

Laboratorio No. 4

Plataforma Base y capa de enlace

Investigación y practica

RECO

Brayan Burgos, Daniel Vargas
Escuela Colombiana de Ingeniería Julio Garavito
brayan.burgos@mail.escuelaing.edu.co; daniel.vargas-o@mail.escuelaing.edu.co



Introducción

Durante el desarrollo de este laboratorio se realizarán montajes que incluyen redes alámbricas e inalámbricas donde debemos configurar switches, puntos de acceso, routers inalámbricos; además crearemos y configuraremos VLANs y revisaremos la información de estas en el frame ethernet, luego integraremos las redes por medio de la conexión multiusuario que nos ofrece Packet Tracer. Por otro lado, revisaremos redes wifi-reales por medio de una aplicación que analiza el tráfico inalámbrico y por último instalaremos diferentes servidores web en sistemas operativos como CentOS y Windows Server.

Marco teórico

- **VLAN (Red de área local virtual)** Es una red lógica vinculada una red física, es útil para separar aquellos segmentos lógicos dentro de una LAN que no necesitan o no deben comunicarse entre sí.
- **ROUTER** Es un dispositivo hardware que se encarga de administrar el tráfico de información que circula por una red, pues se encarga de establecer qué ruta destinará a cada paquete de datos dentro de una red informática. Es útil para la interconexión de computadores, en la conexión de equipos a Internet o para el desarrollo interno de quienes proveen servicios de internet.
- **ACCESS POINT** Es un dispositivo utilizado para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o internet) para interconectar dispositivos móviles o tarjetas de red inalámbricas. Es muy común encontrar esto en redes, pues tanto en el Access Point como el router

son dispositivos muy útiles ya que con ambos se puede lograr establecer una conexión inalámbrica, lo que en la vida real es muy usado, además, los routers son esenciales para enviar información de una red a otra pues este destina cual será la ruta de cada paquete. Por otro lado, las VLANs tienen muchas ventajas una de ellas es el costo, si dentro de una red local hay dispositivos, que por temas de seguridad no deben tener comunicación una red VLAN soluciona el problema sin tener que invertir demasiado dinero. ***Estos conceptos serán usando frecuentemente durante el laboratorio, por lo que es vital entenderlos.***

Configuración básica del switch y Configuración básica del switch.

Por medio de la herramienta Packet Tracer, se realizaron los siguientes montajes.

Montaje Brayan Burgos:



Figura 1. Montaje sin Conexión

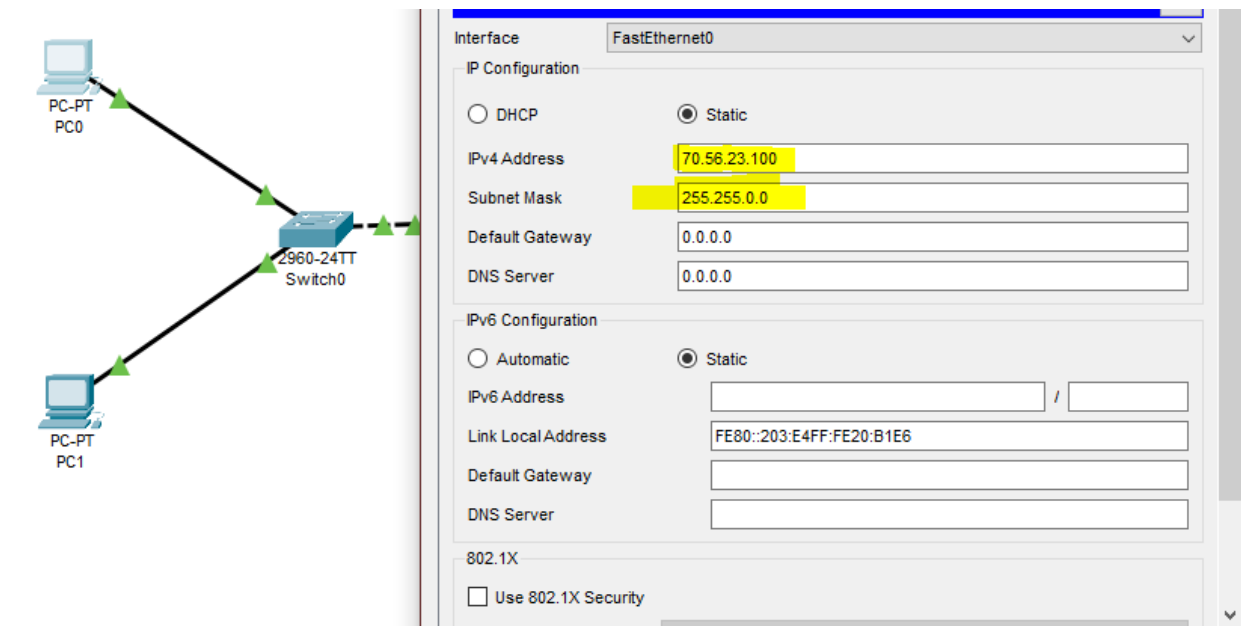


Figura 2. Configuración IP de los equipos.

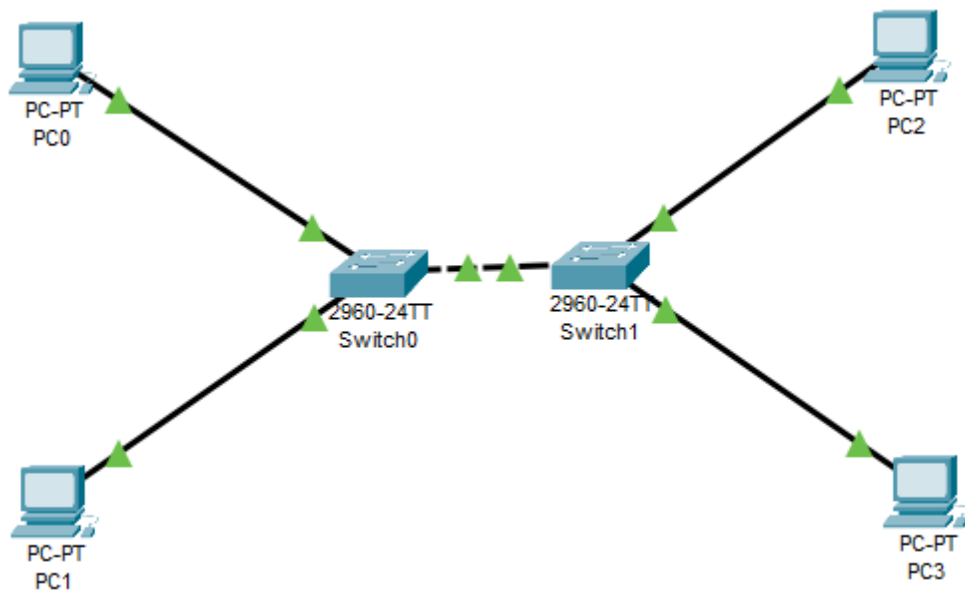


Figura 3. Montaje con Conexiones.

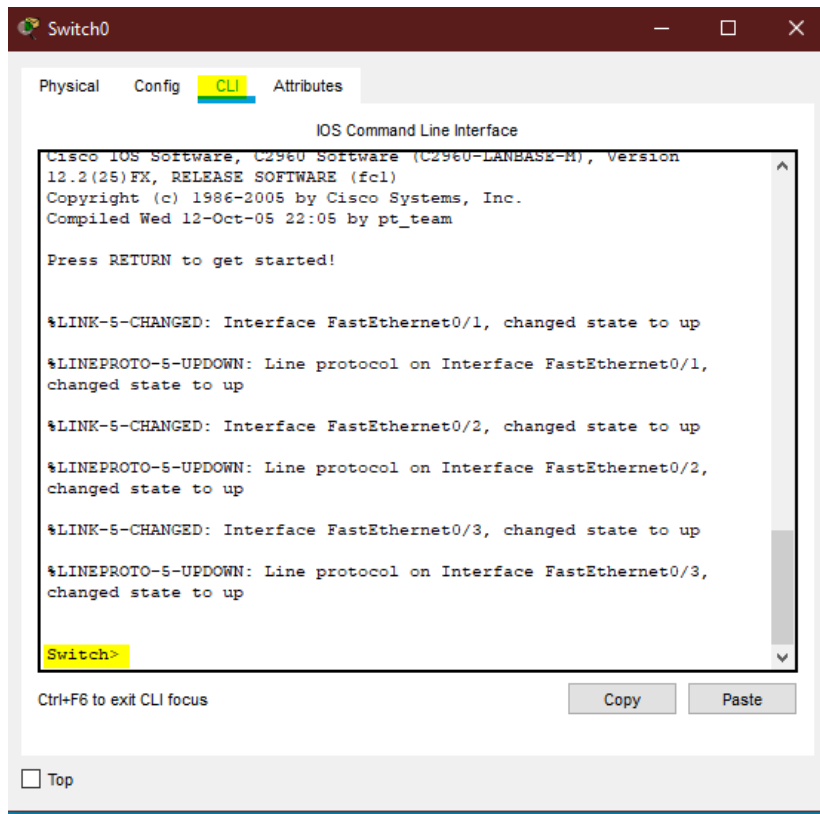


Figura 4. Configuración de Switch.

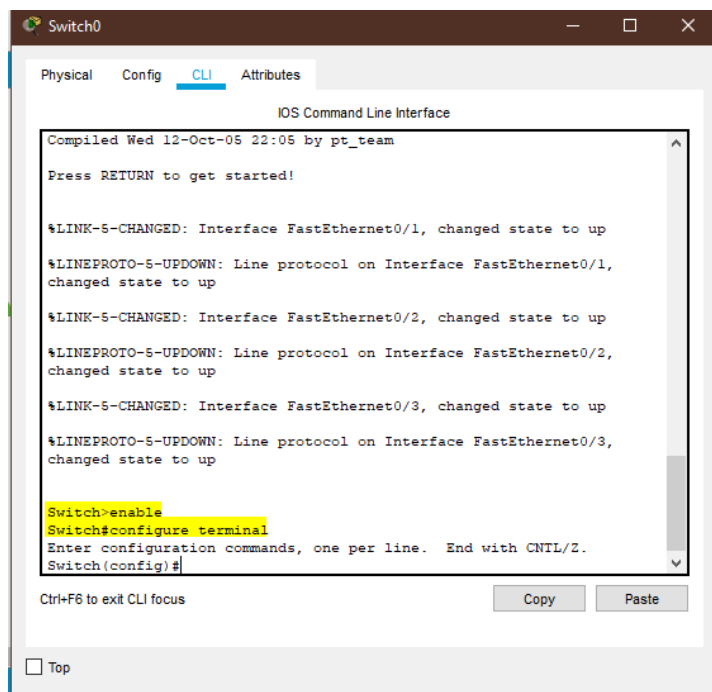


Figura 5. Configuración de Switch inicial, entrada al modo privilegiado

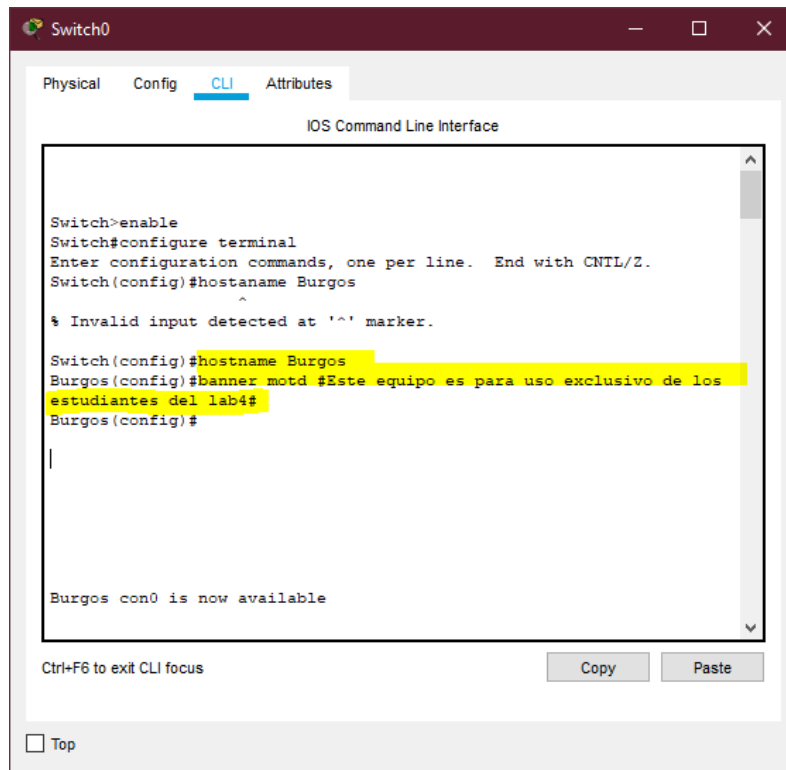


Figura 6. Nombre del host y mensaje.

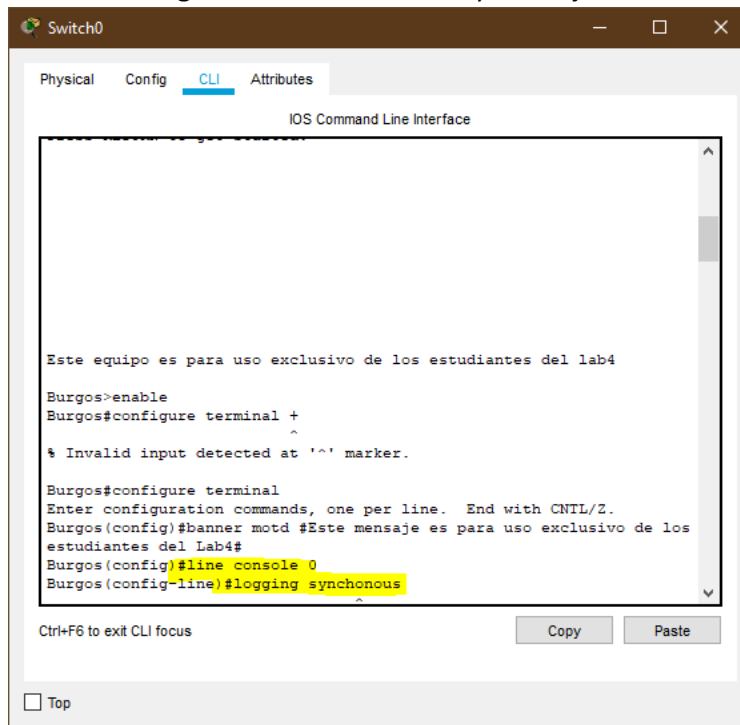


Figura 7. Logearse y entrar para cambiar la pass.

