

Práctico 3: ARP y VLANs

Objetivos:

- Aprendizaje de concepto de VLAN y circuito virtual.
- Aprendizaje de configuración de VLAN en Cisco en el Cisco Packet Tracer y equipos reales.
- Aprendizaje de ARP

Bibliografía y links de ayuda:

- Computer Networking de Kurose y Ross, Sección 5.4.4
- Computer Networks de Andrew S. Tanenbaum, Sección 4.8.5
- https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/switch_module_swcg/cgr-esm-configuration/config_vlans.pdf
- <http://docs.gns3.com/>
- <https://community.cisco.com/t5/switching/subinterfaces-and-vlans/m-p/2057669/highlight/true#M423526>

Ejercicio 1: ARP

- 1.- Requerimiento: estar conectado a una red local.
- 2.- Iniciar el wireshark.
- 3.- Aplicar un filtro para ver solamente mensajes del protocolo ARP.
- 4.- Explicar los paquetes que aparecen con detalle:
 - ¿Qué es lo que se ve en cada capa?
 - ¿Qué se puede decir con respecto a la frecuencia con la que aparecen los mensajes?
 - ¿Cuales son las entradas en la tabla ARP del host?
 - ¿Es posible ver la tabla ARP del router? ¿Cómo se ve dicha tabla?

4.- Petición ARP por Broadcast

arp						
No.	Time	Source	Destination	Protocol	Length	Info
3	4.199700863	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.10
20	14.541217859	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.17? Tell 192.168.0.1
23	15.564237468	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.17? Tell 192.168.0.1
25	16.691199498	SonyMobi_fb:81:22	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.17
27	20.788470144	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.23? Tell 192.168.0.1
28	22.219368191	CiscoSpv_c1:d2:c2	Broadcast	ARP	60	Who has 192.168.0.23? Tell 181.164.143.36
44	43.620791184	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.10
117	190.669089052	Tp-LinkT_3a:14:86	Broadcast	ARP	42	Who has 192.168.0.31? Tell 192.168.0.11
123	191.488681222	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.30? Tell 192.168.0.1
134	209.204303513	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.11? Tell 192.168.0.1
164	228.650433721	LiteonTe_3f:0e:70	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.38
165	228.654691190	CiscoSpv_c1:d2:c1	LiteonTe_3f:0e:70	ARP	42	192.168.0.1 is at e4:48:c7:c1:d2:c1
202	260.712182458	SamsungE_70:24:16	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.23
255	290.819582393	SamsungE_70:24:16	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.23
298	317.880775393	LiteonTe_3f:0e:70	CiscoSpv_c1:d2:c1	ARP	42	Who has 192.168.0.1? Tell 192.168.0.38
299	317.882476225	CiscoSpv_c1:d2:c1	LiteonTe_3f:0e:70	ARP	42	192.168.0.1 is at e4:48:c7:c1:d2:c1
315	355.229172726	CiscoSpv_c1:d2:c2	Broadcast	ARP	60	Who has 181.164.143.1? Tell 181.164.143.36
342	413.700372746	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.37? Tell 192.168.0.1
346	414.727596690	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.37? Tell 192.168.0.1
347	416.056590052	XiaomiCo_5d:3f:e7	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.37
403	483.230081246	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.10
▶ Frame 164: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▼ Ethernet II, Src: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)						
▶ Source: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70)						
Type: ARP (0x0806)						
▼ Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70)						
Sender IP address: 192.168.0.38						
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.0.1						

¿Qué es lo que se ve en cada capa?

En la capa de enlace vemos, en el frame de Ethernet:

- La dirección física del emisor de la petición ARP (Src)
- La dirección física del receptor (como es un mensaje para todos en la red, es la dirección MAC de broadcast).
- El tipo de datos que lleva el payload (en este caso es ARP, puede ser IP).

En cuanto al payload (paquete ARP), tenemos:

- Tipo del hardware usado en la capa física, que es Ethernet,
- Tipo del protocolo de interconexión, que es IPv4.
- Código de operación, específica que es una petición (Request)
- La dirección física del emisor de la petición ARP (Sender)
- La IP del emisor.
- La IP del destino.
- Un campo para la MAC del destino, que está vacía en el mensaje de petición (Target MAC address).

