VRRP

Summary

This chapter describes the Virtual Router Redundancy Protocol (VRRP) support in RouterOS.

Mostly on larger LANs dynamic routing protocols (OSPF or RIP) are used, however, there are a number of factors that may make it undesirable to use dynamic routing protocols. One alternative is to use static routing, but if the statically configured first hop fails, then the host will not be able to communicate with other hosts.

In IPv6 networks, hosts learn about routers by receiving Router Advertisements used by the Neighbor Discovery (ND) protocol. ND already has a built-in mechanism to determine unreachable routers. However, it can take up to 38 seconds to detect an unreachable router. It is possible to change parameters and make detection faster, but it will increase the overhead of ND traffic especially if there are a lot of hosts. VRRP allows the detection of unreachable routers within 3 seconds without additional traffic overhead.
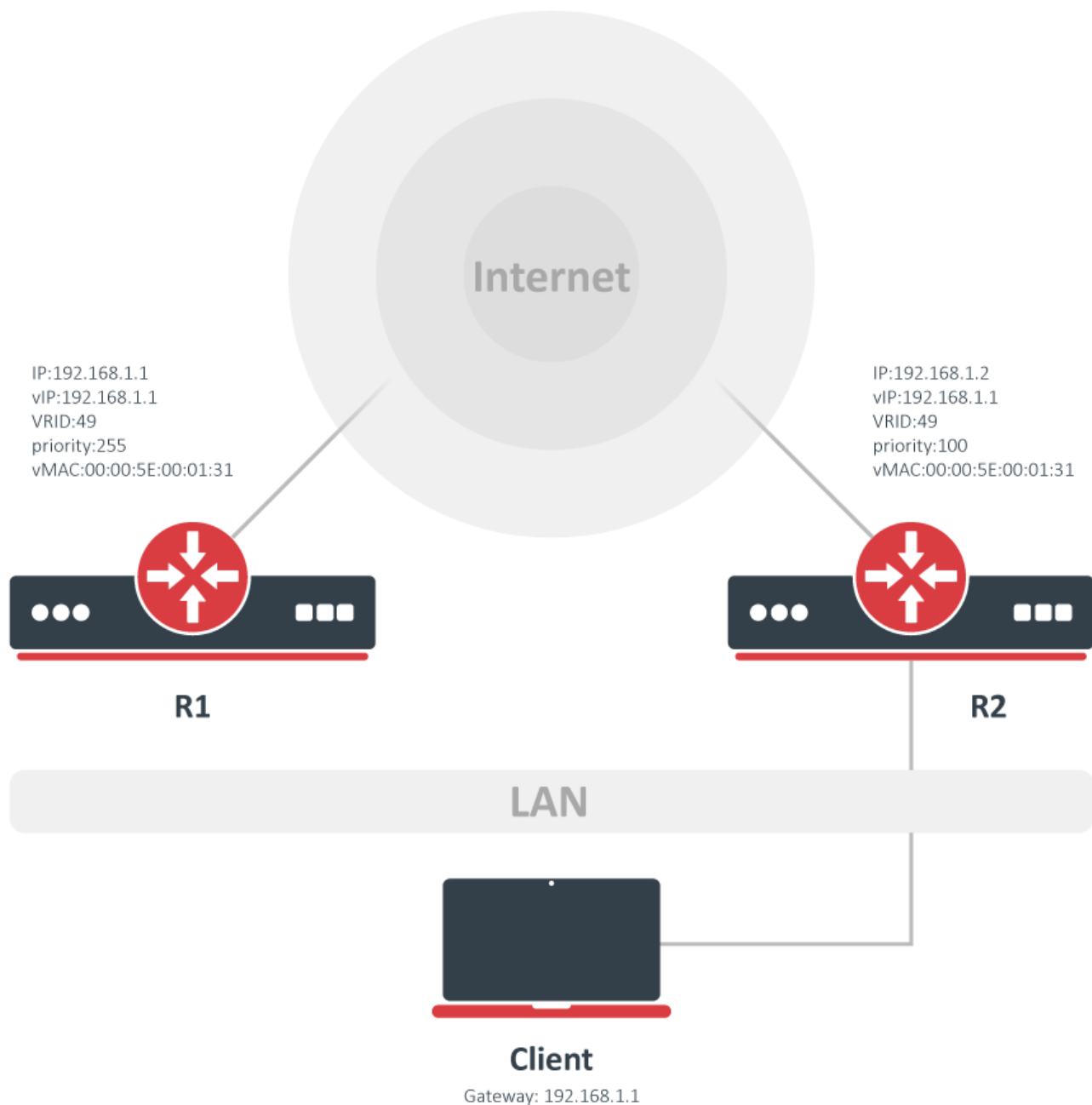
Virtual Router Redundancy Protocol (VRRP) provides a solution by combining a number of routers into a logical group called *Virtual Router* (VR). VRRP implementation in RouterOS is based on VRRPv2 RFC 3768 and VRRPv3 RFC 5798.