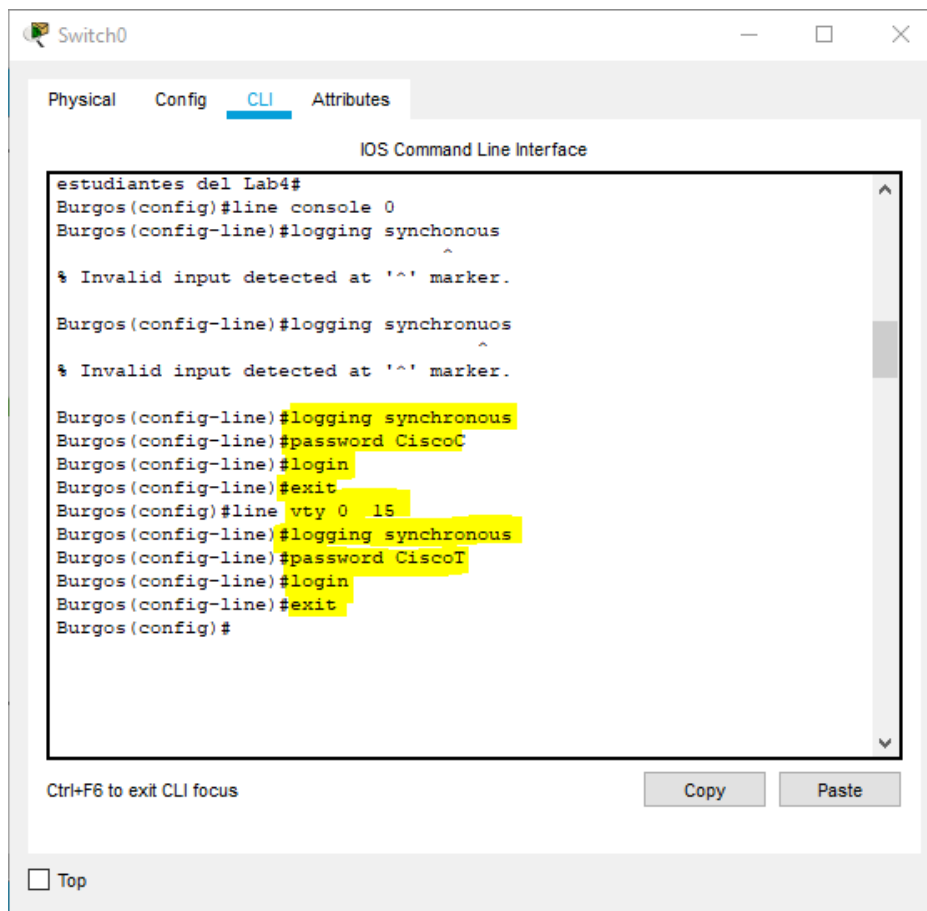
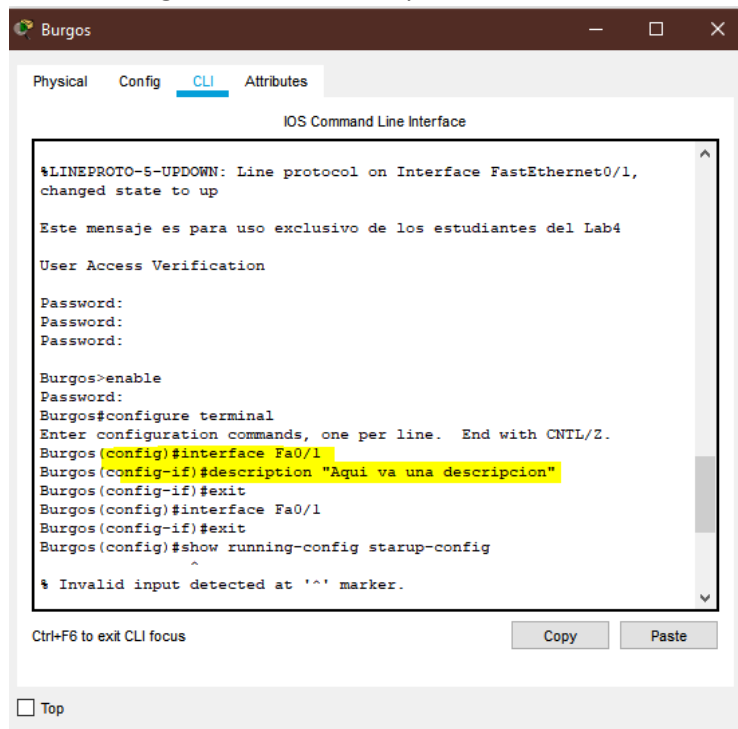


Figura 8. Contraseñas y salida del modo.



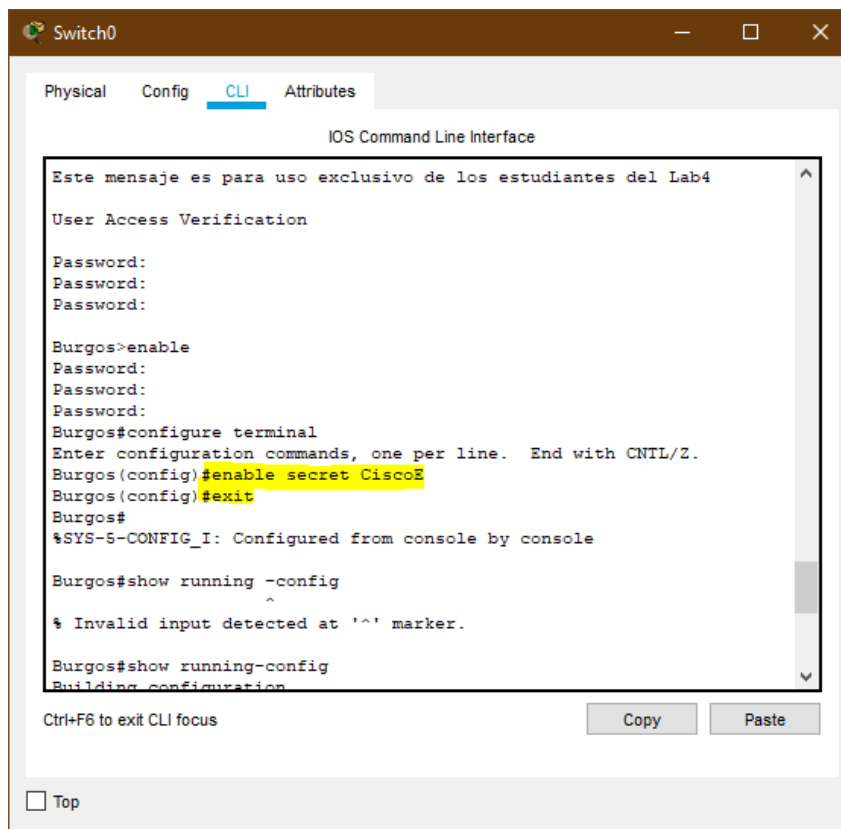


Figura 9. Modo secreto de Cisco y configuración de interface.

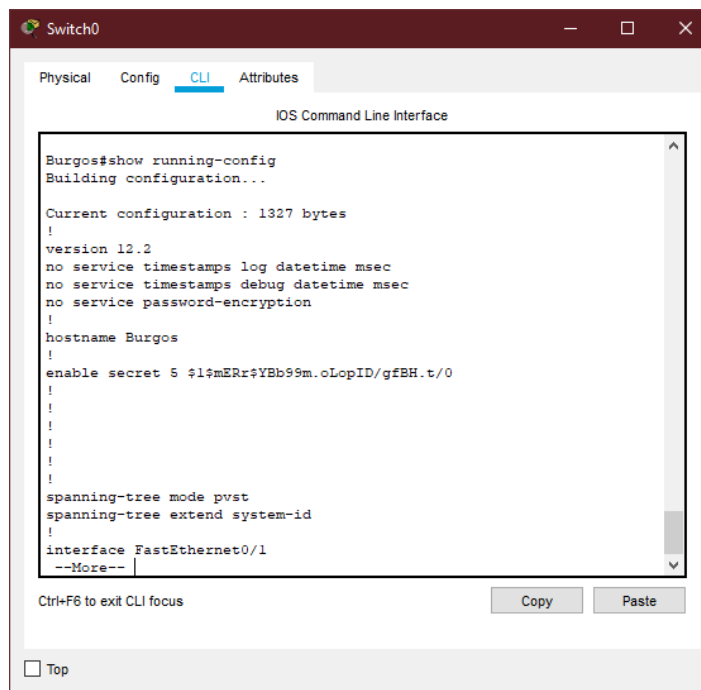


Figura 10. Verificación de los ajustes realizados con el comando.

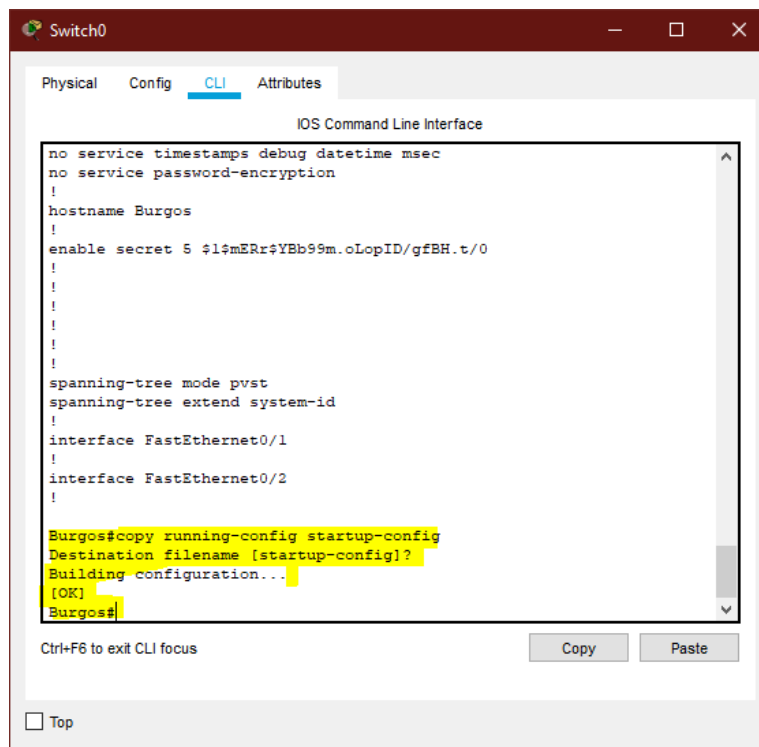


Figura 10. Guardado de la información

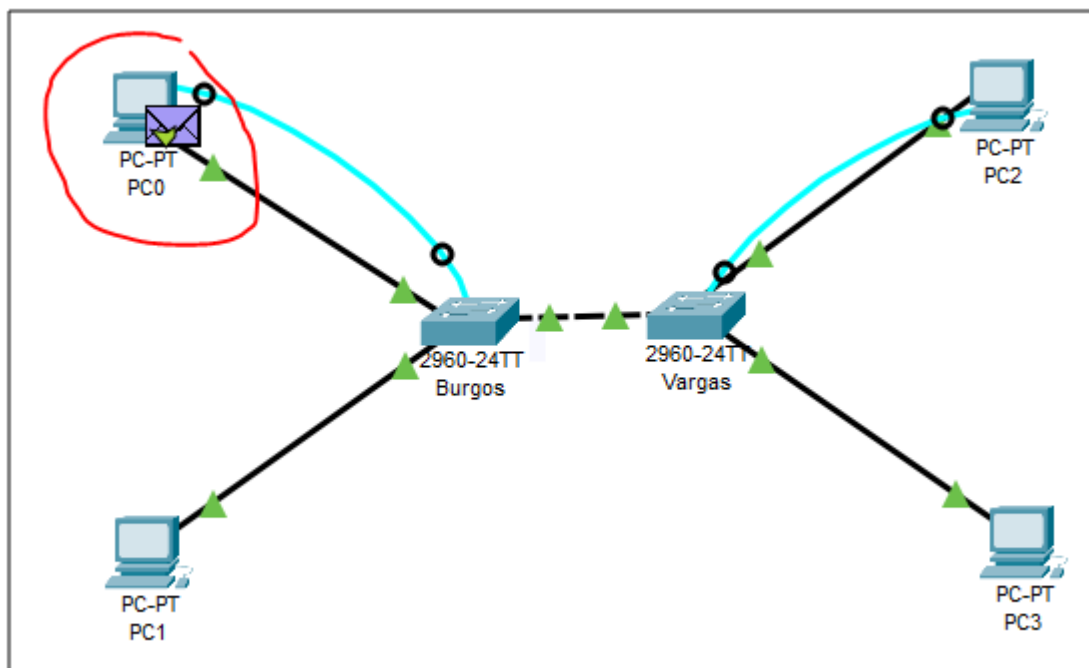


Figura 11. Envío de mensajes de forma correcta.

Montaje Daniel Vargas:

