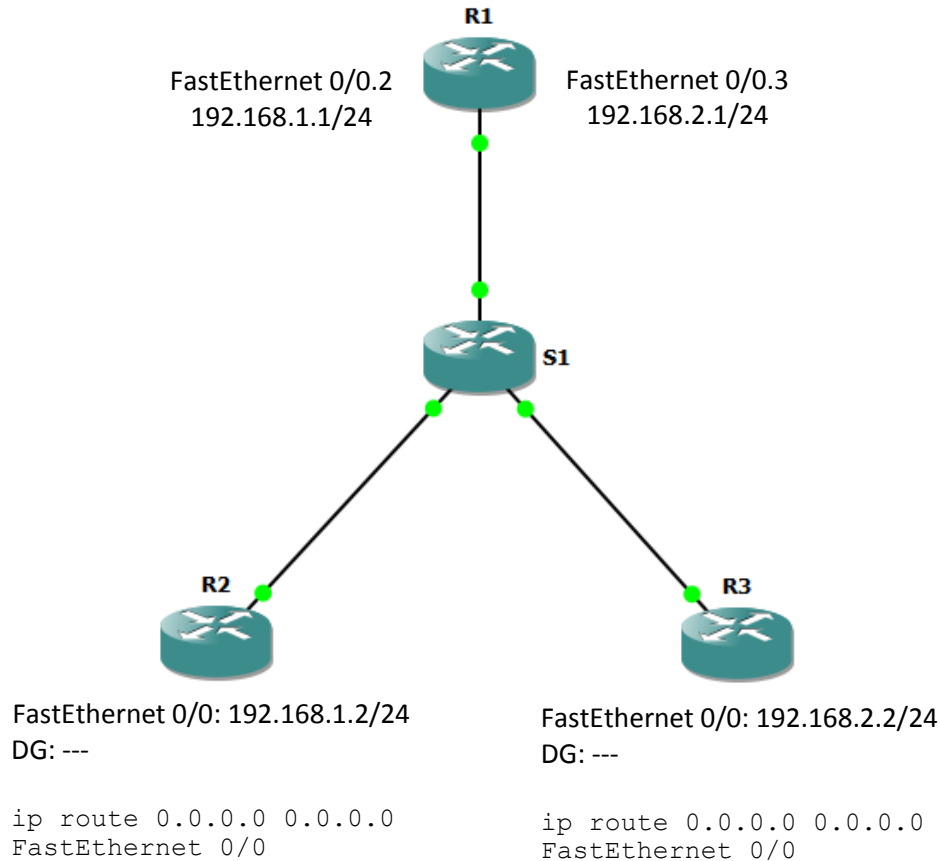


Laboratorio VLAN
Nicola Alessandro Domingo – 177363

4. VLAN Analysis

1.



2.

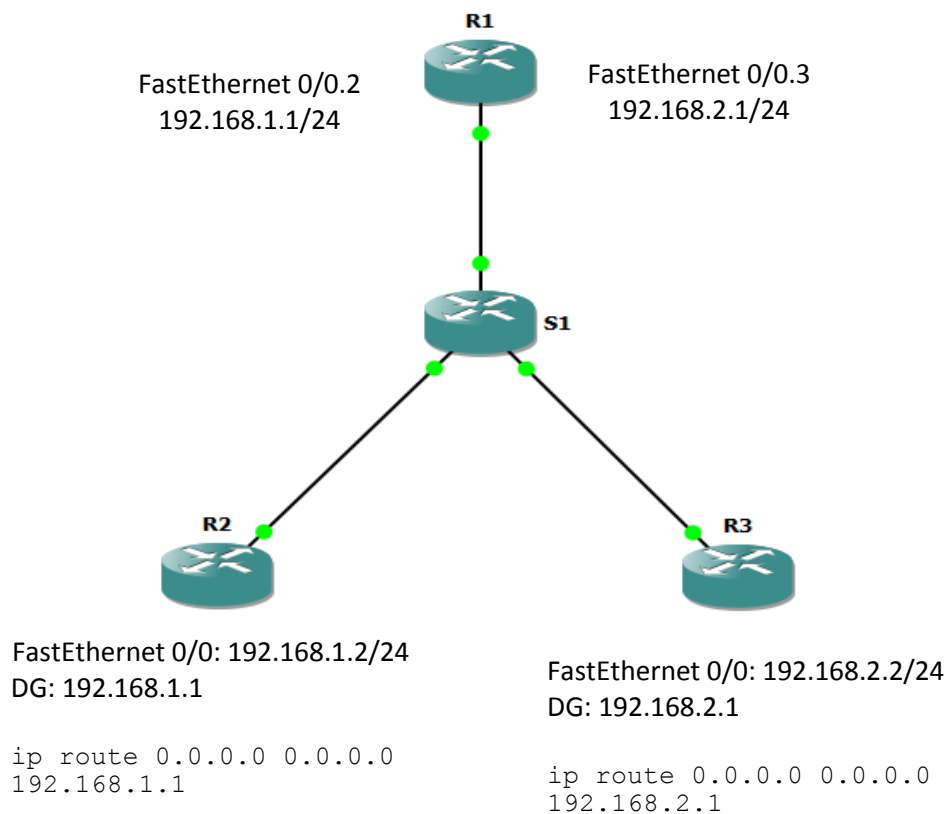
- Le trame sul link trunk hanno 4 byte in più, dato l'incapsulamento 802.1q. Vi è presente, infatti, il tag VLAN corrispondente alle VLAN 12 e 13.
- Alcuni pacchetti risultano duplicati in quanto apparentemente sembra che lo stesso IP, 192.168.2.2, sembra associato a due MAC differenti, quelli di R1 ed R3. Ciò è dovuto al fatto che quando R2 fa l'ARP Request con IP target quello di R3 (192.168.2.2), R1 risponde che lo può trovare al suo indirizzo MAC. Quando R1 fa a sua volta una ARP Request per sapere il MAC di R3, R3 che ha appunto IP 192.168.2.2 risponde con il suo vero MAC. Ciò va in contraddizione con quanto R1 aveva fatto credere ad R2, ma è giusto così, in quanto R2 ed R3 fanno parte di VLAN diverse, interconnesse dal one-arm router R1. Analogamente, quando R3 fa un'ARP Request con target IP quello di R2 per conoscere il suo MAC, R1 risponde invece con il suo MAC, ed anche qui viene rilevato un indirizzo IP apparentemente duplicato su due MAC diversi. Poiché le route statiche impostate non indicano l'IP del default gateway ma l'interfaccia d'uscita dei pacchetti, le catture mostrano come R2 e R3 facciamo una ARP Request per conoscere l'indirizzo MAC di un IP non appartenente alla loro stessa sottorete. Questa tecnica prende il nome di Proxy ARP e consiste nel fatto che un router risponda alle ARP Request di qualsiasi indirizzo IP che non stia su quella sottorete ma che lui sa come raggiungere, annunciando che il proprio MAC corrisponda a tutti gli IP di questo tipo. Ciò facilita la configurazione della rete rendendo non necessaria la configurazione di un default gateway su ogni host.

