

Escuela Colombiana de Ingeniería Julio Garavito

Laboratorio # 4: Plataforma base y capa de enlace

**Juan Sebastián Frásica Galeano
Juan Sebastián Gómez López
Miguel Castellanos
Daniel Alfonso**

Redes de Computadores

Profesora: Ing. Claudia Patricia Santiago Cely

Introducción:

La capa de enlace comprende muchos conceptos, entre los cuales está el funcionamiento de los switches en una red LAN. Esta capa también abarca otro tipo de red llamado VLAN, las cuales serán estudiadas en detalle en esta practica de laboratorio, de manera física y en una simulación.

En este laboratorio se aprenderá a configurar un switch, y una VLAN. Posteriormente se realizará la configuración de un router inalámbrico, y se verificará su conexión mediante el uso de Smartphones.

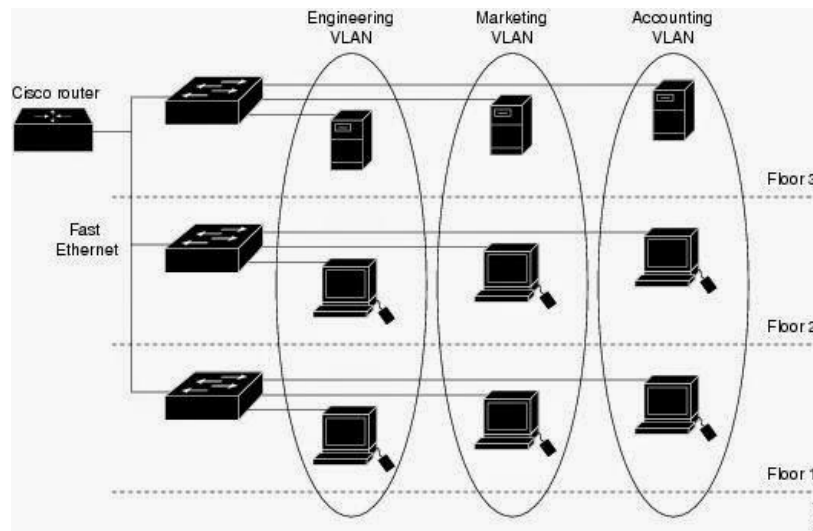
Finalmente se entrará mas a fondo con la infraestructura computacional, instalando en Slackware el motor de bases de datos MariaDB, creando algunas bases de datos, tablas y poblándolas con algunos datos.

Marco teórico:

VLAN:

Virtual LAN (Red de área local y virtual), es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLAN's dentro de un mismo router o switch. Podría decirse que cada una de estas redes agrupa los equipos de un determinado segmento de red. Crear estas particiones tiene unas ventajas bastante claras a la hora de administrar una red.

Hoy en día se configuran a través de software y poseen grandes beneficios a la hora de garantizar la seguridad y administrar los equipos de forma eficaz. En lo que concierne a la seguridad, hay que tener en cuenta que los dispositivos pertenecientes a una VLAN no tienen acceso a los que se encuentren en otras y viceversa. Resulta útil cuando queremos segmentar los equipos y limitar el acceso entre ellos por temas de seguridad.



Tipos de VLAN:

VLAN de nivel 1 (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador.

La VLAN de nivel 2 (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación.

Las VLAN están definidas por los estándares IEEE 802.1D, 802.1p, 802.1Q y 802.10.

Router inalámbrico:

Los routers inalámbricos, son pequeños equipos especialmente diseñados para trabajar sin sistemas de cables y ofrecer conexión de red a un ordenador o a un grupo de ordenadores.

Estos dispositivos, están compuestos por una entrada de cable que los conecta a la red y un sistema de antena que realiza el enlace inalámbrico de los equipos que se requiere conectar al servicio de Internet o, a la red interna de una empresa, institución u hogar, según sea el caso.

El objetivo principal del router inalámbrico, es enviar información de un computador a otro, evitando el molesto sistema de cableado y compartiendo de manera efectiva y simple, servicios como conexión a Internet o a red entre varios equipos a la vez, con un solo dispositivo.

**Access Point:**

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.



Configuración de un sistema operativo de red:

Modos del comando primario:

Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC del usuario	<ul style="list-style-type: none"> • Permite el acceso solamente a una cantidad limitada de comandos básicos de monitoreo. • A menudo se le describe como un modo de “visualización solamente”. 	Switch> Router>
Modo EXEC privilegiado	<ul style="list-style-type: none"> • Permite el acceso a todos los comandos y funciones. • El usuario puede utilizar cualquier comando de monitoreo y ejecutar comandos de configuración y de administración. 	Switch# Router#

En Packet Tracer:

Para **pasar del modo de usuario al privilegiado** utilizar el comando: “**enable**”

Para **pasar del modo privilegiado al de usuario** utilizar el comando: “**disable**”

Para **pasar al modo de configuración global** usar el comando: “**configure terminal**” o “**config t**” o “**conf t**”

Para **salir del modo de configuración global** usar el comando: “**exit**”

Para **pasar de cualquier modo de subconfiguración al modo privilegiado**, usar el comando “**end**” o presionar la combinación de teclas **Ctrl+Z**.

- **Modo de configuración de línea:** se utiliza para configurar la consola, SSH, Telnet o el acceso auxiliar.

- **Modo de configuración de interfaz:** se utiliza para configurar un puerto de switch o una interfaz de red de router.

Para pasar al modo de la subconfiguración de la interfaz, usar el comando:
“interface vlan 1”

Configuración de un nombre de host:

1. Acceder al modo de configuración global (configure terminal)
2. **hostname** switch-piso-1

Configuración de contraseñas:

- **EXEC privilegiado:** (es la más importante)

```
Sw-Floor-1> enable
Sw-Floor-1#
Sw-Floor-1# conf terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
Sw-Floor-1# disable
Sw-Floor-1> enable
Password: ← clase
Sw-Floor-1#
```

El comando es: “**enable secret** *password*”

- **EXEC de usuario:**

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# exit
Sw-Floor-1(config)#
```

El comando es: “**password** *password*”

- Línea de la terminal virtual (VTY): (SSH y Telnet)

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)#
```

El comando es: “**password** *password*”

Cifrado de contraseñas:

En el modo de configuración global:

Para cifrar todas las contraseñas se usa el comando “**service password-encryption**”

Para verificar que las contraseñas se han encriptado se usa el comando “**show running-config**” o “**show run**”

Mensajes de aviso:

Para asegurar con contraseña el modo privilegiado se debe ir al modo de configuración global y ejecutar el comando “**enable secret** *password*”

Para asegurar con contraseña el acceso a un switch se debe ir al modo de configuración global y ejecutar el comando “**line console 0**”, luego enter. Luego “**password** *password*”. Luego “**login**”

Para asegurar el switch desde accesos remotos se utiliza en el modo de configuración global el comando “**line vty** *NumLineasQueQuieroPermitirAlAccesoRemoto*”. Cisco permite máximo 16 terminales virtuales.

Ejemplo: “**line vty 0 15**”, así se permitirá configurar los terminales virtuales de 0 a 15

Luego “**password** *password*”. Luego “**login**”

Para el mensaje de aviso se utiliza el comando “**banner motd** “*mensaje*””

Ejemplo limitar el acceso a un switch:

Limite el acceso a un switch.

- **Cifre todas las contraseñas.**
- **Proteja el acceso a EXEC privilegiado.**
- **Proteja el acceso a la consola.**
- **Proteja el acceso a VTY.**

Cifre todas las contraseñas.

```
Sw-Floor-1(config)# service password-encryption
Sw-Piso-1(config)#
```

Proteja el acceso a EXEC privilegiado con la contraseña. Cla55.

```
Sw-Floor-1(config)# enable secret Cla55
Sw-Piso-1(config)#
```

Proteja la línea de la consola.

- **Utilice la contraseña Cisc0.**
- **Permita el inicio de sesión.**

```
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password Cisc0
Sw-Floor-1(config-line)# login
SW-Piso-1(config-line)#
```

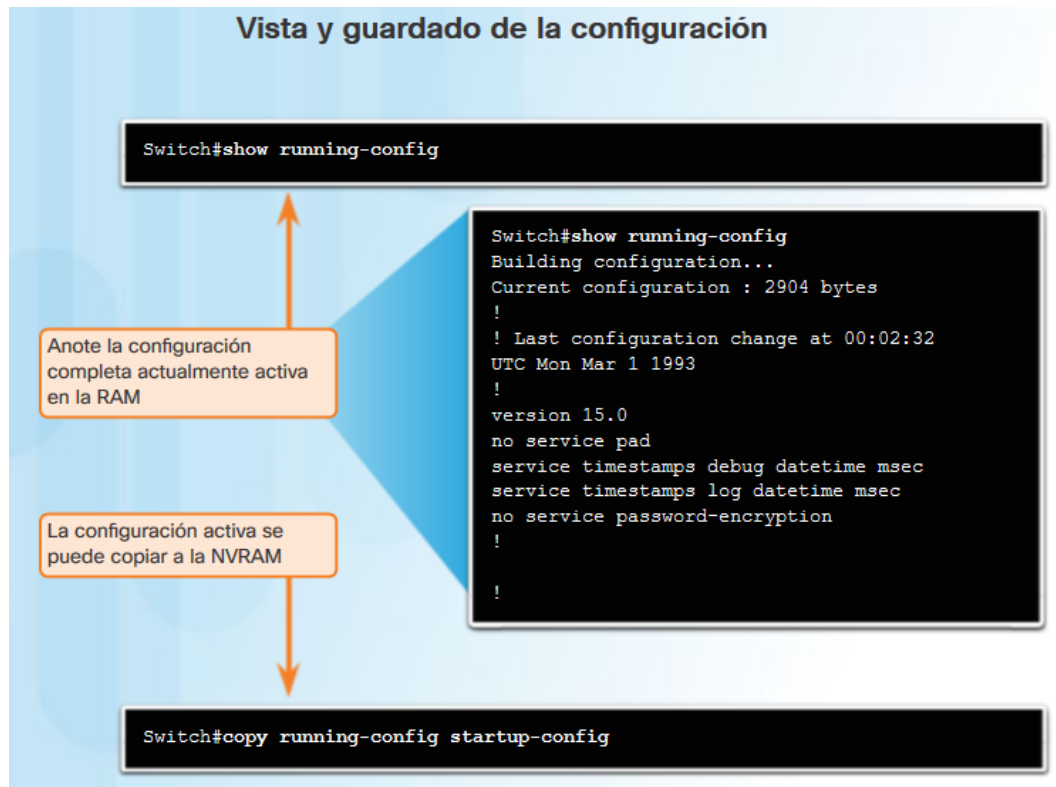
Proteja las primeras 16 líneas VTY.

- **Utilice la contraseña Cisc0.**
- **Permita el inicio de sesión.**

```
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password Cisc0
Sw-Floor-1(config-line)# login
SW-Piso-1(config-line)#
```

Limitó correctamente el acceso a un switch.

Guardar el archivo de configuración en ejecución:



Se utiliza el comando **“copy running-config startup-config”** o **“copy run start”**

Luego enter, enter

La NVRAM contiene el archivo de la configuración. La NVRAM no es volátil, es decir, que, si se reinicia el switch, la configuración prevalecerá.

Luego **“dir nvram”**

Para borrar la configuración se realiza el siguiente comando: **“erase startup-config”**

Configuración de la interfaz virtual de switch:

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI. La dirección IP será configurada a una interfaz de una VLAN.

Para esto se debe acceder al modo privilegiado y ejecutar el comando **“interface vlan 1”**

Luego, para asignar la dirección IP al switch se usa el comando **“ip address direccionIP mascaraDeSubred”**

Ejemplo: **“ip adress 192.168.1.10 255.255.255.0”**

Luego toca activar la interfaz VLAN: “**no shutdown**” o “**no shut**”

Para ver un resumen de la información (examinar las interfaces del switch): “**show ip interface brief**”

Ejemplo:

Configuración de una interfaz virtual de switch

- **Ingresa el modo de configuración de interfaz para la VLAN 1.**
- **Configure la dirección IPv4 como 192.168.10.2 y la máscara de subred como 255.255.255.0.**
- **Habilitar la interfaz.**

```
Switch(config)# interface vlan 1
```

```
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
```

```
Switch(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

```
Switch(config-if)#
```

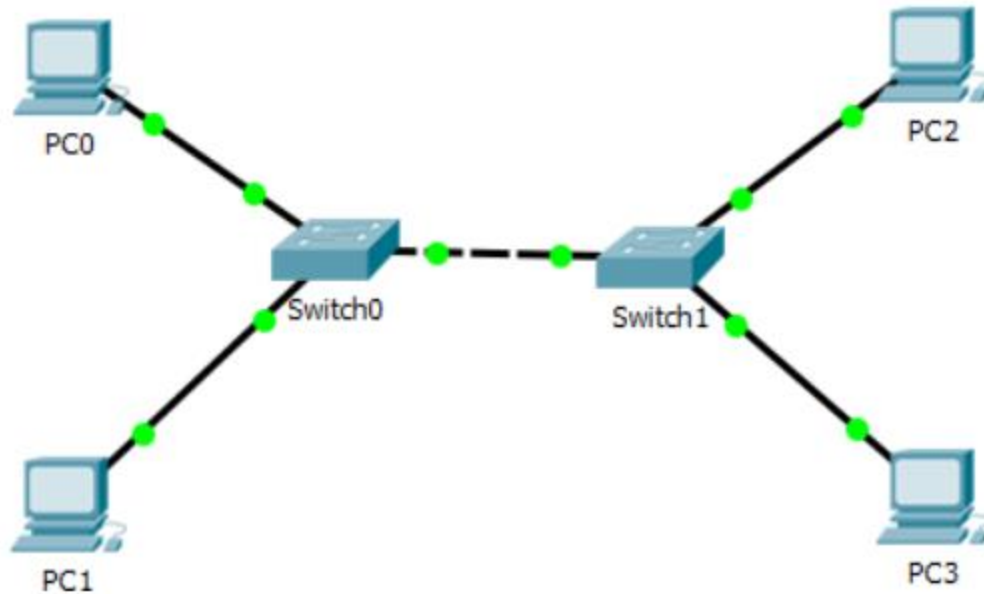
Configuró correctamente la interfaz virtual de switch para VLAN 1.

Desarrollo del tema:

Montaje N°1:

1. Configuración básica del switch:

Realice el siguiente montaje. Una pareja se encargará del Switch0, PC0 y PC1. La otra pareja de Switch1, PC2 y PC3.



Use la configuración de direcciones IP como está usualmente. Para eso,

- Copie la configuración de red (Dirección IP, Máscara, Gateway y Servidor DNS) de los cuatro computadores en un archivo antes de comenzar.

Direcciones IP: 10.2.67.113 al 10.2.67.116

Máscara: 255.255.0.0

Gateway: 10.2.65.1

Servidor DNS: 10.2.65.0

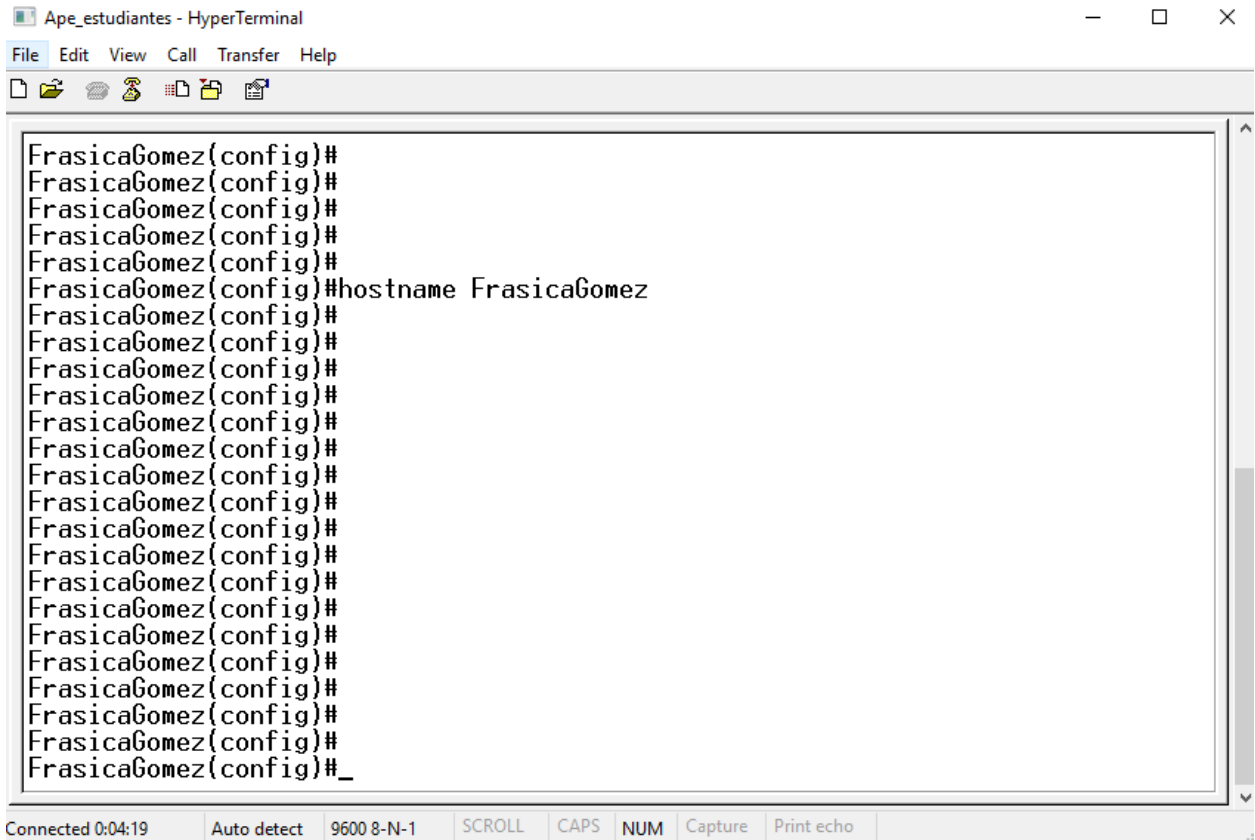
- Realice la configuración física que se presenta en el diagrama
- Verifique si la configuración de red se mantuvo o no.
- De no mantenerse las direcciones IP que estaban configuradas, entre a la configuración de la tarjeta de red y en IPv4 configure manualmente la tarjeta

Verifique conectividad entre los computadores usando el comando ping.

2. Configuración básica del switch:

Los switches tienen un sistema operativo el cual está especializado en las labores de switching. El sistema operativo de los switches Catalyst, IOS, tienen una estructura de operación por capas, las cuales están basadas en los privilegios y las actividades de configuración que se deseen realizar en los mismos. Realice la siguiente configuración:

- Nombre del switch: Ape_estudiantes



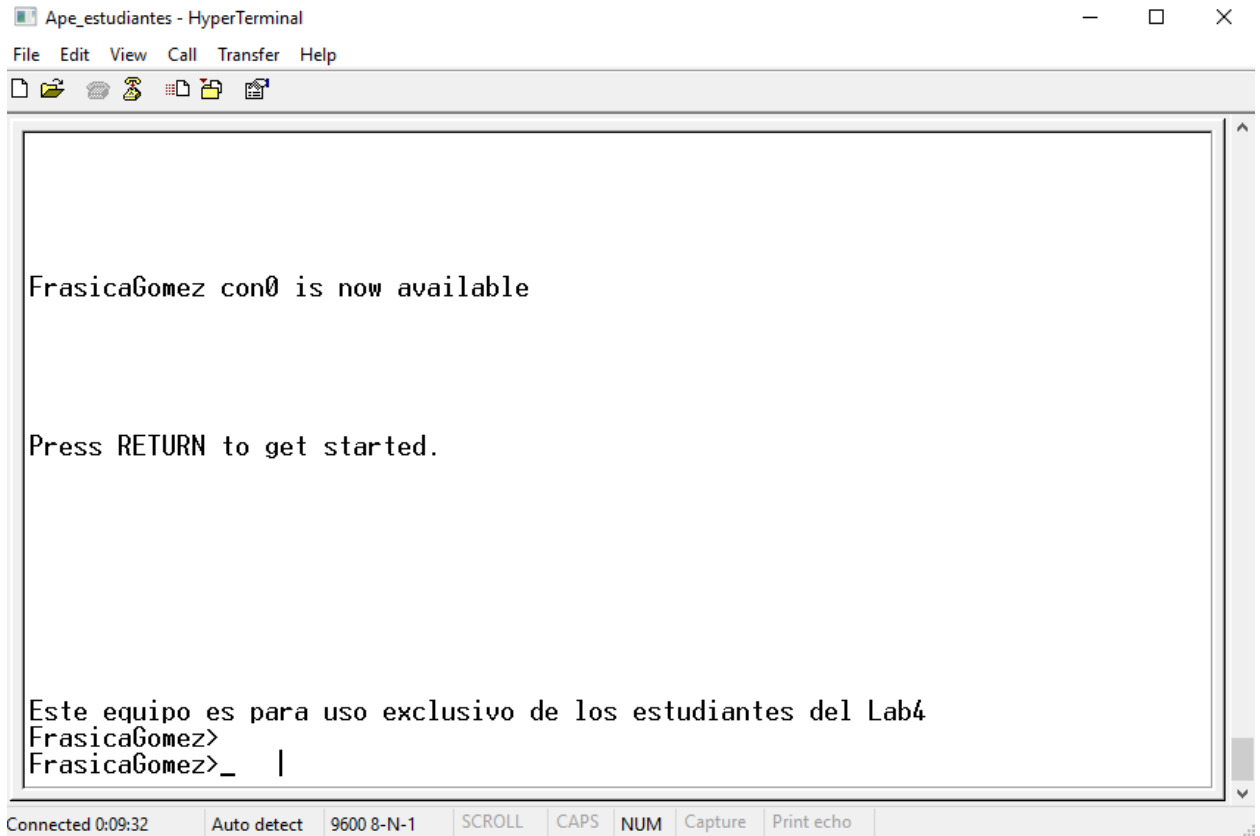
```
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#hostname FrasicaGomez
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#
FrasicaGomez(config)#_
```

Connected 0:04:19 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

El nombre del switch se configura con el comando: **hostname** *NombreDelSwitch*

- Mensaje del día: Este equipo es para uso exclusivo de los estudiantes del Lab4

El mensaje del día se configura mediante el comando **banner motd** "Este equipo es para uso exclusivo de los estudiantes del Lab4"



Como se puede ver en la imagen anterior, cuando se vuelve a iniciar el switch ahora sale con el mensaje del día configurado.

- Sincronización de pantalla.

