



**Escuela de  
Ingeniería y Arquitectura**  
**Universidad Zaragoza**

dar-pr-3

## Diseño y administración de redes

Autor 1:	Toral Pallás, Héctor - 798095
Autor 2:	Lahoz Bernad, Fernando - 800989
Autor 3:	Martínez Lahoz, Sergio - 801621
Grado:	Ingeniería Informática
Curso:	2023-2024

9 de octubre de 2023

# Índice

1. Pregunta 1	3
2. Pregunta 2	5
3. Pregunta 3	7
4. Pregunta 4	8
5. Pregunta 5	9
6. Pregunta 6	10
7. Pregunta 7	11
8. Pregunta 8	12
9. Pregunta 9	13
10.Pregunta 10	14
11.Pregunta 11	15
12.Pregunta 12	16

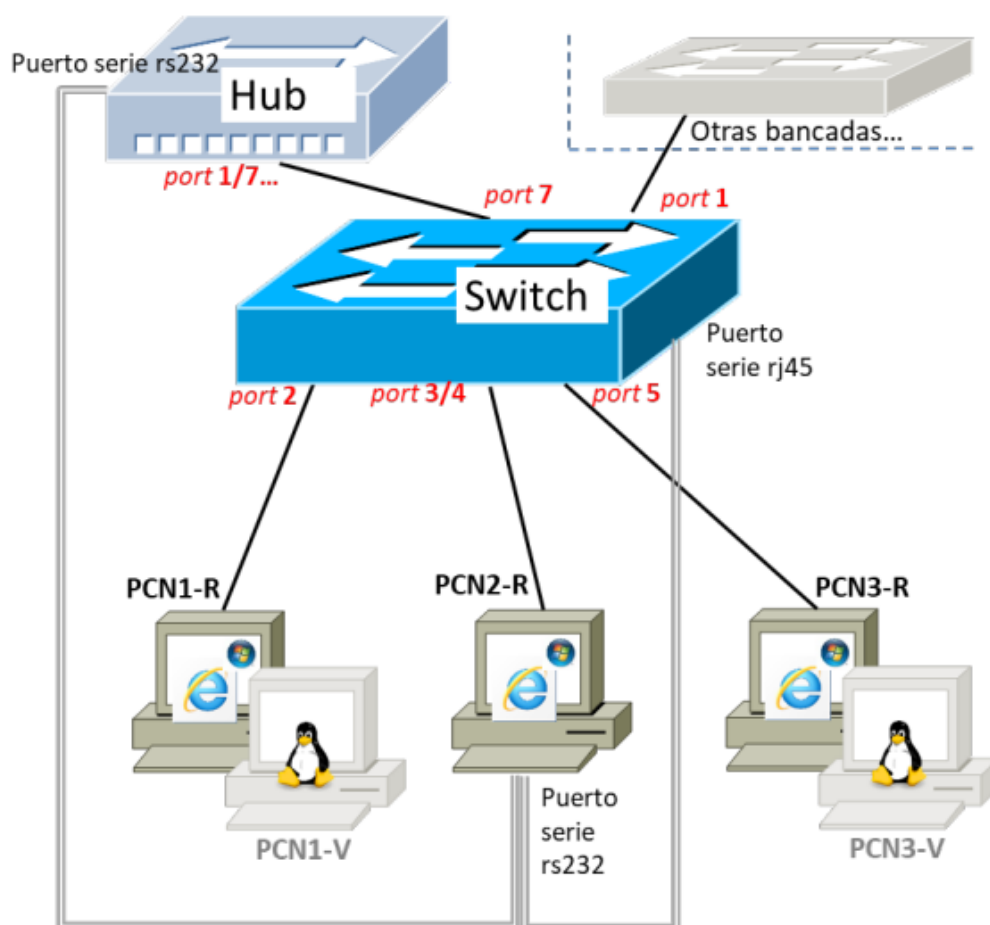


Figura 1: Escenario de interconexión de redes para la bancada N.

01

## Pregunta 1

Identifica la dirección MAC del conmutador, ¿por qué crees que es necesaria? Vamos a entrar en el resto de pestañas (Polling interval, Display Filter y Color Key) y ver la información correspondiente.