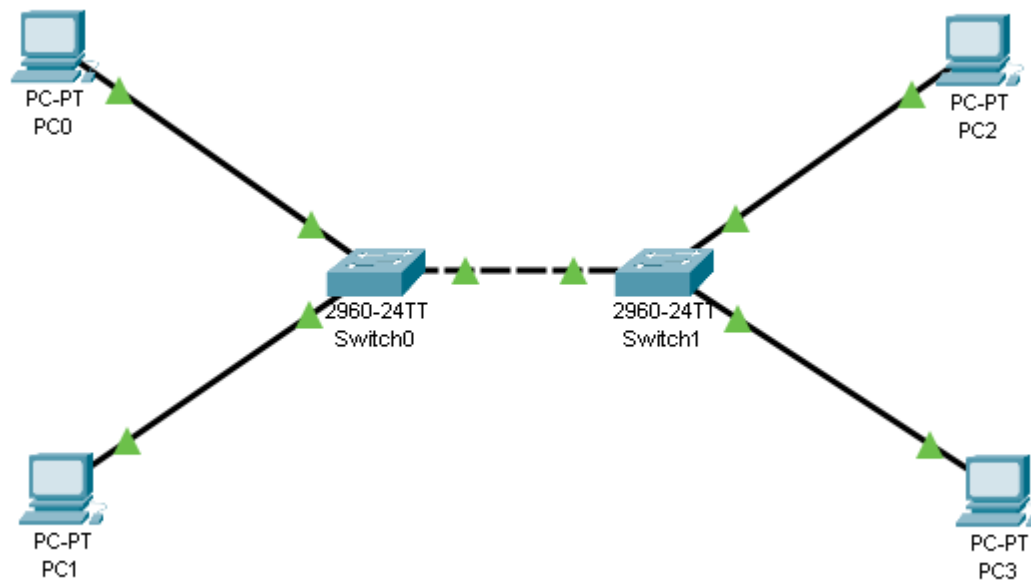


Figura 1. Montaje estudiante Daniel Vargas

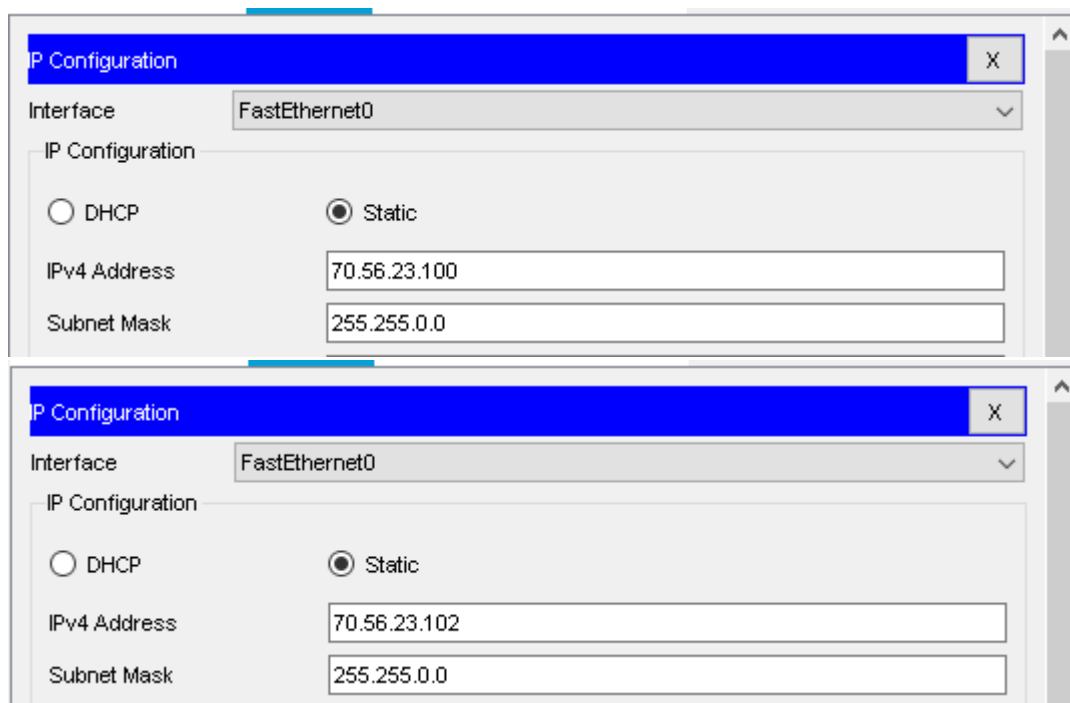
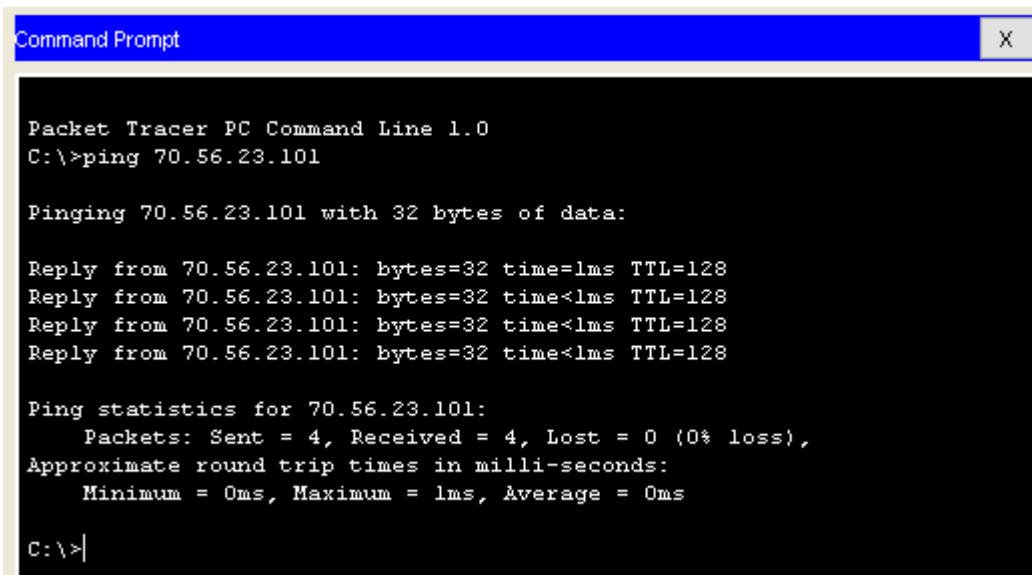


Figura 2. Configuración de la ip de dos equipos del esquema.



```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 70.56.23.101

Pinging 70.56.23.101 with 32 bytes of data:

Reply from 70.56.23.101: bytes=32 time=1ms TTL=128
Reply from 70.56.23.101: bytes=32 time<1ms TTL=128
Reply from 70.56.23.101: bytes=32 time<1ms TTL=128
Reply from 70.56.23.101: bytes=32 time<1ms TTL=128

Ping statistics for 70.56.23.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 3. Comando ping entre el Pc0 (ip: 70.56.23.100) con el Pc1 (ip: 70.56.23.101)

1. Configuración de Switches (Packet Tracer Daniel)

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname Daniel
Daniel(config)# banner motd # Este equipo es para uso exclusivo de
los estudiantes del Lab4 #
```

Figura 4. Configuración de Switch. Nombre y mensaje del día.

```
Daniel(config)# line console 0
Daniel(config-line)# logging synchronous
Daniel(config-line)# password CiscoC
Daniel(config-line)# login
Daniel(config-line)# exit
Daniel(config)#
```

Figura 5. Configuración clave consola.

```
Daniel(config)# line vty 0
Daniel(config-line)# logging synchronous
Daniel(config-line)# password CiscoT
Daniel(config-line)# login
Daniel(config-line)# exit
Daniel(config)#
```

Figura 6. Configuración clave del terminal remoto.

```
Daniel(config)#
Daniel(config)# no ip domain-lookup
```

Figura 7. Bloqueando la búsqueda de comandos con servidor externo.

```

Daniel(config)#
Daniel(config)# enable secret CiscoE
Daniel(config)# exit
Daniel#
%SYS-5-CONFIG_I: Configured from console by console

```

Figura 8. Clave de acceso al modo privilegiado.

```

Daniel# show running-config
Building configuration...

Current configuration : 1430 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Daniel
!
enable secret 5 $l$mERr$YBb99m.oLopID/gfBH.t/0
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
--More--

```

Figura 9. Configuración del equipo.

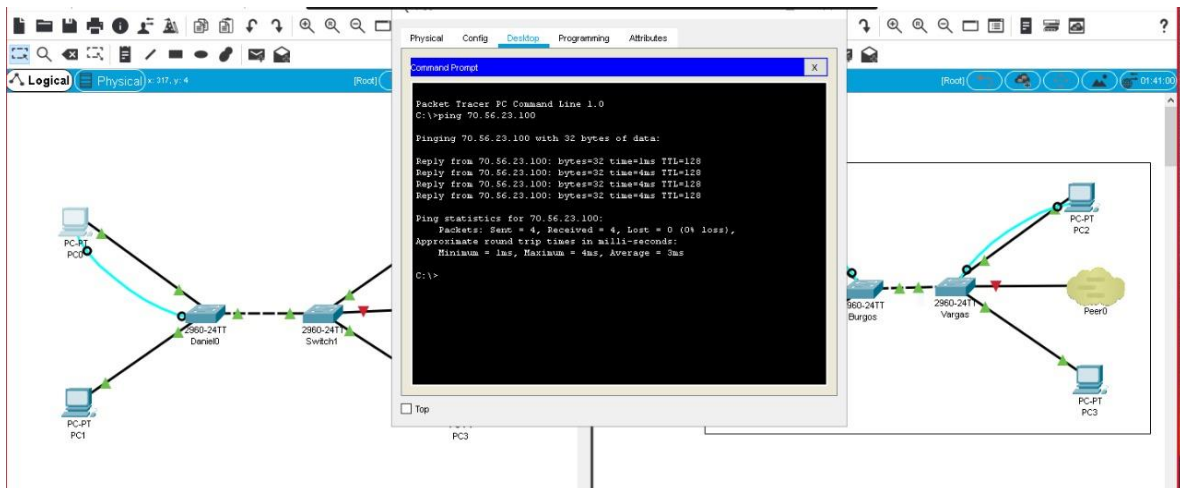
```

Daniel# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Daniel#

```

Figura 10. Guardando la configuración del equipo.

Nota: Se realizó la misma configuración en el segundo switch.



Por último, se realiza la conexión de los dos archivos, donde a mano izquierda se encuentra el archivo de Daniel Vargas y a mano Derecha el archivo de Brayan Burgos, donde, en el centro se verifica la conectividad por medio del comando ping de diferentes máquinas.

Redes de switches más grandes

En este caso no se será tan específico con el montaje, debido a que simplemente es lo mismo que en el punto anterior, configuración de Switches, equipos, cableados. Con se observa el primer montaje, realizado por el estudiante Brayan Burgos:

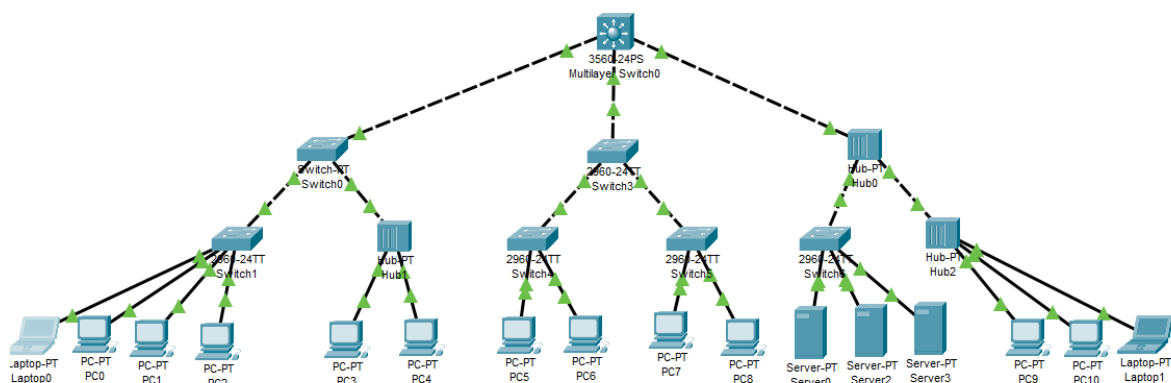


Figura 1. Montaje completo.

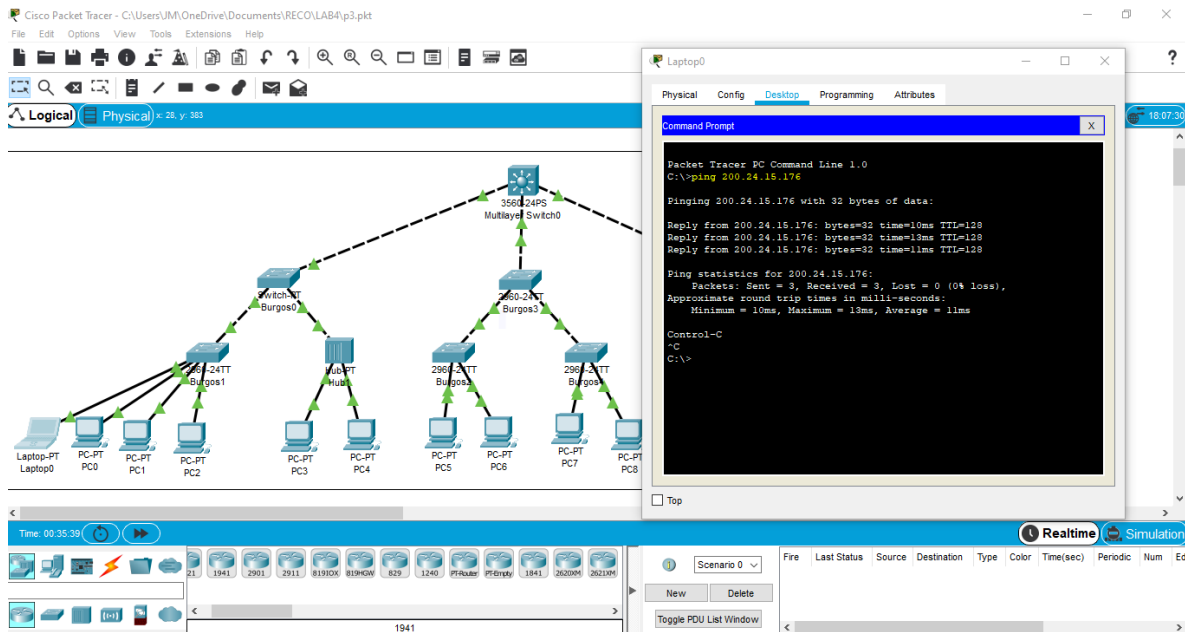


Figura 2. Verificación del ping.

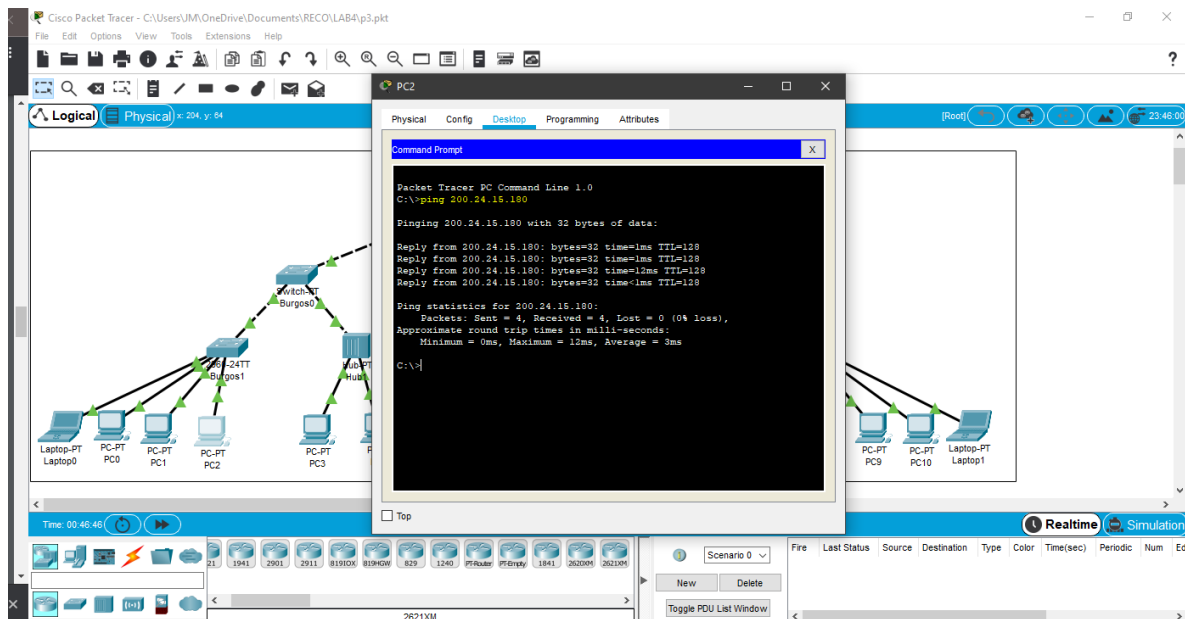


Figura 2. Verificación del ping2.

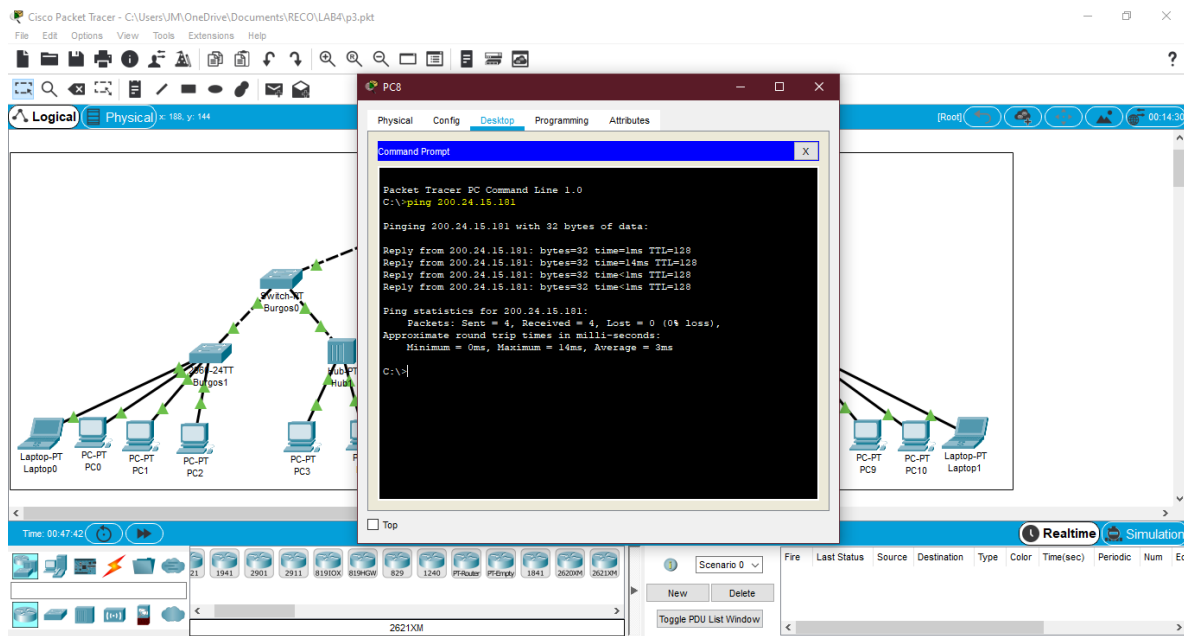


Figura 3. Verificación del ping 3.