```
switchFonso - HyperTerminal
File Edit View Call Transfer Help
[Icons]

privilege          Change privilege level for line
refuse-message     Define a refuse banner
rotary             Add line to a rotary group
rxspeed            Set the receive speed
session-timeout    Set interval for closing connection when there is no
                   input traffic
special-character-bits Size of the escape (and other special) characters
speed              Set the transmit and receive speeds
start-character    Define the start character
stop-character     Define the stop character
stopbits           Set async line stop bits
terminal-type      Set the terminal type
timeout            Timeouts for the line
transport           Define transport protocols for line
txspeed            Set the transmit speeds
vacant-message     Define a vacant banner
width              Set width of the display terminal

AlfonsoCastellanos(config-line)#logging ?
    synchronous    Synchronized message output

AlfonsoCastellanos(config-line)#logging synch
AlfonsoCastellanos(config-line)#logging synchronous
AlfonsoCastellanos(config-line)#_

Connected 0:24:59  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

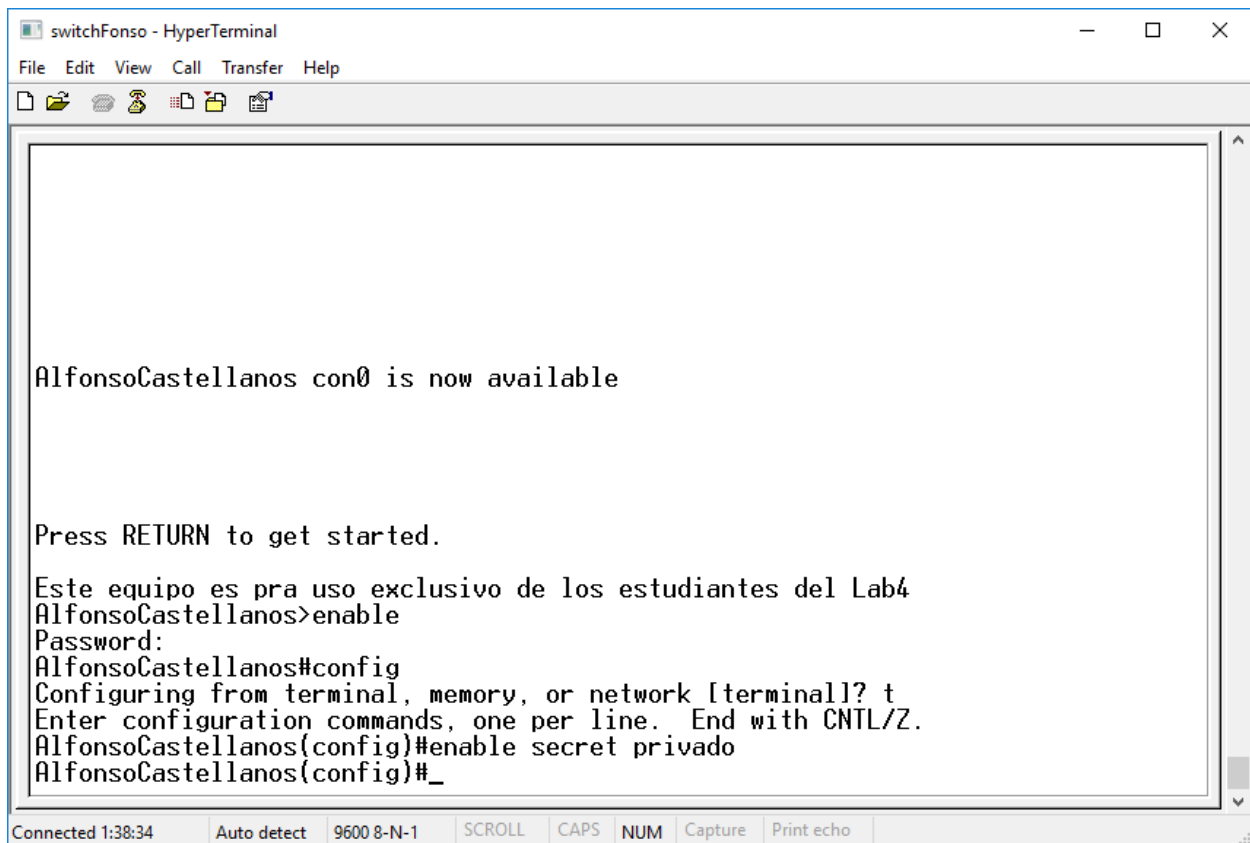
- Descripción de interfaces utilizadas. Ej. Conexión a computador Sistemas1XX

```
FrasicaGomez(config)#in
FrasicaGomez(config)#interface fa
FrasicaGomez(config)#interface fastEthernet 0/1
FrasicaGomez(config-if)#de
FrasicaGomez(config-if)#des
FrasicaGomez(config-if)#description "Conexion a computador Sistemas101"
FrasicaGomez(config-if)#_

Connected 0:33:50  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

```
!
!
interface FastEthernet0/1
  description "Conexion a computador Sistemas101"
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
```

- Claves de acceso al equipo.
 - Modo privilegiado: privado



```
switchFonso - HyperTerminal
File Edit View Call Transfer Help

AlfonsoCastellanos con0 is now available

Press RETURN to get started.

Este equipo es pra uso exclusivo de los estudiantes del Lab4
AlfonsoCastellanos>enable
Password:
AlfonsoCastellanos#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
AlfonsoCastellanos(config)#enable secret privado
AlfonsoCastellanos(config)#_

Connected 1:38:34 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

- Clave de consola: ClaveC

```
FrasicaGomez#config t
Enter configuration commands, one per line. End with CNTL/Z.
FrasicaGomez(config)#line console 0
FrasicaGomez(config-line)#passwor
FrasicaGomez(config-line)#password ClaveC_
```

- Clave de terminal remota: ClaveT



Press RETURN to get started.

Este equipo es para uso exclusivo de los estudiantes del Lab4

User Access Verification

Password:

Password:

FrasicaGomez>_

Connected 0:41:34

Auto detect

9600 8-N-1

SCROLL

CAPS

NUM

Capture

Print echo



Press RETURN to get started.

Este equipo es para uso exclusivo de los estudiantes del Lab4

User Access Verification

Password:

Password:

FrasicaGomez>enable

Password:

FrasicaGomez#config t

Enter configuration commands, one per line. End with CNTL/Z.

FrasicaGomez(config)#line vty 0 15

FrasicaGomez(config-line)#password ClaveT_

Connected 0:52:06

Auto detect

9600 8-N-1

SCROLL

CAPS

NUM

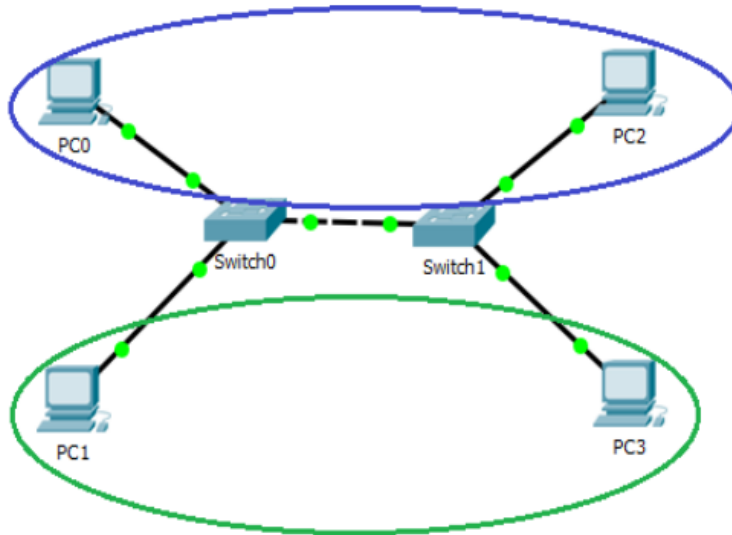
Capture

Print echo

3. Configuración de VLAN:

Configure dos VLAN como se presenta en el dibujo. Los computadores que pertenecen a la VLAN azul

y a la Verde deben ser los físicamente opuesto en la isla del Laboratorio en la que están sentados.



- Ingrese al modo configuración
- Configure dos VLANs1
Abierta: VLAN_ID 30 (marco circular azul)
Produccion: VLAN_ID 40 (marco circular verde)

Agregar una VLAN

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	SI# configure terminal
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	SI (config)# vlan <i>vlan id</i>
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	SI (config-vlan)# name <i>Nombre de VLAN</i>
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	SI (config-vlan)# end

Para verificar:

Switch# **show vlan brief**

Asignar un puerto de switch

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	SI# configure terminal
Ingresar la interfaz para asignar la VLAN.	SI (config)# interface <i>interface id</i>
Definir el modo de asociación de VLAN para el puerto.	SI (config-if)# switchport mode access
Asignar el puerto a una VLAN.	SI (config-if)# switchport access vlan <i>vlan id</i>
Volver al modo EXEC privilegiado.	SI (config-if)# end

```
switchFonso - HyperTerminal
File Edit View Call Transfer Help
[Icons]

AlfonsoCastellanos(config)#vlan ?
WORD      ISL VLAN IDs 1-4094
internal  internal VLAN

AlfonsoCastellanos(config)#vlan 30
AlfonsoCastellanos(config-vlan)#name Abierta
AlfonsoCastellanos(config-vlan)#end
AlfonsoCastellanos#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
                                           Gi0/1, Gi0/2

30   Abierta                  active
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
AlfonsoCastellanos#_

Connected 0:42:59   Auto detect   9600 8-N-1   SCROLL   CAPS   NUM   Capture   Print echo
```

Y se realizó el mismo procedimiento para configurar la VLAN 40 (Producción)

```
switchFonso - HyperTerminal
File Edit View Call Transfer Help
[Icons]

Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
AlfonsoCastellanos(config)#int fa 0/1
AlfonsoCastellanos(config-if)#switchport mode access
AlfonsoCastellanos(config-if)#switchport access vlan 30
AlfonsoCastellanos(config-if)#end
AlfonsoCastellanos#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, Gi0/1
                                           Gi0/2

30   Abierta                  active    Fa0/1
40   Produccion              active
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
AlfonsoCastellanos#show _

Connected 1:01:21   Auto detect   9600 8-N-1   SCROLL   CAPS   NUM   Capture   Print echo
```

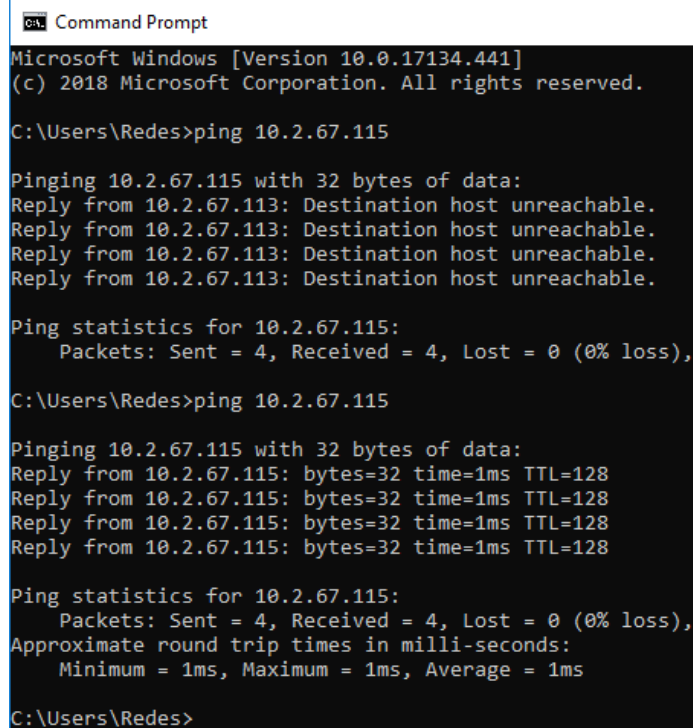
- c. Configure los computadores PC1, PC3 en la VLAN Produccion, los computadores PC2 y PC4 en la VLAN Abierta.

```
FrasticaGomez(config-if)#swi
FrasticaGomez(config-if)#switchport mode
FrasticaGomez(config-if)#switchport mode acc
FrasticaGomez(config-if)#switchport mode access
FrasticaGomez(config-if)#switchport acc
FrasticaGomez(config-if)#switchport access vlan 30
FrasticaGomez(config-if)#exit
FrasticaGomez(config)#int fa0/3
FrasticaGomez(config-if)#switchport mode access
FrasticaGomez(config-if)#switchport access vlan 40
FrasticaGomez(config-if)#_
```

- d. Configure en enlace entre los switches para que permita la conexión de VLANs (Pista: ¿Qué son los enlaces troncales?, ¿para qué se usan?)

```
FrasticaGomez(config)#int Gig0/1
FrasticaGomez(config-if)#swit
FrasticaGomez(config-if)#switchport mode
FrasticaGomez(config-if)#switchport mode trunk
```

- e. Verifique conectividad.