La dirección MAC del conmutador es la dirección del interfaz VLAN1 que se nos muestra en el dibujo de la figura 2, la cual pertenece al módulo de management. Es un identificador único asignado a la interfaz de red del dispositivo. Esta dirección se utiliza para comunicarse dentro de una red local, por lo que sin ella, no se podría conectar los dispositivos de la red local entre sí. Para identificar la MAC del conmutador, lo que hemos hecho ha sido meternos en la configuración del switch y seleccionando la pestaña *Device Summary* en la página de configuración del switch (figura 3), se ha obtenido la dirección MAC: **00-1E-C1-CF-09-C0**.

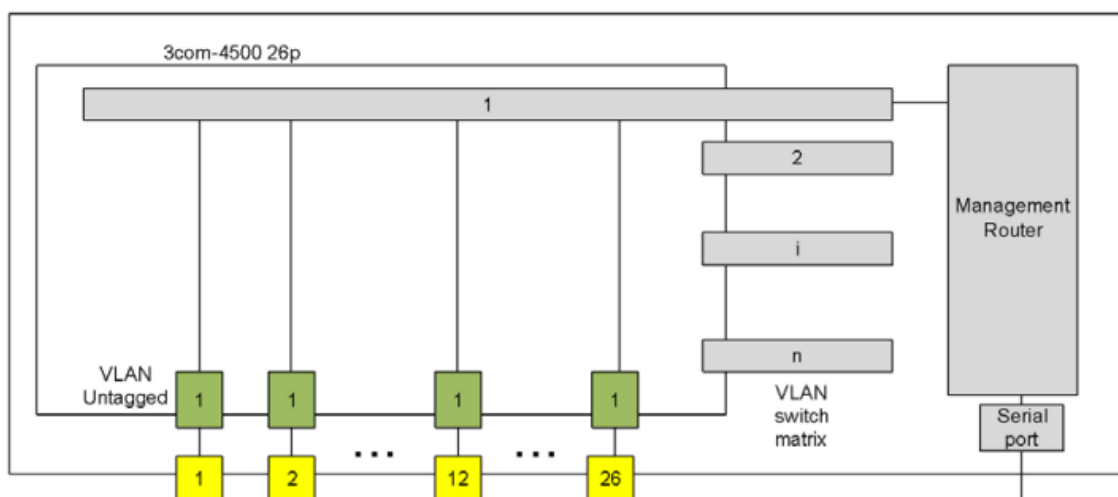


Figura 2: Esquema del switch.

Device Summary Information for Unit1			
Product Description:	3Com Switch 4500 26-Port Software Version 3Com OS V3.03.00s56		
System Location:	Marlborough, MA 01752 USA		
System Contact:	3Com Corporation		
Serial Number:	YECF9WMCF09C0		
Product 3C Number:	3CR17561-91		
MAC Address:	00-1E-C1-CF-09-C0		
Software Version:	3.03.00s56	Bootrom Version:	3.00
Unit Uptime:	70 Days 3 hours 14 minutes 44 seconds	Hardware Version:	00.00.00

Figura 3: Resumen del dispositivo. MAC localizable en el campo MAC Address.

**Polling Interval:** Esta configuración determina cada cuánto tiempo el software o la herramienta de monitoreo verifica el estado del conmutador para recopilar datos. En la figura 4 se puede ver que el intervalo configurado es de 30 segundos.

**Display Filter:** Esta opción te permite filtrar la información que se muestra en la interfaz de monitoreo.



















**Color Key:** En el esquema de colores se explica el significado de cada color utilizado. En la figura 12 se muestra esta pestaña, en la que se ve que el color blanco significa desconectado, el amarillo baja velocidad y el verde velocidad máxima, entre otras cosas.

Device View | **Polling Interval** | Display Filter | Color Key

Please enter a number between 10 and 180 seconds for polling interval, or enter 0 to disable polling:

Figura 4: Tasa de refresco.

Device View | Polling Interval | Display Filter | **Color Key**

Ports			Meaning
RJ45	SFP	10G	
			White: Unconnected. No link detected.
			Yellow: Lower speed on 10/100/1000M capable port.
			Green: Maximum speed 10/100/1000M RJ45, RJ45 SFP or 10G. Link detected.
			Dark Gray: SX SFP. Link detected.
			Light Blue: LX/ZX SFP. Link detected.
			Light Gray: Port has been set to inactive by User or Protocol.
			Dark Blue: Port has been selected by user or highlighted by the Display Filter.
			Red: Port or Module has failed POST or module is not recognized.

Description of port number:

- **Single:** Port number.
- **Underline:** Aggregation number.

Figura 5: Esquema de colores.

