

Trabajo Práctico

TPL 4 - Virtual LAN (VLAN)

Fecha de entrega: 06/10/2021

Franco, Juan Martín 149.615

juanmartin_franco@hotmail.com

Experiencia de laboratorio

En esta experiencia de laboratorio utilizaremos el simulador de redes GNS3 para simular switches que implementan VLAN y crear con ellos un escenario típico de utilización de esta tecnología. Cada fabricante implementa su propia nomenclatura para el comportamiento de los puertos del switch en relación a VLAN. Habitualmente, de acuerdo a la configuración de VLAN, cada puerto del switch puede estar establecido en alguna de las siguientes configuraciones:

- **Untagged** son aquellos donde las tramas ingresan o egresan sin etiqueta y el switch les agrega o elimina la misma (access link según la terminología de Kenyon);
- **Tagged** son aquellos donde las tramas ingresan o egresan ÚNICAMENTE SI YA ESTÁN ETIQUETADAS (trunk link si aceptan más de una etiqueta);
- **No-Miembro y Forbidden** hacen lo correspondiente.
- **Híbrido (según Kenyon)**: son los puertos que pueden recibir tanto tramas ya etiquetadas como no etiquetadas (a las que etiquetará según cierta configuración).

IMPORTANTE: Tener en cuenta que cuando se configuran, habitualmente todos los puertos de un switch están asociados a una VLAN con tag 1 (default), y en el caso que no se quiera que pertenezcan a esa VLAN, se los tiene que pasar para este tag al estado No-Miembro.

Se propone configurar el laboratorio de acuerdo al siguiente esquema (en Figura 1) haciendo uso de VLANs para lograr la separación de los dominios de broadcast.

Dominio de broadcast 1: A, C, E, F Dominio de broadcast 2: B, D, G

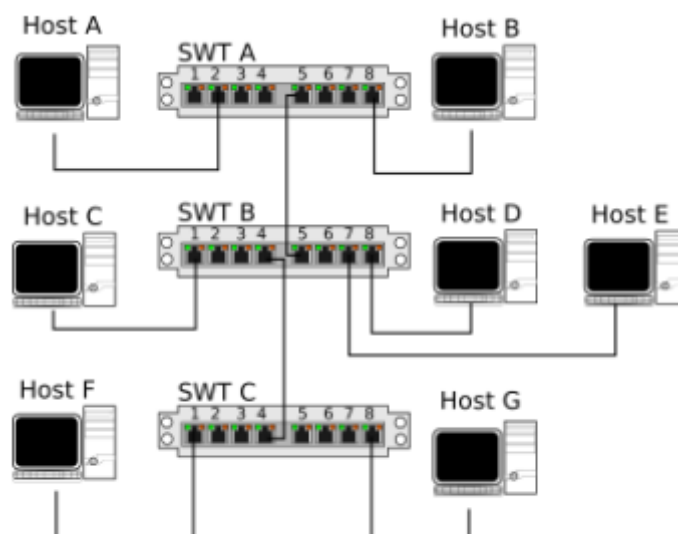
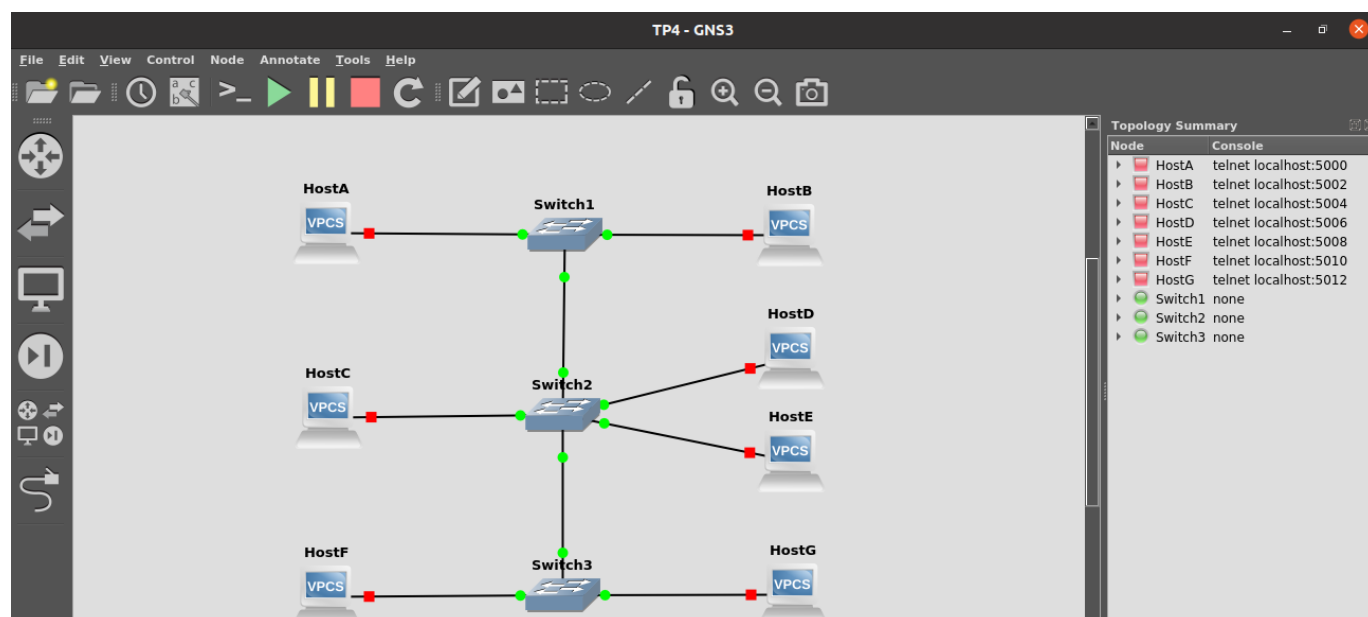