It is recommended to use the same version of RouterOS for all devices with the same VRID used to implement VRRP.

> ⚠ According to RFC authentication is deprecated for VRRP v3

Protocol Overview

IP:192.168.1.1
vIP:192.168.1.1
VRID:49
priority:255
vMAC:00:00:5E:00:01:31

IP:192.168.1.2
vIP:192.168.1.1
VRID:49
priority:100
vMAC:00:00:5E:00:01:31

Internet

R1

R2

LAN

Client
Gateway: 192.168.1.1

The purpose of the VRRP is to communicate to all VRRP routers associated with the Virtual Router ID and support router redundancy through a prioritized election process among them.

All messaging is done by IPv4 or IPv6 multicast packets using protocol 112 (VRRP). The destination address of an IPv4 packet is *224.0.0.18* and for IPv6 it is *FF02:0:0:0:0:0:0:12*. The source address of the packet is always the primary IP address of an interface from which the packet is being sent. In IPv6 networks, the source address is the link-local address of an interface.

These packets are always sent with TTL=255 and are not forwarded by the router. If for any reason the router receives a packet with lower TTL, a packet is discarded.

Each VR node has a single assigned MAC address. This MAC address is used as a source for all periodic messages sent by Master.

Virtual Router is defined by VRID and mapped set of IPv4 or IPv6 addresses. The master router is said to be the **owner** of mapped IPv4/IPv6 addresses. There are no limits to using the same VRID for IPv4 and IPv6, however, these will be two different Virtual Routers.

Only the Master router is sending periodic Advertisement messages to minimize the traffic. A backup will try to preempt the Master only if it has the higher priority and preemption is not prohibited.

☑

✅ All VRRP routers belonging to the same VR must be configured with the same advertisement interval. If the interval does not match router will discard the received advertisement packet.

Virtual Router (VR)

A Virtual Router (VR) consists of one Owner router and one or more backup routers belonging to the same network.

VR includes:

- VRID configured on each VRRP router
- the same virtual IP on each router
- Owner and Backup configured on each router. On a given VR there can be only one Owner.

Virtual MAC address

VRRP automatically assigns MAC address to VRRP interface based on standard MAC prefix for VRRP packets and VRID number. The first five octets are 00:00:5E:00:01 and the last octet is configured VRID. For example, if Virtual Routers VRID is 49, then the virtual MAC address will be *00:00:5E:00:01:31*.

⚠ Virtual mac addresses can not be manually set or edited.

Owner

An Owner router for a VR is the default Master router and operates as the Owner for all subnets included in the VR. Priority on an owner router must be the highest value (255) and virtual IP is the same as real IP (owns the virtual IP address).