## 02

# Pregunta 2

Realizar la comprobación para los puertos 1 y 4. Indicar las diferencias observadas. Por último, se pueden modificar los parámetros seleccionando la pestaña Setup. Dos de los parámetros que cambiaremos en apartados posteriores de la práctica son Link Type y Max MAC Count, así que ahora es el momento de localizarlos y recordarlos.

En la pestaña *summary* se observa el estado de cada puerto: *enabled* o *disabled*. En el caso de los puertos 1 y 4, ambos están habilitados. En la pestaña de detalles (*detail*) se puede ver más en detalle la información relativa a cada puerto (figuras 13 y ??). En este caso, ambos puertos tienen la misma información: están habilitados y conectados a la VLAN 1. Además, por el campo *Max MAC Count* sabemos que ninguno tiene un límite de dispositivos.

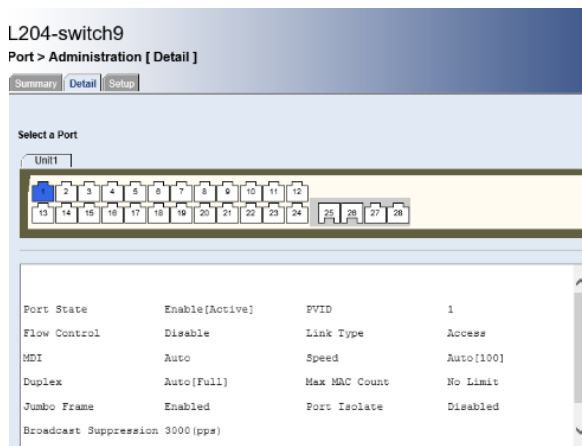


Figura 6: Detalles del puerto 1.

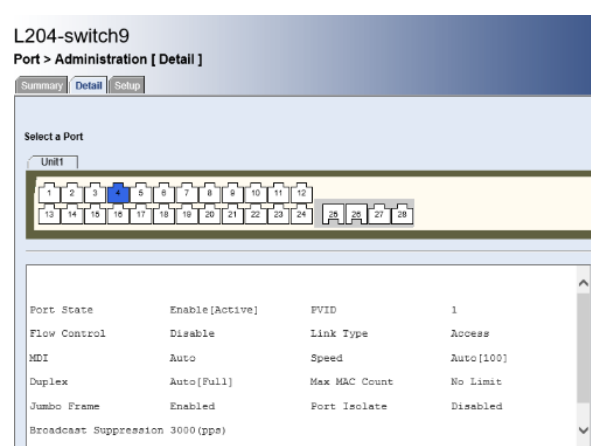


Figura 7: Detalles del puerto 4.

Adicionalmente podemos consultar las direcciones MAC aprendidas por cada puerto en su tabla de direccionamiento (figuras 8 y 9).

**L204-switch9**  
Display device information

Summary | **Port Summary** | Add | Setup | Remove | Port Remove

Select a port

Unit1

State

☒ All ☐ Static ☐ Dynamic ☐ Blackhole

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME (s)
001e-c10e-ce41	1	Learned	Ethernet1/0/1	AGING
1860-249c-e104	1	Learned	Ethernet1/0/1	AGING
b8ae-ed79-e455	1	Learned	Ethernet1/0/1	AGING
cc2d-e002-e6aa	1	Learned	Ethernet1/0/1	AGING

Total: 4

Figura 8: Direcciones aprendidas por el puerto 1 del switch.

**L204-switch9**  
Port > MAC Address [ Port Summary ]

Summary | **Port Summary** | Add | Setup | Remove | Port Remove

Select a port

Unit1

State

☒ All ☐ Static ☐ Dynamic ☐ Blackhole

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME (s)
8cdc-d451-90f3	1	Learned	Ethernet1/0/4	AGING