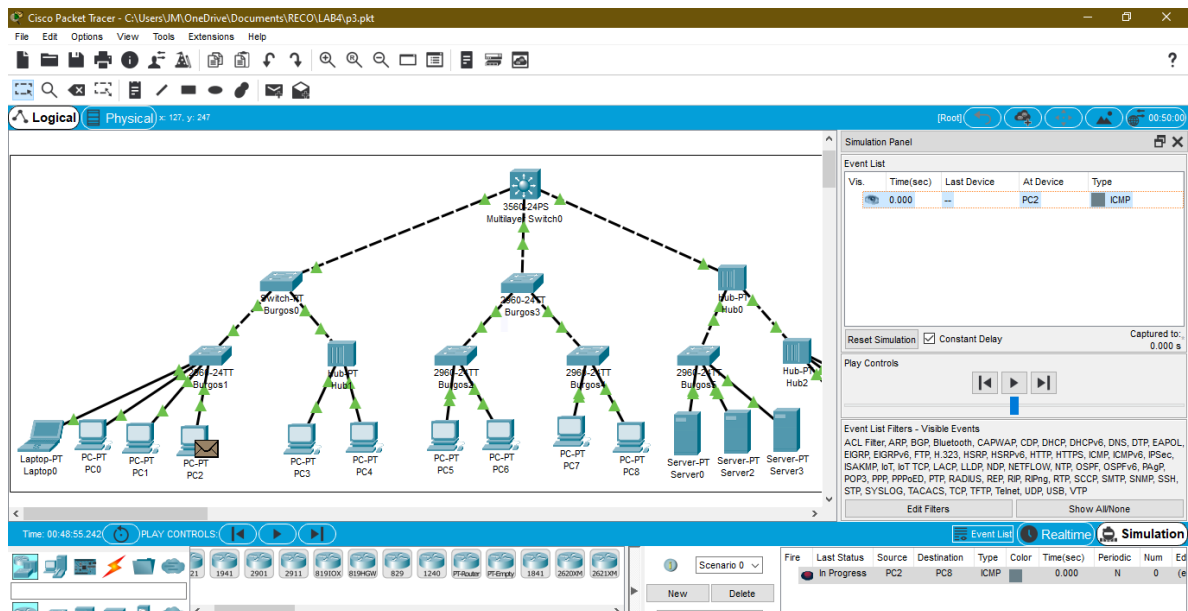


Figura 4. Verificación del ping4.

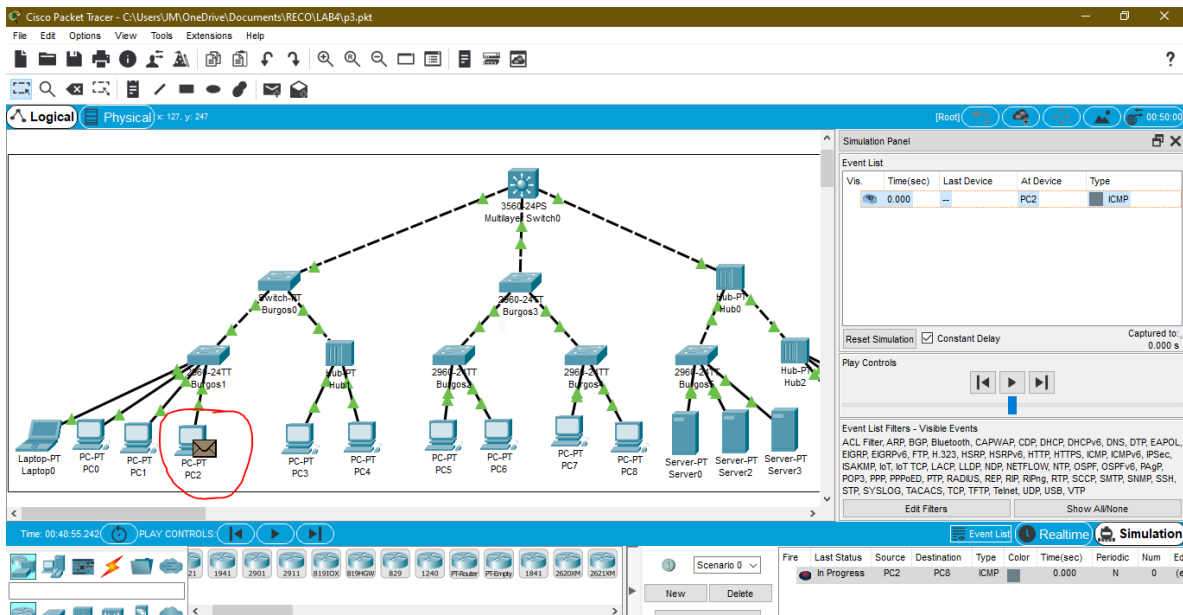


Figura 5. Envío de mensajes exitoso.

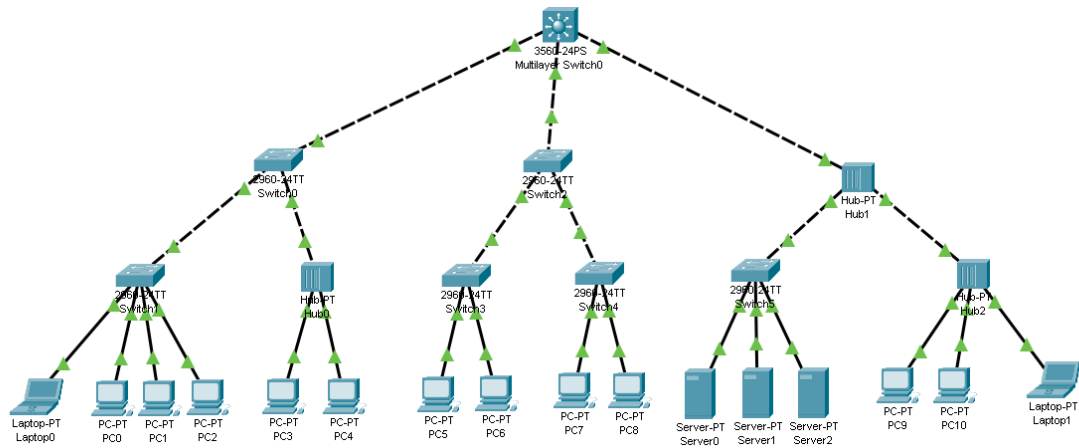


Figura 6. Montaje estudiante Daniel Vargas

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname Daniel
      ^
% Invalid input detected at '^' marker.

Switch(config)#hostname Daniel
Daniel(config)# banner motd # Este equipo es para uso exclusivo de
los estudiantes del Lab4 #
Daniel(config)# line console 0
Daniel(config-line)# logging synchronous
Daniel(config-line)# password CiscoC
Daniel(config-line)# login
Daniel(config-line)# exit
Daniel(config)#
Daniel(config)#
```

Figura 7. Primera parte de la configuración del switch multicapa.

```
Daniel(config)# line vty 0 15
Daniel(config-line)# logging synchronous
Daniel(config-line)# password CiscoT
Daniel(config-line)# login
Daniel(config-line)# exit
Daniel(config)# no ip domain-lookup
Daniel(config)# enable secret CiscoE
Daniel(config)# exit
Daniel#
%SYS-5-CONFIG_I: Configured from console by console

Daniel#copy running-config start up-config
      ^
% Invalid input detected at '^' marker.

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

Figura 8. Segunda parte de la configuración del switch multicapa

Nota: Se hizo la misma configuración para los 6 switches normales del montaje.

Estudiante1
IP: 200.24.15.x (x= número secuencial de 150 a 175)
Máscara: 255.255.0.0
Gateway: 200.24.15.1

Figura 9. Se uso este rango de direcciones IP para el montaje del estudiante Daniel Vargas

Figura 10. Ejemplo de la configuración IP de un equipo del montaje

```
C:\>ping 200.24.15.150

Pinging 200.24.15.150 with 32 bytes of data:

Reply from 200.24.15.150: bytes=32 time=1ms TTL=128
Reply from 200.24.15.150: bytes=32 time<1ms TTL=128
Reply from 200.24.15.150: bytes=32 time<1ms TTL=128
Reply from 200.24.15.150: bytes=32 time<1ms TTL=128

Ping statistics for 200.24.15.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 200.24.15.160

Pinging 200.24.15.160 with 32 bytes of data:

Reply from 200.24.15.160: bytes=32 time=28ms TTL=128
Reply from 200.24.15.160: bytes=32 time<1ms TTL=128
Reply from 200.24.15.160: bytes=32 time<1ms TTL=128
Reply from 200.24.15.160: bytes=32 time<1ms TTL=128

Ping statistics for 200.24.15.160:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 28ms, Average = 7ms

C:\>
```