Figura 1: Esquema del laboratorio

Para realizar esto primero recreo la topología de la figura 1 dentro de un proyecto nuevo de GNS3 y luego conecto los enlaces en los puertos correspondientes:



Ahora, para separar los dominios de broadcast, debo hacer que los dispositivos estén en 2 vlans diferentes.

En mi caso, el dominio de broadcast 1 estará definido en la VLAN 100, y el dominio de broadcast 2 será el correspondiente a la VLAN 200.

Las configuraciones de los switches quedan así:

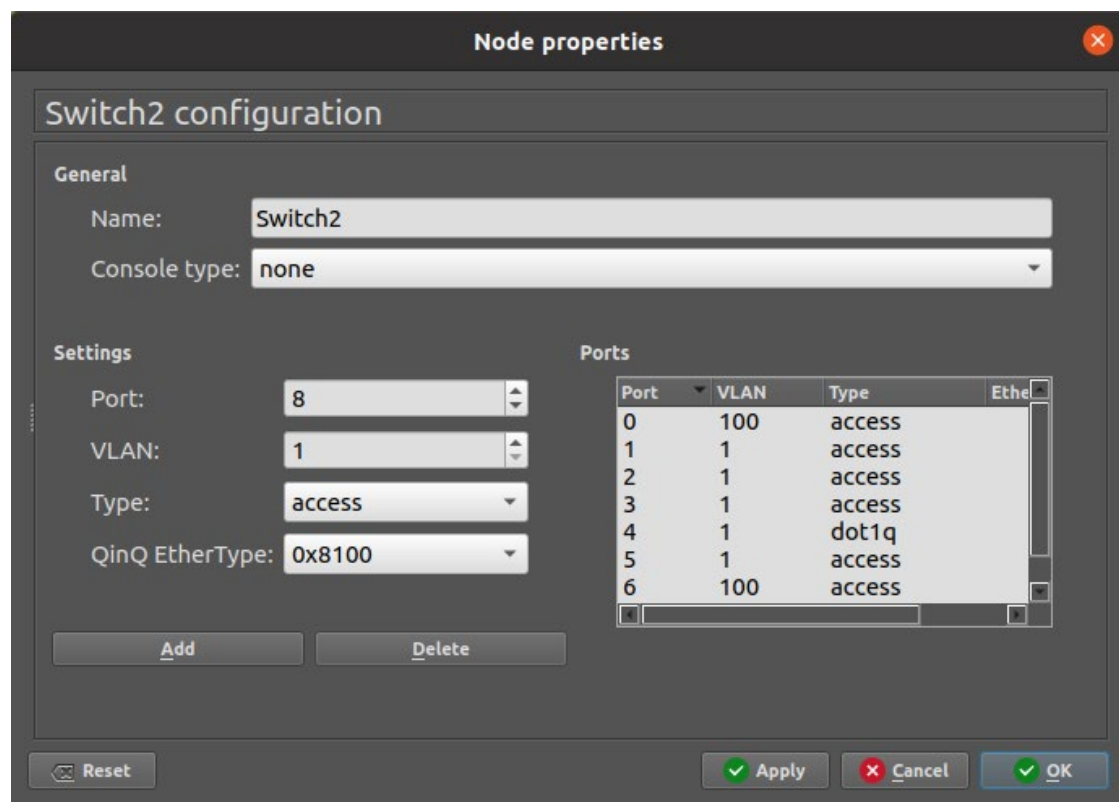
Switch 1:

Port	VLAN	Type	EtherType
0	1	access	
1	100	access	
2	1	access	
3	1	access	
4	1	dot1q	
5	1	access	
6	1	access	

El puerto 1 es el correspondiente al Host A (dominio de broadcast 1) y el puerto 7 es el correspondiente al host B (dominio de broadcast 2).