⚠ RouterOS can not be configured as Owner. The Pure virtual IP configuration is the only valid configuration unless a non-RouterOS device is set as the owner.
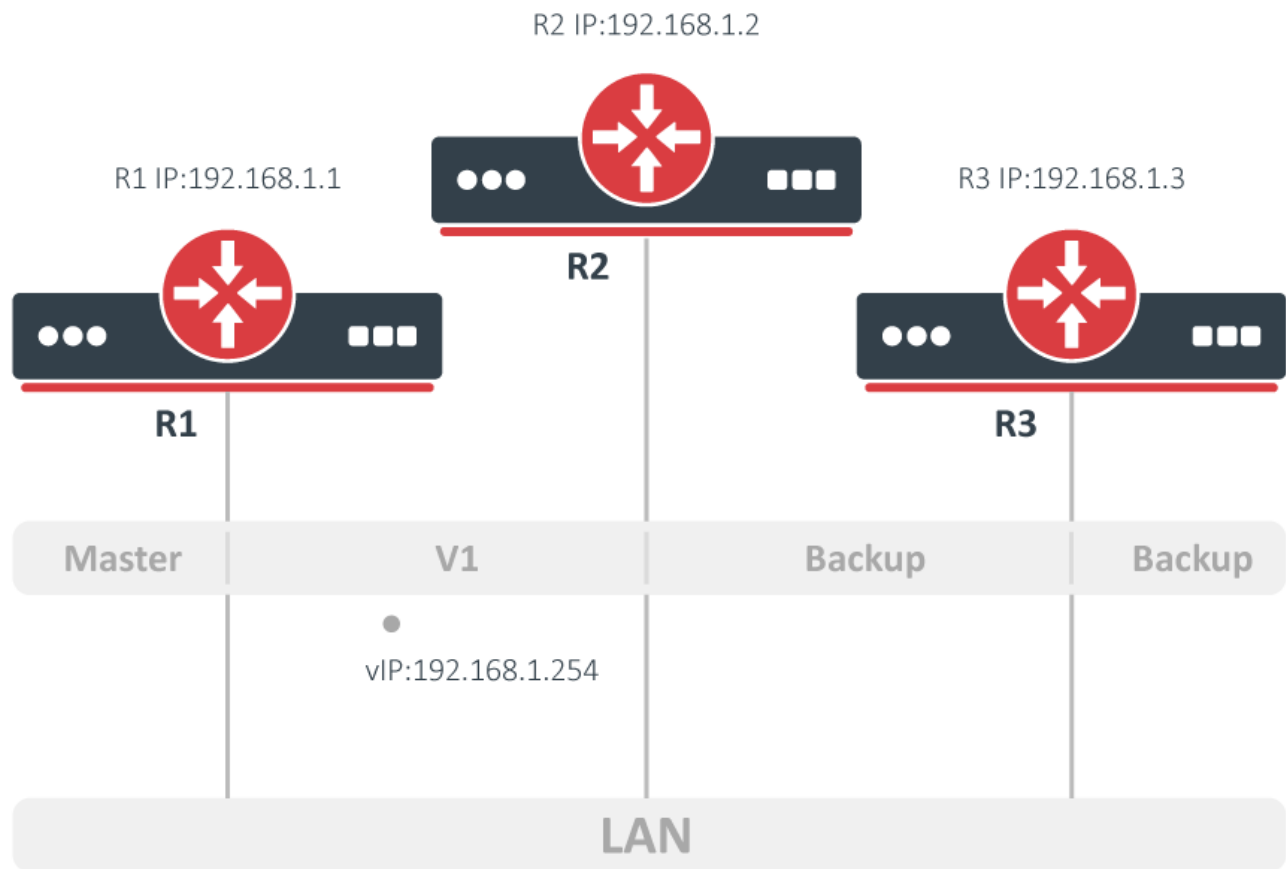
Master

A master router in a VR operates as the physical gateway for the network for which it is configured. The selection of the Master is controlled by priority value. The Master state describes the behavior of the Master router. For example network, **R1** is the Master router. When R1 is no longer available R2 becomes master.

Backup

VR must contain at least one Backup router. A backup router must be configured with the same virtual IP as the Master for that VR. The default priority for Backup routers is 100. When the current master router is no longer available, a backup router with the highest priority will become a current master. Every time when a router with higher priority becomes available it is switched to master. Sometimes this behavior is not necessary. To override it preemption mode should be disabled.