Respuesta ARP por Unicast

arp						
No.	Time	Source	Destination	Protocol	Length	Info
3	4.199700863	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.10
20	14.541217859	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.17? Tell 192.168.0.1
23	15.564237468	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.17? Tell 192.168.0.1
25	16.691199498	SonyMobi_fb:81:22	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.17
27	20.788470144	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.23? Tell 192.168.0.1
28	22.219368191	CiscoSpv_c1:d2:c2	Broadcast	ARP	60	Who has 192.168.0.23? Tell 181.164.143.36
44	43.620791184	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.10
117	190.669089052	Tp-LinkT_3a:14:86	Broadcast	ARP	42	Who has 192.168.0.31? Tell 192.168.0.11
123	191.488681222	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.30? Tell 192.168.0.1
134	209.204303513	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.11? Tell 192.168.0.1
164	228.650433721	LiteonTe_3f:0e:70	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.38
165	228.654691190	CiscoSpv_c1:d2:c1	LiteonTe_3f:0e:70	ARP	42	192.168.0.1 is at e4:48:c7:c1:d2:c1
202	260.712182458	SamsungE_70:24:16	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.23
255	290.819582393	SamsungE_70:24:16	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.23
298	317.880775393	LiteonTe_3f:0e:70	CiscoSpv_c1:d2:c1	ARP	42	Who has 192.168.0.1? Tell 192.168.0.38
299	317.882476225	CiscoSpv_c1:d2:c1	LiteonTe_3f:0e:70	ARP	42	192.168.0.1 is at e4:48:c7:c1:d2:c1
315	355.229172726	CiscoSpv_c1:d2:c2	Broadcast	ARP	60	Who has 181.164.143.1? Tell 181.164.143.36
342	413.700372746	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.37? Tell 192.168.0.1
346	414.727596690	CiscoSpv_c1:d2:c1	Broadcast	ARP	60	Who has 192.168.0.37? Tell 192.168.0.1
347	416.056590052	XiaomiCo_5d:3f:e7	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.37
403	483.230081246	Motorola_2e:20:a3	Broadcast	ARP	42	Who has 192.168.0.14? Tell 192.168.0.10
▶ Frame 165: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
▼ Ethernet II, Src: CiscoSpv_c1:d2:c1 (e4:48:c7:c1:d2:c1), Dst: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70)						
▶ Destination: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70)						
▶ Source: CiscoSpv_c1:d2:c1 (e4:48:c7:c1:d2:c1)						
Type: ARP (0x0806)						
▼ Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						
Sender MAC address: CiscoSpv_c1:d2:c1 (e4:48:c7:c1:d2:c1)						
Sender IP address: 192.168.0.1						
Target MAC address: LiteonTe_3f:0e:70 (3c:a0:67:3f:0e:70)						
Target IP address: 192.168.0.38						

Vemos que ahora, el destino es la dirección MAC del host que originó la petición, y el origen es el host que tiene la IP por la que se está averiguando la MAC.

En el paquete ARP, podemos ver que el campo del emisor (Sender) ahora fue completado con la dirección MAC que se quería averiguar (es el host que ahora está respondiendo a la petición); y el campo que antes estaba vacío (Target MAC address) tiene la dirección del host que originó la petición (al host que se le está enviando la respuesta).

¿Qué se puede decir con respecto a la frecuencia con la que aparecen los mensajes?

Los mensajes de descubrimiento inicial (ARP requests a Broadcast) se hacen cada vez que un host necesita comunicarse con cierta IP y desconoce la MAC de dicho host (no figura en su tabla ARP).

Una vez que obtiene la MAC que necesitaba, la guarda en la tabla así ya no tiene que preguntar de nuevo por Broadcast (de todas formas, cada entrada de la tabla ARP tiene un timeout, por lo que en algún momento se preguntará de nuevo).

Se observan mensajes recurrentes del router a las direcciones IP de los host que tiene conectados (de los cuales desconoce su MAC) para completar la tabla.

