Network Working Group
Internet-Draft
Updates: 9568 (if approved)
Intended status: Informational
Expires: 21 October 2026

A. Dogra
A. Abraham
S. Krishnamurthy
Cisco Systems

19 April 2026

Unicast Support for the Virtual Router Redundancy Protocol (VRRP) draft-abinabraham-vrrp-unicast-00

Abstract

The Virtual Router Redundancy Protocol (VRRP) is specified for multicast operation on a shared LAN in RFC 9568. Some deployments, including virtualized and cloud environments, require VRRP-like first-hop redundancy but cannot use multicast delivery for VRRP advertisements. This document updates RFC 9568 by defining an optional unicast mode for VRRP.

In unicast mode, VRRP advertisements are sent to configured peer addresses rather than to the VRRP multicast group. This document preserves the VRRP packet format, protocol number, virtual IP semantics, and host-facing forwarding behavior defined in RFC 9568, while adding explicit peer configuration and receive-side source validation for unicast operation.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 October 2026.

Copyright Notice

Table of Contents

1. Introduction

[RFC9568] specifies VRRP for IPv4 and IPv6 and assumes multicast operation on a shared LAN. In a number of modern deployments, redundant routers still need fast active/backup failover for a virtual default gateway, but the environment does not provide usable multicast support for VRRP advertisements.

The primary deployment driver is the continued need for the classic VRRP function of protecting a virtual IPv4 or IPv6 first-hop gateway in environments where multicast delivery is unavailable, undesirable, or operationally constrained. This includes virtualized, cloud, overlay, and other deployments in which Virtual Routers still provide

a common host-facing gateway service, but control traffic between the Virtual Routers is exchanged through explicit peer connectivity instead of a simple multicast-capable LAN.

The intended use case for this document is not a generic active/backup role-election mechanism. Rather, it is a narrow extension of VRRP for deployments that want to preserve the familiar VRRP state machine, protocol number, virtual IP address semantics, Virtual Router MAC behavior, and host-facing forwarding model while replacing only the advertisement delivery method.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Scope and Applicability

This document updates [RFC9568] by defining an optional unicast mode of operation for VRRP. The unicast mode is intended for deployments that still want the classic VRRP model of a Virtual Router protecting one or more virtual IPv4 or IPv6 addresses, but that cannot rely on multicast delivery of advertisements.

The unicast mode defined here is limited to deployments in which the participating VRRP Routers can exchange advertisements without traversing a router that decrements the IPv4 TTL or IPv6 Hop Limit. This preserves the receive-side validation model of [RFC9568] and keeps the security and topology assumptions close to those of the base protocol.

This document does not define multi-hop operation. If a deployment requires routed multi-hop active/backup election or transport encapsulation other than IP protocol 112, that deployment is outside the scope of this specification.

4. Use Cases and Deployment Drivers

The operational motivation for unicast VRRP is straightforward: operators still need the classic VRRP function of protecting a virtual IPv4 or IPv6 default gateway, but some modern deployments cannot rely on multicast delivery for VRRP advertisements.

Typical use cases include:

1. Cloud and virtualized environments in which multicast is not available or is not exposed in a way that is operationally equivalent to a simple shared LAN.

2. Overlay or virtualized edge deployments in which the protected routers still present a common host-facing gateway service, but the control traffic between the routers is exchanged using explicit peer connectivity rather than a multicast-capable LAN.

3. Service-provider and data-center designs in which operators want to preserve the familiar VRRP packet format, state machine, and virtual IP semantics of [RFC9568] while replacing only the advertisement delivery method.

This document addresses those use cases by defining a unicast delivery mode that stays close to the original VRRP model. It does not attempt to standardize broader routed active/backup election mechanisms that are no longer centered on protecting a virtual first-hop gateway.

5. Additional Definitions

Unicast Mode	A mode of VRRP operation in which advertisements for a Virtual Router are sent as unicast IPv4 or IPv6 packets to configured peer addresses instead of to the VRRP multicast destination address.
Unicast Peer	A configured VRRP Router participating in the same Virtual Router and address family whose address is used as a permitted source and destination for unicast VRRP advertisements.
Unicast Peer List	The configured set of all other VRRP Routers that participate in a unicast-mode Virtual Router for a given address family.

6. Unicast VRRP Overview

A Virtual Router defined by this document operates in exactly one of two modes:

* multicast mode, as specified in [RFC9568], or

* unicast mode, as specified in this document.

