>	<not set>	000B.BE8D.300A
FastEthernet0/11	Up	10	<not set>	<not set>	000B.BE8D.300B
FastEthernet0/12	Up	20	<not set>	<not set>	000B.BE8D.300C
FastEthernet0/13	Up	20	<not set>	<not set>	000B.BE8D.300D
FastEthernet0/14	Up	20	<not set>	<not set>	000B.BE8D.300E
FastEthernet0/15	Up	30	<not set>	<not set>	000B.BE8D.300F
FastEthernet0/16	Down	1	<not set>	<not set>	000B.BE8D.3010
FastEthernet0/17	Down	1	<not set>	<not set>	000B.BE8D.3011
FastEthernet0/18	Down	1	<not set>	<not set>	000B.BE8D.3012
FastEthernet0/19	Down	1	<not set>	<not set>	000B.BE8D.3013
FastEthernet0/20	Down	1	<not set>	<not set>	000B.BE8D.3014
FastEthernet0/21	Down	1	<not set>	<not set>	000B.BE8D.3015
FastEthernet0/22	Down	1	<not set>	<not set>	000B.BE8D.3016
FastEthernet0/23	Down	1	<not set>	<not set>	000B.BE8D.3017
FastEthernet0/24	Down	1	<not set>	<not set>	000B.BE8D.3018
GigabitEthernet0/1	Up	40	<not set>	<not set>	000B.BE8D.3019
GigabitEthernet0/2	Down	1	<not set>	<not set>	000B.BE8D.301A
Vlan1	Down	1	<not set>	<not set>	0040.0B90.9B01
Vlan10	Up	10	192.168.10.1/24	<not set>	0040.0B90.9B01
Vlan20	Up	20	192.168.20.1/24	<not set>	0040.0B90.9B02
Vlan30	Up	30	192.168.30.1/24	<not set>	0040.0B90.9B03
Vlan40	Up	40	192.168.40.1/24	<not set>	0040.0B90.9B04

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Multilayer Switch0

Lo siguiente es establecer los puertos de entrada en el Switch capa 3, ya que todavía no se han unido los dispositivos con la VLAN correspondiente. Para ello usaremos los siguientes comandos:

```
SwitchPT>enable
SwitchPT#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchPT(config)#interface range fastEthernet 0/1
SwitchPT(config-if-range)#switchport access vlan 10
SwitchPT(config-if-range)#no shutdown
SwitchPT(config-if-range)#exit
SwitchPT(config)#
```

Configuración de puertos del Switch

- Una vez listo, en este caso, el puerto 0/1 que sería el PC 0 ya tendría acceso y unión a la VLAN 10.
- Lo mismo haremos con todos los puertos y dispositivos correspondientes, respetando las VLAN de cada uno.
- Importante, para el router tendremos que hacer lo mismo, pero este será con el comando `ip route 192.168.0.0 255.255.0.0 192.168.40.1` (para que permita la comunicación con todos).

Pruebas de conectividad

- Una vez todo listo, comenzamos a realizar ping a todos los dispositivos, para comprobar que la conexión estuviese bien.
- Una vez viendo que todo está correcto, procederemos a crear las ACL (listas de control de acceso), esto mejora mas aún la red, ya que proporciona una mayor seguridad y gestión.

```
Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
```

Configuración de ACLs

El objetivo es:

- Bloqueo de tráfico VLAN 30 hacia VLANs 10 y 20 e viceversa.
- Y que la VLAN 40 sea vista por todas.
- Utilizando esos comandos, como se muestra en la imagen, ya tendríamos todo listo.

Multilayer Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

Press RETURN to get started.

```
SwitchPT>Enable
SwitchPT# Configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SwitchPT(config)# ip access-list extended FILTRO_WIFI
SwitchPT(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
SwitchPT(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
SwitchPT(config-ext-nacl)# permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
SwitchPT(config-ext-nacl)# exit
SwitchPT(config)# Enable
% Incomplete command.
SwitchPT(config)# Configure terminal
      ^
% Invalid input detected at '^' marker.

SwitchPT(config)# ip access-list extended WIFI_FILTRO
SwitchPT(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
SwitchPT(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
SwitchPT(config-ext-nacl)# permit ip any any
SwitchPT(config-ext-nacl)# exit
SwitchPT(config)# interface vlan 10
SwitchPT(config-if)# ip access-group WIFI_FILTRO out
SwitchPT(config-if)# interface vlan 20
SwitchPT(config-if)# ip access-group WIFI_FILTRO out
SwitchPT(config-if)# interface vlan 30
SwitchPT(config-if)# ip access-group FILTRO_WIFI out
SwitchPT(config-if)#
```

Copy Paste

Pruebas con ACL

- Ping bloqueado desde VLAN 30 hacia VLAN 10/20 y viceversa.
- Como se puede ver, las ACL fueron gestionadas correctamente.

```
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
```

```
C:\>ping 192.168.30.10

Pinging 192.168.30.10 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
```

Seguridad de puertos

- Esto permitirá que solo “x” dispositivos puedan conectarse en el puerto elegido, dando más seguridad.
- Para ello usaremos los comandos que se ve en la primera imagen.
- Para comprobar luego que se configuró correctamente podremos usar el comando `show port-security interface` (puerto a comprobar). Como se ve en la segunda imagen.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fa0/1
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 violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#interface fa0/2
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 violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#interface fa0/3
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 violation restrict
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#
```

```
show port-security interface fa0/15
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0001.C76B.E80D:30
Security Violation Count : 4

Switch#
```

Tabla MAC

- Verificaremos las MAC de los dispositivos conectados a nuestro Switch con el comando 'show mac address-table'.