¿Cuales son las entradas en la tabla ARP del host?

```
andres@andres:~$ arp
Dirección      TipoHW  DirecciónHW  Indic  Máscara  Interfaz
192.168.0.1    ether   e4:48:c7:c1:d2:c1  C      wlp3s0
andres@andres:~$
```

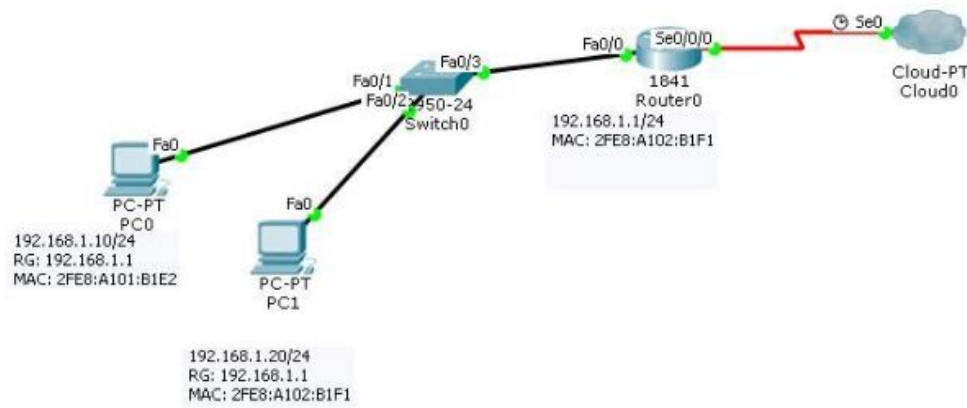
Las entradas en la tabla ARP son:

- Dirección IP
- Tipo Hardware
- Dirección MAC
- Indicador (Flag), la C indica que la entrada está completa.
- Máscara
- Interfaz por la que está conectado el host.

¿Es posible ver la tabla ARP del router? ¿Cómo se ve dicha tabla?

Es posible ver la tabla ARP del router, para obtenerla debemos conectarnos físicamente al router a través del puerto serie y utilizar el comando show arp.

Ejercicio 2: ARP



Inicialmente las tablas ARP, incluida la del router, están vacías.

PC0 desea hacer un ping a PC1: ping 192.168.1.20

Explique lo que sucede cronológicamente:

1. PC0 desea enviar un ping a PC1 pero solo tiene la IP, no conoce su MAC (PC0 deja el paquete pendiente para completar con la MAC de destino una vez la haya averiguado).
2. PC0 realiza un ARP Request por broadcast (MAC ff:ff:ff:ff:ff:ff) con lo siguiente:
 - a. IP origen (PC0)
 - b. MAC origen (MAC de PC0)
 - c. IP destino (PC1)
 - d. MAC destino (00:00:00:00:00:00)
3. Router0 recibe el paquete y lo descarta porque la IP de destino no es la suya, mientras que PC1 recibe el paquete, y al coincidir su IP con la de destino, procede a realizar la respuesta (ARP Reply) enviando lo siguiente:
 - a. IP origen (PC1)
 - b. MAC origen (MAC de PC1) → la MAC solicitada por PC0
 - c. IP destino (PC0)
 - d. MAC destino (MAC de PC0)

Además, la PC1 guarda en su tabla ARP la correspondencia IP PC0 → MAC PC0

4. PC0 ya tiene la MAC que le faltaba, por lo que completa el paquete que había dejado pendiente y procede a enviar el ping (ICMP echo request).
5. Suponiendo que el switch tiene su tabla CAM completa, recibe el paquete y lo manda al puerto que tiene la MAC de destino (MAC de PC1).
6. PC1 recibe el paquete ICMP y, como ya aprendió la MAC de PC0, puede responder sin tener que hacer un ARP Request. PC1 responde con un ICMP echo reply, el cual llega a PC0, finalizando la operación.

Y complete la tabla siguiente:

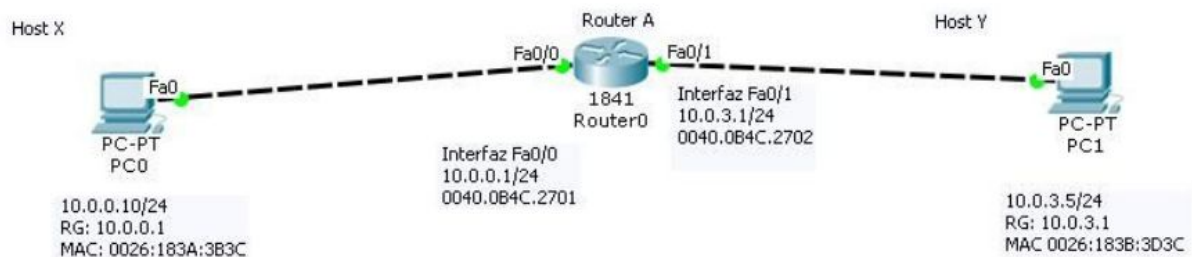
Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ARP	2FE8:A101:B1E2	FFFF:FFFF:FFFF	192.168.1.10	192.168.1.1	ARP Request
ARP	2FE8:A102:B1F1	2FE8:A101:B1E2	192.168.1.1	192.168.1.10	ARP Reply
ICMP	2FE8:A101:B1E2	2FE8:A101:B1F1	192.168.1.10	192.168.1.1	Echo (ping) Request
ICMP	2FE8:A101:B1F1	2FE8:A101:B1E2	192.168.1.1	192.168.1.10	Echo (ping) Reply