Total: 1

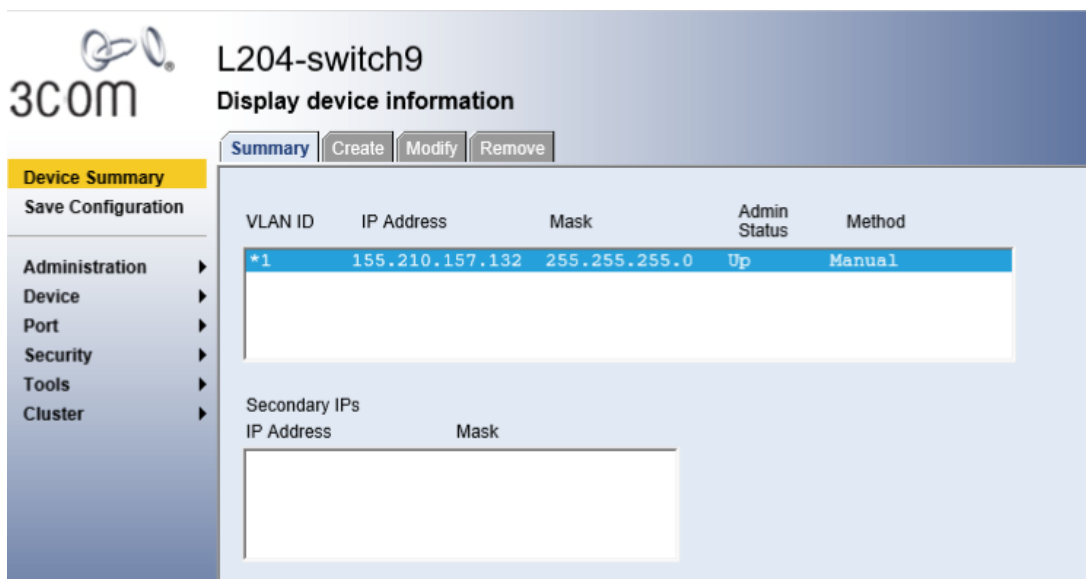
Figura 9: Direcciones aprendidas por el puerto 4 del switch.

03

## Pregunta 3

En este apartado vamos a estudiar la configuración de los parámetros IP de direccionamiento y encaminamiento.

Cuando entramos en la pestaña resumen lo primero que aparece es la tabla de encaminamiento, en la que sólo se encuentra configurada la red virtual 1, a la que estaban vinculados todos los puertos. En la pestaña create podemos crear nuevas entradas de esta tabla, creando nuevas redes virtuales dentro del switch.



The screenshot shows the configuration interface for a 3COM L204-switch9. The main title is "L204-switch9" and the subtitle is "Display device information". There are four tabs: "Summary", "Create", "Modify", and "Remove". The "Summary" tab is selected. On the left, there is a sidebar with a "Device Summary" section and a "Save Configuration" button. Below these are several expandable sections: "Administration", "Device", "Port", "Security", "Tools", and "Cluster". The main content area displays a table of IP addresses and their associated masks. The table has five columns: "VLAN ID", "IP Address", "Mask", "Admin Status", and "Method". There is one entry in the table with the following values: VLAN ID: \*1, IP Address: 155.210.157.132, Mask: 255.255.255.0, Admin Status: Up, and Method: Manual. Below the table, there is a section for "Secondary IPs" with columns for "IP Address" and "Mask", and a large empty text area for input.

VLAN ID	IP Address	Mask	Admin Status	Method
*1	155.210.157.132	255.255.255.0	Up	Manual

Figura 10: Tabla de encaminamiento del switch.



## 04

# Pregunta 4

Recordemos que en el apartado 2 se indicaba cómo debían estar configuradas las direcciones IP de PCN1-virtual y PCN3-virtual. A continuación realiza un ping desde PCN1-virtual a PCN3-virtual. Debe funcionar correctamente. ¿Aparece en las tablas ARP de ambos equipos la correspondiente línea para el encaminamiento directo tras realizar el ping?

El esquema de la conexión con las direcciones IP de cada máquina es el siguiente:

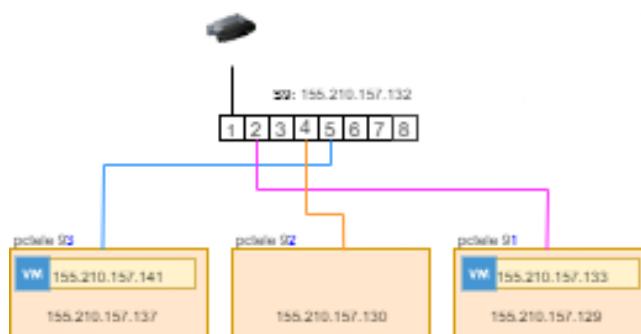


Figura 11: Esquema de conexiones y direcciones.

