March 2022

TRUSTED VIRTUAL ROUTER REDUNDANCY PROTOCOL

NIRANJAN M M

TRUSTED VIRTUAL ROUTER REDUNDANCY PROTOCOL

AUTHOR:
NIRANJAN M M

ABSTRACT

Virtual Router Redundancy Protocol (VRRP) is an open standard protocol, used to provide redundancy in a network. It is used in many products such as Routers, Switches, WLCs, APs etc., VRRP allows for transparent failover at the first-hop IP router, by configuring a group of routers to share a virtual IP address. VRRP selects a Master router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the master router fails. Currently there are no mechanism in VRRP to provide any type of authentication although initial version of VRRP has option for authentication. Without any authentication mechanism, the compromised node can behave as Master and causes multiple Masters in the network, which in-turn causes as much disruption as no routers. If any of the virtual router is compromised, i.e., it is no longer a trusted entity, which could cause compromised router to behave as if they are a VRRP Master, creating multiple Masters in the network. Hence trust among VRRP participants must be established before electing the Master i.e., the trust information should be used as one of the criteria for Master election along with other parameters such as priority etc., The techniques presented herein applies attestation method to VRRP for providing Proof of Integrity while selecting the Master out of multiple virtual routers in high availability deployments.

DETAILED DESCRIPTION

Virtual Router Redundancy Protocol (VRRP) is an open standard protocol, used to provide redundancy in a network. It is a network layer protocol (protocol number=112) used in many products such as Routers, Switches, WLCs, APs etc., VRRP allows for transparent failover at the first-hop IP router, by configuring a group of routers to share a virtual IP address. VRRP selects a Master router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the master router fails. To reiterate, VRRP is not just used for router redundancy, it is used with respect to switches/WLCs/APs as well.

- In connecting redundancy WAN gateway routers or server access switches.

- In cluster setup, to elect one of the devices as Master/Leader, who handles all configuration and management. For example: in Cluster setup, Master/Leader does functionality of load balancing of Access Points across different Workers/Members along with single point of contact for configuration and management.
- In some of the deployments, where containerised WLC would be running only on the Master AP, which is elected one out of many APs. Upon failover, new AP would be elected to run the containerised WLC.
- There are many other products where VRRP is used for providing redundancy (high availability) and load balancing.

Currently there are no mechanism in VRRP to provide any type of authentication although initial version of VRRP has option for authentication. Without any authentication mechanism, the compromised node can behave as Master and causes multiple Masters in the network, which in-turn causes as much disruption as no routers.

If any of the virtual router is compromised, I.e., it is no longer a trusted entity, which could cause compromised router to behave as if they are a VRRP Master, creating multiple Masters in the network. Hence trust among VRRP participants must be established before electing the Master i.e., the trust information should be used as one of the criteria for Master election along with other parameters such as priority etc., There are no existing methods which provides trustworthiness to VRRP used among routers/switches/WLCs/APs to elect the Master/Leader in Redundancy (high availability) deployments.

Currently, VRRP for IPv4/IPv6 (https://tools.ietf.org/html/rfc5798) does not include any type of authentication. Earlier versions of the VRRP specification (https://tools.ietf.org/html/rfc2338#section-5.3.6) includes several types of authentications ranging from none to strong (i.e., no authentication, Simple Text password, IP Authentication Header). These authentication methods supposed to provide security to overcome the vulnerabilities, but instead caused multiple master’s to be elected (whenever secrets are misconfigured). Due to the nature of VRRP, even if VRRP messages are cryptographically

protected, it does not prevent compromised/hostile nodes from behaving as if they are a VRRP Master, creating multiple Masters. Multiple Masters causes as much disruption as no routers.

In other words, authentication of VRRP messages does not prevent a compromised node to become Master and results in multiple Masters. Hence usage of this field is discontinued in later VRRP version (https://tools.ietf.org/html/rfc3768#section-5.3.6) but retained for backwards compatibility. Hence, we need method for VRRP to provide trust among VRRP participant devices, which will be used as a criterion for Master election process.