En la captura siguiente, se observa el proceso descrito en la cronología.

- PC0 tiene la IP 192.168.0.7 y la MAC LiteonTe_3f:0e:70
- PC1 tiene la IP 192.168.0.16 y la MAC IntelCor_f7:f3:23
- El primer frame corresponde al ARP Request.
- El segundo frame corresponde al ARP Reply.
- Los frames siguientes corresponden a los sucesivos ping.

182	109.614860024	LiteonTe_3f:0e:70	Broadcast	ARP	42 Who has 192.168.1.16? Tell 192.168.1.7
183	109.614932022	IntelCor_f7:f3:23	LiteonTe_3f:0e:70	ARP	42 192.168.1.16 is at 78:0c:b8:f7:f3:23
184	109.625823359	192.168.1.7	192.168.1.16	ICMP	98 Echo (ping) request id=0x0f4b, seq=1/256, ttl=64 (reply in 185)
185	109.625921588	192.168.1.16	192.168.1.7	ICMP	98 Echo (ping) reply id=0x0f4b, seq=1/256, ttl=64 (request in 184)
186	109.626478690	192.168.1.7	192.168.1.16	ICMP	98 Echo (ping) request id=0x0f4b, seq=2/512, ttl=64 (reply in 187)
187	109.626566348	192.168.1.16	192.168.1.7	ICMP	98 Echo (ping) reply id=0x0f4b, seq=2/512, ttl=64 (request in 186)
188	109.626605889	192.168.1.7	192.168.1.16	ICMP	98 Echo (ping) request id=0x0f4b, seq=3/768, ttl=64 (reply in 189)
189	109.626633595	192.168.1.16	192.168.1.7	ICMP	98 Echo (ping) reply id=0x0f4b, seq=3/768, ttl=64 (request in 188)
190	110.555165089	192.168.1.7	192.168.1.16	ICMP	98 Echo (ping) request id=0x0f4b, seq=4/1024, ttl=64 (reply in 191)
191	110.555242171	192.168.1.16	192.168.1.7	ICMP	98 Echo (ping) reply id=0x0f4b, seq=4/1024, ttl=64 (request in 190)
192	111.571080914	192.168.1.7	192.168.1.16	ICMP	98 Echo (ping) request id=0x0f4b, seq=5/1280, ttl=64 (reply in 193)
193	111.571159774	192.168.1.16	192.168.1.7	ICMP	98 Echo (ping) reply id=0x0f4b, seq=5/1280, ttl=64 (request in 192)

Ejercicio 3: ARP



Inicialmente las tablas ARP, incluida la del router, están vacías.

- a) El host X desea hacer un ping al host 10.0.3.10 (que no existe). Complete la tabla siguiendo el orden cronológico. **Observe que la dirección 10.0.3.10 no existe.**

El Host X, al tratar de hacer ping observa que la IP de destino (10.0.3.10) no pertenece a la red, por lo que deberá mandar el ping a su default gateway (el Router A). Al no conocer la MAC del Router A, primero realiza un ARP Request con:

- IP origen (Host X)
- MAC origen (MAC de Host X)
- IP destino (Router A)
- MAC destino (00:00:00:00:00:00)

Una vez el Host X tiene la MAC del router, le manda el ping (ICMP echo request) destinado a 10.0.3.10.

El router sabe que la IP de destino pertenece a una de las redes que tiene conectadas a sus interfaces, pero desconoce la MAC a la que corresponde esa IP de destino, por lo que hace un broadcast preguntando por ella. Como no existe la dirección solicitada nunca recibe respuesta y ocurre un time-out.

Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ARP	0026:183A:3B3C	FFFF:FFFF:FFFF	10.0.0.10	10.0.0.1	ARP Request
ARP	0040:0B4C:2701	0026:183A:3B3C	10.0.0.1	10.0.0.10	ARP Reply
ICMP	0026:183A:3B3C	0040:0B4C:2701	10.0.0.10	10.0.3.10	Ping (Echo Request)
ARP	0040:0B4C:2702	FFFF:FFFF:FFFF	10.0.3.1	10.0.3.10	ARP Request

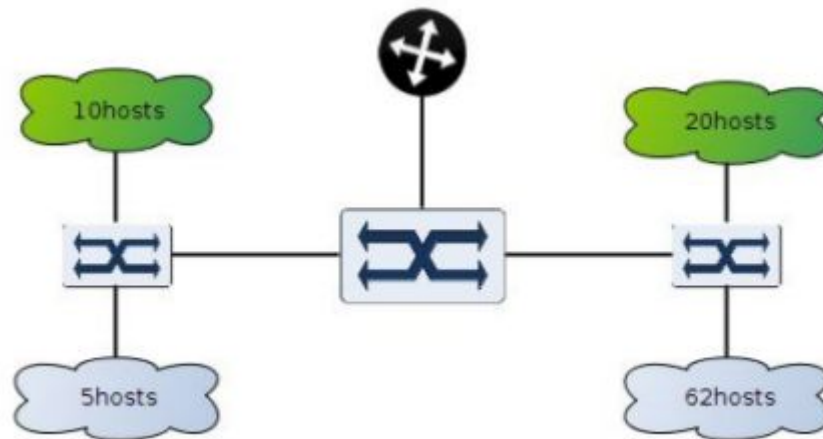
b) El host X desea hacer un ping al host 10.0.3.5. Se pide lo mismo que en el punto anterior. **Considere que se mantienen en las tablas ARP las direcciones cargadas en el punto anterior.**

El Host X ya conoce la MAC del router y manda el ping (ICMP echo request) a éste con la IP de destino 10.0.3.5 (nuevamente el Host X se dio cuenta que la IP de destino no esta en su red, por eso lo manda al default gateway).

El Router A consultará nuevamente, mediante un ARP Request, la MAC que corresponde a la IP de destino, solo que esta vez sí obtiene la respuesta. Una vez que conoce la MAC del destino original del ping, el Echo Request le llega al Host Y y este realiza la respuesta.

Protocolo	MAC origen en trama	MAC destino en trama	IP origen en datagrama	IP destino en datagrama	Contenido
ICMP	0026:183A:3B3C	0040:0B4C:2701	10.0.0.10	10.0.3.10	Ping (Echo Request)
ARP	0040:0B4C:2702	FFFF:FFFF:FFFF	10.0.3.1	10.0.3.5	ARP Request
ARP	0026:183B:3D3C	0040:0B4C:2702	10.0.3.5	10.0.3.1	ARP Reply
ICMP	0040:0B4C:2702	0026:183B:3D3C	10.0.3.1	10.0.3.5	Ping (Echo Request)
ICMP	0026:183B:3D3C	0040:0B4C:2702	10.0.3.5	10.0.3.1	Ping (Echo Reply)
ICMP	0040:0B4C:2701	0026:183A:3B3C	10.0.3.10	10.0.0.10	Ping (Echo Reply)

Ejercicio 4: VLANS



1. Estimar el tamaño de las subredes para dar direccionamiento a la red Verde y Celeste. Mostrar dirección de red, máscara y espacio útil en una tabla.
2. Implementar la presente topología en GNS3: Configurar de forma tal que los hosts de las redes verdes están en una VLAN y los host de las redes celestes están en otra VLAN. Si se desconecta el router, ¿Hay conectividad entre ambas redes? ¿Por qué?/¿Por qué no?
3. ¿Qué característica tiene el switch central?
4. Con respecto a los switches de los extremos, ¿qué diferencia hay entre los puertos que conectan a las LANs respecto de los que conectan al switch central?
5. El router tiene un solo puerto. ¿Cómo se consigue dar funcionalidad de gateway para ambas redes sobre un mismo medio físico?
6. ¿Qué hace un switch cuando recibe un frame Ethernet sobre un puerto acceso? ¿Qué sucede con la tabla MAC del mismo?
7. ¿Cual es el camino que describe una trama que sale de un host de la red Verde para llegar a un host destino, en la red Celeste? ¿Cómo se vería la trama en cada uno de los trayectos que hace en la red?