Después de realizar un ping desde la máquina PCN1 a PCN3 las tablas ARP de cada una contienen la asociación IP-MAC tanto del switch como de la máquina contraria. Esto se verifica con la ayuda del comando arp, que ejecutado en la máquina PCN1 muestra la siguiente información:

```

1 [root@localhost ~]# arp
2 Address          HWtype  HWaddress      Flags Mask    Iface
3 155.210.157.132   ether    00:1e:c1:cf:09:c1  C           eth0
4 155.210.157.141   ether    08:00:27:d6:de:1e  C           eth0

```

En el paquete 22 de la captura de la máquina PCN1 se observa el mensaje ARP que pregunta por la dirección 155.210.157.141, que es la que aparece almacenada.

La máquina PCN3 tiene esta otra tabla:

```

1 [root@localhost ~]# arp
2 Address          HWtype  HWaddress      Flags Mask    Iface
3 155.210.157.132   ether    00:1e:c1:cf:09:c1  C           eth0
4 155.210.157.133   ether    08:00:27:b5:1e:0e  C           eth0

```

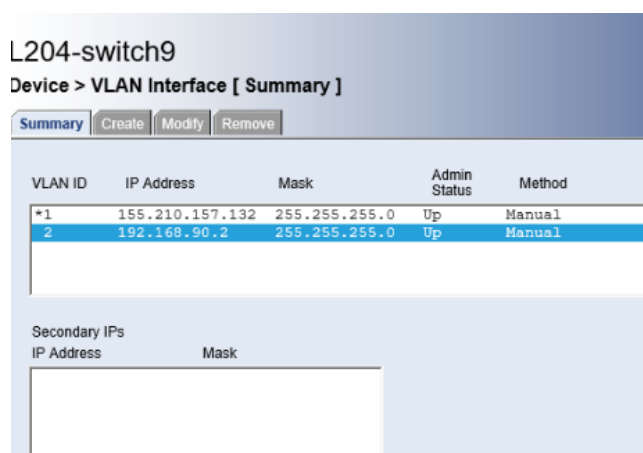
En el paquete 68 de la captura de la máquina PCN3 se vuelve a observar el mismo mensaje ARP que había enviado PCN1. Al recibir este mensaje por parte de 155.210.157.141 con su MAC, PCN3 ya tiene la información necesaria para enviar el paquete de respuesta.

05

## Pregunta 5

Borra de nuevo las tablas ARP de PCN1-virtual y PCN3-virtual y vuelve a realizar el ping desde PCN1-virtual y PCN3-virtual. Mientras tanto ejecuta en PCN1-real y PCN3-real un software de captura (tcpdump o wireshark). Observamos que NO funciona el ping y NO se ve en la VLAN 2 el tráfico ARP broadcast de los equipos de la VLAN 1 ¿Por qué sucede esto?

Desde la misma pestaña consultada en la pregunta 3 hemos creado la VLAN2, con la dirección 192.168.90.0/24. Después, desde la pestaña vista en la pregunta 2 hemos modificado el valor PVID del puerto 5 (el que conecta a PCN3) para que esté vinculado con la VLAN2.



**L204-switch9**  
**Device > VLAN Interface [ Summary ]**

Summary Create Modify Remove

VLAN ID	IP Address	Mask	Admin Status	Method
*1	155.210.157.132	255.255.255.0	Up	Manual
2	192.168.90.2	255.255.255.0	Up	Manual

Secondary IPs

IP Address	Mask

Figura 12: Tabla de encaminamiento actualizada con la nueva VLAN.

En la captura de PCN1 observamos que se está constantemente preguntando por la MAC de PCN3 (por ejemplo en los paquetes 8 y 13). El motivo por el que nadie le responde es que el switch no está redirigiendo los paquetes a través del puerto 5 porque está en una VLAN diferente. Si observamos la captura de PCN3 vemos que no aparece ninguno de los mensajes ARP.

06

## Pregunta 6

Ejecuta un ping desde el switch (menú Tools/ping) hacia PCN3-virtual (dirección IP privada). Mientras tanto captura el tráfico en PCN3-real ¿Se ve el tráfico ARP e ICMP correspondiente al ping? ¿Por qué?

---

En la captura se puede ver cómo después de recibir el primer ICMP request (paquete 1) la máquina PCN3 tiene que preguntar por la MAC del switch para poder enviarle la respuesta. El ARP del switch no se ve porque ya se había realizado un ping anterior a esta captura y sólo se ha borrado la tabla ARP de PCN3.

Como información adicional, en la captura se pueden observar los paquetes de protocolo de enrutamiento utilizados para aprender las rutas mediante el protocolo STP (Spanning Tree Protocol).