Ahora, continúo con la configuración del Switch 2..

Switch 2:



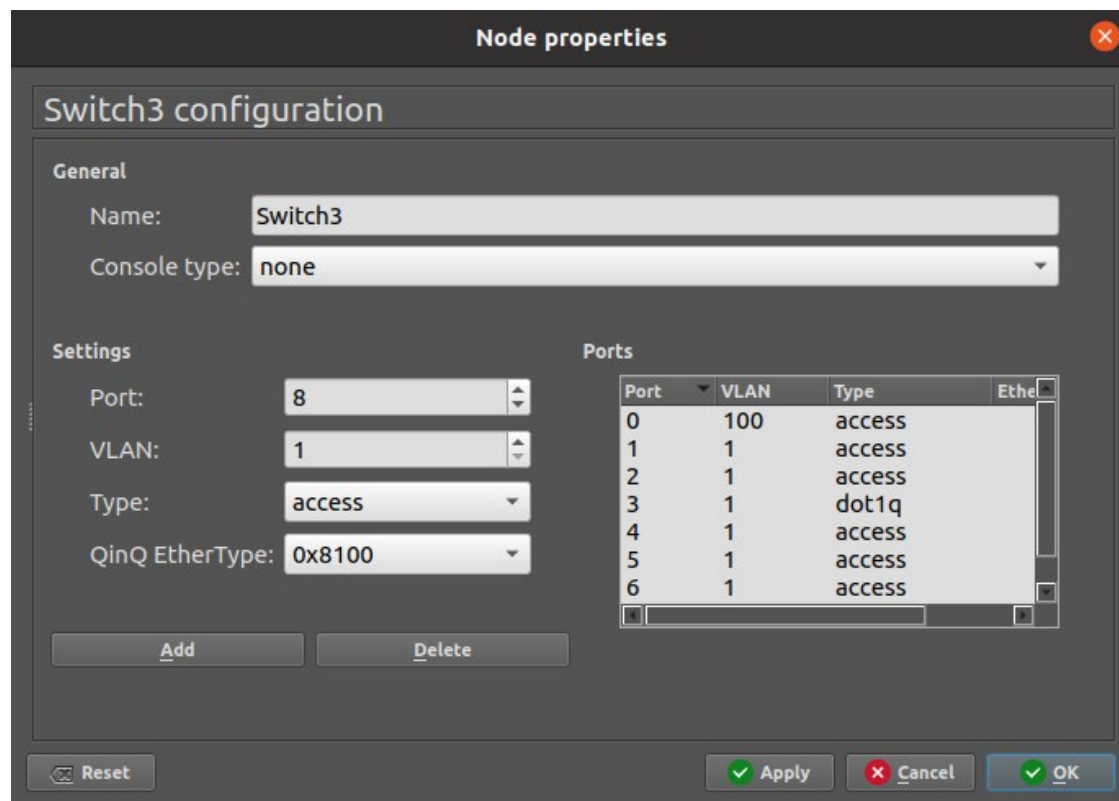
The image shows a 'Node properties' dialog box for 'Switch2 configuration'. It has a 'General' section with 'Name' set to 'Switch2' and 'Console type' set to 'none'. The 'Settings' section on the left includes 'Port' (8), 'VLAN' (1), 'Type' (access), and 'QinQ EtherType' (0x8100). The 'Ports' table on the right lists 7 ports with their respective VLANs and types.

Port	VLAN	Type	Ethe
0	100	access	
1	1	access	
2	1	access	
3	1	access	
4	1	dot1q	
5	1	access	
6	100	access	

El puerto 0 y el puerto 6 corresponden al Host C y al Host E respectivamente (dominio de broadcast 1) mientras que el puerto 7 corresponde al Host D (dominio de broadcast 2).

Por último, resta configurar el Switch 3.

Switch 3:



The image shows a 'Node properties' dialog box for 'Switch3 configuration'. It has a 'General' section with 'Name' set to 'Switch3' and 'Console type' set to 'none'. The 'Settings' section on the left includes 'Port' (8), 'VLAN' (1), 'Type' (access), and 'QinQ EtherType' (0x8100). The 'Ports' table on the right lists 7 ports with their respective VLANs and types.

Port	VLAN	Type	Ethe
0	100	access	
1	1	access	
2	1	access	
3	1	dot1q	
4	1	access	
5	1	access	
6	1	access	

Para finalizar, el puerto 0 del switch 3 corresponde al Host F (dominio de broadcast 1) y el puerto 7 corresponde al Host G (dominio de broadcast 2).

Las IPs quedan configuradas de la siguiente manera:

HostA: 192.168.0.1

HostB: 192.168.0.2

HostC: 192.168.0.3

HostD: 192.168.0.4

HostE: 192.168.0.5

HostF: 192.168.0.6

HostG: 192.168.0.7

Considerar que el host F envía sus tramas con tags ya aplicados.