```
10 0060.3e01.b92c DYNAMIC Fa0/7
10 0060.70bb.aa77 DYNAMIC Fa0/6
10 0090.2140.9cea DYNAMIC Fa0/4
10 00e0.f998.6058 DYNAMIC Fa0/8
30 0001.c76b.e80d DYNAMIC Fa0/15
30 0002.16da.c153 DYNAMIC Fa0/15
30 00d0.ba99.e45d DYNAMIC Fa0/15
Switch#show mac address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
10     0000.0c94.ec8d      DYNAMIC   Fa0/11
10     0001.64d0.ddb9      DYNAMIC   Fa0/1
10     0007.ecbc.2a06      DYNAMIC   Fa0/10
10     000c.857e.338c      DYNAMIC   Fa0/9
10     0060.3e01.b92c      DYNAMIC   Fa0/7
10     00e0.f998.6058      DYNAMIC   Fa0/8
20     00e0.a30b.e87b      DYNAMIC   Fa0/14
30     0001.c76b.e80d      DYNAMIC   Fa0/15
30     0002.16da.c153      DYNAMIC   Fa0/15
30     00d0.ba99.e45d      DYNAMIC   Fa0/15
Switch#show mac address-table
      Mac Address Table
-----
Vlan  Mac Address      Type      Ports
----  -
10     0000.0c94.ec8d      DYNAMIC   Fa0/11
10     0001.64d0.ddb9      DYNAMIC   Fa0/1
10     0007.ecbc.2a06      DYNAMIC   Fa0/10
10     000c.857e.338c      DYNAMIC   Fa0/9
20     0002.1684.dc47      DYNAMIC   Fa0/12
20     000a.413c.e5a5      DYNAMIC   Fa0/13
20     00e0.a30b.e87b      DYNAMIC   Fa0/14
30     0001.c76b.e80d      DYNAMIC   Fa0/15
30     0002.16da.c153      DYNAMIC   Fa0/15
30     00d0.ba99.e45d      DYNAMIC   Fa0/15
Switch#
```


Configuración de STP

- Prioridad configurada para cada VLAN.
- Esto permitirá a cada VLAN ejecutar su propia instancia de STP.
- Permitiendo detectar topologías redundantes, hacer switch raíz, bloquear puertos para prevenir bucles y recalcular enlaces en caso de fallo.

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     0040.0B90.9BC7
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    4106 (priority 4096 sys-id-ext 10)
Address     0040.0B90.9BC7
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time  20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type

Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Desg	FWD	19	128.3	P2p
Fa0/4	Desg	FWD	19	128.4	P2p
Fa0/5	Desg	FWD	19	128.5	P2p
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/7	Desg	FWD	19	128.7	P2p
Fa0/8	Desg	FWD	19	128.8	P2p
Fa0/9	Desg	FWD	19	128.9	P2p
Fa0/10	Desg	FWD	19	128.10	P2p
Fa0/11	Desg	FWD	19	128.11	P2p

```
Switch#show spanning-tree vlan 20
VLAN0020
  Spanning tree enabled protocol ieee
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server community read ro
Router(config)# snmp-server community write rw
Router(config)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

- Primero nos iremos al router, para configurar el SNMP.
- Luego, iremos aun PC cualquiera, nos iremos al apartado Desktopt y nos iremos a MBI Browser.



Monitorización con SNMP

Advanced	
Address	192.168.40.10
Port	161
Read Community
Write Community
SNMP Version	v1
<div>OK Cancel</div>	

Le damos a Advanced, y meteremos la ip del router, el puerto "161" (por defecto), y lo que escribimos antes en el router "read" y "write".

Monitorización SNMP

- Buscamos en el SNMP MIBs, la parte de system, y sysname (Este nos dará el OID del router, identificación). Más arriba como nos muestra la imagen, podremos mirar el tiempo de encendido..etc.

The screenshot shows a network management interface with tabs for 'fig', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active. It displays a configuration area with a text box containing '192.168.40.10', an 'Advanced...' button, an 'OID:' field with the value '.1.3.6.1.2.1.1.5.0', and an 'Operations:' dropdown menu set to 'Get'. Below this is a tree view of SNMP MIBs. The tree is expanded to show the following structure:

- _std MIBs
 - so
 - .org
 - .dod
 - .internet
 - .mgmt
 - .mib-2
 - .system
 - .sysDescr
 - .sysObjectID
 - .sysUpTime
 - .sysContact
 - .sysName
 - .sysLocation
 - .interfaces
 - .ip
 - .ospf
 - .rip2
 - .private
 - _advip MIBs
 - so
 - 1_L2 MIBs
 - 1_multiLayer MIBs

To the right of the tree is a 'Result Table' with the following data:

Name/OID	Value	Ok
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.interne...	Router	Ok

Below the table is a form with the following fields:

Name :	.sysName
OID :	.1.3.6.1.2.1.1.
Syntax :	
Access :	
Description :	

Conclusión

Este diseño permite gestionar toda la red de manera eficiente, segura y con capacidad de crecimiento. Los dispositivos están divididos en segmentos usando VLANs, lo que facilita su administración y ayuda a mantener la infraestructura más segura. Además, la configuración hecha ahora permite ampliar la red en el futuro sin tener que hacer cambios complicados en la estructura existente. Como una posible mejora, se podría pensar en agregar switches de capa 2 para conectar directamente los ordenadores y las impresoras. Esto ayudaría a evitar que los puertos del switch principal de capa 3 se saturen, mejorando el rendimiento y la distribución de la red.