Figura 11. Prueba de conectividad con dos equipos del montaje

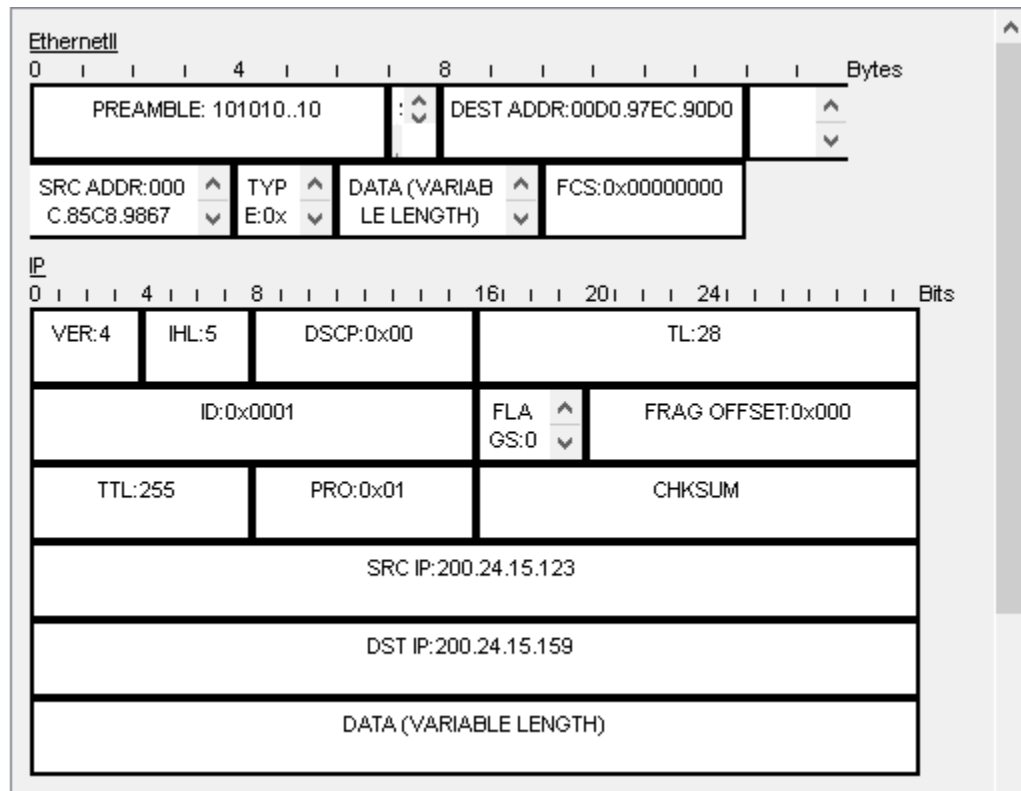


Figura 12. Encabezado de frame de PC2 a PC8

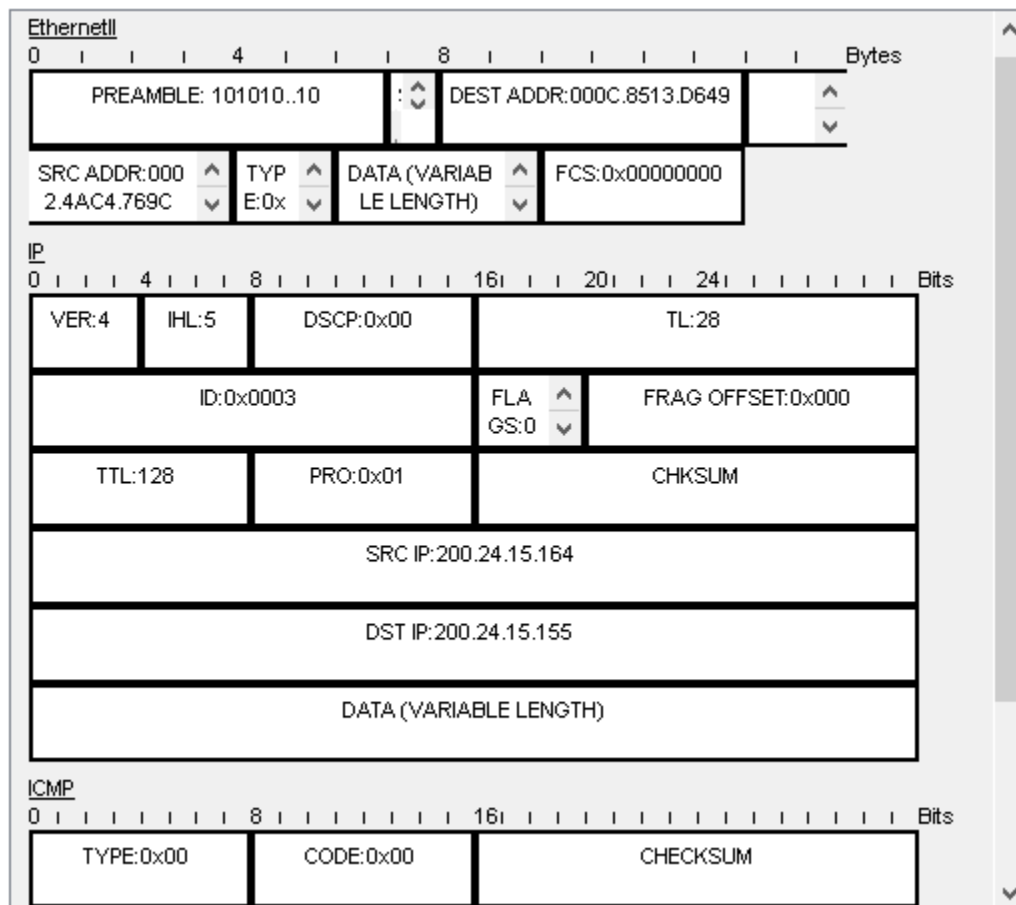


Figura 13. Encabezado de ethernet de PC4 a PC10

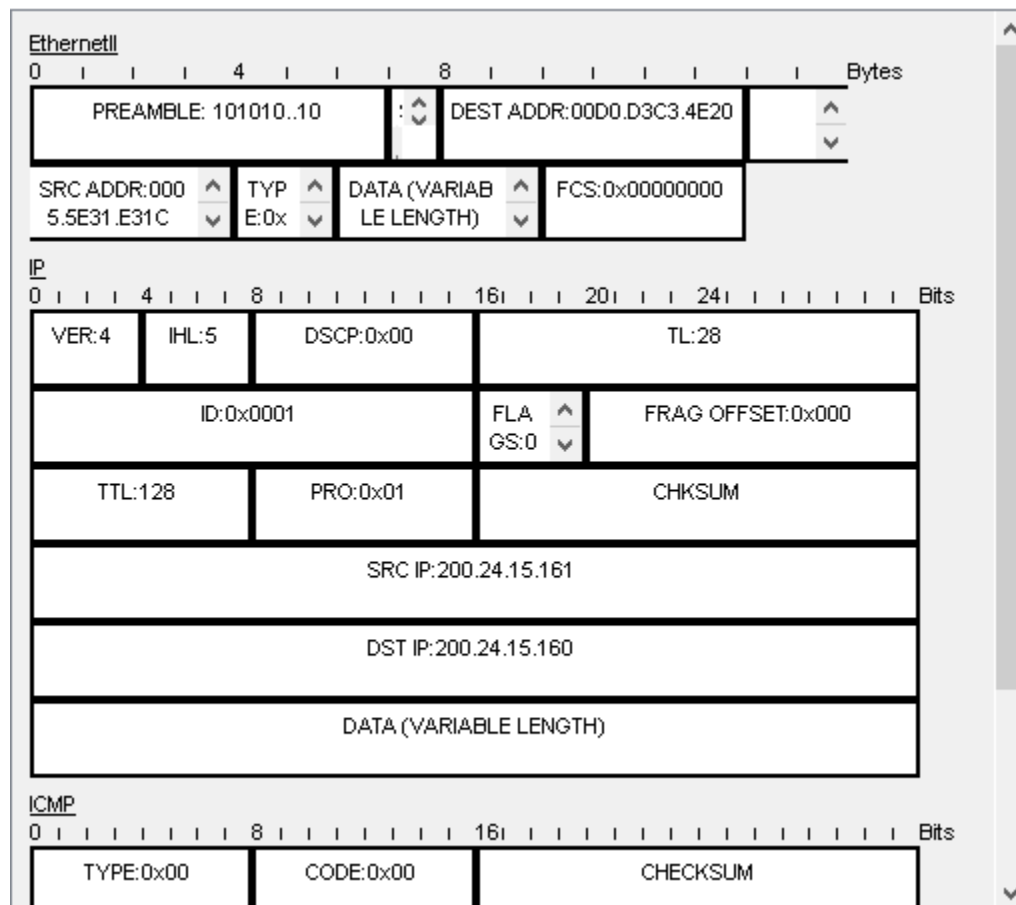


Figura 14. Encabezado de ethernet de Server0 a Server1

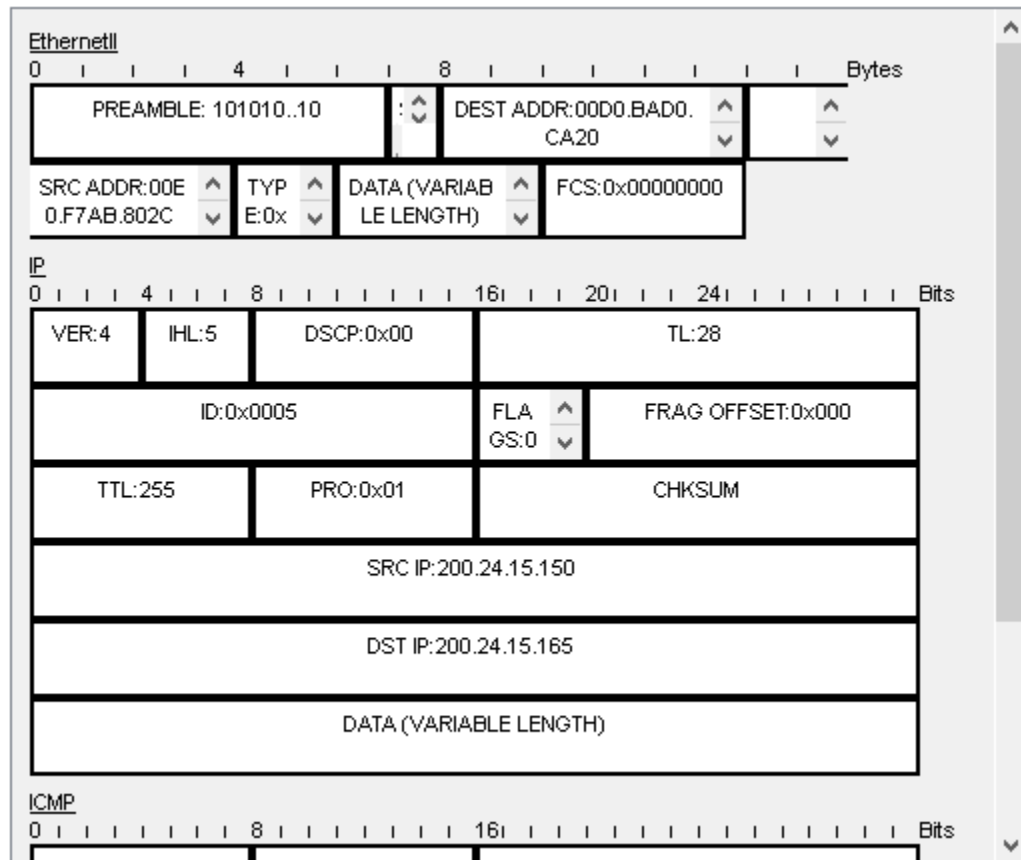


Figura 15. Encabezado de ethernet de Laptop0 a Laptop1

WireShark, tráfico de datos del campus virtual.

No. 1	Time 2	Source 3	Destination 4	Protocol 5	Length 6	Info 7
-------	--------	----------	---------------	------------	----------	--------

Estos son los datos que el programa logra capturar del tráfico de la red:

1. Numero consecutivo que genera para tener un orden en la captura de los datos.
2. Tiempo que transcurrió entre un paquete y otro, medido en segundos.
3. Source, indica quien genero el paquete, es decir, de donde vino el paquete, por medio de una dirección ip.
4. Destination, es para quien va el paquete, es decir el Receptor en este caso, al igual que la anterior, con una dirección IP.
5. Protocol, el protocolo al cual esta asociado el paquete que se trafico el medio.
6. La longitud del paquete.
7. Información adicional del paquete

```
C:\> Command Prompt

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::cc77:c7a2:7e4:5ff9%19
Autoconfiguration IPv4 Address. . : 169.254.95.249
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : Coship
IPv6 Address. . . . . : 2800:484:2989:600::9
IPv6 Address. . . . . : 2800:484:2989:600:ed72:fbb4:fe75:fd96
Temporary IPv6 Address. . . . . : 2800:484:2989:600:b120:dc33:2726:bbde
Temporary IPv6 Address. . . . . : 2800:484:2989:600:b5bb:162:cded:506e
Link-local IPv6 Address . . . . . : fe80::ed72:fbb4:fe75:fd96%8
IPv4 Address. . . . . : 192.168.0.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::96bf:95ff:fea9:7fe2%8
                             192.168.0.1

C:\Users\JM>
```

Figura 1 . Dirección IP del equipo donde se realizará el tráfico.

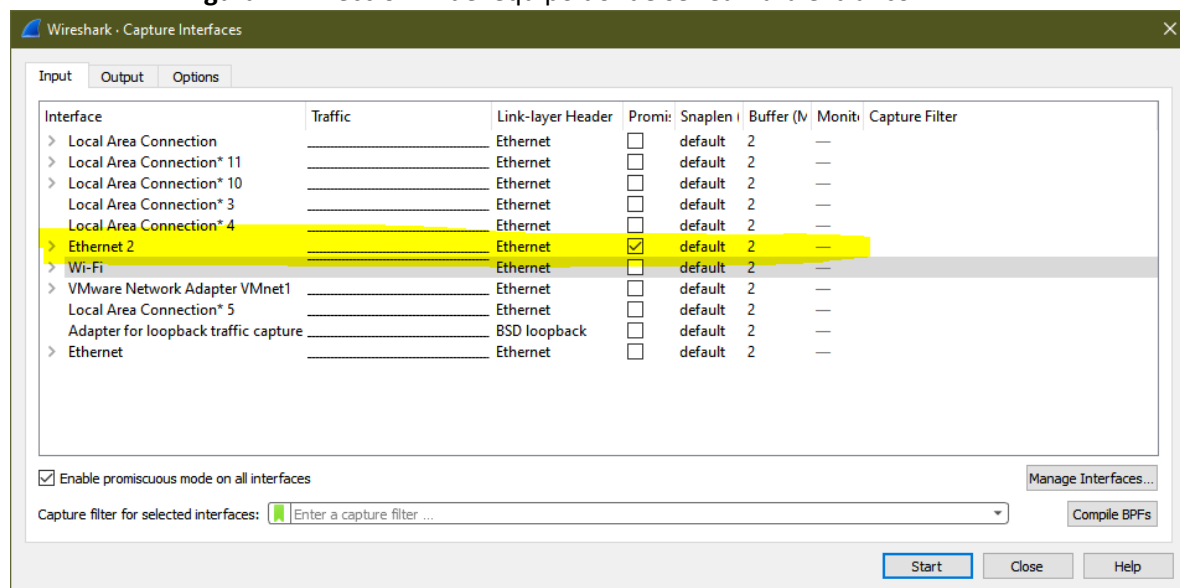


Figura 2. Se elige solo la red ethernet para visualizar el tráfico.

Wi-Fi

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	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
2	0.020072	45.239.88.93	192.168.0.4	TDS	966	Response
3	0.060704	192.168.0.4	45.239.88.93	TCP	54	55365 → 1433 [ACK] Seq=220 Ack=913 Win=252 Len=0
4	0.316338	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
5	0.330999	45.239.88.93	192.168.0.4	TDS	966	Response
6	0.331949	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call
7	0.347371	45.239.88.93	192.168.0.4	TDS	131	Response
8	0.347430	192.168.0.4	45.239.88.89	OpenVPN	96	MessageType: P_DATA_V2
9	0.368941	45.239.88.89	192.168.0.4	OpenVPN	96	MessageType: P_DATA_V2
10	0.400845	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=486 Ack=990 Win=256 Len=0
11	0.416410	192.168.0.4	45.239.88.89	TCP	54	54600 → 1194 [ACK] Seq=43 Ack=43 Win=251 Len=0
12	0.433264	192.168.0.4	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
13	0.434693	13.107.42.12	192.168.0.4	TCP	54	443 → 56076 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.532636	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
15	0.549438	45.239.88.93	192.168.0.4	TDS	966	Response
16	0.586190	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call
17	0.602901	45.239.88.93	192.168.0.4	TDS	131	Response
18	0.640273	192.168.0.4	45.239.88.93	TCP	54	55365 → 1433 [ACK] Seq=705 Ack=1902 Win=256 Len=0
19	0.831548	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
20	0.845105	45.239.88.93	192.168.0.4	TDS	966	Response
21	0.886719	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=705 Ack=1902 Win=252 Len=0
22	1.051224	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
23	1.071655	45.239.88.93	192.168.0.4	TDS	966	Response
24	1.118015	192.168.0.4	45.239.88.93	TCP	54	55365 → 1433 [ACK] Seq=924 Ack=2814 Win=252 Len=0
25	1.268287	fe80::96bf:95ff:fea... fe80::ed72:fb4:fe7...	ICMPv6	86	Neighbor Solicitation for fe80::ed72:fb4:fe75:fd96 from 94:bf:95:a9:7f:e2	
26	1.268527	fe80::ed72:fb4:fe7... fe80::96bf:95ff:fea...	ICMPv6	86	Neighbor Advertisement fe80::ed72:fb4:fe75:fd96 (sol, ovr) is at 00:db:df:8c:09:1a	
27	1.335813	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call
28	1.349648	45.239.88.93	192.168.0.4	TDS	131	Response
29	1.351957	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
30	1.369892	45.239.88.93	192.168.0.4	TDS	966	Response
31	1.420099	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=1190 Ack=2891 Win=256 Len=0
32	1.574066	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
33	1.580777	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call

Frame 13: 273 bytes on wire (2184 bits) 273 bytes captured (2184 bits) on interface \Device\NPF{3D0R12BA-CF7A-46F8-8FCE-2C43FE783521} id 0

wireshark_Wi-Fi_202009290032401_s20088.pcapng

Packets: 1341 · Displayed: 1341 (100.0%)

Profile: Default

Figura 2. Tráfico de datos.

En este caso se observa que la dirección IP que se enuncia en la figura 1, envía y recibe mensajes al equipo 45.239.88.89, donde la gran mayoría de sus equipos trabajan con protocolo TCP. Increíblemente, en 26.5 seg, se capturaron 1341 datos, como se observa en la siguiente imagen:

No.	Time	Source	Destination	Protocol	Length	Info
1310	24.771281	45.239.88.93	192.168.0.4	TDS	966	Response
1311	24.812254	192.168.0.4	45.239.88.93	TCP	54	56168 → 1433 [ACK] Seq=8300 Ack=21500 Win=64512 Len=0
1312	24.867030	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1313	24.886192	45.239.88.93	192.168.0.4	TDS	966	Response
1314	24.926771	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=22905 Ack=26539 Win=256 Len=0
1315	25.124602	192.168.0.4	172.217.172.10	UDP	75	59520 → 443 Len=33
1316	25.170299	172.217.172.10	192.168.0.4	UDP	67	443 → 59520 Len=25
1317	25.231091	192.168.0.4	172.217.30.206	UDP	75	56300 → 443 Len=33
1318	25.269642	172.217.30.206	192.168.0.4	UDP	67	443 → 56300 Len=25
1319	25.284793	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1320	25.306170	45.239.88.93	192.168.0.4	TDS	966	Response
1321	25.346812	192.168.0.4	45.239.88.93	TCP	54	56168 → 1433 [ACK] Seq=8519 Ack=22412 Win=65536 Len=0
1322	25.400472	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1323	25.416474	45.239.88.93	192.168.0.4	TDS	966	Response
1324	25.462697	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=23124 Ack=27451 Win=253 Len=0
1325	25.500754	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call
1326	25.518006	45.239.88.93	192.168.0.4	TDS	131	Response
1327	25.563012	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=23390 Ack=27528 Win=252 Len=0
1328	25.606407	192.168.0.4	45.239.88.93	TDS	320	Remote Procedure Call
1329	25.705286	45.239.88.93	192.168.0.4	TDS	131	Response
1330	25.748011	192.168.0.4	45.239.88.93	TCP	54	56168 → 1433 [ACK] Seq=8785 Ack=22489 Win=65536 Len=0
1331	25.807063	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1332	25.821851	45.239.88.93	192.168.0.4	TDS	966	Response
1333	25.861966	192.168.0.4	45.239.88.93	TCP	54	56168 → 1433 [ACK] Seq=9004 Ack=23401 Win=64512 Len=0
1334	25.917320	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1335	25.933569	45.239.88.93	192.168.0.4	TDS	966	Response
1336	25.985984	192.168.0.4	45.239.88.93	TCP	54	55508 → 1433 [ACK] Seq=23609 Ack=28440 Win=256 Len=0
1337	26.333743	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1338	26.349006	45.239.88.93	192.168.0.4	TDS	966	Response
1339	26.398611	192.168.0.4	45.239.88.93	TCP	54	56168 → 1433 [ACK] Seq=9223 Ack=24313 Win=65536 Len=0
1340	26.439571	192.168.0.4	45.239.88.93	TDS	273	Remote Procedure Call
1341	26.456497	45.239.88.93	192.168.0.4	TDS	966	Response

Figura 3. Número de datos.