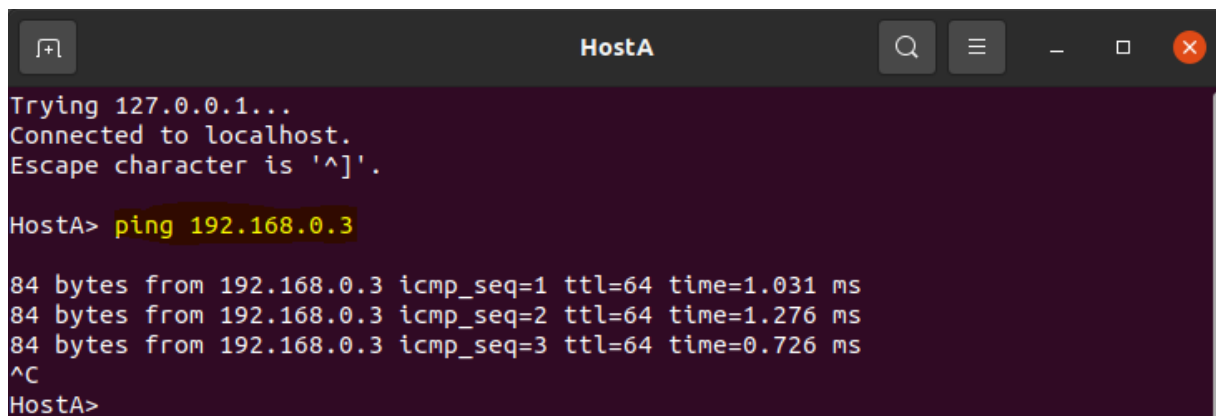
Una vez que se haya terminado de configurar el laboratorio se solicita:

1. Verificar que existe conectividad entre: host A - host C, host A - host F, host B - host G.

Para verificar que existe conectividad primero debo iniciar todos los nodos.

Una vez hecho esto, abro una consola e intento hacer un ping desde Host Origen hacia Host Destino.

Host A – Host C:

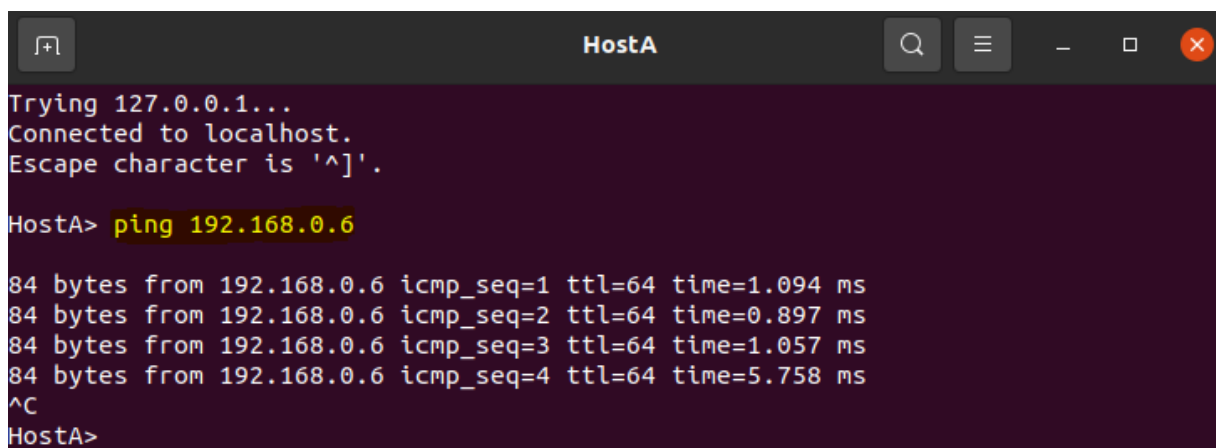


```
HostA
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

HostA> ping 192.168.0.3

84 bytes from 192.168.0.3 icmp_seq=1 ttl=64 time=1.031 ms
84 bytes from 192.168.0.3 icmp_seq=2 ttl=64 time=1.276 ms
84 bytes from 192.168.0.3 icmp_seq=3 ttl=64 time=0.726 ms
^C
HostA>
```

Host A – Host F:



```
HostA
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

HostA> ping 192.168.0.6

84 bytes from 192.168.0.6 icmp_seq=1 ttl=64 time=1.094 ms
84 bytes from 192.168.0.6 icmp_seq=2 ttl=64 time=0.897 ms
84 bytes from 192.168.0.6 icmp_seq=3 ttl=64 time=1.057 ms
84 bytes from 192.168.0.6 icmp_seq=4 ttl=64 time=5.758 ms
^C
HostA>
```