The techniques presented herein applies attestation method to Virtual Router Redundancy Protocol (VRRP) for providing Proof of Integrity while selecting the Master out of multiple virtual routers in high availability deployments. VRRP being used by multiple products such as Routers, switches, WLCs etc., this method is applicable for all those products which uses VRRP for providing High availability (redundancy) by electing new Master out of many devices upon failover of existing Master i.e., along with other parameters, trust information is also used for Master election.

For simplicity, router deployment is used while describing here, but applicable for other products such as switches, WLC etc., This method adds attestation information to the VRRP as an extension that embeds:

- Hardware fingerprint - Derived from SUDI or similar.
- Software - OS, BIOS, kernel, version, application binaries/libraries, KGV (Known Good Values) etc.,
- Platform Information - PCRs (Platform Config Registers), time-ticks, counters, signature.,

As mentioned in https://tools.ietf.org/html/rfc2338#section-5.1, VRRP provides support for sharing "Authentication Data", for providing authentication to VRRP messages, but due to the issues mentioned above it is not being used. This method includes attestation information in this payload. VRRP participants will use this attestation information to verify whether the virtual router who sent the VRRP multicast packet is trustworthy or not. Later trustworthiness of the virtual router is used for new Master election along with other parameters (viz., priority etc.,).

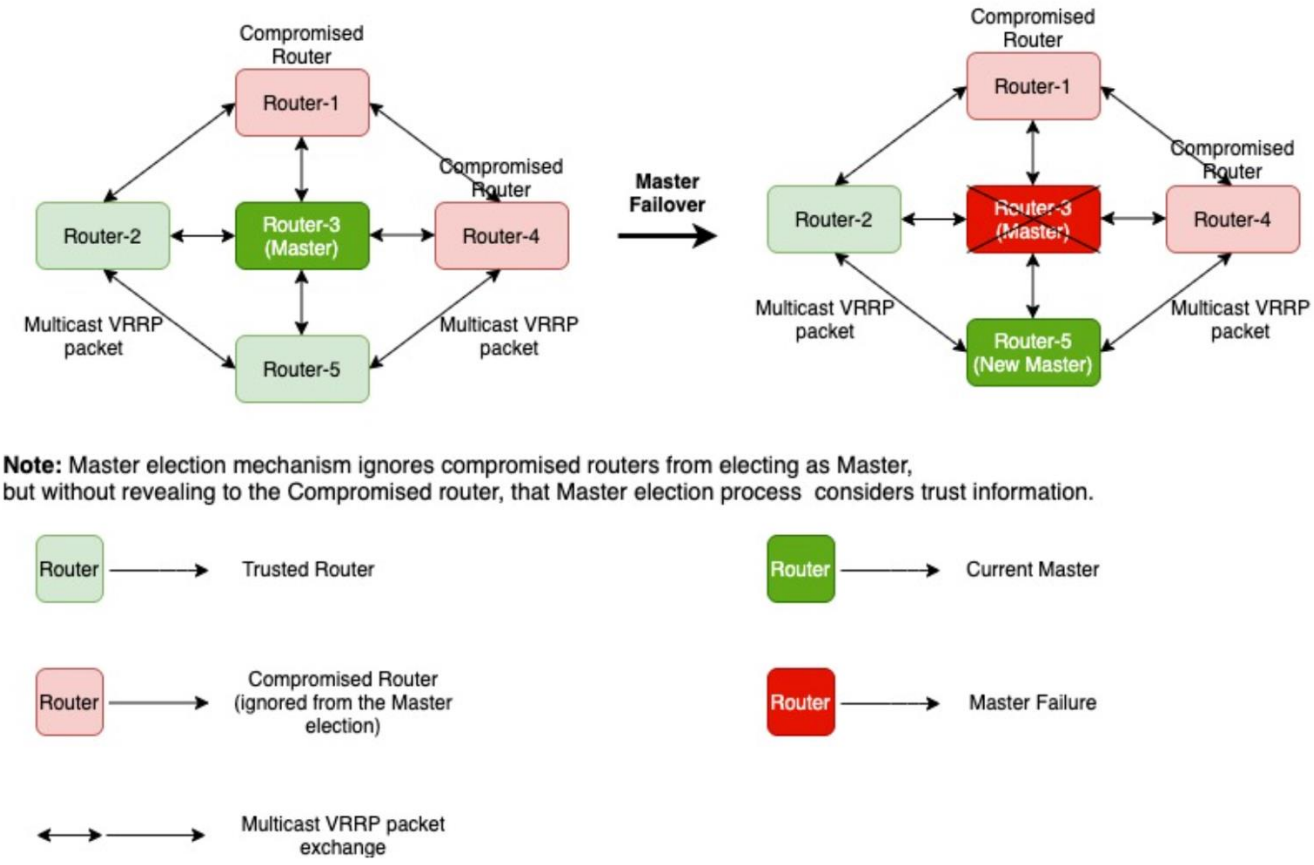

Figure-1

Scenario-A:

1. Let us say, Router-1 is UP, and all other Routers are still booting up which are in the same VRRP group (VRID).
2. Assume Router-1 is a Compromised Router.
3. Since Router-1 is the only router UP and running, would become Master as per VRRP and continue sending multicast VRRP packets.
4. Now, Router-2 came UP and start receiving VRRP packets from the current Master (Router-1).
5. Router-2 uses attestation information available in the VRRP packets to see whether the Router-1 is trustworthy or not.
6. Router-2 is not able to verify the trustworthiness of Router-1 (as it is a compromised router, as per the step (2)). Adds Router-1 into the compromised list.

7. Router-2 would send this information to the syslog as well as update (through traps) to management entity to make further action.
8. Management entity uses this information to filter ARP, ND and VRRP messages from switch ports associated with Compromised Router-1 (on the L2 Switch).
9. Now onwards, Router-1 will not be able to send VRRP as well as ARP (or GARP) and ND packets but will be able to receive VRRP packets from the other Routers (to avoid multiple Master scenario).
