

Laboratorio Filtering database
Nicola Alessandro Domingo – 177363

4.1 – Informazioni sulle interfacce

Dispositivo	Interfaccia	Indirizzo MAC
R1	FastEthernet 0/0	C003.4ACF.0000
R2	FastEthernet 0/0	C004.4ACF.0000
S1	FastEthernet 1/0	C002.4ACF.F100
	FastEthernet 1/1	C002.4ACF.F101
	FastEthernet 1/2	C002.4ACF.F102
	FastEthernet 1/3	C002.4ACF.F103
S2	FastEthernet 1/0	C001.4ACF.F100
	FastEthernet 1/1	C001.4ACF.F101
S3	FastEthernet 1/0	C000.4ACF.F100
	FastEthernet 1/1	C000.4ACF.F101

4.2 – Filtering Database (prima del ping)

Dispositivo	Destination Address	Address Type	VLAN	Destination Port
S1	C002.4ACF.0000	Self	1	VLAN1
S2	C001.4ACF.0000	Self	1	VLAN1
S3	C000.4ACF.0000	Self	1	VLAN1

4.3

Gli indirizzi MAC al punto 1 non sono presenti nei filtering database degli switch perché gli host R1 e R2 non hanno ancora immesso alcuna trama nella LAN.

4.7 – Filtering Database (dopo il ping)

Dispositivo	Destination Address	Address Type	VLAN	Destination Port
S1	C002.4ACF.0000	Self	1	VLAN1
	C003.4ACF.0000	Dynamic	1	FastEthernet 1/0
	C004.4ACF.0000	Dynamic	1	FastEthernet 1/1
S2	C001.4ACF.0000	Self	1	VLAN1
	C003.4ACF.0000	Dynamic	1	FastEthernet 1/0
S3	C000.4ACF.0000	Self	1	VLAN1
	C003.4ACF.0000	Dynamic	1	FastEthernet 1/1

Adesso gli indirizzi MAC al punto 1 sono presenti nei filtering database in quanto R1 e R2 inviano le trame del ping e gli switch cominciano a popolare i loro filtering database.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=0/0, ttl=255)
2	0.000042	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=0/0, ttl=255)
3	0.000070	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=0/0, ttl=255)
4	0.000095	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=0/0, ttl=255)
5	0.000107	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=0/0, ttl=255)
6	0.004574	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=0/0, ttl=255)
7	0.004588	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=0/0, ttl=255)
8	0.008720	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=1/256, ttl=255)
9	0.008738	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=1/256, ttl=255)
10	0.010798	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=1/256, ttl=255)
11	0.010814	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=1/256, ttl=255)
12	0.012889	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=2/512, ttl=255)
13	0.012905	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=2/512, ttl=255)
14	0.014952	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=2/512, ttl=255)
15	0.014966	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=2/512, ttl=255)
16	0.017045	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=3/768, ttl=255)
17	0.017061	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=3/768, ttl=255)
18	0.019109	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=3/768, ttl=255)
19	0.019122	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=3/768, ttl=255)
20	0.021200	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=4/1024, ttl=255)
21	0.021217	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0000, seq(be/le)=4/1024, ttl=255)
22	0.023267	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=4/1024, ttl=255)
23	0.023280	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0000, seq(be/le)=4/1024, ttl=255)

4.8

R1 invia l'echo request ad S1 che aggiunge l'entry a lui relativa nel suo filtering database. Non conoscendo ancora l'interfaccia con cui raggiungere R2, invia la trama in flooding che raggiunge R2 e S2 (l'interfaccia verso S3 è down).

S2 aggiunge l'entry nel suo filtering database relativa a R1 e inoltra la trama verso S3, che a sua volta aggiunge anche lui l'entry corrispondente a R1.

R2 che ha ricevuto l'echo request invia l'echo reply ad S1.

Questi aggiunge l'entry relativa ad R2 nel suo filtering database e siccome già è presente l'entry relativa a R1 inoltra l'echo reply solo nella sua interfaccia Fa1/0 verso R1; tale trama quindi non raggiungerà né S2, né S3, che non impareranno il MAC di R2.

5.4

No.	Time	Source	Destination	Protocol	Info
3826	44.295880	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3827	44.295883	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3828	44.295905	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3829	44.295920	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3830	44.295954	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3831	44.295974	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3832	44.295984	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3833	44.296010	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3834	44.296028	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3835	44.296036	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3836	44.296059	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3837	44.296073	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3838	44.296095	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3839	44.296110	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3840	44.296145	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3841	44.296165	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3842	44.296175	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3843	44.296202	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3844	44.296219	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3845	44.296234	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3846	44.296263	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3847	44.296284	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
3848	44.296320	192.168.0.1	192.168.0.2	ICMP	Echo (ping) request (id=0x0002, seq(be/le)=0/0, ttl=255)
5656	44.314953	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5657	44.314960	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5658	44.314965	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5659	44.314967	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5660	44.314974	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5661	44.314979	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5662	44.314981	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5663	44.314989	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5664	44.314993	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5665	44.314995	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5666	44.315003	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5667	44.315007	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5668	44.315009	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5669	44.315017	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5670	44.315021	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5671	44.315023	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5672	44.315031	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5673	44.315035	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5674	44.315038	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5675	44.315045	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5676	44.315050	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)
5677	44.315052	192.168.0.2	192.168.0.1	ICMP	Echo (ping) reply (id=0x0002, seq(be/le)=0/0, ttl=255)

5.5

In questo caso la cattura presenta un gran numero di echo request ed echo reply. La nuova topologia di rete, infatti, presenta un loop e le trame al suo interno continuano a girare in tutte le direzioni poiché i filtering database degli switch si aggiornano in continuazione.

Infatti, gli switch vedono arrivare trame provenienti dallo host da interfacce diverse, e perciò modificano la rispettiva entry nel filtering database di conseguenza. In pratica ecco quello che succede.

L'host R1 invia un echo request ed S1 vede tale host raggiungibile attraverso la sua interfaccia Fa1/0. S1 non ha nel suo filtering database il MAC di R2 ed invia la trama in flooding su tutte le porte tranne quella dalla quale l'ha ricevuta.

S2 riceve la trama, e vede R1 raggiungibile dalla sua interfaccia Fa1/0 ed inoltra la trama verso S3 che vede R1 raggiungibile dalla sua interfaccia Fa1/1 ed inoltra la trama ad S1.

S1, che prima credeva che R1 fosse raggiungibile da Fa1/0, a causa della trama che ha appena ricevuto da S3, aggiorna il suo filtering database ed indica R1 come raggiungibile da Fa1/3. Se ancora S1 non ha ricevuto alcuna trama da R2, reinoltrerà questa trama in flooding su tutte le porte tranne quella dalla quale l'ha ricevuta. Lo stesso discorso è valido per la trama contenente l'echo reply di R2 e all'interno della LAN vedremo un gran numero di trame che girano.