A VRRP Router operating a given Virtual Router in unicast mode MUST NOT send VRRP advertisements for that Virtual Router to the VRRP multicast destination address. Instead, it MUST send a copy of each advertisement to each address in the configured Unicast Peer List.

Except as updated by this document, the VRRP packet format, VRRP state machine, timer calculations, preemption behavior, Virtual Router semantics, virtual IP address behavior, and host-facing forwarding behavior remain as specified in [RFC9568].

Unicast mode is configured per Virtual Router. A VRRP Router MUST NOT mix multicast mode and unicast mode for the same Virtual Router instance.

7. Peer Configuration

A Virtual Router operating in unicast mode MUST be configured with one or more Unicast Peers. A configuration that enables unicast mode without at least one peer is invalid, and the Virtual Router MUST NOT operate in unicast mode until corrected.

Each VRRP Router participating in a unicast-mode Virtual Router MUST be configured with the addresses of all other participating VRRP Routers for that Virtual Router and address family.

For IPv4 operation, each configured peer address MUST be an IPv4 address that the receiving peer uses as the source address for VRRP advertisements, as described in Section 8.3. For IPv6 operation, each configured peer address MUST be an IPv6 link-local address used by the receiving peer as the source address for VRRP advertisements, as described in Section 8.4.

The local router’s own address MUST NOT appear in its Unicast Peer List.

8. Updates to RFC 9568

8.1. VRRP Overview

The references to multicast-only operation in Section 3 of [RFC9568] are updated to allow an advertisement to be delivered either to the VRRP multicast destination address, as specified in [RFC9568], or to configured Unicast Peers, as specified in this document.

8.2. Protocol Processing

Section 5 of [RFC9568] is updated so that a Virtual Router operating in unicast mode sends and receives VRRP advertisements only through the configured Unicast Peer List for that Virtual Router and address family.

8.3. IPv4 Field Descriptions

For a Virtual Router operating in unicast mode, the IPv4 field descriptions in Section 5.1.1 of [RFC9568] are updated as follows:

1. The IPv4 source address MUST be the primary IPv4 address of the sending interface, as specified in [RFC9568].

2. The IPv4 destination address MUST be the IPv4 address of the configured Unicast Peer to which the copy of the advertisement is being sent.

3. The IPv4 TTL MUST be set to 255, and a received packet whose IPv4 TTL is not 255 MUST be discarded.

4. The IPv4 Protocol field MUST remain 112.

8.4. IPv6 Field Descriptions

For a Virtual Router operating in unicast mode, the IPv6 field descriptions in Section 5.1.2 of [RFC9568] are updated as follows:

1. The IPv6 source address MUST be the link-local address of the sending interface, as specified in [RFC9568].

2. The IPv6 destination address MUST be the configured IPv6 link-local address of the Unicast Peer to which the copy of the advertisement is being sent.

3. The IPv6 Hop Limit MUST be set to 255, and a received packet whose Hop Limit is not 255 MUST be discarded.

4. The IPv6 Next Header field MUST remain 112.

8.5. Transmitting VRRP Packets

Section 7.2 of [RFC9568] is updated so that a VRRP Router operating a Virtual Router in unicast mode sends one copy of each VRRP advertisement to each configured Unicast Peer instead of sending the advertisement to the VRRP multicast group.

Other than the destination address, the packet contents MUST be the same for each transmitted copy.

8.6. Receiving VRRP Packets

A VRRP Router operating a Virtual Router in unicast mode MUST process only advertisements whose source address matches an address in the configured Unicast Peer List for that Virtual Router and address family.

A received VRRP packet for a unicast-mode Virtual Router MUST be discarded if:

* the source address is not a configured Unicast Peer,
* the IPv4 TTL or IPv6 Hop Limit is not 255,
* the packet is received for the wrong address family, or
* the packet is otherwise invalid according to [RFC9568].

A VRRP Router operating a Virtual Router in unicast mode MUST ignore VRRP advertisements for that same Virtual Router received through multicast delivery.

8.7. Host-Facing Behavior

This document changes only advertisement delivery. The Active Router’s behavior with respect to the Virtual Router MAC address, ARP, gratuitous ARP, IPv6 Neighbor Discovery, Router Advertisements, Unsolicited Neighbor Advertisements, and forwarding responsibility remains as specified in [RFC9568].