No.	Time	Source	Destination	Protocol	Length	Info
136	5.927741	192.168.0.1	192.168.0.4	DNS	118	Standard query response 0x8d4e A safebrowsing.google.com CNAME sb.l.google.com A 172.217.173.46
137	5.927741	192.168.0.1	192.168.0.4	DNS	130	Standard query response 0x6664 AAAA safebrowsing.google.com CNAME sb.l.google.com AAAA 2800:3f0:4005:404::200e
463	8.803121	192.168.0.1	192.168.0.4	DNS	169	Standard query response 0xe142 AAAA www.mineduacion.gov.co SOA name1.mediacommerce.com.co
467	8.824848	192.168.0.1	192.168.0.4	DNS	176	Standard query response 0xadf6 AAAA www.colombiasaprende.edu.co SOA name1.mediacommerce.com.co
469	8.834826	192.168.0.1	192.168.0.4	DNS	149	Standard query response 0xc9df AAAA www.escuelaing.edu.co CNAME stark-cherimoya-jg38tzyu4qth9c74416vz0y.herokudns.c...
470	8.834826	192.168.0.1	192.168.0.4	DNS	277	Standard query response 0x462f A www.escuelaing.edu.co CNAME stark-cherimoya-jg38tzyu4qth9c74416vz0y.herokudns.c...
490	8.969801	192.168.0.1	192.168.0.4	DNS	133	Standard query response 0x2099 AAAA www.rumbo.edu.co SOA ns1.he.net
506	9.020768	192.168.0.1	192.168.0.4	DNS	123	Standard query response 0xbd27 A www.relps.org CNAME relpeapp.educ.gov.ar A 186.153.174.115
507	9.022644	192.168.0.1	192.168.0.4	DNS	107	Standard query response 0xa843 AAAA www.relps.org CNAME relpeapp.educ.gov.ar
716	10.023772	192.168.0.1	192.168.0.4	DNS	174	Standard query response 0x6788 A www.googleapis.com A 172.217.172.10 A 172.217.173.42 A 172.217.173.202 A 216.58...
719	10.028463	192.168.0.1	192.168.0.4	DNS	190	Standard query response 0x39ba AAAA www.googleapis.com AAAA 2800:3f0:4005:400::200a AAAA 2800:3f0:4005:401::200a ...
737	10.238618	192.168.0.1	192.168.0.4	DNS	112	Standard query response 0xccec A passwordsleakcheck-pa.googleapis.com A 172.217.173.202
738	10.238618	192.168.0.1	192.168.0.4	DNS	124	Standard query response 0x4b9a AAAA passwordsleakcheck-pa.googleapis.com AAAA 2800:3f0:4005:403::200a
800	11.181434	192.168.0.1	192.168.0.4	DNS	267	Standard query response 0xca04 AAAA d.docs.live.net CNAME odc-routekey-meta-geo.onedrive.akadns.net CNAME odc-rou...
822	11.428421	192.168.0.1	224.0.0.1	IGMPv2	46	Membership Query, general
951	13.696714	192.168.0.1	192.168.0.4	DNS	107	Standard query response 0xa6d5 AAAA bizagi.is.escuelaing.edu.co CNAME opalo.is.escuelaing.edu.co
1120	17.854572	192.168.0.1	192.168.0.4	DNS	126	Standard query response 0xff10 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.28.99
1121	17.855450	192.168.0.1	192.168.0.4	DNS	138	Standard query response 0xda1e AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com AAAA 2800:3f0:4005:40...

> Frame 136: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{3D812BAC-E574-46F8-8FCE-2C43EF7B3252}, id 0
 > Ethernet II, Src: Shenzhen_a9:7f:e2 (94:bf:95:a9:7f:e2), Dst: IntelCor_8c:09:1a (00:bd:df:8c:09:1a)
 > Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.4
 > User Datagram Protocol, Src Port: 53, Dst Port: 57676
 > Domain Name System (response)

Figura 4. Datos enviados por la maquina física ip figura 1.

Configuración VLANs

```

Daniel#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Daniel(config)#vlan VLAN_ID 50
      ^
% Invalid input detected at '^' marker.

Daniel(config)#vlan 50
Daniel(config-vlan)#name AtencionUsuario
Daniel(config-vlan)#end
Daniel#
%SYS-5-CONFIG_I: Configured from console by console

Daniel#
  
```

Figura 1. Creación de la VLAN AtencionUsuario

```

Daniel#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Daniel(config)#vlan 60
Daniel(config-vlan)#name Administracion
Daniel(config-vlan)#end
Daniel#
%SYS-5-CONFIG_I: Configured from console by console

Daniel#
  
```

Figura 2. Creación d la VLAN Administración

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
50 AtencionUsuario	active	
60 Administracion	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Figura 3. Revisión de las VLAN

Nota: Se repitió la creación de estas dos VLAN en el Switch #2

Daniel#show interface status					
Port	Name	Status	Vlan	Duplex	Speed
Type					
Fa0/1		connected	60	auto	auto
10/100BaseTX					
Fa0/2		connected	50	auto	auto

Figura 4. Configuración de interfaces para que usen las VLAN creadas.

Nota: Se repitió la configuración de interfaces en el segundo switch.

¿Qué son los enlaces troncales? ¿Para qué se usan?: Los enlaces troncales se configuran en uno o más puertos de un switch para permitir el paso del tráfico de las distintas VLANs. Este enlace puede funcionar en una conexión de switch a otro switch, de un switch a un router, e incluso de un switch a un servidor que soporte el estándar 802.1Q para permitir el tráfico de varias VLANs simultáneamente.

```
Daniel>enable
Password:
Daniel#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Daniel(config)#interface Fa 0/3
Daniel(config-if)#switchport mode trunk
```

Figura 5. Configuración de interfaz-enlace troncal.

Nota: Se repitió la configuración en la otra interfaz del switch.




Successful	PC0	PC2	ICMP		0.000	N	0	(edit)	(delete)
Failed	PC0	PC3	ICMP		0.000	N	1	(edit)	(delete)
Successful	PC1	PC3	ICMP		0.000	N	2	(edit)	(delete)

Figura 6. Verificación de conectividad (El paquete fallido es entre VLANs)

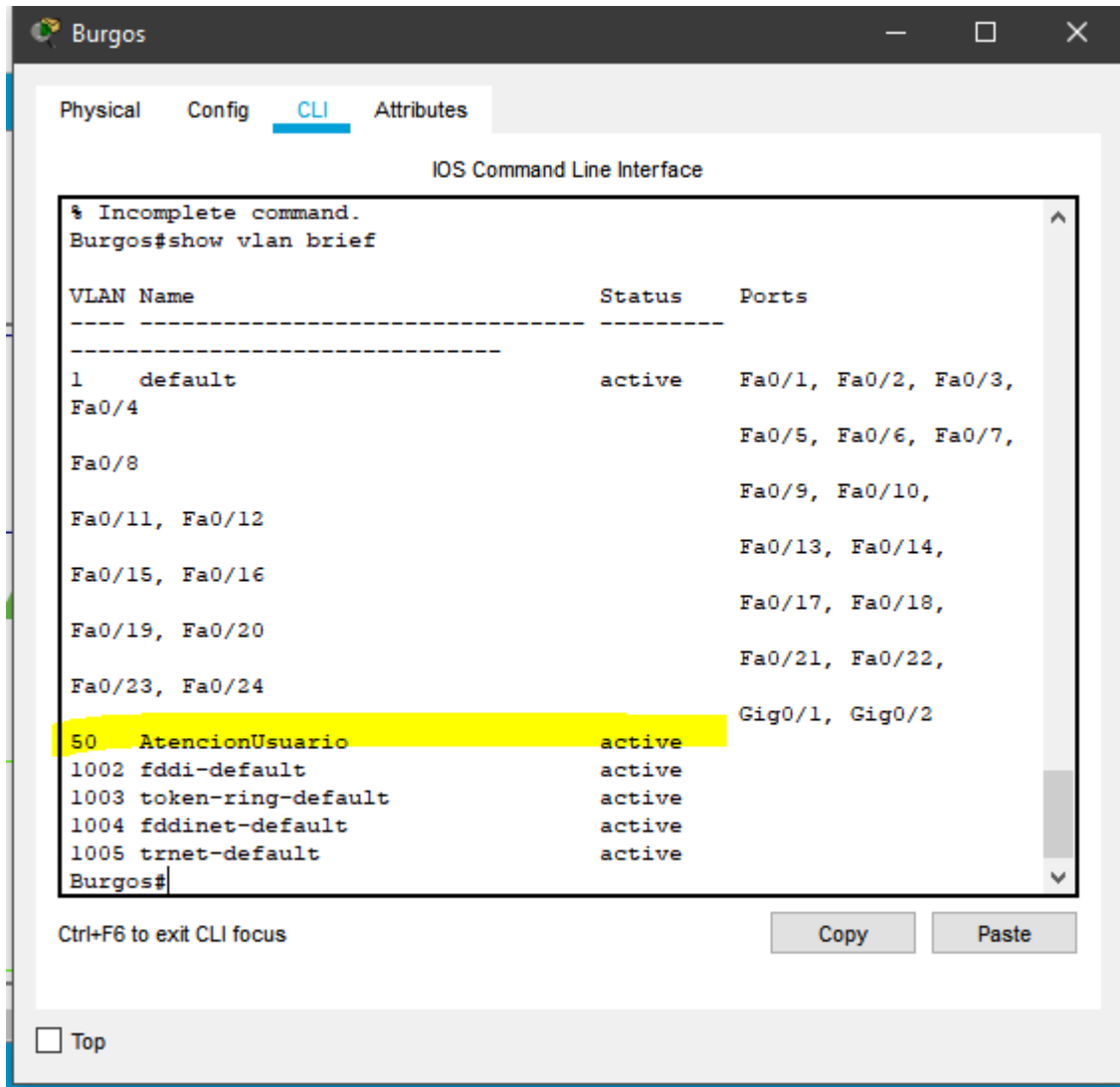


Figura 7. Configuración de la segunda Vlan para verificar configuración.

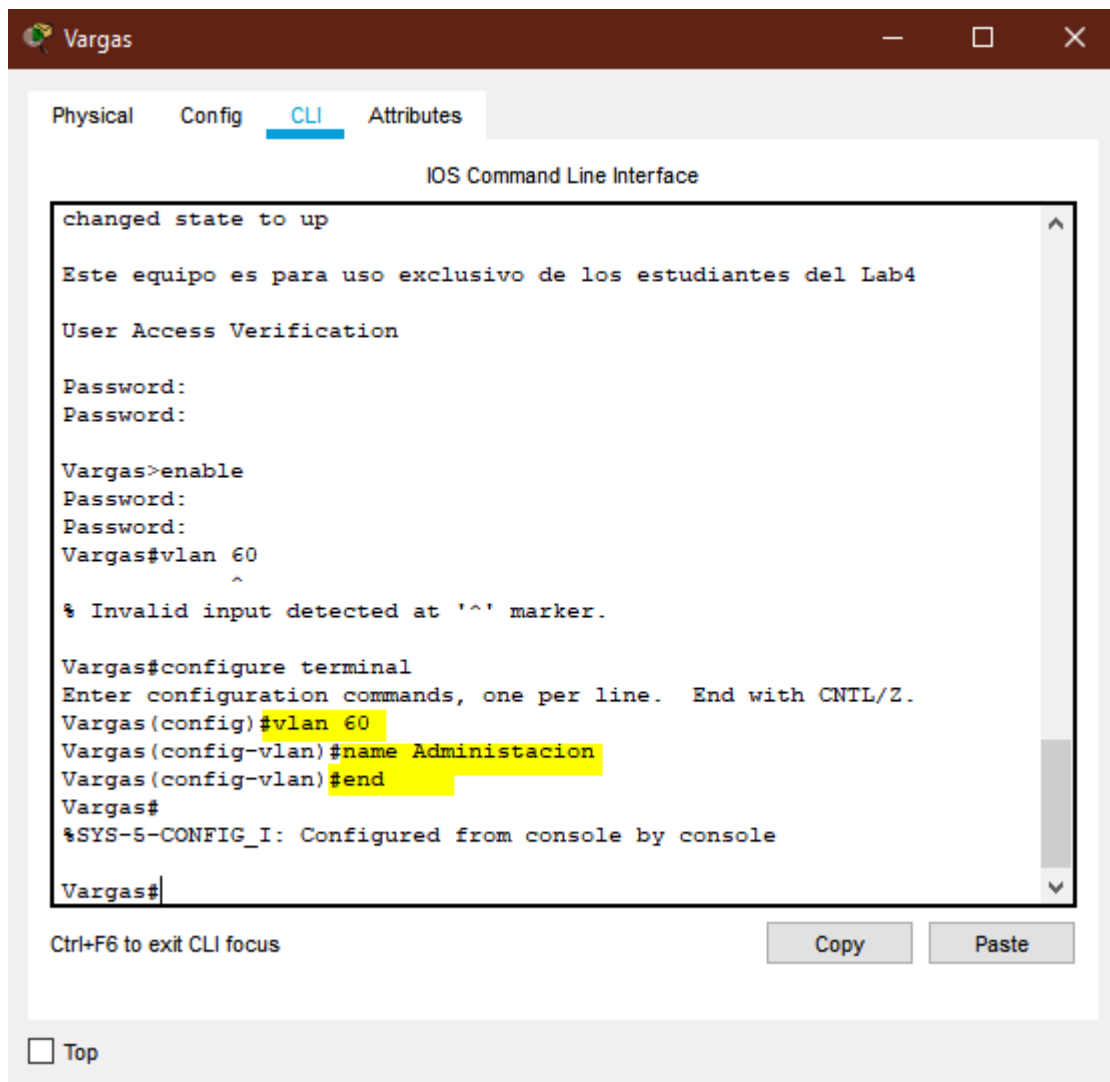


Figura 8. Configuración de las VLANs.