Host B – Host G:

```
HostB
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.

HostB> ping 192.168.0.7

84 bytes from 192.168.0.7 icmp_seq=1 ttl=64 time=2.274 ms
84 bytes from 192.168.0.7 icmp_seq=2 ttl=64 time=2.302 ms
84 bytes from 192.168.0.7 icmp_seq=3 ttl=64 time=2.483 ms
84 bytes from 192.168.0.7 icmp_seq=4 ttl=64 time=1.283 ms
^C
HostB> 
```

2. Verificar la falta de conectividad: host A - host B, host F - host G

Host A – Host B:

```
HostA
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.

HostA> ping 192.168.0.2

host (192.168.0.2) not reachable

HostA> 
```

Host F – Host G:

```
HostF
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.

HostF> ping 192.168.0.7

host (192.168.0.7) not reachable

HostF> 
```

3. Realizar una captura en un puerto trunk (alguno de los que interconecta switches) mientras realiza ping entre host A - host C. Guardarla con el nombre captura_trunk.pncap.

Para realizar una captura en GNS3, clic derecho sobre el enlace → Start Capture, esto automáticamente abrirá Wireshark e iniciará la captura.

Una vez iniciada la captura, procedo a realizar un ping entre el HostA y el HostC:

Situándome en la terminal del Host A ejecuto el comando:

```
ping 192.168.0.3
```

```

HostA
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

HostA> ping 192.168.0.3

84 bytes from 192.168.0.3 icmp_seq=1 ttl=64 time=0.966 ms
84 bytes from 192.168.0.3 icmp_seq=2 ttl=64 time=1.095 ms
84 bytes from 192.168.0.3 icmp_seq=3 ttl=64 time=1.481 ms
84 bytes from 192.168.0.3 icmp_seq=4 ttl=64 time=1.047 ms
84 bytes from 192.168.0.3 icmp_seq=5 ttl=64 time=0.912 ms

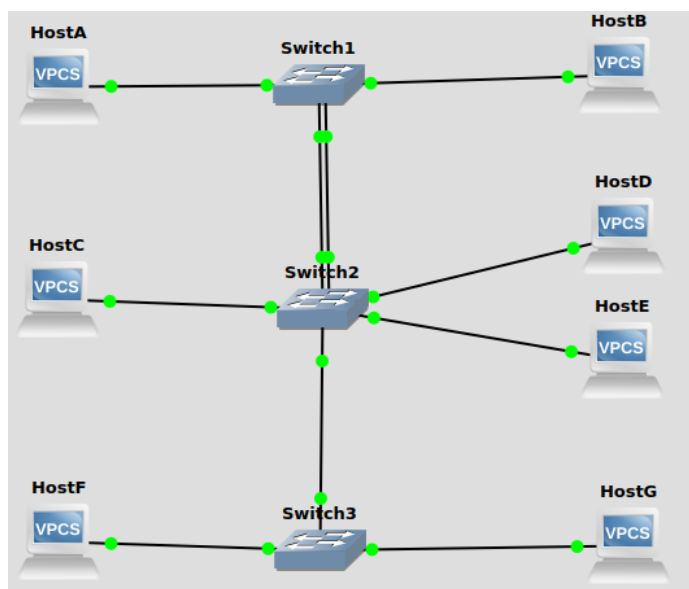
HostA>

```

4. Interconectar SWITCH A y el SWITCH B con otro patchcord, ¿Se genera un bucle? ¿Por qué?

Para hacer esto, me dirijo hacia la opción “Add a link” del menú de GNS3 y conecto los 2 switches en algún puerto que no esté siendo utilizado.

En mi caso, opté por utilizar el puerto 5 de ambos switches, quedando la topología de la siguiente manera:



Efectivamente, ocurre un bucle al agregar otro patchcord (el cual puede ser solucionado con el protocolo STP). Para visualizar esto, decidí hacer una captura y luego realizar el mismo procedimiento (un ping desde Host A hacia Host C), obteniendo los siguientes resultados:

No.	Time	Source	Destination	Protocol	Length	Info
228210	56.286374	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228213	56.286573	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228230	56.293345	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228235	56.294902	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228252	56.300277	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228259	56.301317	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228274	56.305686	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228284	56.307475	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228296	56.311670	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228311	56.314266	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228314	56.315630	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228334	56.319772	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228337	56.323686	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228352	56.339843	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228363	56.339959	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228374	56.353752	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228390	56.359333	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228395	56.360670	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228415	56.364538	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228418	56.366042	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228437	56.369823	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228445	56.372185	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1
228456	56.373630	Private_66:68:00	Broadcast	ARP	68	Who has 192.168.0.3? Tell 192.168.0.1

Como se sabe, lo primero que sucede antes de los mensajes ICMP Echo-Request y Echo-Reply, son los mensajes ARP a la dirección de **broadcast** preguntando cual es la MAC de la dirección IP a la cual se le quiere hacer el ping.

En este caso, se generan demasiados mensajes ARP ya que el mensaje se envía por los 2 enlaces.