Command Prompt

Microsoft Windows [Version 10.0.17134.441]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Redes>ping 10.2.67.115

Pinging 10.2.67.115 with 32 bytes of data:
Reply from 10.2.67.113: Destination host unreachable.
Reply from 10.2.67.113: Destination host unreachable.
Reply from 10.2.67.113: Destination host unreachable.
Reply from 10.2.67.113: Destination host unreachable.

Ping statistics for 10.2.67.115:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Redes>ping 10.2.67.115

Pinging 10.2.67.115 with 32 bytes of data:
Reply from 10.2.67.115: bytes=32 time=1ms TTL=128
Reply from 10.2.67.115: bytes=32 time=1ms TTL=128
Reply from 10.2.67.115: bytes=32 time=1ms TTL=128
Reply from 10.2.67.115: bytes=32 time=1ms TTL=128

Ping statistics for 10.2.67.115:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Redes>

- f. Muestre al profesor su trabajo.

4. Revisión de frames:

Haciendo uso de wireshark revise el encabezado del frame Ethernet. Para eso haga uso del comando ping.

Se utilizaron los siguientes computadores para realizar el ping:

Dirección MAC del source:

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : A0-D3-C1-0F-73-21
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::fc52:395d:8062:92e0%11(Preferred)
IPv4 Address. . . . . : 10.2.67.116(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.2.65.1
DHCPv6 IAID . . . . . : 60871617
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-C5-FF-A0-D3-C1-0F-73-21
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

Dirección MAC del destination:

```
Select Command Prompt

IPv4 Address. . . . . : 192.168.56.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
DHCPv6 IAID . . . . . : 436863015
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-B7-1E-A0-D3-C1-0F-70-FD
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) Ethernet Connection I217-LM
Physical Address. . . . . : A0-D3-C1-0F-70-FD
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::656e:ff69:70af:5f8f%11(Preferred)
IPv4 Address. . . . . : 10.2.67.114(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.2.65.1
DHCPv6 IAID . . . . . : 60871617
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-A9-B7-1E-A0-D3-C1-0F-70-FD
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                       : fec0:0:0:ffff::2%1
                       : fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:
```

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.2.67.116	10.2.67.114	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 2)
2	0.000078	10.2.67.114	10.2.67.116	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=128 (request in 1)
3	0.738809	Cisco_09:f6:03	Spanning-tree-(for--	STP	60	Conf. Root = 32768/40/fc:fb:09:f6:00 Cost = 0 Port = 0x8003
4	1.016008	10.2.67.116	10.2.67.114	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 5)
5	1.016155	10.2.67.114	10.2.67.116	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=128 (request in 4)
6	2.031441	10.2.67.116	10.2.67.114	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 7)
7	2.031602	10.2.67.114	10.2.67.116	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128 (request in 6)
8	2.744037	Cisco_09:f6:03	Spanning-tree-(for--	STP	60	Conf. Root = 32768/40/fc:fb:09:f6:00 Cost = 0 Port = 0x8003
9	2.844613	Cisco_09:f6:03	Cisco_09:f6:03	LOOP	60	Reply
10	3.047037	10.2.67.116	10.2.67.114	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 11)
11	3.047171	10.2.67.114	10.2.67.116	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=128 (request in 10)
12	4.748912	Cisco_09:f6:03	Spanning-tree-(for--	STP	60	Conf. Root = 32768/40/fc:fb:09:f6:00 Cost = 0 Port = 0x8003

Wireshark · Packet 4 · Ethernet

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

▼ Ethernet II, Src: HewlettP_0f:73:21 (a0:d3:c1:0f:73:21), Dst: HewlettP_0f:70:fd (a0:d3:c1:0f:70:fd)

> Destination: HewlettP_0f:70:fd (a0:d3:c1:0f:70:fd)

> Source: HewlettP_0f:73:21 (a0:d3:c1:0f:73:21)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.2.67.116, Dst: 10.2.67.114

> Internet Control Message Protocol

0000	a0 d3 c1 0f 70 fd a0 d3 c1 0f 73 21 08 00 45 00p... ..s!...E.
0010	00 3c 6a 6b 00 00 80 01 35 6c 0a 02 43 74 0a 02	..<jk... ..5l..Ct..
0020	43 72 08 00 4d 44 00 01 00 17 61 62 63 64 65 66	Cr..MD... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
0040	77 61 62 63 64 65 66 67 68 69	wabdefg hi

Como se puede observar, se realizó correctamente el ping entre los dos computadores.

5. Cierre

Borre y organice el switch y los equipos utilizados en el punto anterior de tal manera que queden listos para ser usados en una nueva práctica.

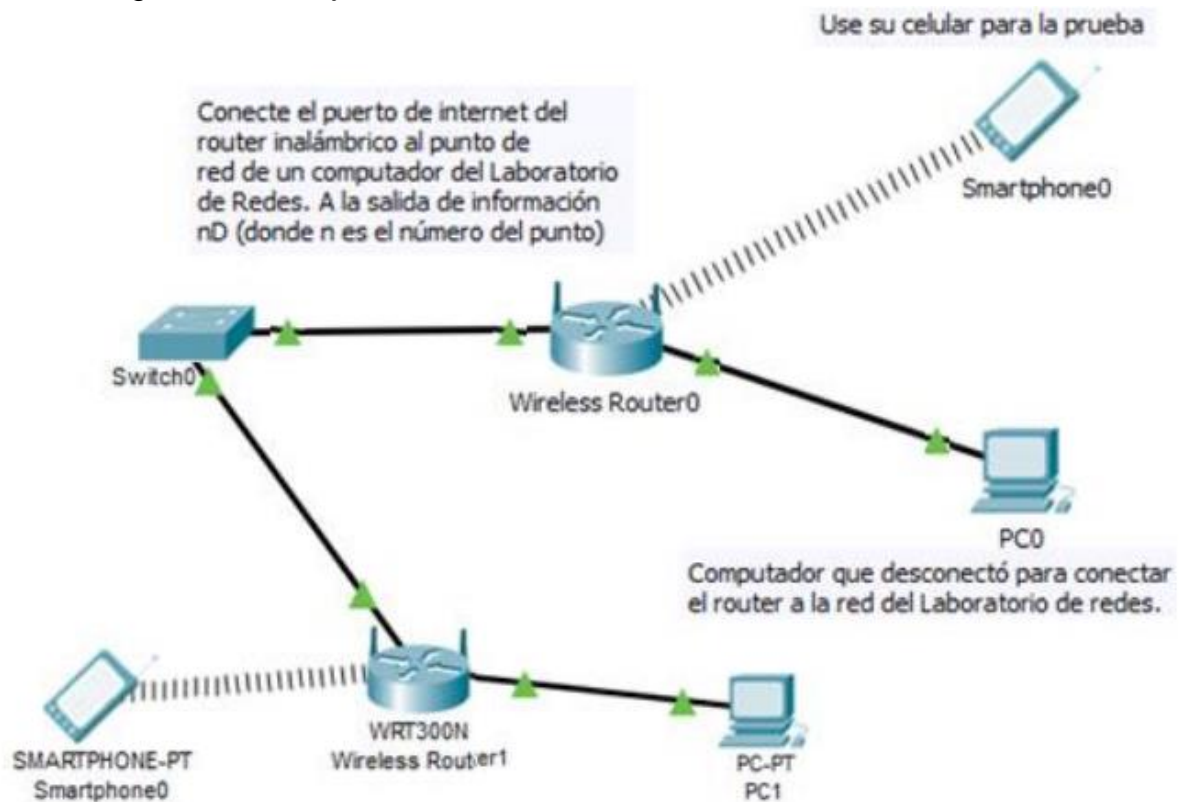
OJO: En los switches no es suficiente con borrar el archivo de configuración general. ¿Cómo se borra una VLAN de forma definitiva de un Switch? ¿Por qué?

La VLAN se borra con el comando **no vlan NombreVLAN**

Y para borrar la configuración del switch se utiliza el comando **erase startup-config**

Montaje N°2:

Realice el siguiente montaje:



1. Configuración router inalámbrico:

Por parejas conéctese a los routers inalámbricos desde los computadores que desconectaron. Desde allí se configurará cada router.

Utilice la configuración IP del computador que desconectó para enchufar cada router inalámbrico por el puerto de internet para configurar la salida hacia internet y configure la red inalámbrica como se indica a continuación:

- Identificador de la red inalámbrica - SSID: Lab4_ape (donde ape es el apellido de uno de los estudiantes del grupo)
- IP de la red inalámbrica: 192.168.0.0/24
- Dirección IP del router inalámbrico hacia la inalámbrica: 192.168.0.1
- Rango de direcciones IP a asignar a dispositivos móviles (DHCP): 192.168.0.1 a 192.168.0.10.
- Mecanismos de acceso a los clientes inalámbricos: WPA2-PSK con AES

- Clave de acceso al router desde los dispositivos móviles: Lab4pwd
- ¿Qué opción de canales puede configurar en cada router inalámbrico?

DIR-300

Internet Setup

Wireless Setup

LAN Setup

Time and Date

Parental Control

Logout

Internet Offline

Reboot

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

WIRELESS CONNECTION

There are 2 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection.

Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Wireless Router to the Internet, click on the button below.

Wireless Connection Setup Wizard

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL WIRELESS CONNECTION OPTIONS

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

Manual Wireless Connection Setup

Helpful Hints..

- If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Connection Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.
- If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Connection Setup** to input all the settings manually.

Internet Offline
Reboot

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : **07477836**

Generate New PIN Reset PIN to Default

Wi-Fi Protected Status : Enabled / Configured

Reset to Unconfigured

Add Wireless Device with WPS

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : (Also called the SSID)

Wireless Channel :

Enable Auto Channel Selection : ☐

Transmission Rate : (Mbit/s)

WMM Enable : ☐ (Wireless Qos)

Enable Hidden Wireless : ☐ (Also called the SSID Broadcast)

WIRELESS SECURITY MODE

Security Mode :

WPA2 ONLY

WPA2 Only requires stations to use high grade encryption and authentication.

Cipher Type :

PSK / EAP :

Network Key : (8~63 ASCII or 64 HEX)

Save Settings Don't Save Settings

driver in order to take advantage of this feature.

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.
- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

Tuvimos que colocar la clave "Lab4pwd1" porque la configuración requería una contraseña de al menos 8 caracteres.

Parental Control
Logout
 Internet Offline
Reboot

Save Settings
192.168.0.1 says
The length of Passphrase should be 8~63.
OK

WI-FI PROTECTED SETUP

Generate New PIN Reset PIN to Default


Wi-Fi Protected Status : Enabled / Configured

Reset to Unconfigured

wireless card supports such feature or uses a certified Windows Vista driver in order to take advantage of this feature.

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.

	<h2 style="text-align: center;">WIRELESS SECURITY MODE</h2> <p style="text-align: center;">Security Mode : Enable WPA2 Only Wireless Security (enhanced) ▼</p> <hr/> <h3 style="text-align: center;">WPA2 ONLY</h3> <p>WPA2 Only requires stations to use high grade encryption and authentication.</p> <p style="text-align: center;">Cipher Type : AES ▼</p> <p style="text-align: center;">PSK / EAP : PSK ▼</p> <p style="text-align: center;">Network Key : Lab4pwd1 (8~63 ASCII or 64 HEX)</p> <p style="text-align: center;"> Save Settings Don't Save Settings </p>	<ul style="list-style-type: none"> If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.
--	---	---

<ul style="list-style-type: none"> Internet Setup Wireless Setup LAN Setup Time and Date Parental Control Logout <div style="text-align: center;">  <p>Internet Online</p> <p>Reboot</p> </div>	<h2 style="text-align: center;">INTERNET CONNECTION</h2> <p>Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider.</p> <p>Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.</p> <p style="text-align: center;"> Save Settings Don't Save Settings </p> <hr/> <h3 style="text-align: center;">ACCESS POINT MODE</h3> <p>Use this to disable NAT on the router and turn it into an Access Point.</p> <p><input type="checkbox"/> Enable Access Point Mode</p> <hr/> <h3 style="text-align: center;">INTERNET CONNECTION TYPE</h3> <p>Choose the mode to be used by the router to connect to the Internet.</p> <p>My Internet Connection is : Static IP ▼</p> <hr/> <h3 style="text-align: center;">STATIC IP ADDRESS INTERNET CONNECTION TYPE</h3> <p>Enter the static address information provided by your Internet Service Provider (ISP).</p> <p>IP Address : 10.2.67.104 (assigned by your ISP)</p> <p>Subnet Mask : 255.255.0.0</p> <p>ISP Gateway Address : 10.2.65.1</p> <p>MAC Address : - - - - - (optional) Clone MAC Address</p> <p>Primary DNS Address : 10.2.65.60</p> <p>Secondary DNS Address : (optional)</p> <p>MTU : 1500</p>	<p>Helpful Hints...</p> <ul style="list-style-type: none"> Internet Connection: When configuring the router to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, please contact your Internet Service Provider (ISP). Support: If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.
---	--	---



Internet
Online

Reboot

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : **07477836**

Generate New PIN

Reset PIN to Default

Wi-Fi Protected Status : Enabled / Configured

Reset to Unconfigured

Add Wireless Device with WPS

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : (Also called the SSID)

Wireless Channel : ▼

Enable Auto Channel Selection : ☐

Transmission Rate : ▼ (Mbit/s)

WMM Enable : ☐ (Wireless Qos)

Enable Hidden Wireless : ☐ (Also called the SSID Broadcast)

WIRELESS SECURITY MODE

Security Mode : ▼

WPA2 ONLY

WPA2 Only requires stations to use high grade encryption and authentication.

Cipher Type : ▼

PSK / EAP : ▼

Network Key : (8~63 ASCII or 64 HEX)

Save Settings

Don't Save Settings

advantage of this feature.

- Changing your Wireless Network Name is the first step in securing your wireless network. We recommend that you change it to a familiar name that does not contain any personal information.


- Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

- If you have enabled Wireless Security, make sure you write down WEP Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

WIRELESS

Parental Control

Logout

 Internet Online

Reboot

Network Setup

Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.

Save Settings

Don't Save Settings

ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

192.168.0.1

Default Subnet Mask :

255.255.255.0

Local Domain Name :

Enable DNS Relay :

☒

DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server :

☒

DHCP IP Address Range :

2

to

10

(addresses within the LAN subnet)

DHCP Lease Time :

10080

(minutes)

DHCP CLIENT LIST

Host Name	IP Address	MAC Address	Expired Time
android-2434268f4e0ee980	192.168.0.2	F4:8E:92:78:90:8C	6 day(s) 23 hr(s) 58 min(s) 47 sec(s)
Sebas	192.168.0.3	D4:DC:CD:AC:96:AC	6 day(s) 23 hr(s) 59 min(s) 7 sec(s)
	192.168.0.4	80:58:F8:5D:22:BB	6 day(s) 23 hr(s) 59 min(s) 23 sec(s)


10 - DHCP RESERVATION

Server to disable this feature.

Se hizo lo mismo con el segundo router:

← → ↻ ⓘ Not secure | 192.168.0.1/bsc_wlan.php ☆

LAN Setup
Time and Date
Parental Control
Logout

 Internet Online

Reboot

made on this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2.

Save Settings Don't Save Settings

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : **60979933**

Generate New PIN Reset PIN to Default

Wi-Fi Protected Status : Enabled / Configured

Reset to Unconfigured

Add Wireless Device with WPS

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Network Name : (Also called the SSID)

Enable Auto Channel Selection : ☐

Wireless Channel : ▼

Transmission Rate : ▼ (Mbit/s)

WMM Enable : ☐ (Wireless QoS)

Enable Hidden Wireless : ☐ (Also called the SSID Broadcast)

WIRELESS SECURITY MODE

Security Mode : ▼

WPA/WPA2

WPA/WPA2 requires stations to use high grade encryption and authentication.

Cipher Type : ▼

PSK / EAP : ▼

Network Key :

(8~63 ASCII or 64 HEX)

Save Settings Don't Save Settings

provides a more
way of setting
security between
router and the
client. Make su
wireless card su
such feature or
certified Windo
driver in order t
advantage of th

- Changing yo
Network Name
step in securin
wireless netwo
recommend tha
change it to a f
name that doe
contain any pe
information.

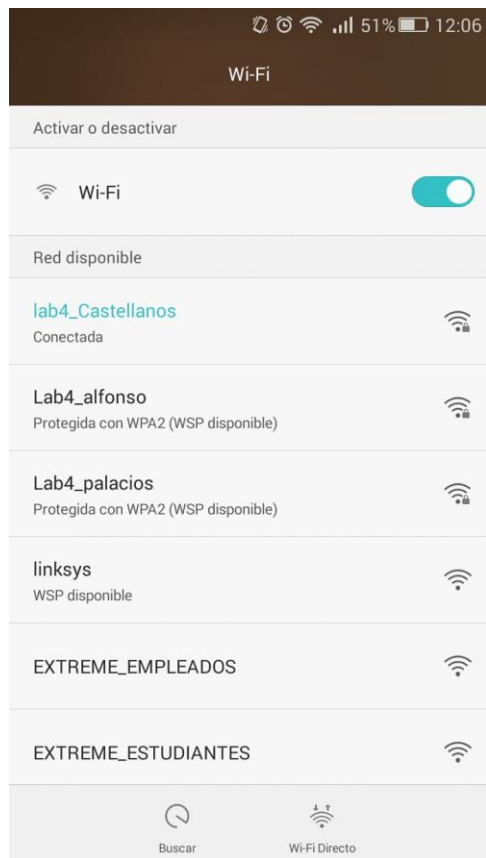
- Enabling Hid
is another way
your network. V
option enabled,
clients will be a
your wireless n
when they perf
see what's avai
order for your v
devices to conn
router, you will
manually enter
Wireless Netwo
each device.

- If you have
Wireless Securi
sure you write
Key or Passphr
have configure
need to enter t
information on
wireless device
connect to your
network.