Virtual Address

Virtual IP associated with VR must be identical and set on all VR nodes. All virtual and real addresses should be from the same network.

> ⚠ RouterOS can not be configured as Owner. VRRP address and real IP address should not be the same.

If the Master of VR is associated with multiple IP addresses, then Backup routers belonging to the same VR must also be associated with the same set of virtual IP addresses. If the virtual address on the Master is not also on Backup a misconfiguration exists and VRRP advertisement packets will be discarded.

All Virtual Router members can be configured so that virtual IP is not the same as physical IP. Such a virtual address can be called a floating or pure virtual IP address. The advantage of this setup is the flexibility given to the administrator. Since the virtual IP address is not the real address of any one of the participant routers, the administrator can change these physical routers or their addresses without any need to reconfigure the virtual router itself.

In IPv6 networks, the first address is always a link-local address associated with VR. If multiple IPv6 addresses are configured, then they are added to the advertisement packet after the link-local address.
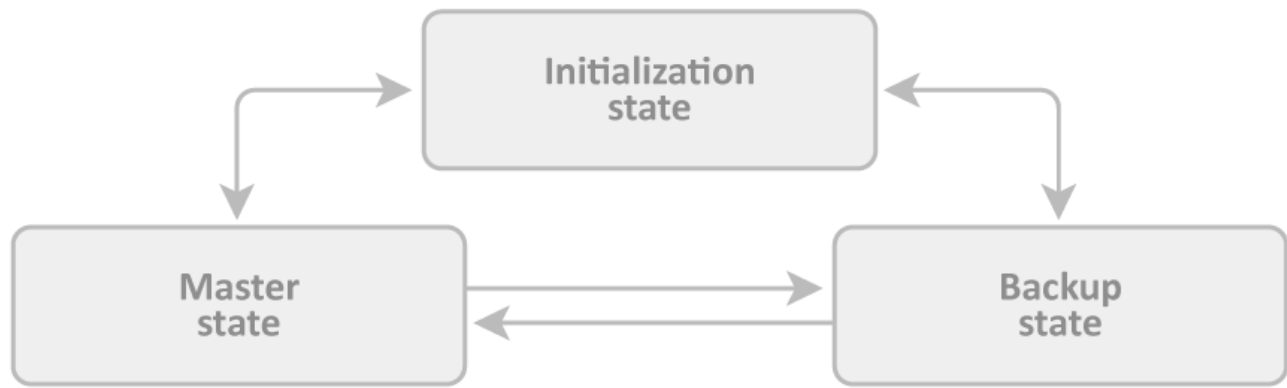
IPv4 ARP

The Master for a given VR responds to ARP requests with the VR's assigned MAC address. The virtual MAC address is also used as the source MAC address for advertisement packets sent by the Master. To ARP requests for non-virtual IP, addresses router responds with the system MAC address. Backup routers are not responding to ARP requests for Virtual IPs.

IPv6 ND

As you may know, in IPv6 networks, the Neighbor Discovery protocol is used instead of ARP. When a router becomes the Master, an unsolicited ND Neighbor Advertisement with the Router Flag is sent for each IPv6 address associated with the virtual router.

VRRP state machine

As you can see from the diagram, each VRRP node can be in one of three states:

- Init state
- Backup state
- Master state

Init state

The purpose of this state is to wait for a Startup event. When this event is received, the following actions are taken:

- if priority is 255,
- * for IPv4 send advertisement packet and broadcast ARP requests
- * for IPv6 send an unsolicited ND Neighbor Advertisement for each IPv6 address associated with the virtual router and set target address to link-local address associated with VR.
- * transit to MASTER state;
- else transit to BACKUP state.

Backup state

When in the backup state,

- in IPv4 networks, a node is not responding to ARP requests and is not forwarding traffic for the IP associated with the VR.
- in IPv6 networks, a node is not responding to ND Neighbor Solicitation messages and is not sending ND Router Advertisement messages for VR-associated IPv6 addresses.