Por último, el host destino responde dicho mensaje con su dirección IP al host origen.

ip.src == ip.src == ip.src == ip.src == 192.168.0.3						
No.	Time	Source	Destination	Protocol	Length	Info
	110438 32.029430	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x96ec, seq=3/768,
	117424 33.281579	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	117591 33.304796	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	117753 33.328845	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	117915 33.354874	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118091 33.387258	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118254 33.413398	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118422 33.437660	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118601 33.466473	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118790 33.495907	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	118930 33.526608	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	117262 33.257057	192.168.0.3	192.168.0.1	ICMP	102	Echo (ping) reply id=0x97ec, seq=4/1024
	94328 28.993283	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x93ec, seq=1/256,
	99526 30.002013	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x94ec, seq=2/512,
	99546 30.005283	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x94ec, seq=2/512,
	99568 30.009347	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x94ec, seq=2/512,
	110256 32.002687	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x96ec, seq=3/768,
	110275 32.005659	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x96ec, seq=3/768,
	110295 32.009232	192.168.0.1	192.168.0.3	ICMP	102	Echo (ping) request id=0x96ec, seq=3/768,

Como se ve en la imagen anterior, se generan muchos mensajes para tan solo 5 pings, y esto es porque los mensajes ICMP devuelven su respuesta por ambos enlaces.

Algunos mensajes ICMP quedan dando vuelta (por del bucle generado por los 2 enlaces) y no obtienen respuesta.

Esto puede visualizarse en la siguiente imagen:

Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Code: 0	
Checksum: 0x871a [correct]	
[Checksum Status: Good]	
Identifier (BE): 39148 (0x98ec)	
Identifier (LE): 60568 (0xec98)	
Sequence number (BE): 5 (0x0005)	
Sequence number (LE): 1280 (0x0500)	
▶ [No response seen]	
▶ Data (56 bytes)	

Trabajo práctico

1. Analizar la captura realizada en la experiencia anterior, elegir una trama ethernet 802.1Q, identificar qué es lo que se agrega a la trama original, cual es el tag de la VLAN y comparar el campo “Ether Type” con otra trama sin etiquetar. ¿Qué diferencia observa? ¿Por qué?

Trama de Ethernet 802.1Q:

```
Frame 5: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:02 (00:50:79:66:68:02)
  Destination: Private_66:68:02 (00:50:79:66:68:02)
  Source: Private_66:68:00 (00:50:79:66:68:00)
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
    000. .... = Priority: Best Effort (default) (0)
    ...0 .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0xe759 (59225)
  Flags: 0x0000
  Fragment offset: 0
  Time to live: 64
```

Como se ve en la imagen, a la PDU original se le agrega dos campos los cuales corresponden a la sección 802.1Q VLAN, los cuales son TPID y TCI.

Primero, el campo TPID (Tag Protocol Identifier) es un campo de 16 bits el cual siempre contiene el valor 0x8100 (valor correspondiente a 802.1Q Virtual LAN).

El campo TPID se encuentra en la misma posición que el campo EtherType en tramas sin etiquetar y, por lo tanto, se utiliza para distinguir la trama de las tramas sin etiquetar.

Luego, se agrega otro apartado que se llama TCI (Tag Control Information).

Esta sección de la PDU contiene 3 campos:

1. El campo Priority: Este campo, el cual es de 3 bits, identifica la prioridad de la trama (relacionado con QoS).
2. El campo DEI: Anteriormente conocido como CFI, este campo de 1 bit se utiliza para indicar tramas elegibles para descartarse en presencia de congestión. Su valor es siempre 0.
3. El campo ID: Este campo de 12 bits se utiliza para identificar la VLAN a la cual pertenece la trama, en este caso 100 (la trama pertenece a la VLAN 100). Los valores 0x000 y 0xFFFF están reservados.

2. Identifique los diferentes dominios de broadcast existentes y los hosts que pertenecen a cada uno en el esquema de una LAN de la Figura 2.

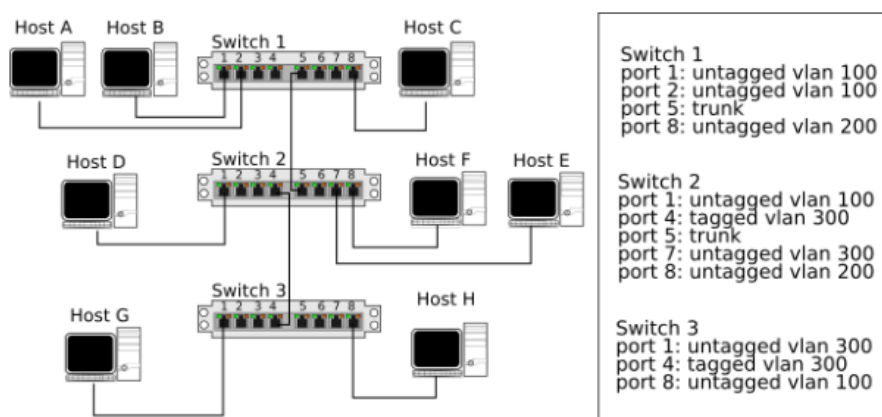


Figura 2: Separación de dominios de broadcast

Los dominios de Broadcast son los siguientes:

Dominio de Broadcast #1:

- VLAN 100.
 1. Host A.
 2. Host B.
 3. Host D.