2. Configuración Smartphone

Por cada pareja, use un celular (Smartphone) para la prueba o si no cuenta con uno, en la Tablet suministrada por el Laboratorio de Informática, realice lo siguiente:

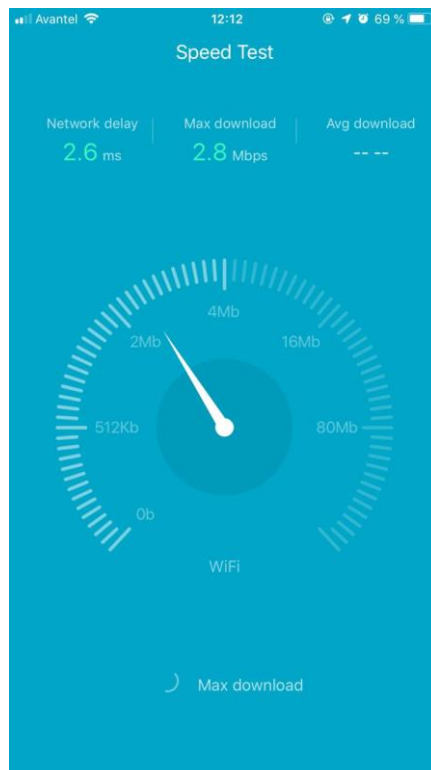
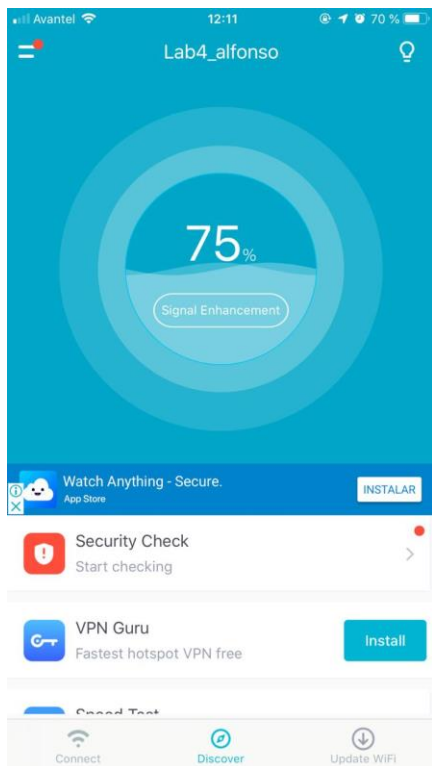
- Deshabilite su plan de datos y active la red WiFi.
- Conecte el celular al router inalámbrico que acaba de configurar
- Navegue por Internet desde el celular.





3. Revisión de canales

Monte en el celular una aplicación para revisar el tráfico inalámbrico, un ejemplo de estas aplicaciones es WiFi Analyzer para Android y descubra las redes inalámbricas en la zona del laboratorio de Redes, entre ellas, debería encontrar las redes de sus compañeros. También revise el canal por el que están transmitiendo. Muestre su configuración y montaje a su profesor



Simulaciones:

La documentación se realizó con la simulación del estudiante Juan Sebastián Frásica.

4. VLANs y Wireless LAN:

- Realice un montaje como el que se presenta en el dibujo.
- A todos los equipos alámbricos colóquele la siguiente configuración
 - IP: 10.0.0.x. donde x es un número diferente para cada equipo
 - Máscara: 255.0.0.0

Así se configuró la dirección IP y la máscara para todos los equipos alámbricos:

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address: 10.0.0.1

Subnet Mask: 255.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:C9FF:FEED:DECD

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

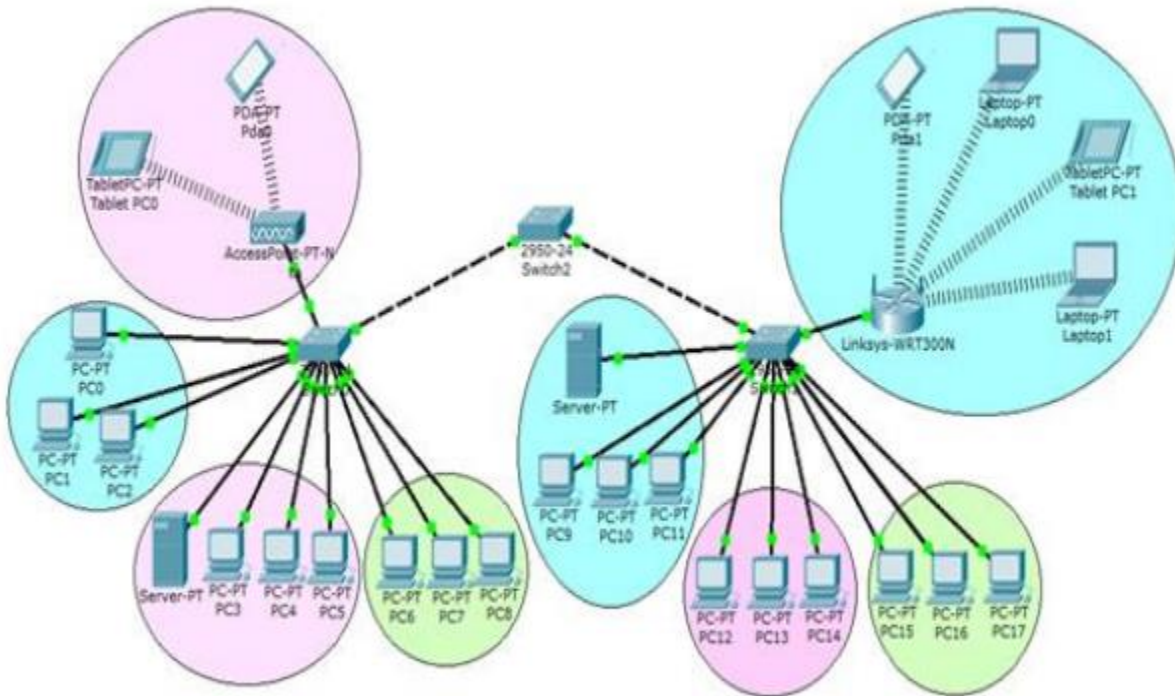
Username:

Password:

☐ Top

- En la VLAN azul una conexión WIFI con router inalámbricos para que se usen equipos inalámbricos como portátiles, tablets y smartphones dentro de la red y se consulte el servidor de esa misma red.

- En la VLAN rosada una conexión WIFI con un AccessPoint para que se usen tablets y smartphones dentro de la red y se consulte el servidor de esa misma red. La siguiente figura presenta un esquema de la red que se espera obtener



Para la configuración de la red inalámbrica tenga en cuenta lo siguiente:

- Red inalámbrica azul
 - Identificador de la red inalámbrica - SSID: W_Ventas

Physical Config **GUI** Attributes

Wireless-N Broadband Router

Firmware Version: WRT30

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings

Network Mode: Mixed

Network Name (SSID): W_Ventas

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

Help...

- Dirección IP del router inalámbrico hacia la inalámbrica: 172.18.0.1

Network Setup

Router IP

IP Address: 172 . 18 . 0 . 1

Subnet Mask: 255.255.255.0

- Rango de direcciones IP a asignar a dispositivos móviles: 172.18.0.20 a 172.18.0.30

DHCP Server Settings

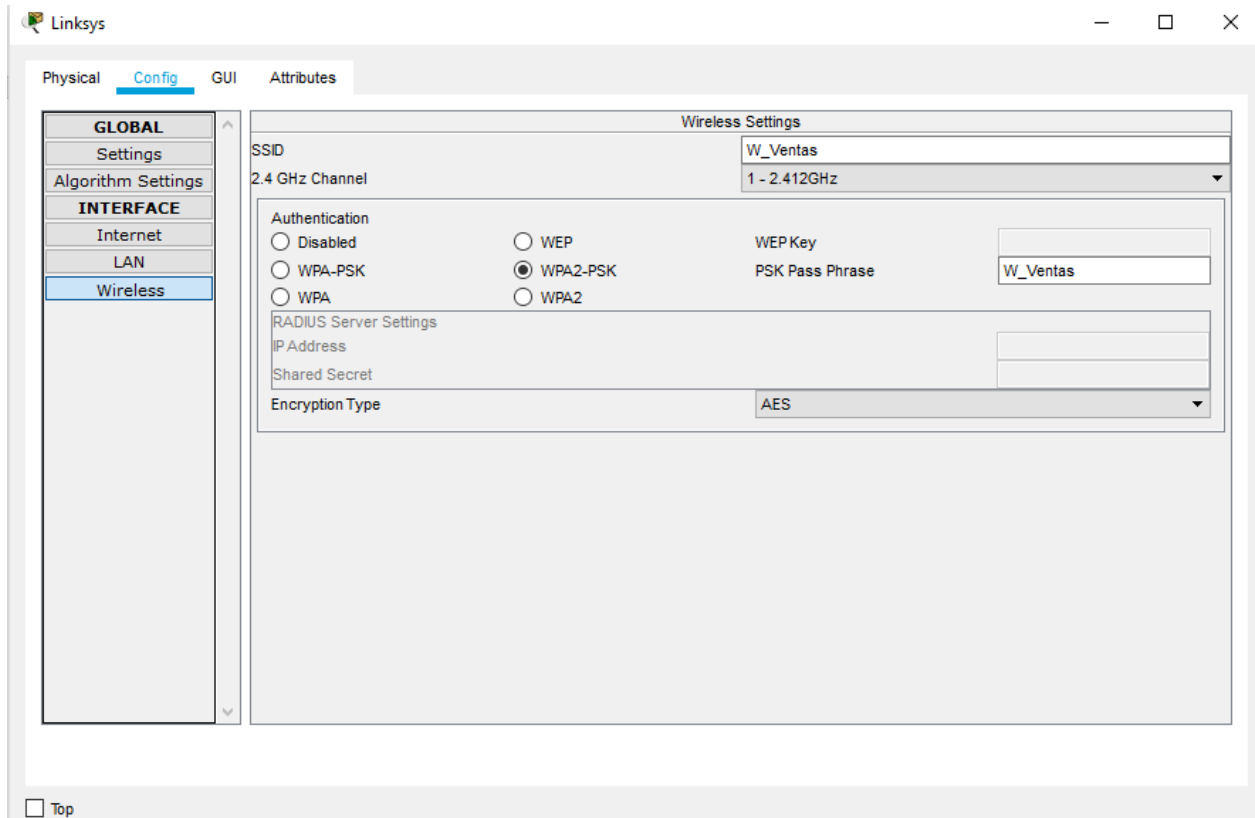
DHCP Server: ☒ Enabled ☐ Disabled

Start IP Address: 172.18.0. 20

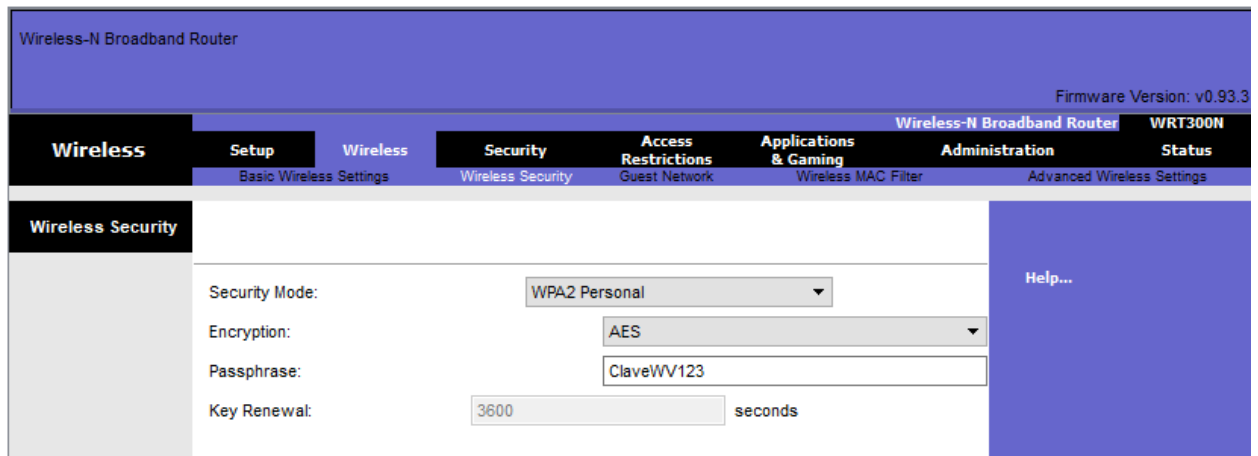
Maximum number of Users: 11

IP Address Range: 172.18.0. 20 - 30

- Mecanismos de acceso a los clientes inalámbricos: WPA2-PSK con AES



- Clave de acceso al router desde los dispositivos móviles: ClaveWV

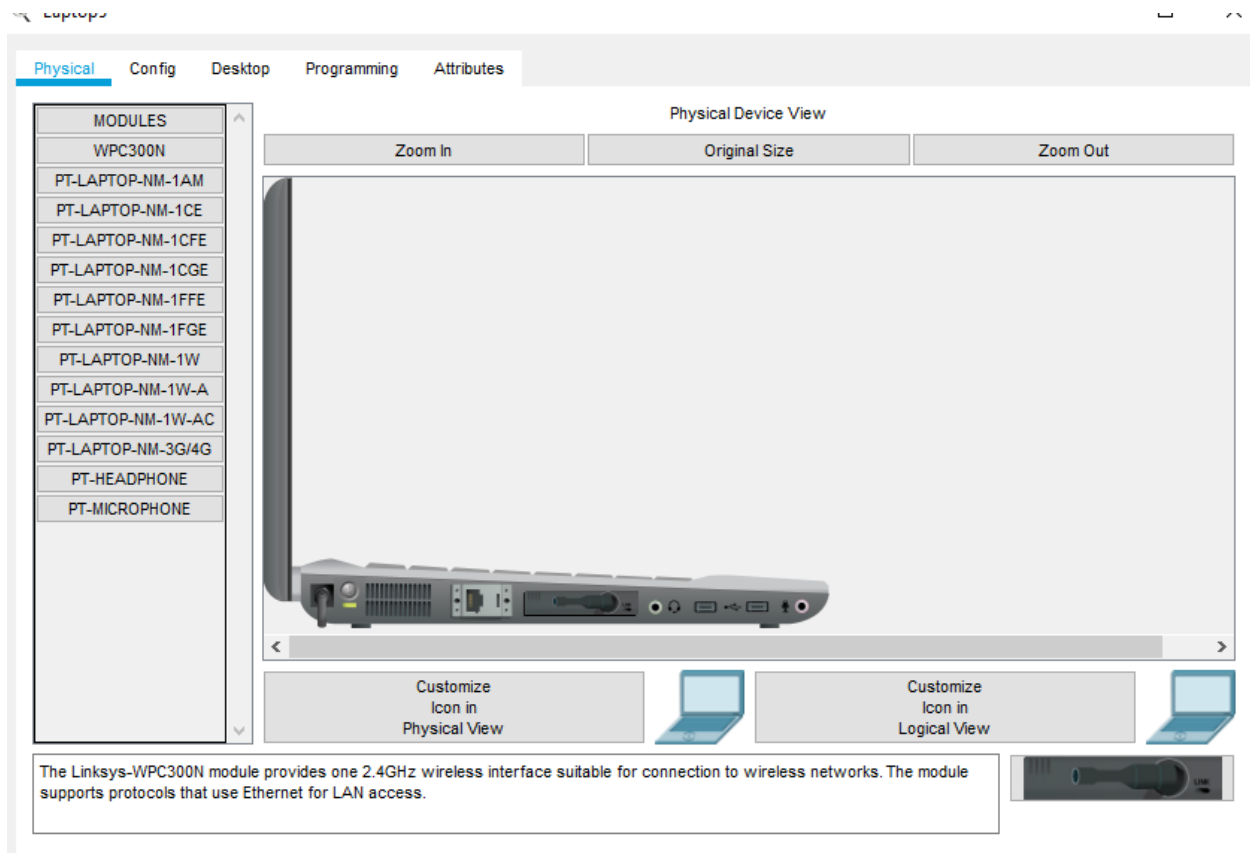


La clave tuvo que ser ClaveWV123 porque se requería una clave de mínimo 8 caracteres.

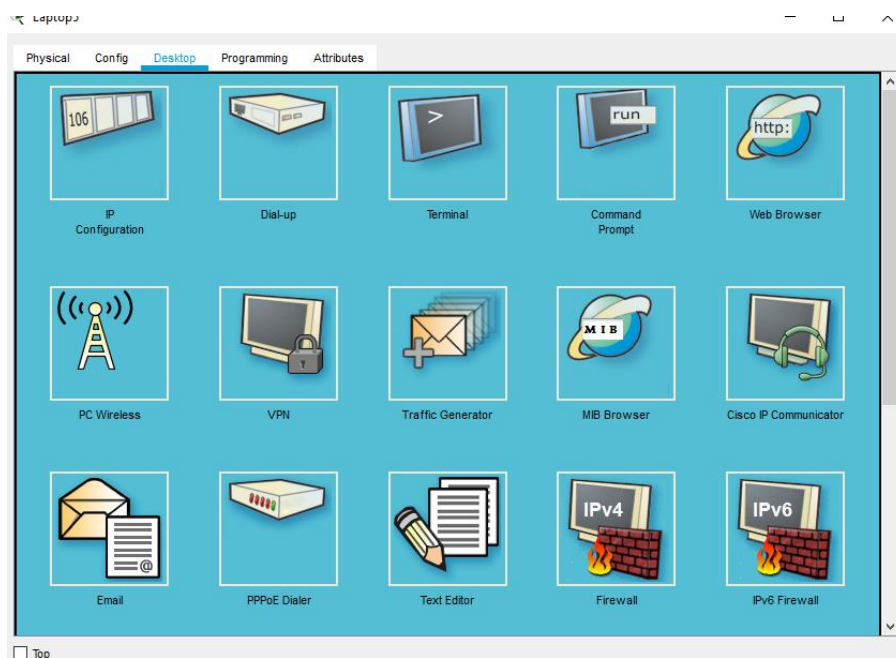
Luego de realizar la configuración del router inalámbrico, toca conectar los dispositivos con la respectiva contraseña.