10. Also, as Router-2 successfully verified the trustworthiness of Router-1 with the Remote attester, we can consider as trusted (but not yet mutually trusted),
    a. If priority of Router-2 is less than that of Router-1, then it raises the priority more than that of Router-1 to defend its role as Master (to own the virtual IP and MAC address binding).
    b. If priority of Router-2 is greater than that of Router-1, then Router-2 becomes Master (as per VRRP).

Scenario-B:

1. Now Router-3 comes UP and start receiving VRRP packets from the Router-2.
2. Router-3 uses attestation information present in the VRRP packets to see whether the Router-2 is trustworthy or not.
    a. If Router-2 is Trustworthy and Master:
        i. If Priority of Router-3 is less than that of Router-2, then Router-3 becomes Backup Router.
        ii. If Priority of Router-3 is greater than that of Router-2, then as per VRRP, Router-3 would have sent the VRRP packets along with attestation information. Router-2 uses this attestation information present in VRRP packets from Router-3 to see whether the Router-3 is trustworthy or not.
            - If Router-3 is Trustworthy: As Router-3 is having high priority and trusted, it becomes Master and Router-2 becomes Backup. (As in the Figure-1).
            - If Router-3 is Compromised: As Router-3 is having high priority, it will become Master (on its own) and Router-2 defend by raising the

priority more than that of Router-3 to defend its role as Master. In case if priority matches (or reached the max), trustworthiness of the Router is used to break the tie. (Along with current behaviour of using IP address to break the tie). (This is not shown in the Figure-1).

b. If Router-2 is Compromised and Master:
    i. If Priority of Router-3 is less than that of Router-2: Same as that of Scenario-1.
    ii. If Priority of Router-3 is greater than that of Router-2: Same as that of Scenario-1.

The techniques presented herein provides trustworthiness to VRRP messages exchanged between virtual devices, used for Master election in case of failover of current Master. This method is required in Routers/Switches deployments to elect only the non-compromised virtual device as Master upon failover of current Master. Moreover, this method is required in Cluster development to elect only the non-compromised Member/Worker WLC as Leader/Master. Leader/Master WLC is the WLC where all the configuration and management functionalities, load balancing of Access Points (APs) across the Member/Worker WLCs etc., takes place. Additionally, in some of the deployments, where containerised WLC would be running only on the Master AP which is elected one out of many APs. Upon failover, new AP would be elected to run the containerised WLC. With this method, only the non-compromised AP would be elected as Master for running the containerised WLC.