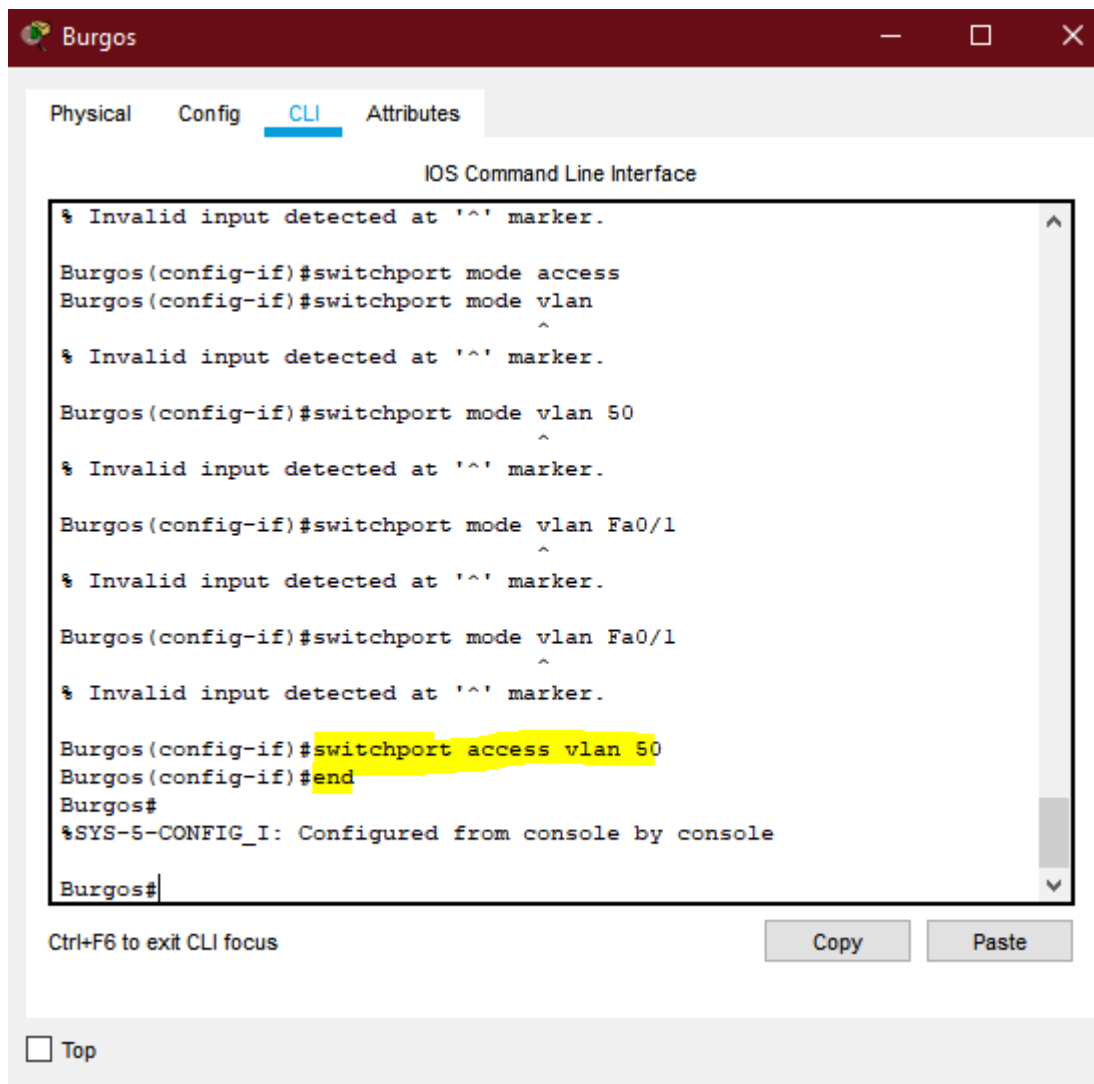


Figura 9. Configuración de las VLANs, switchport Access.

Revisión de frames con VLANs

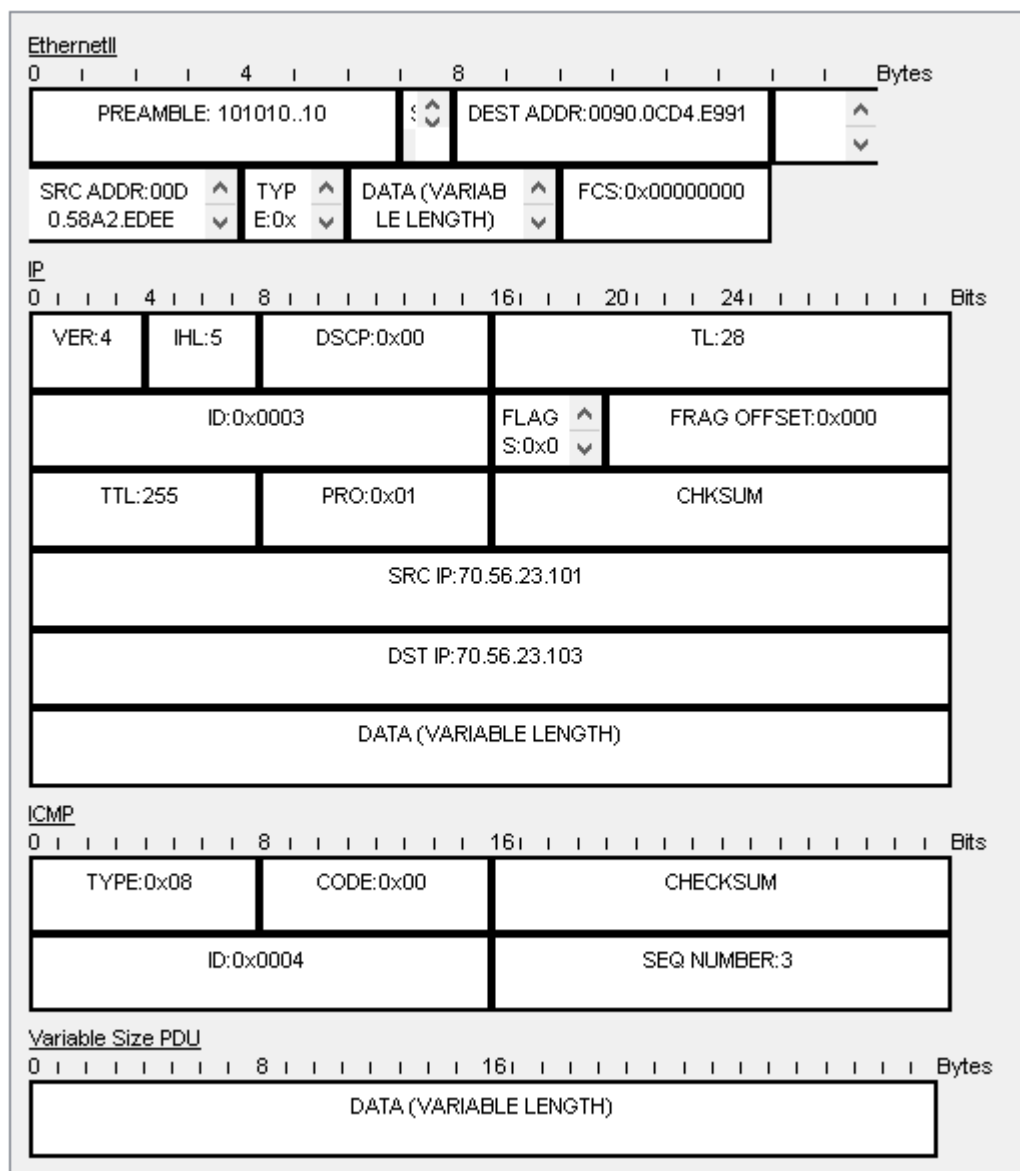


Figura 1. Encabezado del frame ethernet.

Configuración básica Wifi.

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server: ☒ Enabled ☐ Disabled

DHCP Reservation

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Figura 1. Configuración de IP de la red inalámbrica.

Network Mode: Mixed

Network Name (SSID): daniel_vargas

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: ☒ Enabled ☐ Disabled

Figura 2. Configuración de identificador de la red inalámbrica.

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: 20202R_Escuela

Key Renewal: 3600 seconds

Figura 30. Configuración de mecanismo de acceso a clientes inalámbricos y clave de acceso al router

¿Qué opción de canales puede configurar en cada router inalámbrico?

Usando el estándar IEEE 802.11 que regula las redes locales inalámbricas, se especificaron los rangos de frecuencia disponibles para que los dispositivos emitan sus señales: 2.4 GHz, 3.6 GHz y 5 GHz, donde actualmente a pesar de que muchos dispositivos son capaces de transmitir en la banda de frecuencia de 5 GHz, la banda de 2,4 GHz sigue siendo el estándar más habitual que las operadoras ofrecen a sus clientes y, por lo tanto, el más extendido.

La banda de frecuencia de transmisión de datos 2.4 GHz se divide en 14 canales de 20 Mhz cada uno, a través de los que se transmite toda la información entre el router y los dispositivos conectados a él. Entonces si vives en una casa aislada cualquiera de estos 14 canales servirá, pero cuando vives en una zona densamente poblada y todos tus vecinos tienen configurados sus routers para transmitir en el mismo canal de frecuencia que usas tú, entonces la velocidad de la conexión a Internet puede variar mucho en función del

canal WiFi que tengamos seleccionado en el router, donde para conseguir la máxima velocidad para tu Wi-Fi, debes elegir el canal menos masificado para que los datos que transmiten entre tus dispositivos y el router sufran el mínimo de interferencias posible. No obstante, dentro de esos 14 canales existen tres que ofrecen un rendimiento por encima del resto ya que no se solapan entre sí ya que no se tocan en el espectro de frecuencia: 1, 6 y 11. Por lo tanto, su elección debe priorizarse. Pero si tienes un router de 5 GHz y tus dispositivos lo soportan, esta es la mejor opción porque sus canales no se solapan y como es un estándar que todavía no se utiliza demasiado hace que exista una menor “competencia” con tus vecinos sobre la misma banda, por lo cual mejorará la velocidad y estabilidad de la red Wi-Fi en tu casa, además es posible que también incluya tecnologías de doble banda que permiten transferir tus datos a través de varios canales simultáneamente, por lo que se mejorará su eficiencia.

Port 1

Port Status ☒

SSID AP_DanielVargas

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase 2020A_Escuela

User ID

Password

Encryption Type AES

Figura 3. SSID y clave del Access point.}

Wireless0

Port Status

Bandwidth 300 Mbps

MAC Address 0090.21B3.26ED

SSID daniel_vargas

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase 20202R_Escuela

☐ WPA ☐ WPA2

User ID

Password

☐ 802.1X Method: MD5

User Name

Password

Encryption Type AES

Figura 4. Conectando el celular al router.

Port Status

Bandwidth 300 Mbps

MAC Address 0002.4A46.6C6C

SSID daniel_vargas

Authentication

☐ Disabled ☐ WEP WEP Key

☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase 20202R_Escuela

☐ WPA ☐ WPA2 User ID

☐ 802.1X Method: MD5 Password

User Name

Password

Encryption Type AES

Figura 5. Conectando la laptop al router.

Nota: Se hicieron pasos similares para la conexión del segundo celular y laptop al Access point.

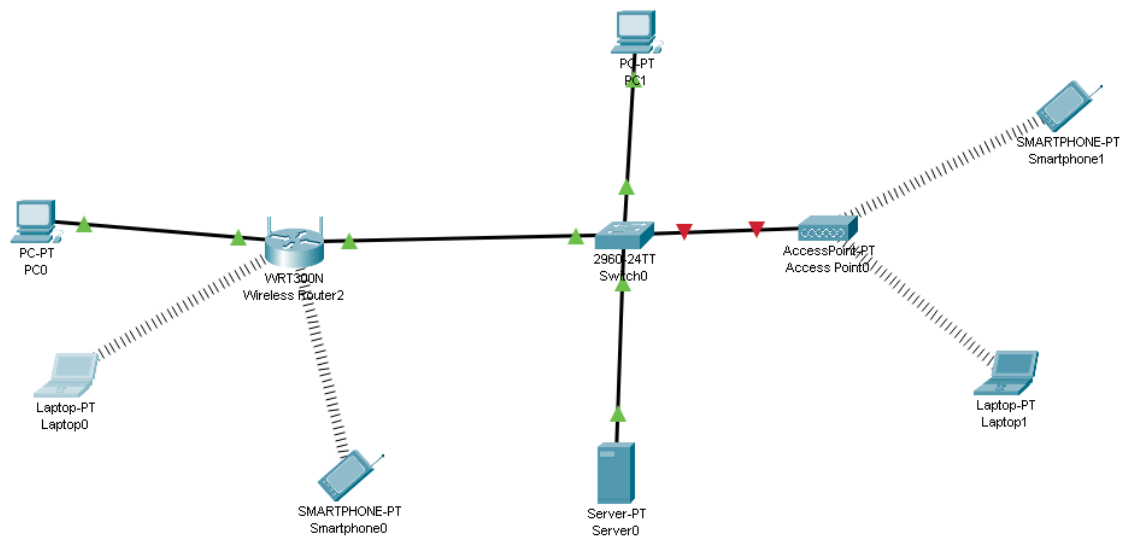


Figura 6. Montaje completo.

	Successful	Laptop0	Smartphone1	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Smart...	Laptop1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Smart...	Smartphone1	ICMP		0.000	N	3	(edit)	(delete)

Figura 7. Revision de algunos pasos de mensajes.

¿Entre cuáles equipos se puede hacer ping? ¿por qué?:

Se puede hacer ping entre la laptop0 y el celular 1 pero no se puede hacer ping desde pc0 a laptop1 porque solo se puede hacer ping entre equipos conectados al mismo router o al mismo acceso point.

Configuración de LAN alámbrica e inalámbrica

Wireless Settings	
SSID	Visitantes
2.4 GHz Channel	6 - 2.437GHz
Authentication	
<input checked="" type="radio"/> Disabled	<input type="radio"/> WEP
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK
<input type="radio"/> WPA	<input type="radio"/> WPA2
WEP Key	
PSK Pass Phrase	
RADIUS Server Settings	
IP Address	
Shared Secret	
Encryption Type	Disabled

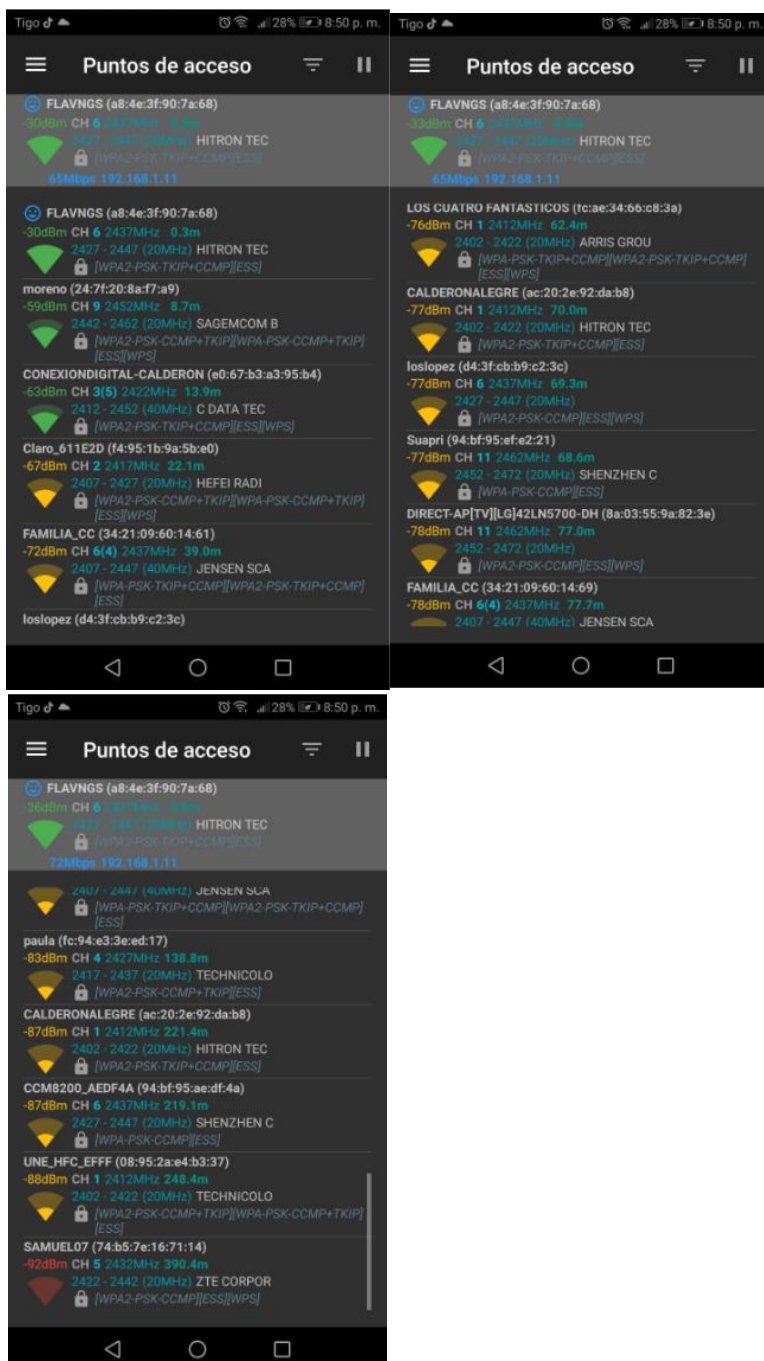
Figura 1. Configuración red inalámbrica azul