Dominio de Broadcast #2:

- VLAN 200.
 1. Host C.
 2. Host F.

Dominio de Broadcast #3:

- VLAN 300.
 1. Host E.
 2. Host G.

El Host H quedó aislado ya que pertenece al Switch 3 y dicho Switch solo pasa tramas pertenecientes a la VLAN 300 (ya que el enlace en ambos extremos está configurado como “tagged vlan 300”).

3. Teniendo en cuenta la topología de red de la Figura 3, suponga que el usuario del Host 1 ejecuta el siguiente comando en su terminal: `ping www.polito.it`

Determine cuales serían las tramas y de qué tipo las capturadas por el sniffer localizado en el cable que conecta el switch SW-1 con el SW-2 (simbolizado con una lupa), suponiendo que:

- Todas las tablas ARP están vacías
- Todos los caché DNS están vacíos
- El servidor DNS `polito.it` tiene la capacidad y la información para contestar la consulta acerca del dominio `www.polito.it`
- Los routers están correctamente configurados, y
- Las VLANs están correctamente configuradas (hosts, servers, routers, switches).

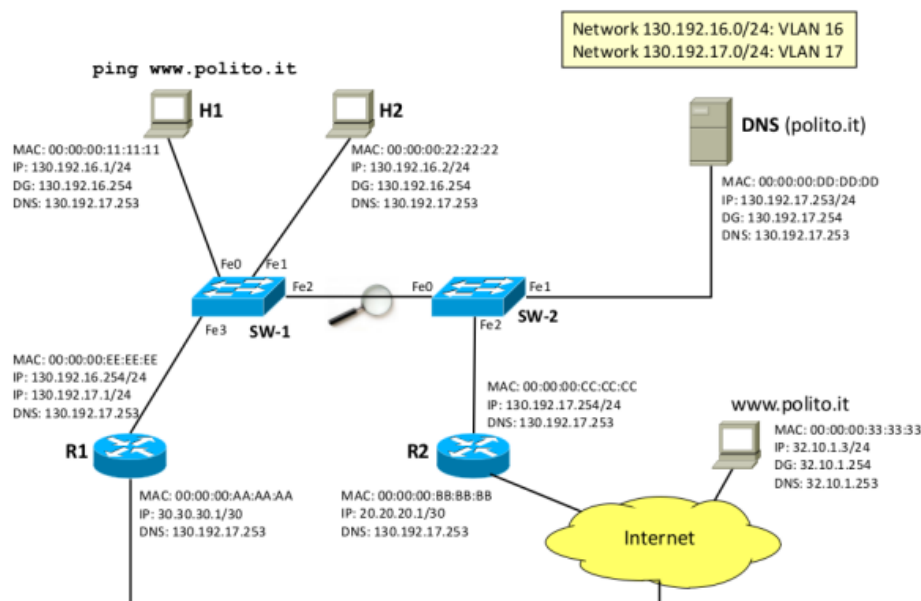
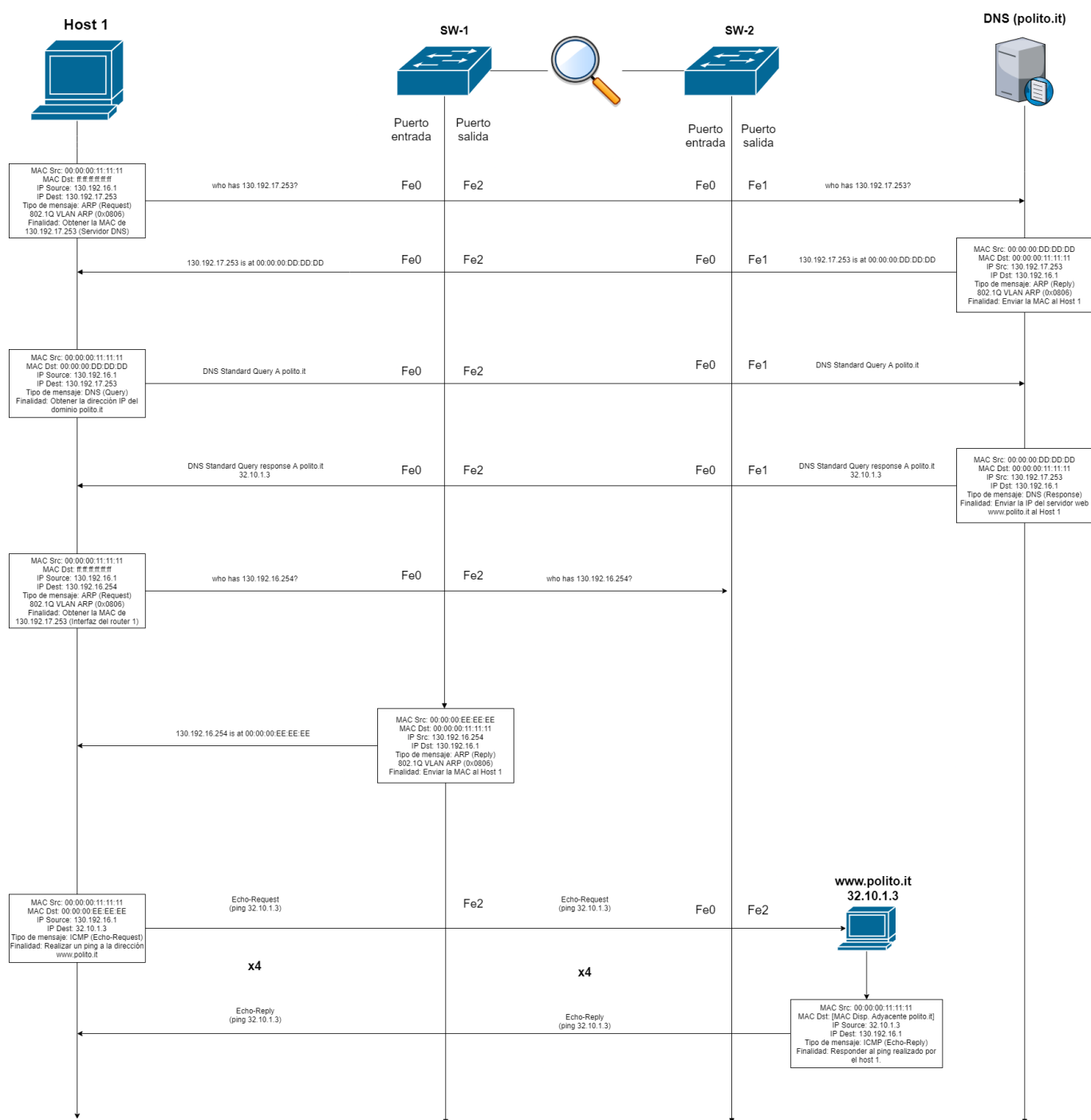