07

## Pregunta 7

Efectúa un ping desde PCN1-virtual a PCN3-virtual y captura el tráfico en PCN1-real y PCN3-real. Comprueba, en base a las capturas, la dirección MAC de las tramas ICMP en ambas VLAN y el valor del TTL

El paquete 68 de la captura en PCN1 es el primer echo request enviado. Si observamos las direcciones MAC de la trama ethernet vemos que la dirección de destino es la del switch, no la de PCN3, ya que este se encuentra en una red distinta. El TTL que aparece a nivel IP es inicialmente 64.

El paquete correspondiente en la captura de PCN3 es el paquete 1. En él comprobamos que la dirección MAC origen es la del switch y que el TTL ha disminuido en 1, ya que el paquete ICMP ha tenido que ser enrutado de una red virtual a otra.

No.	Time	Source	Destination	Protocol	Length	Info
68	5.433875	155.210.157.133	192.168.90.141	ICMP	98	Echo (ping) request
69	5.435536	192.168.90.141	155.210.157.133	ICMP	98	Echo (ping) reply

> Frame 68: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0	0000	00 1e c1 cf 09 c1 08 00 2
Ethernet II, Src: PcsCompu_b5:1e:0e (08:00:27:b5:1e:0e), Dst: 3ComEuro_cf:09:c1 (00:1e:c1:cf:09:c1)	0010	00 54 00 00 40 00 40 01 e
Destination: 3ComEuro_cf:09:c1 (00:1e:c1:cf:09:c1)	0020	5a 8d 08 00 19 42 88 0b e
Source: PcsCompu_b5:1e:0e (08:00:27:b5:1e:0e)	0030	00 00 08 09 0a 0b 0c 0d e
Type: IPv4 (0x0800)	0040	16 17 18 19 1a 1b 1c 1d 1
Internet Protocol Version 4, Src: 155.210.157.133, Dst: 192.168.90.141	0050	26 27 28 29 2a 2b 2c 2d 2
0100 .... = Version: 4	0060	36 37
.... 0101 = Header Length: 20 bytes (5)		
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 84		
Identification: 0x0000 (0)		
010 .... = Flags: 0x2, Don't fragment		
...0 0000 0000 0000 = Fragment Offset: 0		
Time to Live: 64		
Protocol: ICMP (1)		
Header Checksum: 0xe61b [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 155.210.157.133		
Destination Address: 192.168.90.141		
Internet Control Message Protocol		

Figura 13: Ping capturado en PCN1-real.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	155.210.157.133	192.168.90.141	ICMP	98	Echo (ping) request
2	0.000202	192.168.90.141	155.210.157.133	ICMP	98	Echo (ping) reply

> Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0	0000	08 00 27 d6 de 1e 00 00
Ethernet II, Src: 3ComEuro_cf:09:c1 (00:1e:c1:cf:09:c1), Dst: PcsCompu_d6:de:1e (08:00:27:d6:de:1e)	0010	00 54 00 00 40 00 3f 4
Destination: PcsCompu_d6:de:1e (08:00:27:d6:de:1e)	0020	5a 8d 08 00 19 42 88 0b e
Source: 3ComEuro_cf:09:c1 (00:1e:c1:cf:09:c1)	0030	00 00 08 09 0a 0b 0c 0d e
Type: IPv4 (0x0800)	0040	16 17 18 19 1a 1b 1c 1d 1
Internet Protocol Version 4, Src: 155.210.157.133, Dst: 192.168.90.141	0050	26 27 28 29 2a 2b 2c 2d 2
0100 .... = Version: 4	0060	36 37
.... 0101 = Header Length: 20 bytes (5)		
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)		
Total Length: 84		
Identification: 0x0000 (0)		
010 .... = Flags: 0x2, Don't fragment		
...0 0000 0000 0000 = Fragment Offset: 0		
Time to Live: 63		
Protocol: ICMP (1)		
Header Checksum: 0xe71b [validation disabled]		
[Header checksum status: Unverified]		
Source Address: 155.210.157.133		
Destination Address: 192.168.90.141		
Internet Control Message Protocol		

Figura 14: Ping capturado en PCN3-real.

08

## Pregunta 8

Realiza un ping desde PCN1-virtual hacia la dirección del interfaz eth0.2 de PCN3-virtual. Mientras tanto captura el tráfico en PCN1-real y PCN3-real. Explica en base a las capturas en los diferentes interfaces dónde aparecen tramas 802.1Q (tagged).