Port 1	
Port Status	<input checked="" type="checkbox"/>
SSID	Empleados
2.4 GHz Channel	6
Coverage Range (meters)	140,00
Authentication	
<input type="radio"/> Disabled	<input type="radio"/> WEP
<input type="radio"/> WPA-PSK	<input checked="" type="radio"/> WPA2-PSK
WEP Key	
PSK Pass Phrase	
ClaveSegura	
User ID	
Password	
Encryption Type	AES

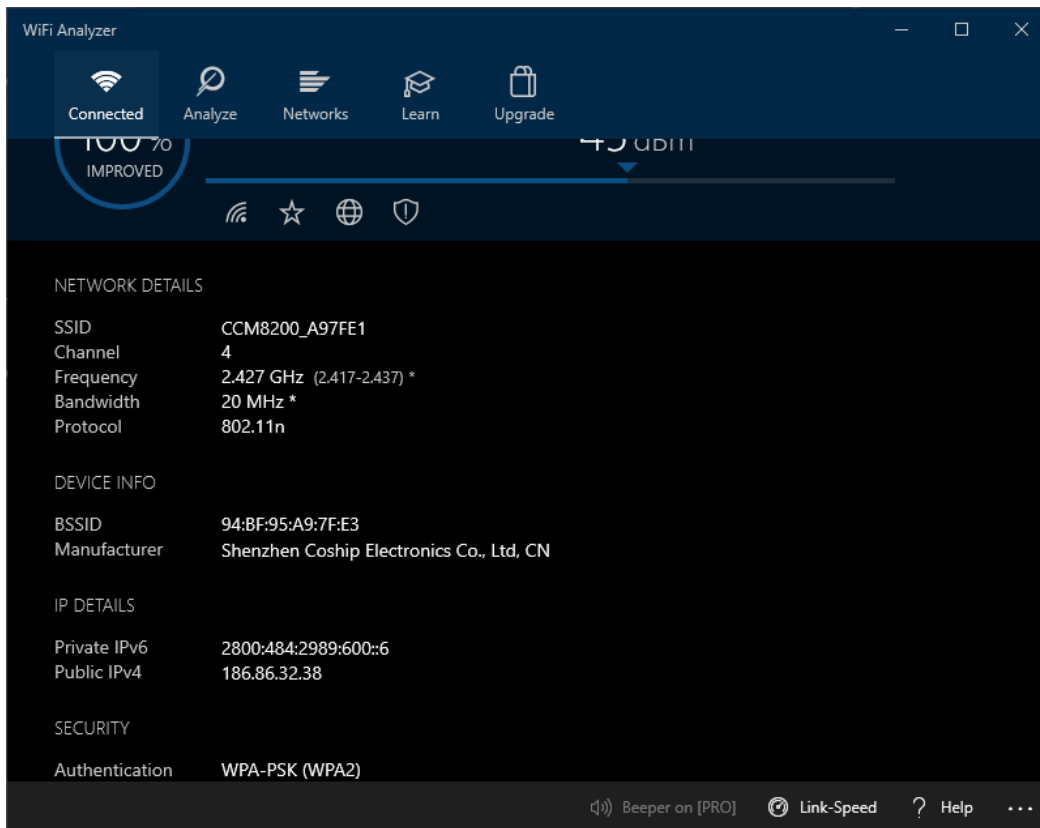
Figura 2. Configuración red inalámbrica rosa

Nota: Se configuraron todos los switches como en los puntos anteriores, se crearon las VLANs y se designó dispositivos de manera que se conectarán a la VLAN que le correspondiera a cada uno. Se realizaron los enlaces troncales también como se explicó antes.

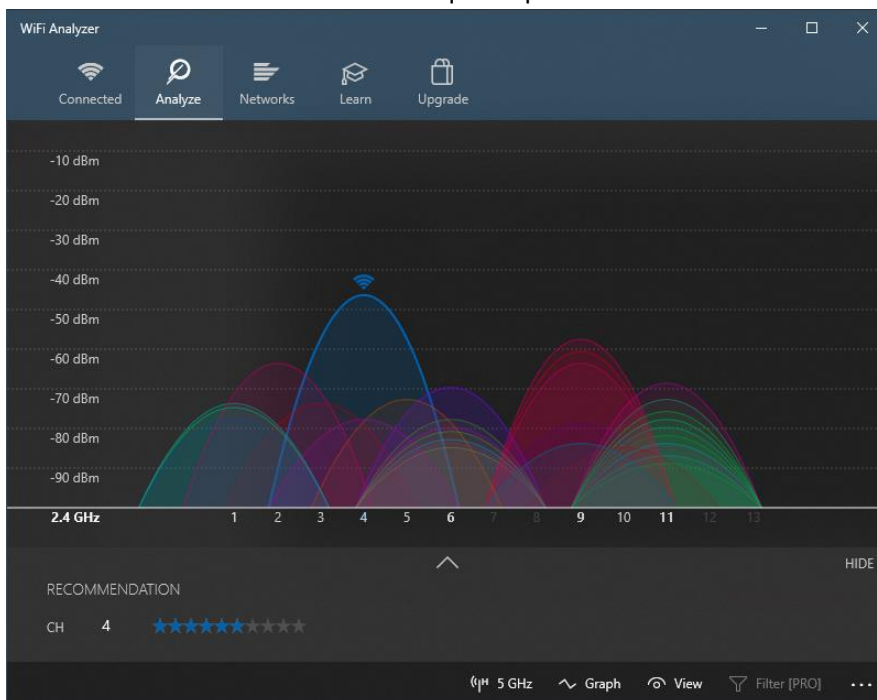
Revisión de las Wifi reales



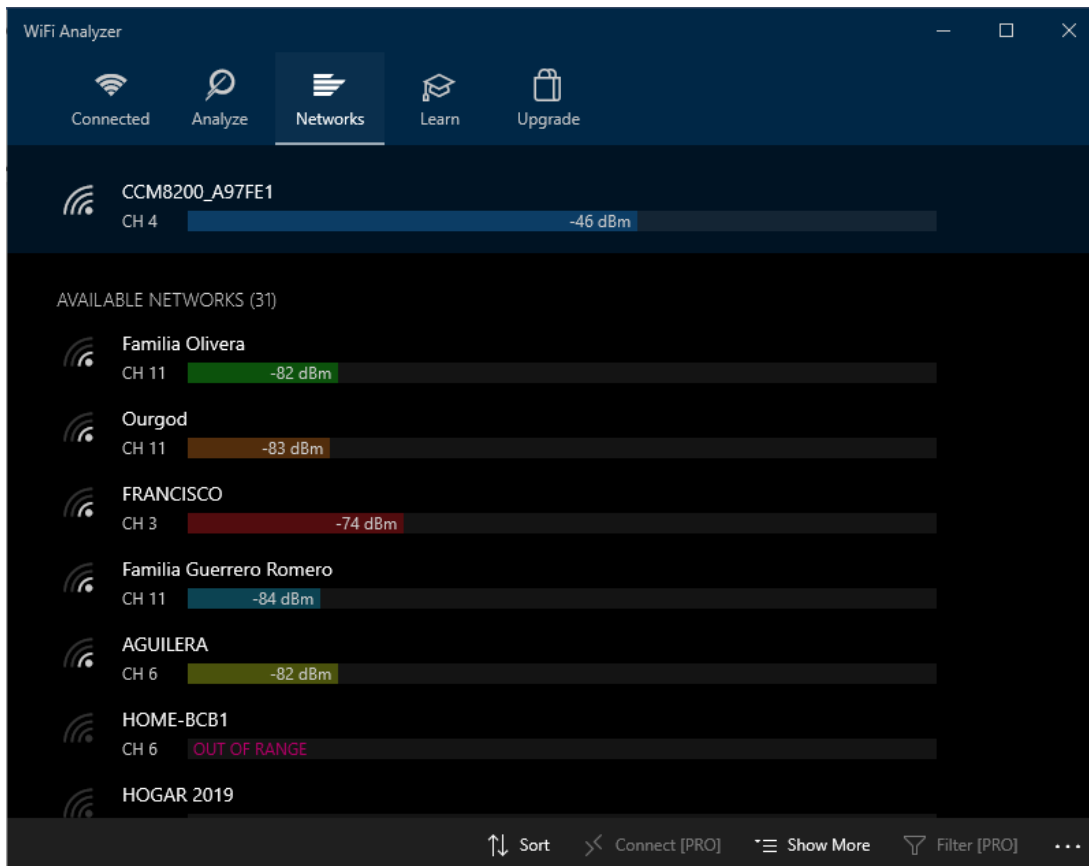
En mi red no se encuentran bandas que operen en los rangos dados, de las encontradas se pueden leer varios canales, por ejemplo, CH6, CH11, CH1. De las bandas de red encontradas todas se encuentran entre los 20 MHz a los 40MHz y se aprecia las redes por ejemplo la de mi casa se llama FLAVNGS que significa Familia Vanegas, el apellido de mi madre.



Se uso una aplicación de Microsoft llamada Wifi Analyzer y resultado ser mas interesante debido a la información que se puede extraer de este analizador.



Por ejemplo, en este caso vemos una gráfica que muestra la cantidad de GHZ vs el rango que permite la red



Aquí se ven las redes disponibles donde se ve los dBm de las redes que transitan por el espacio cercano al computador que estamos explorando.

Shells- Oracle en Centos.

```
#!/bin/bash

echo '=====
echo '          MENU
echo '=====
read -p "Escriba la tarea que quiere realizar: " tarea
echo "¿Que minuto? (0-50) o * para todos los minutos de una hora "
read -p "" minuto
echo "¿Que hora? (0-23) o * para todas las horas del dia "
read -p "" hora
echo "¿Que dia del mes? (1-31) o * para todos los dias del mes "
read -p "" diaMes
echo "¿Que mes? (1-12) o * para todos los meses "
read -p "" mes
echo "¿Que dia de la semana? (0-6) donde 0 es domingo o * para todos los dias de la semana "
read -p "" diaSemana

$2 $3 $4 $5 $6 $1
echo $tarea
```

- **Netstat:** Herramienta de la línea de comandos útil para controlar las conexiones de red entrantes y salientes, visualizar las tablas de enrutamiento, estadísticas de la interfaz, etc.. En CentOS la equivalencia es ss
- **Vnstat:** Es una línea de comandos que muestra y registra el tráfico de red de las interfaces en sus sistemas, dependiendo de las estadísticas de red proporcionadas por el núcleo, por ende, no agrega ninguna carga adicional a su sistema para monitorear y registrar el tráfico de la red.
- **Route:** El comando route se usa para mostrar/manipular la tabla de enrutamiento IP, principalmente se usa para configurar rutas estáticas a hosts o redes específicas a través de una interfaz.
- **Ethtool:** El comando ethtool se usa para mostrar/cambiar la configuración del adaptador Ethernet, puede cambiar la velocidad de la tarjeta de red, la negociación automática, la configuración de activación en LAN y el modo dúplex.

Oracle- Instalación base

```
[root@localhost Shells]# chkconfig --list

Nota: Esta salida muestra sólo servicios SysV y no incluye servicios nativos
de systemd. Los datos de configuración SysV pueden verse invalidados por
la configuración nativa de systemd.

Si desea una lista de servicios systemd use 'systemctl list-unit-files'.
Para ver los servicios que se activan para un objetivo concreto use
'systemctl list-dependencies [objetivo]'.

networkd      0:desactivado  1:desactivado  2:desactivado  3:desactivado  4:desactivado  5:de
sactivado     6:desactivado
network       0:desactivado  1:desactivado  2:activo       3:activo       4:activo       5:ac
tivo         6:desactivado
oracle-xe     0:desactivado  1:activo       2:activo       3:activo       4:activo       5:ac
tivo         6:desactivado
[root@localhost Shells]# chkconfig --level 0 oracle-xe on
[root@localhost Shells]# chkconfig --list
```

Figura 1. Listamos los chkconfig y miramos cual debemos activar

```
[root@localhost Shells]# chkconfig --level 0 oracle-xe on
```

Figura 2. Lo activamos y revisamos de nuevo.

```
[root@localhost Shells]# chkconfig --list

Nota: Esta salida muestra sólo servicios SysV y no incluye servicios nativos
de systemd. Los datos de configuración SysV pueden verse invalidados por
la configuración nativa de systemd.

Si desea una lista de servicios systemd use 'systemctl list-unit-files'.
Para ver los servicios que se activan para un objetivo concreto use
'systemctl list-dependencies [objetivo]'.

networkd      0:desactivado  1:desactivado  2:desactivado  3:desactivado  4:desactivado  5:de
sactivado     6:desactivado
network       0:desactivado  1:desactivado  2:activo       3:activo       4:activo       5:ac
tivo         6:desactivado
oracle-xe     0:activo       1:activo       2:activo       3:activo       4:activo       5:ac
tivo         6:desactivado
[root@localhost Shells]#
```

Figura 3. Revisamos que quedo activado al inicio de CentOS

Conclusiones.

- Se fortaleció el concepto trabajado en anteriores laboratorios y las configuraciones básicas de IPs en equipos de packet tracer.
- Se aprendió el procedimiento para configurar switches desde el terminal usando comandos estándar, no se usó el modo configuración de packet tracer ya que en la práctica no se pueden configurar los switches así.
- Se aprendió a realizar la conexión multiusuario que ofrece packet tracer
- Se estudió los formatos de frame que usa ethernet y se identificó sus componentes
- Se aprendió a configurar las VLANs en packet tracer, se estudió sobre los enlaces troncales. Además, se revisó los encabezados del frame ethernet por VLAN
- Se configuró VLANs a través de redes inalámbricas, se identificó estas redes, sus componentes, bandas y canales de estas.
- Estudiamos 6 nuevos comandos útiles en Linux con los cuales se realizaron unos Shell muy útiles.
- Configuramos de manera exitosa Oracle para que se iniciara con el arranque del sistema operativo y se intentó conectar de manera remota a esta base de datos.

Bibliografía.

- [1]enlaces troncales de vlans<https://sites.google.com/site/paginamodulo3vlan/3-2-enlaces-troncales>
- [2]configuración de Switch <https://www.redeszone.net/tutoriales/redes-cable/configurar-enlace-troncal-switch/>
- [3]Comandos de ejemplo <https://linuxide.com/linux-how-to/ethtool-command-with-examples/>