3.

No.	Time	Source	Destination	Protocol	Info
961	289.968680	c0:02:41:81:00:00	Broadcast	ARP	who has 192.168.2.2? Tell 192.168.1.2
962	289.968710	c0:02:41:81:00:00	Broadcast	ARP	who has 192.168.2.2? Tell 192.168.1.2
963	289.972796	c0:01:41:81:00:00	c0:02:41:81:00:00	ARP	192.168.2.2 is at c0:01:41:81:00:00
964	289.972819	c0:01:41:81:00:00	c0:02:41:81:00:00	ARP	192.168.2.2 is at c0:01:41:81:00:00
973	291.990469	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=1/256, ttl=255)
974	291.990479	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=1/256, ttl=255)
975	291.994618	c0:01:41:81:00:00	Broadcast	ARP	who has 192.168.2.2? Tell 192.168.2.1
976	291.994639	c0:01:41:81:00:00	Broadcast	ARP	who has 192.168.2.2? Tell 192.168.2.1
977	292.004914	c0:03:41:81:00:00	c0:01:41:81:00:00	ARP	192.168.2.2 is at c0:03:41:81:00:00
978	292.004936	c0:03:41:81:00:00	c0:01:41:81:00:00	ARP	192.168.2.2 is at c0:03:41:81:00:00
986	293.992550	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=2/512, ttl=255)
987	293.992569	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=2/512, ttl=255)
989	293.994619	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=2/512, ttl=254)
990	293.994631	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=2/512, ttl=254)
992	294.000857	c0:03:41:81:00:00	Broadcast	ARP	who has 192.168.1.2? Tell 192.168.2.2 (duplicate use of 192.168.2.2 detected)
993	294.000876	c0:03:41:81:00:00	Broadcast	ARP	who has 192.168.1.2? Tell 192.168.2.2 (duplicate use of 192.168.2.2 detected)
994	294.002966	c0:01:41:81:00:00	c0:03:41:81:00:00	ARP	192.168.1.2 is at c0:01:41:81:00:00 (duplicate use of 192.168.2.2 detected)
995	294.002981	c0:01:41:81:00:00	c0:03:41:81:00:00	ARP	192.168.1.2 is at c0:01:41:81:00:00 (duplicate use of 192.168.2.2 detected)
1000	295.975890	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=3/768, ttl=255)
1001	295.975912	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=3/768, ttl=255)
1002	295.977956	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=3/768, ttl=254)
1003	295.977966	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=3/768, ttl=254)
1004	295.980018	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=3/768, ttl=255)
1005	295.980027	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=3/768, ttl=255)
1006	295.982084	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=3/768, ttl=254)
1007	295.982107	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=3/768, ttl=254)
1008	295.986205	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=4/1024, ttl=255)
1009	295.986217	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=4/1024, ttl=255)
1010	295.988268	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=4/1024, ttl=254)
1011	295.988278	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=4/1024, ttl=254)
1012	295.990331	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=4/1024, ttl=255)
1013	295.990338	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=4/1024, ttl=255)
1014	295.992397	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=4/1024, ttl=254)
1015	295.992406	192.168.2.2	192.168.1.2	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=4/1024, ttl=254)
1026	299.214773	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
1027	299.214790	192.168.1.2	192.168.2.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)

Si ripropone l'esercitazione stavolta impostando un default gateway ad R2 e R3.

1.



2.

- Le trame sul link trunk hanno 4 byte in più, dato l'incapsulamento 802.1q. Vi è presente, infatti, il tag VLAN corrispondente alle VLAN 12 e 13.
- I pacchetti sembrano essere duplicati sul link trunk tra S1 ed R1 in quanto essi lo attraversano una prima volta con il tag della VLAN 12, ed una seconda volta con il tag della VLAN 13. Stavolta, come normalmente ci si aspetta, R2 ed R3 fanno una ARP Request con IP target quello del loro default gateway.

■ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
 ■ Ethernet II, Src: c0:02:63:e0:00:00 (c0:02:63:e0:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ■ Address Resolution Protocol (request)

Per gli host R2 ed R3 il settaggio di una route è invece necessaria, e si è vista la differenza nel caso in cui venga fornita sia l'interfaccia d'uscita che l'indirizzo IP del default gateway.