Si observamos uno de los mensajes ICMP enviados en la captura de PCN1, por ejemplo el paquete 66, vemos que no tiene información adicional porque la red VLAN 1 es untagged. Por otro lado, los paquetes ICMP capturados en PCN3, véase el paquete 26, aparecen con un campo extra entre la cabecera ethernet e IP. En ese campo se especifica el identificador de la VLAN en la que se encuentra el puerto al que está conectado la máquina, además de información relativa a la prioridad de la trama y el tipo de protocolo encapsulado (el de la trama ethernet ha sido sustituido por 802.1Q).

No.	Time	Source	Destination	Protocol	Length	Info
56	4.126431	155.210.157.133	192.168.90.141	ICMP	102	Echo (ping) request id=0x440b, seq=1/256, ttl=63
57	4.127158	192.168.90.141	155.210.157.133	ICMP	102	Echo (ping) reply id=0x440b, seq=1/256, ttl=64

> Frame 56: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on > Ethernet II, Src: 3ComEuro_cf:09:c1 (00:1e:c1:cf:09:c1), Dst: PcsCompu > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2 000. .... = Priority: Best Effort (default) (0) ...0 .... = DEI: Ineligible ... 0000 0000 0010 = ID: 2 Type: IPv4 (0x0800) > Internet Protocol Version 4, Src: 155.210.157.133, Dst: 192.168.90.141 > Internet Control Message Protocol	0000 08 00 27 d6 de 1e 00 1e c1 cf 09 c1 81 00 00 02 0010 08 00 45 00 00 54 00 00 40 00 3f 01 e7 1b 9b d2 0020 9d 85 c0 a8 5a 8d 08 00 b0 d2 44 0b 00 01 bd ae 0030 64 65 ec 09 0a 00 08 09 0a 0b 0c 0d 0e 0f 10 11 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 0060 32 33 34 35 36 37
---	--

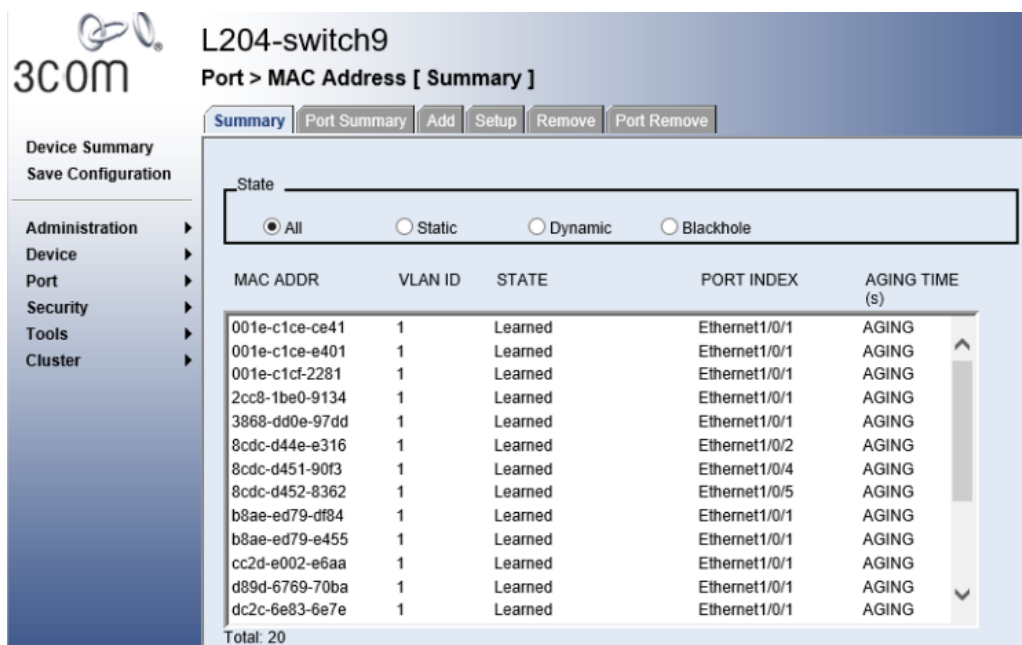
Figura 15: Ping capturado en PCN3-real. VLAN tagged.

09

## Pregunta 9

Haz una captura de pantalla (esto no es necesario para E9) con la tabla de conmutación y comprueba que en los puertos aparezcan las direcciones MAC de los PC. ¿En qué puerto aparecen la mayoría de las direcciones y por qué ocurre esto?