Para conectar **el Laptop**:

Primero toca cambiar la NIC de Ethernet a una inalámbrica (WPC300N)



Toca ir a la sección “PC Wireless”

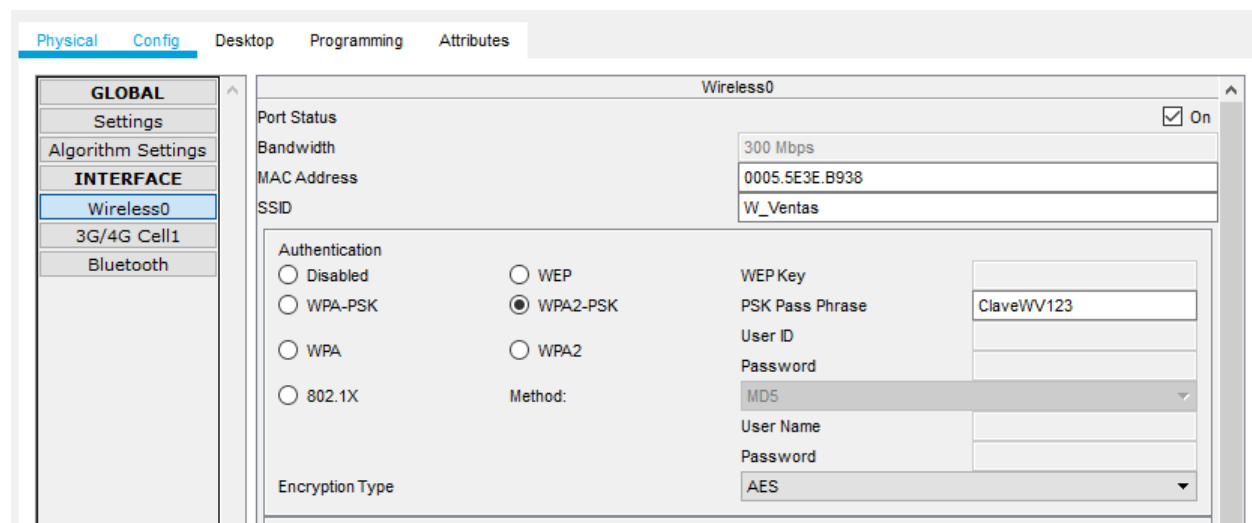




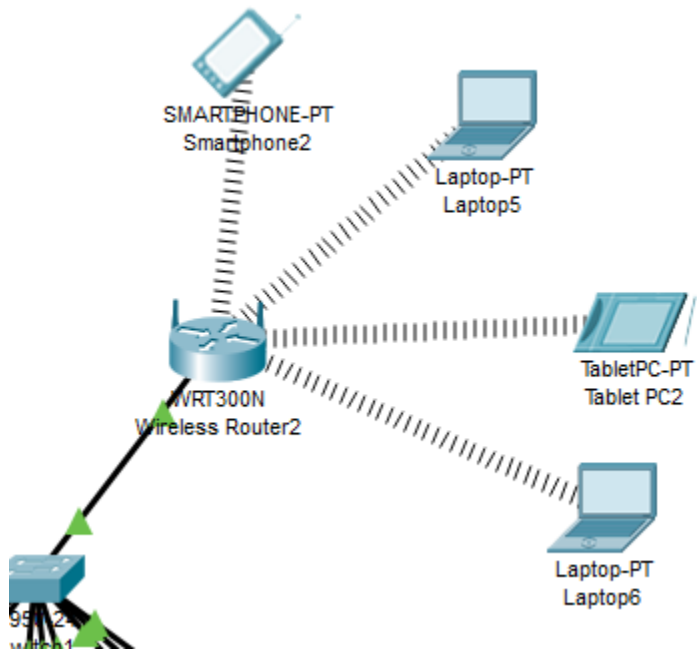
Se selecciona el SSID “W_Ventas” y se escribe la respectiva contraseña.

Para el Smartphone:

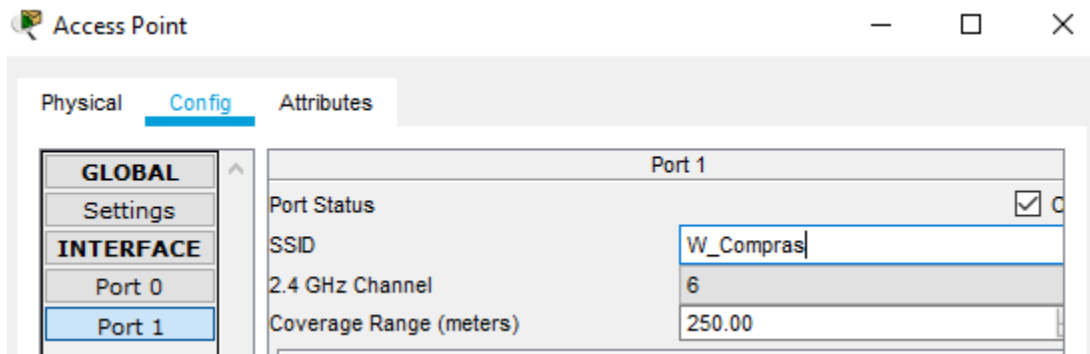
En la parte de SSID se coloca el SSID del router al que se quiere conectar. Se selecciona el tipo de autenticación (WPA2-PSK) y se coloca la clave del router en la parte de PSK Pass Phrase



Y finalmente se conecta la red azul inalámbrica



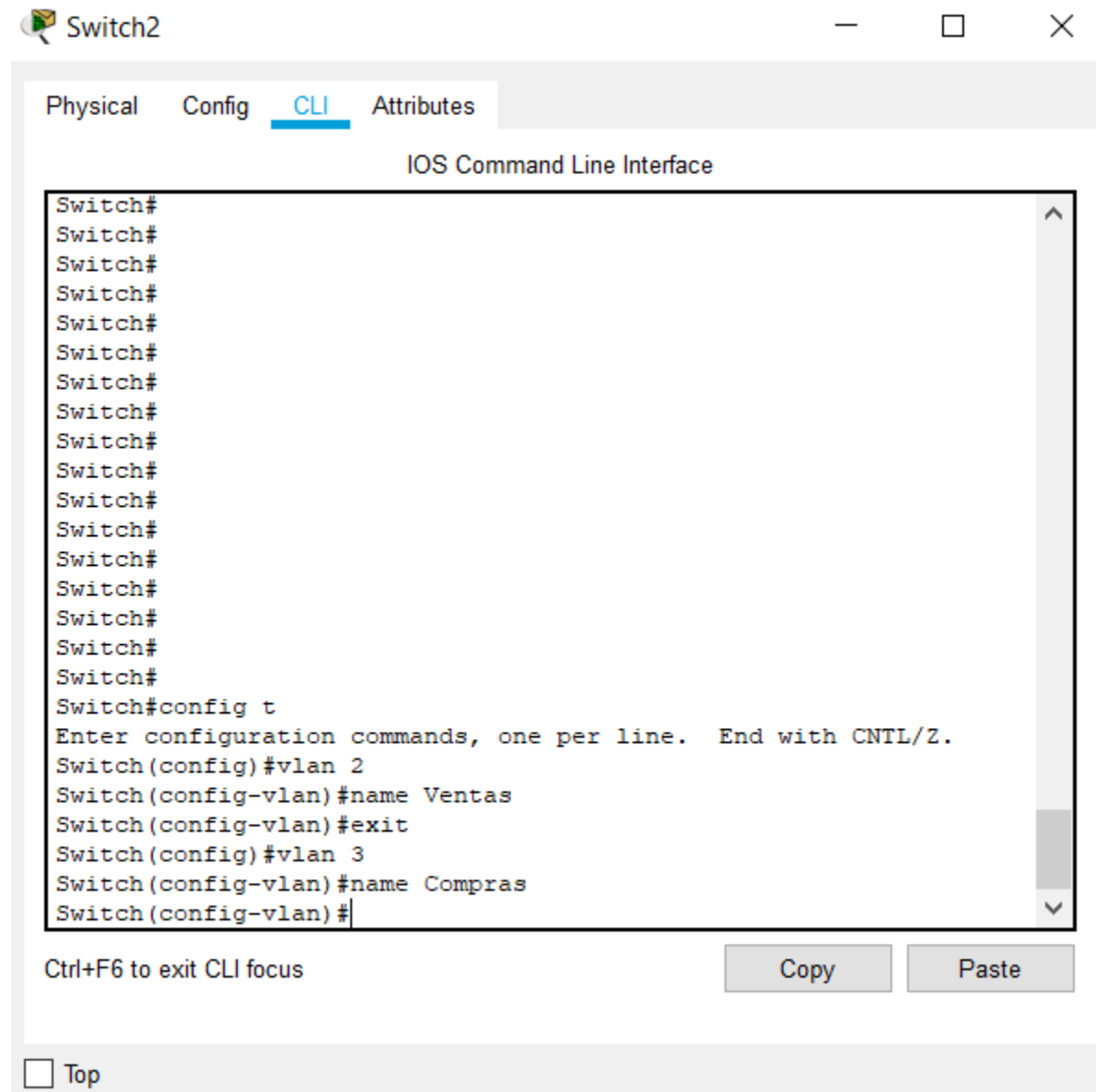
- Red inalámbrica rosa
 - Identificador de la red inalámbrica - SSID: W_Compras

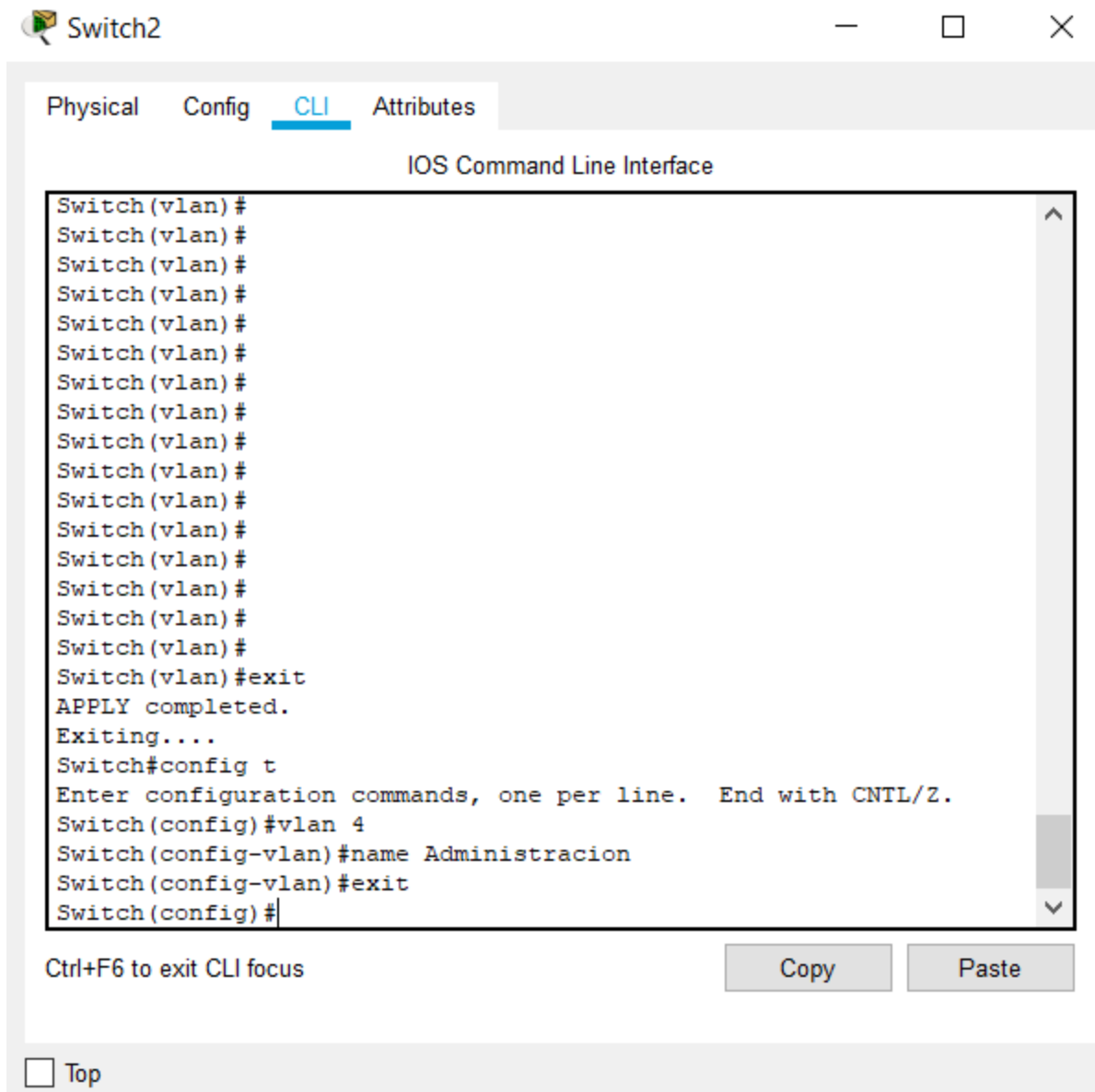


- Mecanismos de acceso a los clientes inalámbricos: WPA2-PSK con AES
- Clave de acceso al router desde los dispositivos móviles: ClaveWC

Mientras que la VLAN rosa será la VLAN #3 y será la VLAN de Compras.
Como la VLAN de color verde no fue asignada, decidimos colocarle #4 y nombrarla "Administración"

En los 3 switches tenemos que crear las VLAN's, vamos a la parte de CLI de cada switch. Primero tenemos que entrar en el modo de configuración global, y ejecutar los siguientes comandos:





Hacemos lo mismo con el switch 0 y con el switch 1:

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config-if)#  
Switch(config-if)#end  
Switch#vlan database  
% Warning: It is recommended to configure VLAN from config mode,  
as VLAN database mode is being deprecated. Please consult user  
documentation for configuring VTP/VLAN in config mode.  
  
Switch(vlan)#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Switch(vlan)#  
Switch(vlan)#exit  
APPLY completed.  
Exiting....  
Switch#  
Switch#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#vlan 2  
Switch(config-vlan)#name Ventas  
Switch(config-vlan)#exit  
Switch(config)#vlan 3  
Switch(config-vlan)#name Compras  
Switch(config-vlan)#exit  
Switch(config)#  
Switch(config)#|
```

Ctrl+F6 to exit CLI focus

Copy

Paste

☐ Top

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Compras
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#
Switch(config)#end
Switch#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

Switch(vlan)#
%SYS-5-CONFIG_I: Configured from console by console

Switch(vlan)#
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 4
Switch(config-vlan)#name Administracion
Switch(config-vlan)#exit
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy

Paste

☐ Top

Physical Config CLI Attributes

IOS Command Line Interface

Press RETURN to get started.

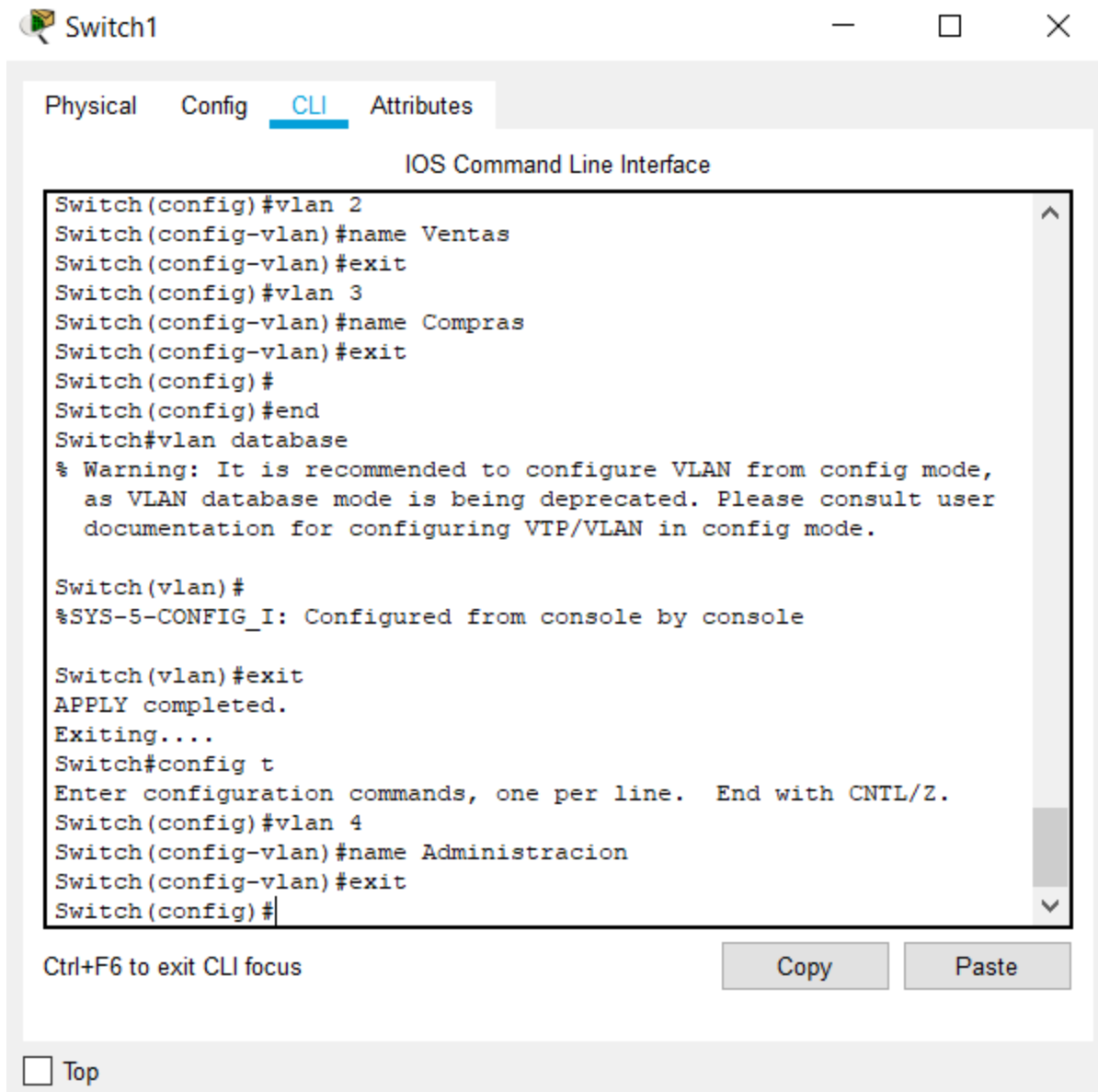
```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name Ventas
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name Compras
Switch(config-vlan)#exit
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy

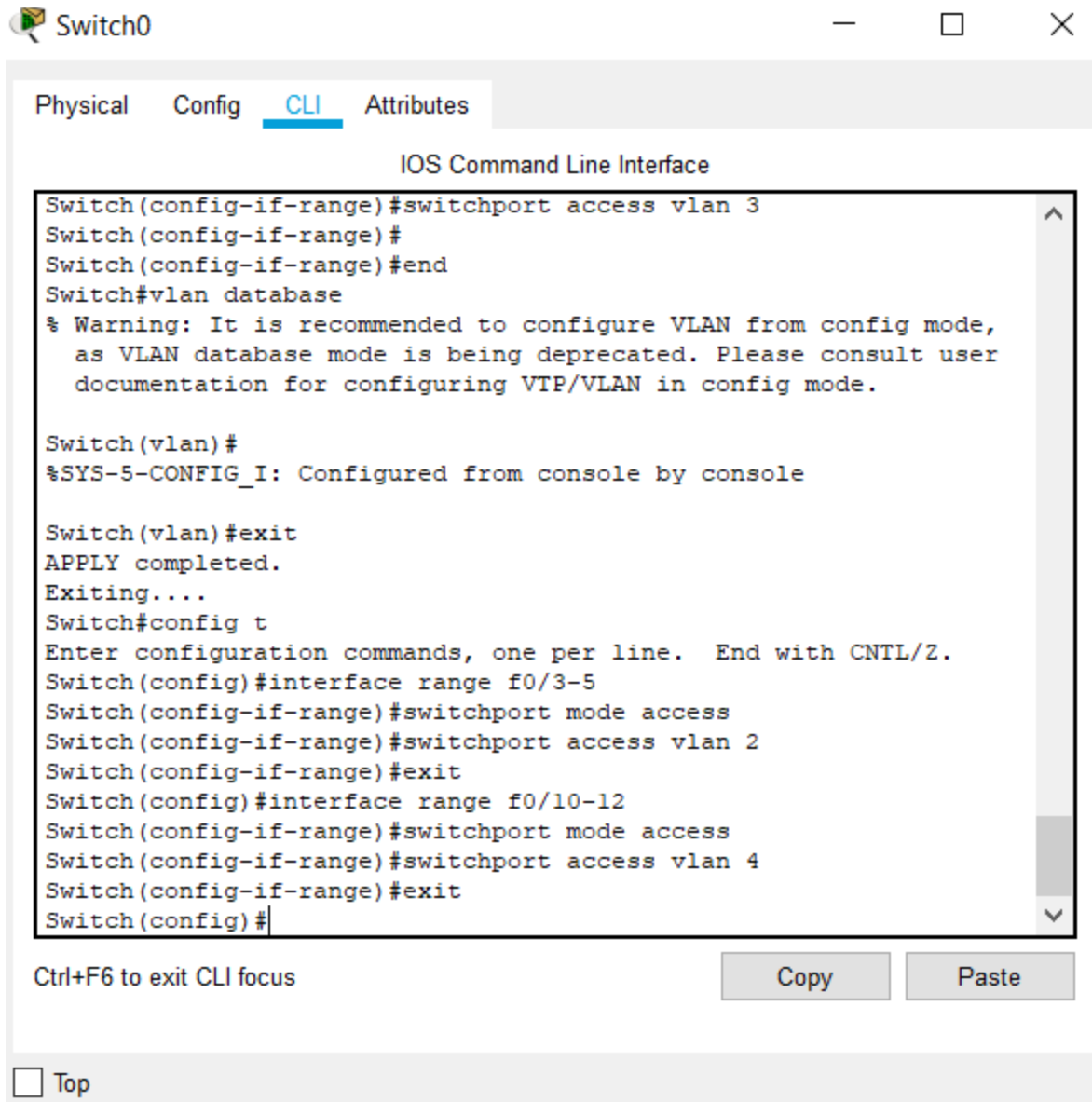
Paste

☐ Top



El siguiente paso es asignar cada puerto del switch a su respectiva VLAN, siguiendo el diagrama propuesto por la profesora.

Entonces, en el switch 0 tenemos los puertos 2 y del 6 al 9 para la VLAN rosa (Compras). Recordemos que esta VLAN es la # 3. Por lo que se ejecutan los siguientes comandos:

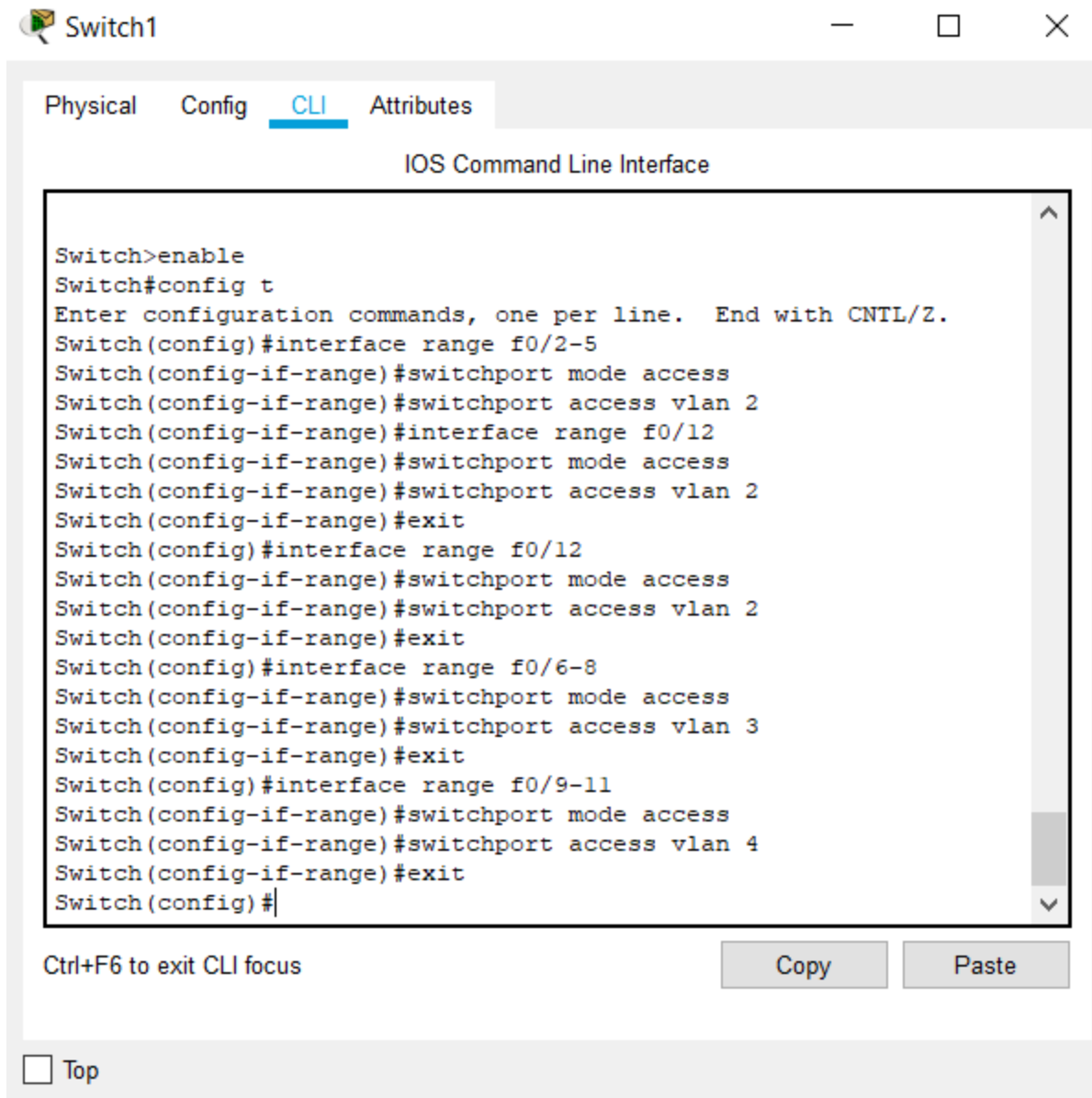


Lo mismo se realiza con el switch 1 para configurar los puertos con sus respectivas VLAN.

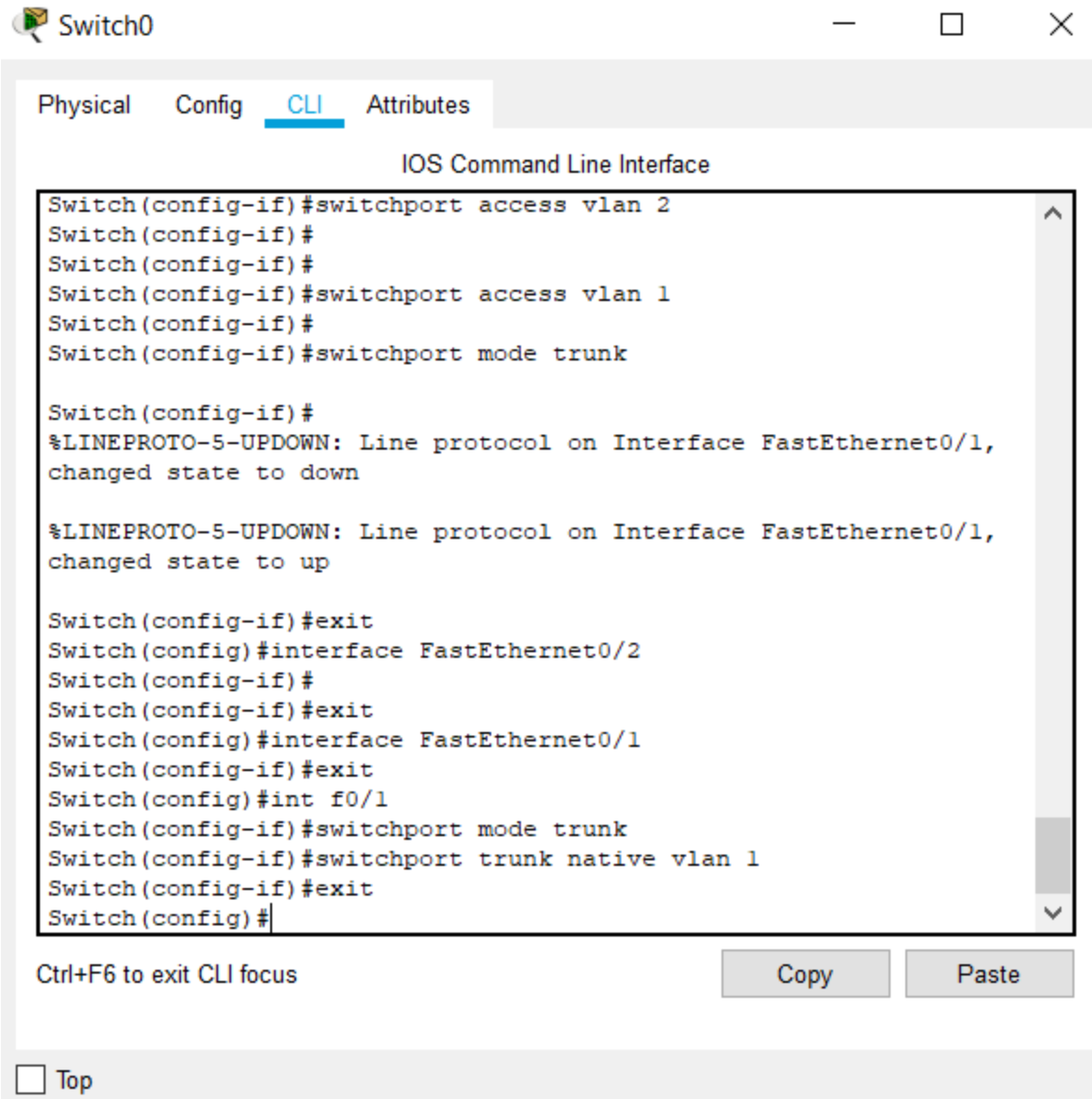
VLAN azul #2 (Ventas): Puertos 2 a 5 y puerto 12

VLAN rosa #3 (Compras): Puertos 6 a 8

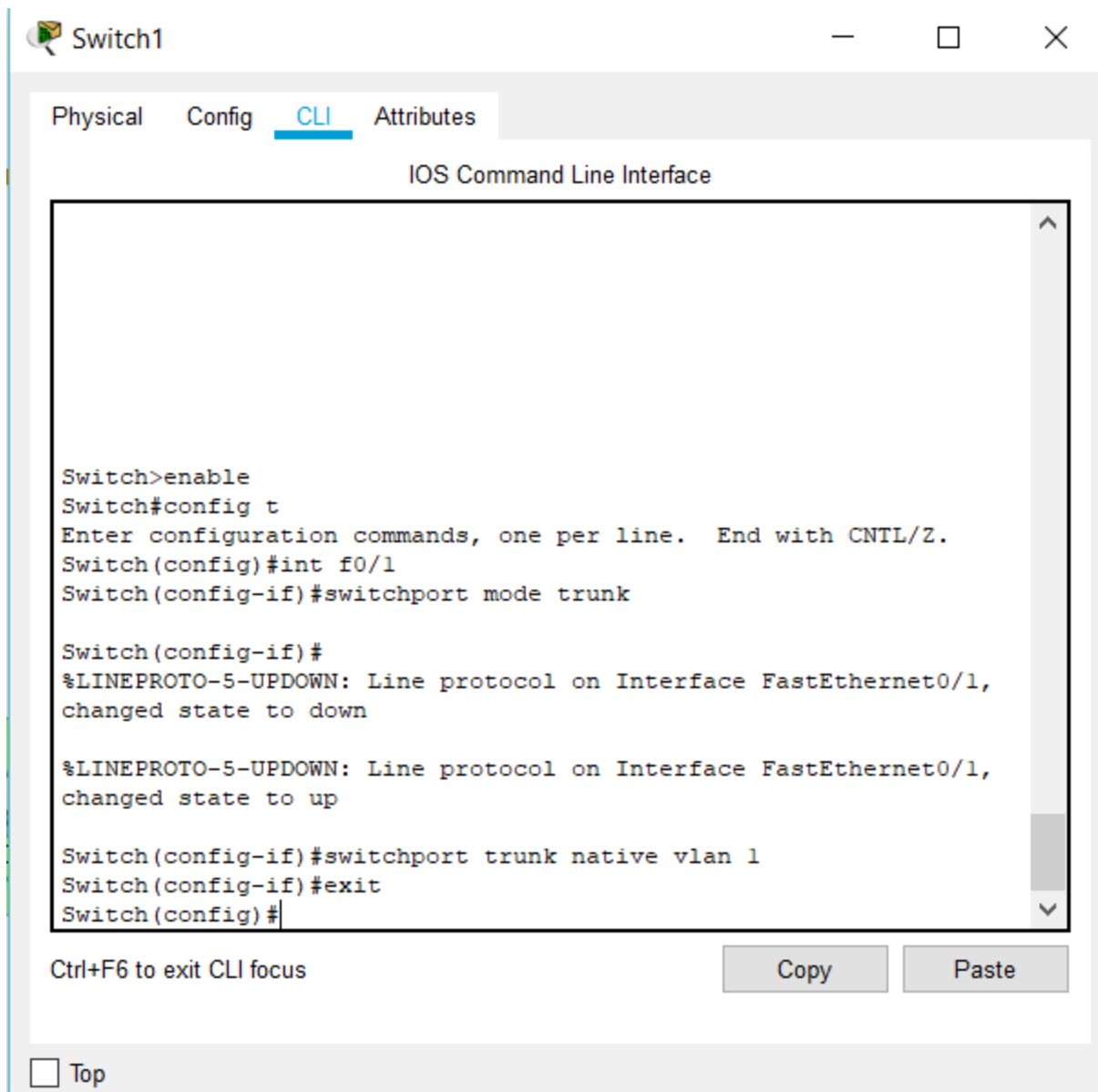
VLAN verde #4 (Administración): Puertos 9 a 11



Sin embargo, falta configurar los puertos con los que los switches se comunican entre sí. En el switch 0 realizamos la siguiente configuración:



En el switch 1 igualmente:



Y finalmente en el switch 2, se realiza la configuración trunk de ambos puertos:

Physical Config CLI Attributes

IOS Command Line Interface

```
%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
```

```
Switch(config)#  
Switch(config)#int f0/1  
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,  
changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,  
changed state to up
```

```
Switch(config-if)#switchport trunk native vlan 1  
Switch(config-if)#exit  
Switch(config)#int f0/2  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#switchport trunk native vlan 1  
Switch(config-if)#exit  
Switch(config)#
```