Figura 3: Ping con VLANs

Teniendo en cuenta la topología de la Figura 3, en el escenario donde el usuario ubicado en el Host 1 realiza un ping a la dirección `www.polito.it`, las tramas que pasarían por el enlace en donde se está realizando la captura son las siguientes:



Aclaración: Solo se han detallado las tramas que pasan por el enlace donde se está capturando el tráfico, por lo que hay detalles que no se visualizan, como por ej.: las consultas iterativas del resolver DNS (ya que el DG del DNS es 130.192.17.254, por lo que la salida es por el puerto Fe2 del Sw2).

4. Dada la siguiente topología, ¿Es posible realizar un ping entre A y B? ¿Es posible realizar un ping A y C?

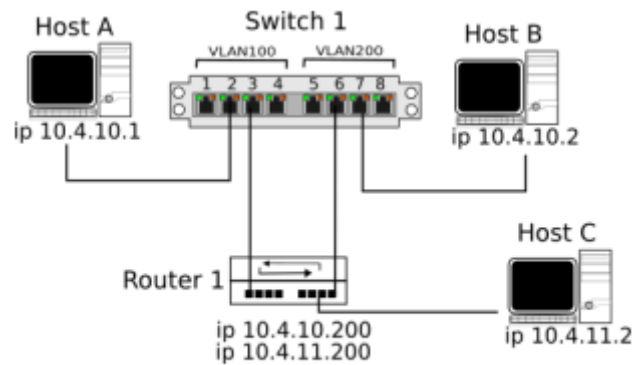


Figura 4: Ruteo y VLAN

Es posible realizar un ping entre el Host A y el Host B debido a que se está aplicando la técnica conocida como “enrutamiento entre VLANs” (o Inter-VLAN Routing), la cual permite que 2 VLANs distintas se comuniquen entre si mediante el reenvío de trafico por medio de un router.

Obviamente, para que esto funcione, las interfaces que forman los enlaces entre el Switch y el Router deben estar definidas en modo “trunk”.

No es posible realizar un ping entre Host A y Host C ya que, pertenecen a distinta subred y el default Gateway del Host C es 10.4.11.200, por lo que la trama sería enviada a la VLAN 200, pero nunca llegaría dicha respuesta al Host A.