

# Анализ сетевых Дампов

## Dump №1

Извиняюсь что после делаина, в предыдущем не успел вообще ничего проанализировать. Вот сел в выходные, и решил скинуть. Может зачтется за исключение штрафных баллов.

На первом дампе можно увидеть протокол VRRP. VRRP (Virtual Router Redundancy Protocol) — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Фактически, если один маршрутизатор(мастер) выйдет из строя, подключится запасной. Два физических маршрутизатора объединяются и создают виртуальный маршрутизатор, ip которого проставляется у хостов как Шлюз по-умолчанию.

P.S. Думал какая то атака на этот протокол, но в первом дампе меня лишь смущает одинаковые MAC адреса ip 10.10.10.2 и 10.10.12.6.

10.10.10.2 по идее мастер роутер, которые отправляет VRRP сообщения остальным о своем состоянии. Ему назначается вируатльный MAC адрес с началом 00:00:5E:00:01:{VRID(01)}.

Так вот, на пинге от 10.10.10.8 до 10.10.12.6 мы видим одни Мак Адреса на запросе 43.

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
35	13.591023	10.10.10.8	10.10.12.6	ICMP	98	Echo (ping) request id=0xf2d2, seq=2/512, ttl=64 (no response found!)
36	14.386001	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
37	14.614985	10.10.10.8	10.10.12.6	ICMP	98	Echo (ping) request id=0xf2d2, seq=3/768, ttl=64 (no response found!)
38	15.219347	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
39	15.228928	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
40	15.638253	10.10.10.8	10.10.12.6	ICMP	98	Echo (ping) request id=0xf2d2, seq=4/1024, ttl=64 (no response found!)
41	16.187261	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
42	16.602000	10.10.10.8	10.10.12.6	ICMP	98	Echo (ping) request id=0xf2d2, seq=5/1280, ttl=64 (no response found!)
43	17.022848	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
44	17.236026	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
45	17.596409	Vmware_39:b5:1f	IETF-VRRP-VRID_01	ARP	42	Who has 10.10.10.1? Tell 10.10.10.8
46	17.598844	IETF-VRRP-VRID_01	Vmware_39:b5:1f	ARP	60	10.10.10.1 is at 00:00:5e:00:01:01
47	17.982714	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
48	18.794959	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
49	18.188988	10.10.10.2	224.0.0.5	OSPF	90	Hello Packet
50	19.253999	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
51	19.721379	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
52	20.722316	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
53	21.261938	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
54	21.673945	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
55	22.628891	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
56	23.267891	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
57	23.613525	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
58	24.609273	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
59	25.276924	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
60	25.516707	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
61	26.508038	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
62	27.285578	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
63	27.315298	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
64	28.150999	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
65	28.980671	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
66	29.190716	10.10.10.2	224.0.0.5	OSPF	90	Hello Packet
67	29.290710	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST. Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
68	29.943625	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)

Frame 42: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface  
Ethernet II, Src: Vmware\_39:b5:1f (00:0c:29:39:b5:1f), Dst: IETF-VRRP-VRID\_01 (00:00:5e:00:01:01)  
Internet Protocol Version 4, Src: 10.10.10.8, Dst: 10.10.12.6  
Internet Control Message Protocol

А на следующем пинге на запросе 71 у src другой мас адрес, а dst - широковещательный.

No.	Time	Source	Destination	Protocol	Length	Info
50	19.253999	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
51	19.721379	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
52	20.722316	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
53	21.261038	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
54	21.673945	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
55	22.028001	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
56	23.267001	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
57	23.613525	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
58	24.609273	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
59	25.276914	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
60	25.516707	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
61	26.500838	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
62	27.295570	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
63	27.315298	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
64	28.150099	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
65	28.908671	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
66	29.190716	10.10.10.2	224.0.0.5	OSPF	90	Hello Packet
67	29.290710	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
68	29.943625	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
69	30.852853	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
70	31.297003	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
71	31.604040	10.10.10.8	10.10.12.6	ICMP	62	Echo (ping) request id=0x0042, seq=66/16896, ttl=64 (no response found!)
72	31.852962	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
73	32.730971	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
74	33.300304	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
75	33.561900	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
76	34.559071	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
77	34.675960	10.10.10.8	10.10.12.6	ICMP	62	Echo (ping) request id=0x0042, seq=66/16896, ttl=64 (no response found!)
78	35.309612	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
79	35.479710	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
80	36.386486	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
81	37.291079	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)
82	37.912504	aa:bb:cc:00:01:30	Spanning-tree-(for-...	STP	60	RST, Root = 32768/101/aa:bb:cc:00:01:00 Cost = 0 Port = 0x8004
83	38.121200	10.10.10.2	224.0.0.18	VRRP	60	Announcement (v2)

\* Frame 71: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)  
 \* Ethernet II, Src: 0e:5c:49:19:32:bf (0e:5c:49:19:32:bf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 \* 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 101  
 \* 802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 212  
 \* Internet Protocol Version 4, Src: 10.10.10.8, Dst: 10.10.12.6  
 \* Internet Control Message Protocol

То есть пинги летят всем устройствам в сети. А получателем станет MAC адрес, который появился в src - 0e:5c:49:19:32:bf  
 Выглядит как ICMP flood атака или Smurf атака.

## Dump №2

На втором дампе видно, что происходит DDoS SYN сообщениями по протоколу TCP. Жертва должна отвечать пакетами SYN/ACK. Атака называется SYN-FLOOD.