Routers' main task is to receive advertisement packets and check if the master node is available.

The backup router will transmit itself to the master state in two cases:

- If priority in advertisement packet is 0;
- When Preemption_Mode is set to yes and Priority in the ADVERTISEMENT is lower than the local Priority

After the transition to Master state node is:

- in IPv4 broadcasts gratuitous ARP request;
- in IPv6 sends an unsolicited ND Neighbor Advertisement for every associated IPv6 address.

In other cases, advertisement packets will be discarded. When the shutdown event is received, transit to Init state.

> ⚠ Preemption mode is ignored if the Owner router becomes available.

Master state

When the MASTER state is set, the node functions as a forwarding router for IPv4/IPv6 addresses associated with the VR.

In IPv4 networks, the Master node responds to ARP requests for the IPv4 address associated with the VR. In IPv6 networks Master node:

- responds to ND Neighbor Solicitation message for the associated IPv6 address;

- sends ND Router Advertisements for the associated IPv6 addresses.

If the advertisement packet is received by master node:

- If priority is 0, send advertisement immediately;
- If priority in advertisement packet is greater than nodes priority then transit to the backup state
- If priority in advertisement packet is equal to nodes priority and primary IP Address of the sender is greater than the local primary IP Address, then transit to the backup state
- Ignore advertisement in other cases

When the shutdown event is received, send the advertisement packet with priority=0 and transit to Init state.

Connection tracking synchronization

Similar to different High availability features, RouterOS v7 supports VRRP connection tracking synchronization.

The VRRP connection tracking synchronization requires that RouterOS connection tracking is running. By default, connection tracking is working in `auto` mode. If VRRP devices do not contain any firewall rules, you need to manually enable connection tracking:

```
/ip/firewall/connection/tracking/set enabled=yes
```

To sync connection tracking entries configure the device as follows:

```
/interface/vrrp/set vrrp1 sync-connection-tracking=yes
```

Verify configuration in the logging section:

```
16:14:06 vrrp,info vrrp1 now MASTER, master down timer
16:14:06 vrrp,info vrrp1 stop CONNTRACK
16:14:06 vrrp,info vrrp1 starting CONNTRACK MASTER
```

Connection tracking entries are synchronized only from the Master to the Backup device.

When both **sync-connection-tracking** and **preemption-mode** are enabled, and a router with higher VRRP priority becomes online, the connections get synchronized first, and only then the router with higher priority becomes the VRRP master.

> ✅ If multiple VRRP interfaces are configured between two units, then it is enough to enable sync-connection-tracking=yes on one (preferably master) VRRP interface.

Configuring VRRP

IPv4

Setting up Virtual Router is quite easy, only two actions are required - create VRRP interface and set Virtual Routers IP address.

For example, add VRRP to ether1 and set VRs address to 192.168.1.1

```
/interface vrrp add name=vrrp1 interface=ether1
/ip address add address=192.168.1.2/24 interface=ether1
/ip address add address=192.168.1.1/32 interface=vrrp1
```

Notice that only the 'interface' parameter was specified when adding VRRP. It is the only parameter required to be set manually, other parameters if not specified will be set to their defaults: `vrid=1, priority=100` and `authentication=none`.

⚠️

⚠ Address on the VRRP interface must have /32 netmask if the address configured on VRRP is from the same subnet as on the router's any other interface.

Before VRRP can operate correctly correct IP address is required on ether1. In this example, it is 192.168.1.2/24

IPV6

To make VRRP work in IPv6 networks, several additional options must be enabled - v3 support is required and the protocol type should be set to IPv6:

```
/interface vrrp add name=vrrp1 interface=ether1 version=3 v3-protocol=ipv6
```

Now when the VRRP interface is set, we can add a global address and enable ND advertisement:

```
/ipv6 address add address=FEC0:0:0:FFFF::1/64 advertise=yes interface=vrrp1
```

No additional address configuration is required as it is in the IPv4 case. IPv6 uses link-local addresses to communicate between nodes.