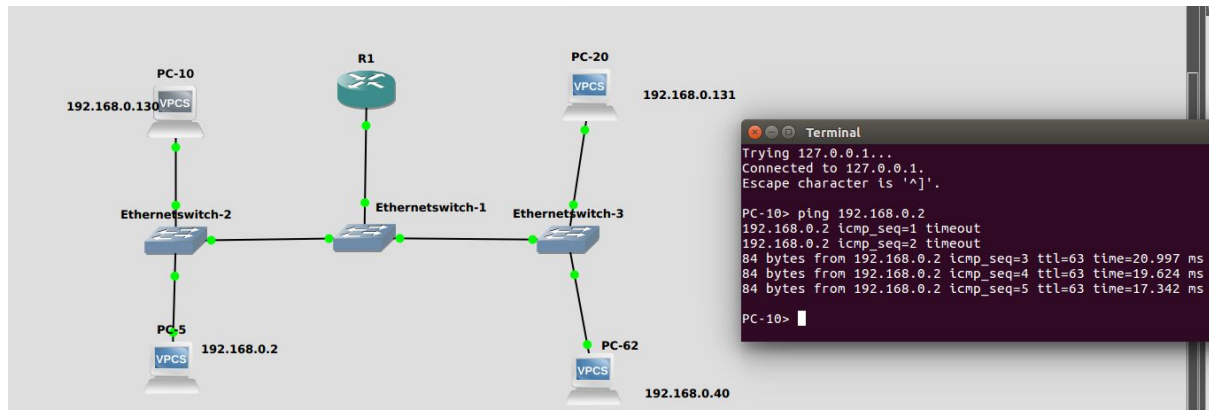
1.-

Partimos de una red cuya dirección es: 192.168.0.0/24, con 254 host disponibles.

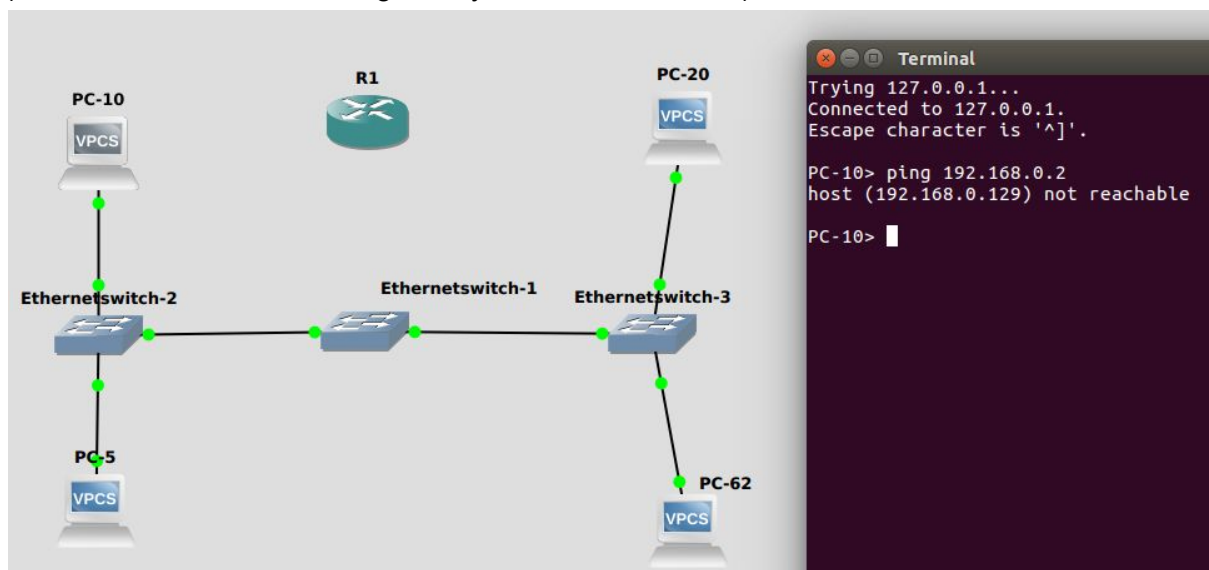
Red	Dirección de red	Máscara de red	Broadcast	Espacio útil
Celeste (67 hosts)	192.168.0.0	255.255.255.128 (/25)	192.168.0.127	192.168.0.1 - 192.168.0.126 (126 hosts)
Verde (30 hosts)	192.168.0.128	255.255.255.192 (/26)	192.168.0.191	192.168.0.129 - 192.168.0.190 (62 hosts)

2.- Al desconectar el router, no hay conectividad entre la red Verde y la red Celeste, esto se debe a que están en dos subredes distintas, y el router es el que realizaba el reenvío los paquetes de una subred a otra (por medio de subinterfaces).