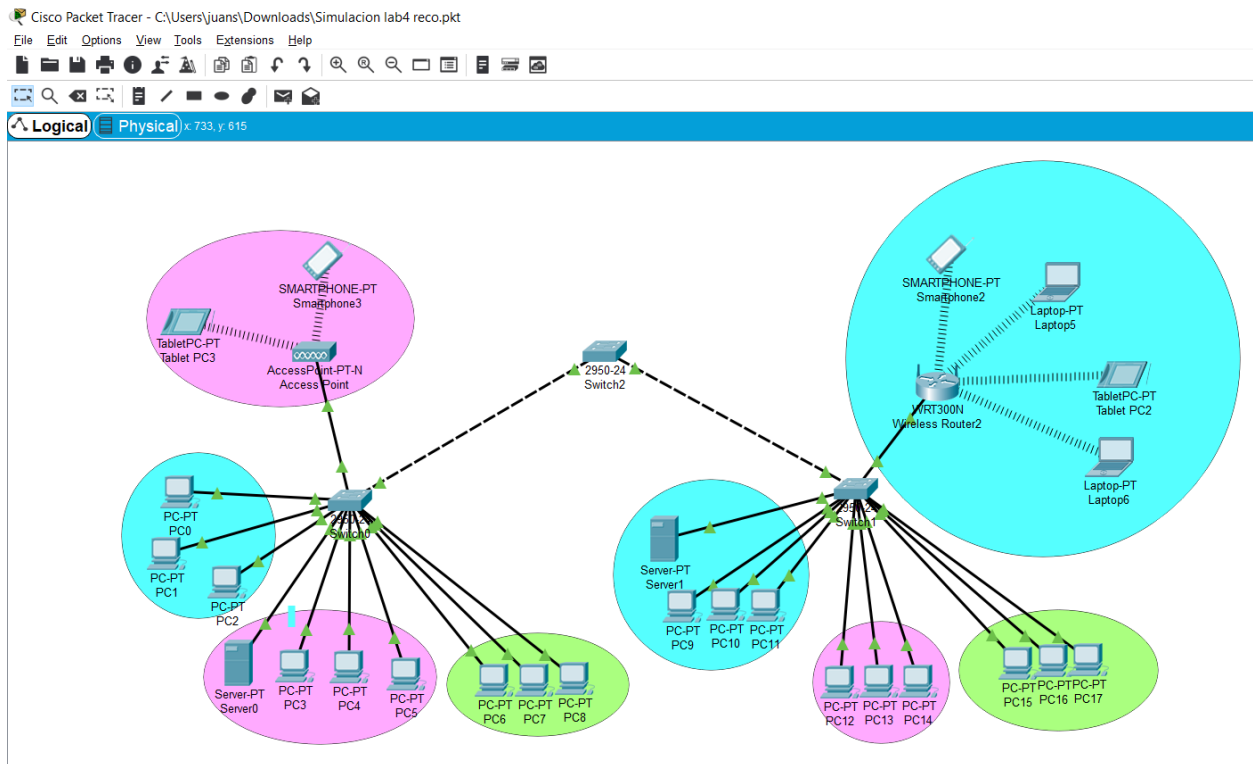
Ctrl+F6 to exit CLI focus

Copy

Paste

☐ Top

Finalmente se tiene la conexión de toda la red simulada:

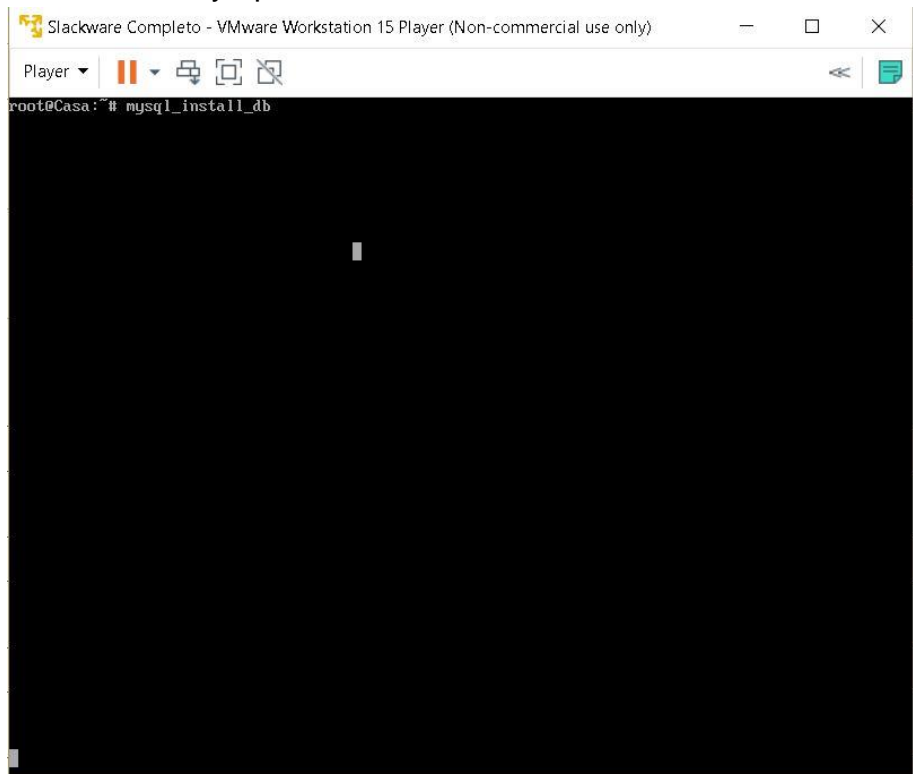


Instalación de software base:

Parte de la plataforma base de una infraestructura computacional de una organización son los motores de base de datos. En ellos se almacenan los datos estructurados de la organización y son usados desde diferentes aplicativos que soportan su operación. En los mismos grupos en los que se realizó todo este laboratorio, realice las siguientes actividades:

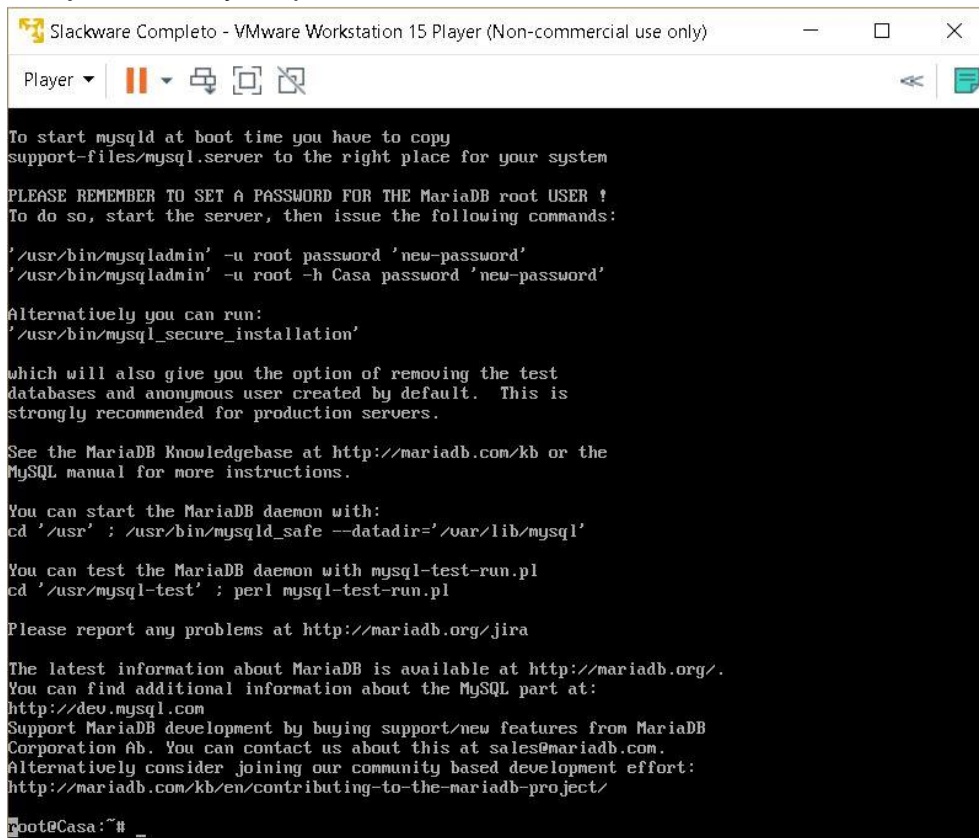
1. Instale el motor de base de datos MaríaDB sobre la máquina virtual con sistema operativo Linux Slackware.

El comando `mysql_install_db` instalara el sistema de bases de datos.



```
Slackware Completo - VMware Workstation 15 Player (Non-commercial use only)
Player
root@Casa:~# mysql_install_db
```

Lo ejecutamos y empezara la instalación como se observa



```
Slackware Completo - VMware Workstation 15 Player (Non-commercial use only)
Player
To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MariaDB root USER !
To do so, start the server, then issue the following commands:

'/usr/bin/mysqladmin' -u root password 'new-password'
'/usr/bin/mysqladmin' -u root -h Casa password 'new-password'

Alternatively you can run:
'/usr/bin/mysql_secure_installation'

which will also give you the option of removing the test
databases and anonymous user created by default. This is
strongly recommended for production servers.

See the MariaDB Knowledgebase at http://mariadb.com/kb or the
MySQL manual for more instructions.

You can start the MariaDB daemon with:
cd '/usr' ; /usr/bin/mysqld_safe --datadir='/var/lib/mysql'

You can test the MariaDB daemon with mysql-test-run.pl
cd '/usr/mysql-test' ; perl mysql-test-run.pl

Please report any problems at http://mariadb.org/jira

The latest information about MariaDB is available at http://mariadb.org/.
You can find additional information about the MySQL part at:
http://dev.mysql.com
Support MariaDB development by buying support/new features from MariaDB
Corporation Ab. You can contact us about this at sales@mariadb.com.
Alternatively consider joining our community based development effort:
http://mariadb.com/kb/en/contributing-to-the-mariadb-project/

root@Casa:~# _
```

```
Slackware Complete - VMware Workstation 15 Player (Non-commercial use only)

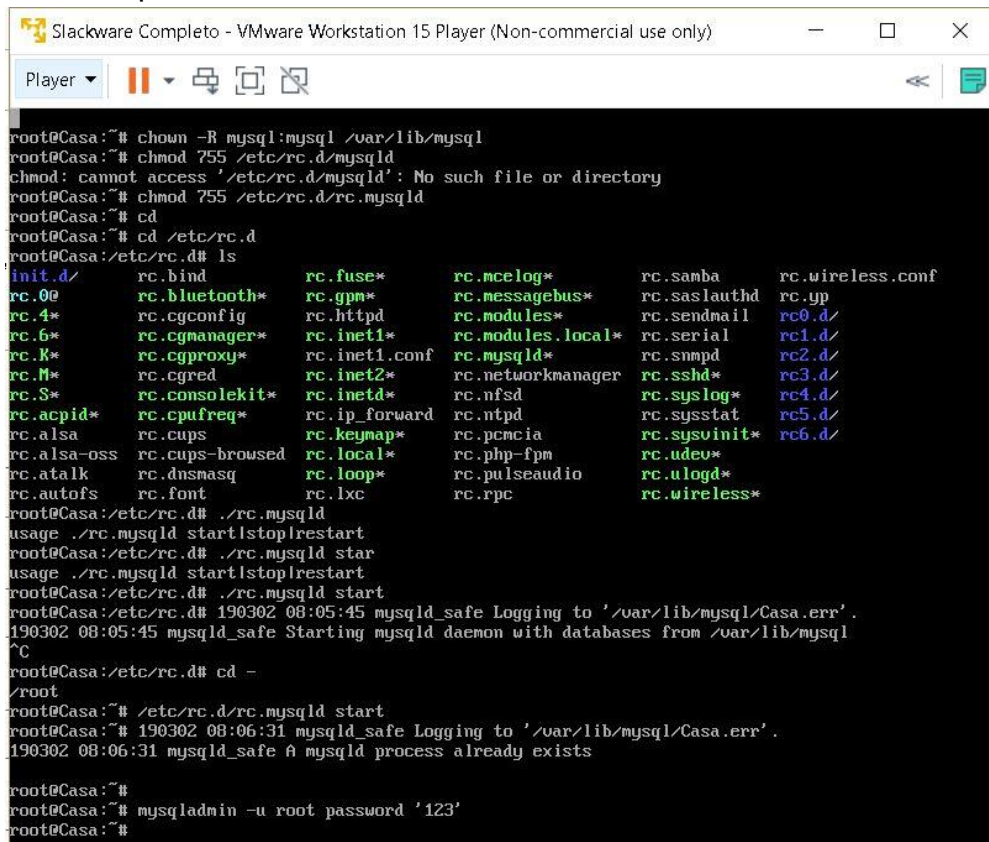
Player

The latest information about MariaDB is available at http://mariadb.org/.
You can find additional information about the MySQL part at:
http://dev.mysql.com
Support MariaDB development by buying support/new features from MariaDB
Corporation Ab. You can contact us about this at sales@mariadb.com.
Alternatively consider joining our community based development effort:
http://mariadb.com/kb/en/contributing-to-the-mariadb-project/

root@Casa:~# chown -R mysql:mysql /var/lib/mysql
root@Casa:~# chmod 755 /etc/rc.d/mysqld
chmod: cannot access '/etc/rc.d/mysqld': No such file or directory
root@Casa:~# chmod 755 /etc/rc.d/rc.mysqld
root@Casa:~# cd
root@Casa:~# cd /etc/rc.d
root@Casa:/etc/rc.d# ls
init.d/      rc.bind      rc.fuse*     rc.mcelog*   rc.samba     rc.wireless.conf
rc.00*      rc.bluetooth* rc.gpm*      rc.messagebus* rc.saslauthd rc.ypp
rc.4*       rc.cgconfig  rc.httpd     rc.modules*  rc.sendmail  rc0.d/
rc.6*       rc.cgmanager* rc.inet1*    rc.modules.local* rc.serial    rc1.d/
rc.K*       rc.cgproxy*  rc.inet1.conf rc.mysqld*   rc.snmpd     rc2.d/
rc.M*       rc.cgred     rc.inet2*    rc.networkmanager rc.sshd*     rc3.d/
rc.S*       rc.consolekit* rc.inetd*    rc.nfsd      rc.syslog*   rc4.d/
rc.acpid*   rc.cpubufreq* rc.ip_forward rc.ntpd      rc.sysstat   rc5.d/
rc.alsa     rc.cups      rc.keymap*   rc.pcscia    rc.sysvinit* rc6.d/
rc.alsa-oss rc.cups-browsed rc.local*    rc.php-fpm   rc.udev*     rc6.d/
rc.ataalk   rc.dnsmasq   rc.loop*    rc.pulseaudio rc.ulogd*
rc.autofs   rc.font      rc.lxc      rc.rpc       rc.wireless*

root@Casa:/etc/rc.d# ./rc.mysqld
usage ./rc.mysqld start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysqld star
usage ./rc.mysqld start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysqld start
root@Casa:/etc/rc.d# 190302 08:05:45 mysqld_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:05:45 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
rc
root@Casa:/etc/rc.d#
```

Ahora ejecutamos `chown -R mysql:mysql /var/lib/mysql` para actualizar las librerías que usa mariaDB



```
Slackware Completo - VMware Workstation 15 Player (Non-commercial use only)
Player
root@Casa:~# chown -R mysql:mysql /var/lib/mysql
root@Casa:~# chmod 755 /etc/rc.d/mysql
chmod: cannot access '/etc/rc.d/mysql': No such file or directory
root@Casa:~# chmod 755 /etc/rc.d/rc.mysql
root@Casa:~# cd
root@Casa:~# cd /etc/rc.d
root@Casa:/etc/rc.d# ls
init.d/      rc.bind      rc.fuse*     rc.mcelog*   rc.samba     rc.wireless.conf
rc.0e        rc.bluetooth* rc.gpm*      rc.messagebus* rc.saslauthd rc.ypp
rc.4         rc.cgconfig  rc.httptd   rc.modules*  rc.sendmail  rc0.d/
rc.6         rc.cgmanger* rc.inet1*    rc.modules.local* rc.serial     rc1.d/
rc.K*        rc.cgxproxy* rc.inet1.conf rc.mysql*     rc.snmpd      rc2.d/
rc.M*        rc.cgred     rc.inet2*    rc.networkmanager rc.sshd*      rc3.d/
rc.S*        rc.consolekit* rc.inetd*    rc.nfsd       rc.syslog*    rc4.d/
rc.acpid*    rc.cpufreq*   rc.ip_forward rc.ntpd       rc.sysstat    rc5.d/
rc.alsa      rc.cups       rc.keymap*   rc.pcmcia    rc.sysvinit*  rc6.d/
rc.alsa-oss  rc.cups-browsed rc.local*    rc.php-fpm   rc.udev*
rc.atalk     rc.dnsmasq    rc.loop*     rc.pulseaudio rc.udev*
rc.autofs    rc.font        rc.lxc       rc.rpc        rc.wireless*
root@Casa:/etc/rc.d# ./rc.mysql
usage ./rc.mysql start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysql start
usage ./rc.mysql start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysql start
root@Casa:/etc/rc.d# 190302 08:05:45 mysql_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:05:45 mysql_safe Starting mysql daemon with databases from /var/lib/mysql
^C
root@Casa:/etc/rc.d# cd -
/root
root@Casa:~# /etc/rc.d/rc.mysql start
root@Casa:~# 190302 08:06:31 mysql_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:06:31 mysql_safe A mysql process already exists
root@Casa:~#
root@Casa:~# mysqladmin -u root password '123'
root@Casa:~#
```