La figura 16 muestra las direcciones MAC que el switch ha aprendido. La mayor parte de ellas están registradas en el puerto 1. Esto es debido a que el puerto 1 es el que se conecta con el resto de la red del laboratorio, y por ello está expuesto a un número mayor de dispositivos.



MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME (s)
001e-c1ce-ce41	1	Learned	Ethernet1/0/1	AGING
001e-c1ce-e401	1	Learned	Ethernet1/0/1	AGING
001e-c1cf-2281	1	Learned	Ethernet1/0/1	AGING
2cc8-1be0-9134	1	Learned	Ethernet1/0/1	AGING
3868-dd0e-97dd	1	Learned	Ethernet1/0/1	AGING
8cdc-d44e-e316	1	Learned	Ethernet1/0/2	AGING
8cdc-d451-90f3	1	Learned	Ethernet1/0/4	AGING
8cdc-d452-8362	1	Learned	Ethernet1/0/5	AGING
b8ae-ed79-df84	1	Learned	Ethernet1/0/1	AGING
b8ae-ed79-e455	1	Learned	Ethernet1/0/1	AGING
cc2d-e002-e6aa	1	Learned	Ethernet1/0/1	AGING
d89d-6769-70ba	1	Learned	Ethernet1/0/1	AGING
dc2c-6e83-6e7e	1	Learned	Ethernet1/0/1	AGING

Total: 20

Figura 16: Direcciones aprendidas por el switch.

## 10

# Pregunta 10

Crea en PCN3-virtual una entrada en la tabla arp estática con la información de la máquina inexistente (Ejemplo: arp -s 157.55.85.212 00:aa:bb:cc:11:22). Recordar que la dirección IP de la máquina inexistente debe pertenecer a la red del laboratorio pero que no debe estar usada por otra máquina (podemos usar la dirección reservada a la máquina virtual de PCN2 que no está encendida, la real de PCN2 más 4. Realiza un ping desde PCN1 a PCN3. Conecta el cable ethernet de PCN2, a distintos puertos del switch. Captura en todo los casos, y explica lo que le sucede a las tramas arp request y reply cuando no aparece la MAC en la tabla de conmutación del switch

---

Al asignar una dirección MAC inexistente en el sistema, el switch difunde la trama ARP a través de todos los puertos, utilizando un broadcast, con el propósito de determinar por qué puerto debe salir dicha trama.

Como consecuencia, notamos que nuestro mensaje de ping no recibe respuesta, ~~ya que hemos encomendado al switch una tarea imposible al proporcionarle una dirección inexistente.~~

## 11

# Pregunta 11

En el puerto en el que tenemos la mayoría de las direcciones, vamos a limitar a 5 el número de direcciones MAC aprendidas para este puerto (menú Port/Administration). Comprueba el correcto funcionamiento con Port/MAC Address. A continuación localiza un equipo de las otras bancadas cuya dirección MAC no se encuentre entre las 5 aprendidas por tu switch para dicho puerto, e intenta realizar un ping a dicho equipo. ¿Qué está ocurriendo? ¿Qué ocurre con los ARP? ¿Llegan a transmitirse los request del ping? ¿Por qué?

---

Al limitar el número de direcciones MAC a 5, el switch solo puede aprender información sobre 5 máquinas, que serán, por ende, las que se utilicen con mayor frecuencia. Para poner a prueba la conectividad al realizar un ping a una máquina de otra subred, ejecutamos un ping a la subred 7 donde se encontraban nuestros compañeros. Lo que se pudo observar finalmente fue cómo una de las entradas en nuestra tabla de enrutamiento fue reemplazada, permitiendo al switch conocer el puerto de salida para este nuevo destino.



12

## Pregunta 12

A continuación ponemos el límite de direcciones aprendidas en el puerto a 0. Configura manualmente la tabla de conmutación del switch con la dirección MAC del router del laboratorio de tal forma que se permita el acceso a internet de los equipos de la bancada. ¿Puedes comunicarte con los equipos de otras bancadas? Configura de nuevo la tabla de conmutación añadiendo la MAC oportuna para poder comunicarte con un PC de otra bancada

---

Al configurar el límite de direcciones MAC a 0, el switch no aprende automáticamente ninguna MAC. Para permitir el acceso a internet, agregamos manualmente la dirección MAC del router a la tabla de conmutación. Esto permite la conexión externa, pero aún no podemos comunicarnos con equipos de otras bancadas. Para lograrlo, necesitamos añadir también las direcciones MAC de esas bancadas a la tabla de conmutación, lo que nos permitirá establecer conexión con esos equipos.