Parameters

Property	Description
arp (*disabled | enabled | proxy-arp | reply-only*; Default: **enabled**)	ARP resolution protocol mode
arp-timeout *(integer; Default: auto)*	
authentication (*ah | none | simple*; Default: **none**)	Authentication method to use for VRRP advertisement packets. • none - should be used only in low-security networks (e.g., two VRRP nodes on LAN). • ah - IP Authentication Header. This algorithm provides strong protection against configuration errors, replay attacks, and packet corruption/modification. Recommended when there is limited control over the administration of nodes on a LAN. HMAC-MD5 is used. • simple - uses a clear-text password. Protects against accidental misconfiguration of routers on a local network.
group-authority (*interface;* Default: **none**)	Allows combining multiple VRRP interfaces to maintain the same VRRP status within the group. For example, VRRP instances run on LAN and WAN networks with NAT in-between. If one VRRP instance is Master and the other is Backup on the same device, the entire network malfunctions due to NAT failure. Grouping LAN and WAN VRRP interfaces ensures that both are either VRRP Master or Backup. In a VRRP group, VRRP control traffic gets sent only by the group authority. That's why in a typical WAN+LAN setup, it is recommended to use the LAN network as the group master to keep VRRP control traffic in the internal network. ```/interface vrrp\nadd name=vrrp-wan interface=sfp-sfpplus1 vrid=1 priority=100\nadd name=vrrp-lan interface=bridge1 vrid=2 priority=100\nset [find] group-authority=vrrp-lan``` Group-authority was previously called "group-master", "group-master" is kept for compatibility with scripts, but if both are set only "group-authority" will be taken into account.
interface (*string*; Default:)	Interface name on which VRRP instance will be running

interval (*time [10ms..4m15s]*; Default: **1s**)	VRRP update interval in seconds. Defines how often the master sends advertisement packets.
mtu (*integer*; Default: **1500**)	Layer3 MTU size. Since RouterOS v7.7, the VRRP interface always uses slave interface MTU
name (*string*; Default:)	VRRP interface name
on-backup (*string*; Default:)	Script to execute when the node is switched to the backup state
on-master (*string*; Default:)	Script to execute when the node is switched to master state
on-fail (*string*; Default:)	Script to execute when the node fails
password (*string*; Default:)	Password required for authentication. Can be ignored if authentication is not used.
preemption-mode (*yes | no*; Default: **yes**)	Whether the master node always has the priority. When set to 'no' the backup node will not be elected to be a master until the current master fails, even if the backup node has higher priority than the current master. This setting is ignored if the owner router becomes available
priority (*integer: 1..254*; Default: **100**)	Priority of VRRP node used in Master election algorithm. A higher number means higher priority. '255' is reserved for the router that owns VR IP and '0' is reserved for the Master router to indicate that it is releasing responsibility.
remote-address (*IPv4;* Default:)	Specifies the remote address of the other VRRP router for syncing connection tracking. If not set, the system autodetects the remote address via VRRP. The remote address is used only if sync-connection-tracking=yes. Explicitly setting a remote address has the following benefits: • Connection syncing starts faster since there is no need to wait for VRRP's initial message exchange to detect the remote address. • Faster VRRP Master election. • Allows sending connection tracking data via a different network interface (e.g., a dedicated secure line between two routers). Sync connection tracking uses UDP port 8275.
v3-protocol (*ipv4 | ipv6*; Default: **ipv4**)	A protocol that will be used by VRRPv3. Valid only if the **version** is 3.
version (*integer [2, 3]*; Default: **3**)	Which VRRP version to use.
vrid (*integer: 1..255*; Default: **1**)	Virtual Router identifier. Each Virtual router must have a unique id number
sync-connection-tracking (*string*; Default: **no**)	Synchronize connection tracking entries from Master to Backup device. The VRRP connection tracking synchronization requires that RouterOS connection tracking is running.