Router conectado: permite la conectividad entre la subred Verde y la subred Celeste.



Router desconectado: la conectividad entre la subred Verde y la subred Celeste desaparece (192.168.0.129 es el default gateway de la subred Verde)



3.- El switch central tiene la característica de tener sus 3 puertos configurados como troncales (dot1q). Los puertos troncales procesan paquetes de múltiples VLANs, permitiendo la comunicación entre ellas, pero no realizan una diferenciación por VLAN (como sí lo hacen los puertos de acceso de los switch de los extremos).

4.- Los puertos que conectan a las LANs están configurados como puertos de acceso (significa que el puerto está configurado para una VLAN en especial), mientras que el puerto que va al switch central está configurado como puerto troncal (permite recibir tramas de VLANs distintas).

5.- Para que el router funcione como si tuviera 2 interfaces se crean subinterfaces (lógicas), logrando así que funcione como un gateway individual para cada subred. A continuación se muestra una captura de la configuración de las subinterfaces del router.

```
FastEthernet0/0.1 is up, line protocol is up
Hardware is Gt96k FE, address is c401.142c.0000 (bia c401.142c.0000)
Internet address is 192.168.0.129/26
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 1.
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters never
FastEthernet0/0.2 is up, line protocol is up
Hardware is Gt96k FE, address is c401.142c.0000 (bia c401.142c.0000)
Internet address is 192.168.0.1/25
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 2.
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters never
```

6.- Cuando un host manda un paquete, dicho paquete no lleva ningún identificador ni sabe a qué VLAN pertenece, y será el switch quien le asigne el identificador de la VLAN a la que esté asociado el puerto de acceso. Cuando el switch recibe un frame Ethernet con una MAC de origen y una MAC de destino, sucede lo siguiente: (se supone que la transmisión es unicast)

- El switch “aprende” el mapeo MAC-Puerto del host origen (si es que este mapeo no existe ya en su tabla).
- El switch, viendo la MAC de destino del frame, se fija si en su tabla hay un puerto (de la misma VLAN que el puerto origen) mapeado con esa MAC para reenviar el frame por dicho puerto. Si no encuentra una correspondencia, manda el frame a todos los puertos correspondientes a esa VLAN excepto por el de origen (esto se denomina unicast desconocido)

7.-

- Si el host de destino está en la misma subred, se realiza una entrega directa sin pasar por el router (suponiendo que los host tienen su caché ARP actualizada)
- Si el host de destino se encuentra en una subred diferente, el frame llega al router (default gateway) y éste realiza el reenvío correspondiente (utilizando las subinterfaces y su tabla de ruteo). El proceso detallado es el siguiente:
 - Al no tener las direcciones MAC el host en el VLAN 1 (red verde) utiliza ARP para saber hacia dónde debe enviar la trama Ethernet.
 - Al saber que el destino no está en la red inmediata (la VLAN 1) el host envía el paquete ICMP hacia el router.
 - El router no conoce las direcciones MAC de los hosts que están en la VLAN 2 (red celeste) así que utiliza ARP para obtenerlos.
 - Ahora el router envía el paquete ICMP hacia el host en la VLAN 2.
 - El host en la VLAN 2 envía el paquete ICMP al router y este al host en la VLAN 1, ahora se toma un camino directo ya que los hosts y el router saben hacia donde deben enviar los paquetes.

Bibliografía

- [1] <https://capa8net.wordpress.com/2014/02/13/tipos-de-puertos-access-trunk/>
- [2] <http://jodies.de/ipcalc>
- [3] <http://www.mustbegeek.com/understanding-vlans-in-switching-world/>
- [4] <https://www.oreilly.com/library/view/network-warrior/9780596101510/ch04.html>
- [5] <https://www.youtube.com/watch?v=QsJ1NArSkOs>