Seguidamente damos los permisos para que podamos ejecutar mariaDB desde el directorio de instalación de la siguiente manera: `chmod 755 /etc/rc.d/rc.mysql`


```
Slackware Completo - VMware Workstation 15 Player (Non-commercial use only)

rc.acpid*   rc.cpufreq*   rc.ip_forward rc.ntpd       rc.sysstat   rc5.d/
rc.alsa     rc.cups        rc.keymap*     rc.pcmcia     rc.sysvinit* rc6.d/
rc.alsa-oss rc.cups-browsed rc.local*      rc.php-fpm    rc.udev*
rc.atalk    rc.dnsmasq     rc.loop*       rc.pulseaudio rc.ulogd*
rc.autofs   rc.font         rc.lxc         rc.rpc        rc.wireless*

root@Casa:/etc/rc.d# ./rc.mysql
usage ./rc.mysql start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysql start
usage ./rc.mysql start|stop|restart
root@Casa:/etc/rc.d# ./rc.mysql start
root@Casa:/etc/rc.d# 190302 08:05:45 mysqld_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:05:45 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
^C
root@Casa:/etc/rc.d# cd -
/root
root@Casa:~# /etc/rc.d/rc.mysql start
root@Casa:~# 190302 08:06:31 mysqld_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:06:31 mysqld_safe A mysqld process already exists

root@Casa:~#
root@Casa:~# mysqladmin -u root password '123'
root@Casa:~# mysql -version
ERROR 1045 (2B000): Access denied for user 'root'@'localhost' (using password: NO)
root@Casa:~# mysqladmin -u root -p version
Enter password:
mysqladmin Ver 9.1 Distrib 10.0.26-MariaDB, for Linux on x86_64
Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Server version          10.0.26-MariaDB
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysql/mysql.sock
Uptime:                 1 min 58 sec

Threads: 1 Questions: 5 Slow queries: 0 Opens: 0 Flush tables: 1 Open tables: 63 Queries per s
econd avg: 0.042
root@Casa:~# _
```

Ahora usamos el comando `mysqladmin -u root password '123'` para cambiar la contraseña que tiene por defecto el usuario root para la ejecución de mariaDB todo lo estamos haciendo desde el usuario root

```
Slackware Completo - VMware Workstation 15 Player (Non-commercial use only)
Player
root@Casa:/etc/rc.d# 190302 08:05:45 mysqld_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:05:45 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
^C
root@Casa:/etc/rc.d# cd -
/root
root@Casa:~# /etc/rc.d/rc.mysqld start
root@Casa:~# 190302 08:06:31 mysqld_safe Logging to '/var/lib/mysql/Casa.err'.
190302 08:06:31 mysqld_safe A mysqld process already exists

root@Casa:~#
root@Casa:~# mysqladmin -u root password '123'
root@Casa:~# mysql -version
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
root@Casa:~# mysqladmin -u root -p version
Enter password:
mysqladmin Ver 9.1 Distrib 10.0.26-MariaDB, for Linux on x86_64
Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Server version          10.0.26-MariaDB
Protocol version        10
Connection              Localhost via UNIX socket
UNIX socket             /var/run/mysql/mysql.sock
Uptime:                 1 min 58 sec

Threads: 1 Questions: 5 Slow queries: 0 Opens: 0 Flush tables: 1 Open tables: 63 Queries per s
econd avg: 0.042
root@Casa:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 10.0.26-MariaDB MariaDB Server

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> _
```

Procedemos a ejecutar mariaDB en modo root con el comando `mysql -u root -p`

2. Cree 2 usuarios:

a. Deporte:

Para la creación de usuarios usamos el comando `CREATE USER`

'*nombredeUsuario*'@'localhost' IDENTIFIED BY '*contraseña*' como se muestra a continuación con la creación del usuario 'Deporte'

```
MariaDB [(none)]> CREATE USER 'Deporte'@'localhost' IDENTIFIED BY '12345';
Query OK, 0 rows affected (0.00 sec)
```

b. Coach: Seguidamente creamos el usuario 'Coach'

```
MariaDB [(none)]> CREATE USER 'Coach'@'localhost' IDENTIFIED BY '123456';
Query OK, 0 rows affected (0.00 sec)
```

3. Cree 3 bases de datos:

a. Torneo. Base de datos para inscripciones al torneo de futbol de la Decanatura.

```

MariaDB server version for the right syntax to use near 'users' at line 1
MariaDB [(none)]> CREATE DATABASE Torneo;
Query OK, 1 row affected (0.00 sec)

```

Para crear una base de datos usamos CREATE DATABASE '*NombreBasededatos*';
En este caso como se observa en la imagen creamos la base de datos Torneo.

- b. Circuito. Base de datos para registrar las competencias que se realizan entre maratonistas a nivel Colombia dentro del circuito CCPL (se realiza cada 15 días y la sede es una universidad colombiana que reciben a estudiantes de otras universidades en una fecha particular).

```

MariaDB [(none)]> CREATE DATABASE Circuito;
Query OK, 1 row affected (0.01 sec)

```

Creamos la base de datos Circuito

- c. Entrenamiento. Base de datos donde el coach de la Escuela registra las sesiones de entrenamiento para nuestros maratonistas y los estudiantes que asisten a dichos entrenamientos.

Creamos la base de datos Entrenamiento

```

MariaDB [(none)]> CREATE DATABASE Entrenamiento;
Query OK, 1 row affected (0.00 sec)

```

```

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| Circuito |
| Entrenamiento |
| Torneo |
| information_schema |
| mysql |
| performance_schema |
| test |
+-----+
7 rows in set (0.00 sec)

```

Al ejecutar "show databases", aparecerán todas las bases de datos creadas, como vemos se crearon satisfactoriamente las bases de datos.

4. Autorice al usuario coach para administrar las bases de datos Circuito y Entrenamiento y el usuario deporte para administra la base de datos.

```

MariaDB [Entrenamiento]> GRANT ALL PRIVILEGES ON Entrenamiento.* TO 'Coach';
Query OK, 0 rows affected (0.00 sec)

MariaDB [Entrenamiento]> GRANT ALL PRIVILEGES ON Circuito.* TO 'Coach';
Query OK, 0 rows affected (0.00 sec)

```

Para dar todos los permisos de administración (acceder, insertar, eliminar, actualizar) ejecutamos el comando GRANT ALL PRIVILEGES ON 'BasedeDatos' .* TO 'usuario'

Como observamos en la imagen estamos dando permisos de administración al usuario Coach sobre la base de datos Circuito y Entrenamiento.

Ahora damos permisos de administración al usuario Deporte en la base de datos Torneo como se observa

```
MariaDB server version for the right syntax to use near 'Torneo.* TO Deporte' at line 1
MariaDB [(none)]> GRANT ALL PRIVILEGES ON Torneo.* TO Deporte;
Query OK, 0 rows affected (0.00 sec)
```

También podemos denegar los privilegios otorgados con el siguiente comando REVOKE ALL ON 'Base/tabla' .* FROM usuario;

```
MariaDB server version for the right syntax to use near 'ON Torneo FROM Coach' at line 1
MariaDB [Entrenamiento]> REVOKE ALL ON Torneo.* FROM Coach;
Query OK, 0 rows affected (0.00 sec)
```

5. Cree las siguientes tablas en la base de datos

a. Torneo

Primero debemos acceder a la base de datos torneo lo hacemos ejecutando "use Torneo;"

```
MariaDB [Entrenamiento]> USE Torneo;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

i. Equipos: ID_equipo, nombre

```
MariaDB [Torneo]> CREATE TABLE Equipos( ID_equipo VARCHAR(6) NOT NULL, nombre VARCHAR(15) NOT NULL,
CONSTRAINT pk_equipos PRIMARY KEY (ID_equipo));_
```

Creamos la tabla equipos de la siguiente manera CREATE TABLE *nombreTabla* (*atributo tipo*,...); También en la misma creación de las tablas podemos asignar las llaves primarias, foráneas, checks como se muestra en la imagen
Podemos usar el comando Show tables; para ver las tablas que se encuentran en la base de datos que estamos usando

```
MariaDB [Torneo]> SHOW tables ;
+-----+
| Tables_in_Torneo |
+-----+
| Equipos           |
+-----+
1 row in set (0.00 sec)
```

ii. Jugadores: ID_jugador, nombre, celular, edad, tipo (jugados o capitán), ID_equipo

```
MariaDB [Torneo]> CREATE TABLE Jugadores( ID_jugador VARCHAR(6) NOT NULL,nombre VARCHAR(20) NOT NULL,
celular VARCHAR(10) NOT NULL, edad VARCHAR(2) NOT NULL, tipo VARCHAR(7) NOT NULL, ID_equipo VARCHAR(6) NOT NULL, CONSTRAINT pk_jugadores PRIMARY KEY (ID_jugador), CONSTRAINT ck_jugadoresTipo CHECK(tipo IN ('jugador','capitán')));
Query OK, 0 rows affected (0.06 sec)
```

Creamos la tabla jugadores con sus atributos y además agregan una restricción que es que el tipo solo puede ser o jugador o capitán creamos el check como se observa en la imagen

Creando correctamente la tabla

```
MariaDB [Torneo]> show tables;
+-----+
| Tables_in_Torneo |
+-----+
| Equipos           |
| Jugadores         |
+-----+
2 rows in set (0.00 sec)
```

b. Circuito

```
MariaDB [Torneo]> USE Circuito;
Database changed
MariaDB [Circuito]> show tables;
Empty set (0.00 sec)
```

Ahora cambiamos de base de datos usando “USE Circuito; y confirmamos que no existen tablas aun

i. Ronda: ID_ronda, universidad, fecha

```
MariaDB [Circuito]> CREATE TABLE Ronda(ID_ronda VARCHAR(6) NOT NULL,universidad VARCHAR(30) NOT NULL,
-> fecha VARCHAR(30) NOT NULL, CONSTRAINT pk_circuito PRIMARY KEY(ID_ronda));
Query OK, 0 rows affected (0.05 sec)
```

Creamos la tabla Ronda como se observa en la imagen y creamos su PK que es el ID_ronda

ii. Equipos: Id_equipo, nombre_est1, nombre_est2, nombre_est3, ID_ronda, Puesto

```
MariaDB [Circuito]> CREATE TABLE Equipos(ID_equipo VARCHAR(6) NOT NULL, nombre_est1 VARCHAR(30) NOT NULL, nombre_est2 VARCHAR(30) NOT NULL, nombre_est3 VARCHAR(30) NOT NULL, ID_ronda VARCHAR(6) NOT NULL, puesto VARCHAR(2) NOT NULL, CONSTRAINT pk_circuito PRIMARY KEY(ID_equipo));
Query OK, 0 rows affected (0.04 sec)
```

Creamos la tabla equipos como se muestra en la figura

c. Entrenamiento

Usamos “use Entrenamiento” para cambiar a la base de datos entrenamiento

i. Sesiones: ID_sesión, fecha, entrenador, tema

Creamos la tabla sesiones con cada uno de sus atributos y tipos además creamos una llave primaria que será ID_sesion

```

t line 1
MariaDB [Entrenamiento]> CREATE TABLE Sesiones(ID_sesion VARCHAR(6) NOT NULL,fecha VARCHAR(20) NOT N
ULL, entrenador VARCHAR(30) NOT NULL, tema VARCHAR(20) NOT NULL, CONSTRAINT pk_entrenamiento PRIMARY
KEY(ID_sesion));
Query OK, 0 rows affected (0.01 sec)
```

ii. Asistentes: ID_estudiante, nombre, rendimiento (Alto, medio o bajo), ID_sesión

Creamos la tabla “asistentes” de la siguiente manera añadiendo una restricción de tipo la cual rendimiento solo podrá tomar los valores medio, bajo o alto

```
MariaDB [Entrenamiento]> CREATE TABLE Asistentes(ID_estudiante VARCHAR(7) NOT NULL,nombre VARCHAR(30) NOT NULL, rendimiento VARCHAR(5) NOT NULL, ID_sesion VARCHAR(6) NOT NULL, CONSTRAINT pk_entrenamiento PRIMARY KEY(ID_estudiante), CONSTRAINT ck_asistentesRendimiento CHECK(rendimiento IN('medio','bajo','alto')));
Query OK, 0 rows affected (0.03 sec)
```

6. Inserte datos a las bases de datos

Para la inserción de datos como estamos desde el usuario root podremos insertar libremente datos en cada una de las tablas creadas como se muestra a continuación ya que este usuario no tiene ningún tipo de restricción.

Procedemos a insertar en la base de datos Torneo

```
Database changed
MariaDB [Torneo]> INSERT INTO Equipos(ID_equipo,nombre) VALUES (123,Chelsea);
ERROR 1054 (42S22): Unknown column 'Chelsea' in 'field list'
MariaDB [Torneo]> INSERT INTO Equipos(ID_equipo,nombre) VALUES (123,'Chelsea');
Query OK, 1 row affected (0.00 sec)
```

Como vemos hace correctamente la ejecución de la consulta e inserta en la tabla Torneo podemos verificar el contenido de la tabla ejecutando la consulta `SELECT * from Torneo;`

Ahora si salimos del usuario root en ingresamos con alguno de los usuarios que creamos en este caso Coach vamos a observar cómo no nos dejara entrar en la base de datos torneo ya que no dimos permisos sobre esta base de datos si no sobre Circuito y Entrenamiento:

```
MariaDB [(none)]> exit
Bye
root@Casa:~# mysql -u Coach -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 20
Server version: 10.0.26-MariaDB MariaDB Server

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use Torneo;
ERROR 1044 (42000): Access denied for user 'Coach'@'localhost' to database 'Torneo'
MariaDB [(none)]> _
```

Ingresamos ahora en el usuario de la siguiente manera `mysql -u usuario -p`, seguidamente pedirá la contraseña que configuramos anteriormente en el momento de la creación de usuarios y como vemos no niega el acceso a torneo ya que no tiene

permisos. Es decir, no podremos ni modificarla ni acceder a ella para consultar.

```
MariaDB [(none)]> use Torneo;
ERROR 1044 (42000): Access denied for user 'Coach'@'localhost' to database 'Torneo'
MariaDB [(none)]> use Entrenamiento;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Entrenamiento]> INSERT INTO Sesiones(ID_sesion,fecha,entrenador,tema) VALUES (1,'12 de enero', 'fred', 'baloncesto');
Query OK, 1 row affected (0.00 sec)

MariaDB [Entrenamiento]> INSERT INTO Asistentes (ID_estudiante,nombre,rendimiento,ID_sesion) VALUES (2124467,'Daniel','medio',123);
Query OK, 1 row affected (0.00 sec)
```

Ahora ingresamos a la base de datos entrenamiento que es una a la cual le dimos permisos como vemos nos deja usarla mediante el comando “use Entrenamiento” y procedemos a insertar para ver que tiene permisos completos sobre la base de datos, hace una inserción correcta en las tablas como observamos.

Ahora igualmente probamos con la otra base de datos que tenemos permisos con el usuario Coach y nos dejara acceder e insertar libremente

```
MariaDB [(none)]> use Circuito
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [Circuito]> INSERT INTO Equipos(Id_equipo,nombre_est1,nombre_est2,nombre_est3,ID_ronda,puesto) VALUES (123,'Daniel','Sebastian','Miguel',3,1);
Query OK, 1 row affected (0.00 sec)

MariaDB [Circuito]> INSERT INTO Ronda(ID_ronda,universidad,fecha) VALUES (3,'sabana','23 de abril');
Query OK, 1 row affected (0.02 sec)
```

Salimos del usuario Coach ahora accederemos al usuario Deporte que este tiene permisos sobre la base de datos Torneo

```
MariaDB [Circuito]> exit
Bye
root@Casa:~# mysql -u Deporte -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 24
Server version: 10.0.26-MariaDB MariaDB Server

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use Entrenamiento
ERROR 1044 (42000): Access denied for user 'Deporte'@'localhost' to database 'Entrenamiento'
MariaDB [(none)]> use Circuito
ERROR 1044 (42000): Access denied for user 'Deporte'@'localhost' to database 'Circuito'
MariaDB [(none)]> use Torneo;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```


Verificamos que no tenemos acceso a las otras dos bases de datos, pero al momento de usar torneo nos permite perfectamente insertar modificar y acceder a las tablas de Torneo como se muestra en la imagen anterior.

Conclusiones:

- Mediante este laboratorio se aprendió a configurar un router inalámbrico en la vida real y en una simulación de Packet Tracer.
- Se aprendió a configurar un switch y una VLAN, también en la vida real y en una simulación.
- Se aprendió a instalar MariaDB en Slackware y a crear bases de datos en ella.
- Se entendieron y se vio en practica algunas de las funcionalidades que realiza la capa de enlace en una red.

Bibliografía:

- Anónimo. Install MariaDB On Slackware [consulta: 3 de marzo de 2019]
Disponible en:
https://docs.slackware.com/howtos:databases:install_mariadb_on_slackware
- Julio Yañez. Tutorial MariaDB (2): Creando tablas en SQL [consulta: 3 de marzo de 2019] Disponible en:
<http://codigoxules.org/tutorial-mariadb-creando-tablas-en-sql/>
- Anónimo. Comandos de administración de MariaDB para principiantes [consulta: 3 de marzo de 2019] Disponible en:
<https://maslinux.es/comandos-de-administracion-de-mariadb-para-principiantes/>
- CISCO Networking Academy. Configuración de un sistema operativo de red [consulta: 3 de marzo de 2019] Disponible en:
<https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>
- Claudia Santiago. *Capa de Enlace* [online]. [consulta: 28 de febrero de 2019].
Disponible en:
http://campusvirtual.escuelaing.edu.co/moodle/pluginfile.php/149311/mod_resource/content/2/03-capaEnlace_20191_p1.pdf
- Adrián Crespo. VLANs: Qué son, tipos y para qué sirven [consulta: 3 de marzo de 2019] Disponible en:
<https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/>

- Anónimo. VLAN – Redes Virtuales [consulta: 3 de marzo de 2019] Disponible en:
<https://es.ccm.net/contents/286-vlan-redes-virtuales>
- Anónimo. Como funciona un router inalámbrico [consulta: 3 de marzo de 2019]
Disponible en:
<http://culturacion.com/como-funciona-un-router-inalambrico/>
- Anónimo. Como funciona un router inalámbrico [consulta: 3 de marzo de 2019]
Disponible en:
<http://culturacion.com/como-funciona-un-router-inalambrico/>