In particular, unicast mode does not replace the Virtual Router MAC with a multicast MAC. The Virtual Router MAC remains the well-known unicast VRRP MAC associated with the VRID, as specified in [RFC9568].

9. Operational Considerations

A deployment using unicast mode SHOULD ensure that all routers in a given Virtual Router are configured with a consistent peer inventory. Inconsistent peer lists can create asymmetric reachability and can lead to multiple routers independently deciding that the Active Router has failed.

A deployment using unicast mode SHOULD continue to use distinct priority values as recommended in [RFC9568] so that Backup Routers do not transition to Active state simultaneously after a failure.

This document does not update the VRRP management model. Future work may standardize YANG or other management objects for peer lists, source validation policy, and related unicast-mode configuration.

10. Implementation Status

This section records publicly documented implementation experience for the benefit of reviewers. It is not part of the protocol specification.

Public documentation reviewed by the authors shows that unicast VRRP support already exists in multiple products and open-source implementations, although not all of them match the protocol profile defined in this document.

One implementation detail that varies across products is the interaction between unicast advertisement delivery and Virtual Router MAC behavior. Implementations that remain close to classic VRRP tend to preserve the standard unicast Virtual Router MAC and change only the control-packet delivery method, while more divergent "unicast VRRP" modes move away from the classic virtual-gateway and neighbor handling model.

Implementation	Support status	Notes
Cisco IOS XR	Documented	Documents a unicast peer model that preserves VRRP first-hop redundancy semantics; published operational output still shows the standard VRRP Virtual MAC while unicast transport is enabled, indicating that only advertisement delivery changes [CISCO-XR-VRRP]
Keepalived	Documented	Documents unicast peers, source validation, and TTL controls; documentation and reviewed source show that VMAC behavior remains available, but that vmac_xmit_base is required when VMAC is combined with unicast peers [KEEPALIVED] [KEEPALIVED-SRC]
VyOS	Documented	Documents peer-based unicast VRRP configuration and a separate rfc3768-compatibility mode that

		creates a VRRP interface and assigns the virtual MAC and virtual IP, illustrating that classic VRRP VMAC behavior is a compatibility choice in some unicast deployments [VYOS-HA]
Huawei VRP	Documented	Documents a proprietary VRRPv2-based unicast mode, including configurable transport details, that is related to but broader than the scoped profile in this document [HUAWEI-UC-VRRP] [HUAWEI-UC-VRRP-PORT]
Juniper Cloud-Native Router	Documented	Documents unicast VRRP use in cloud workflows and route-table ownership scenarios, illustrating deployment demand in cloud environments [JUNIPER-CNR-VRRP] [JUNIPER-CNR-EKS]
MikroTik RouterOS	No public unicast support found	Public documentation reviewed by the authors remains aligned with multicast VRRP behavior [MIKROTIK-VRRP]
FRRouting	No public unicast support found	Public documentation reviewed by the authors describes VRRPv2 and VRRPv3 behavior with the standard RFC Virtual MAC and multicast advertisements; reviewed source code likewise remains aligned with the classic multicast model and does not show a unicast mode [FRR-VRRP] [FRR-SRC]

Table 1: Examples of publicly documented unicast VRRP support

The reviewed material also suggests that the MAC-related differences are not about changing the VRRP Virtual Router MAC into a multicast MAC. Instead, the main implementation differences are whether a given product preserves the classic VRRP virtual-gateway model at all, and, if it does, whether unicast advertisements are sent on the same logical interface that owns the virtual MAC or on the base interface beneath it.

The existence of multiple deployed implementations supports the case for standardization. At the same time, the documented differences across implementations show why this document intentionally standardizes only a narrow unicast mode that remains close to [RFC9568].

11. Security Considerations

The security considerations of [RFC9568] continue to apply. In particular, VRRP still provides no confidentiality and does not prevent a hostile node from attempting to act as an Active Router.

Unicast mode introduces explicit peer configuration and requires that a receiver validate the source address against the configured Unicast Peer List. This provides an additional filtering mechanism beyond the receive-side IPv4 TTL or IPv6 Hop Limit check.

Because this document preserves the requirement that the IPv4 TTL or IPv6 Hop Limit be 255 on transmitted and accepted packets, the protection against packets arriving from a remote network described in [RFC5082] continues to apply.

A future specification for multi-hop unicast operation would need a different security model and is outside the scope of this document.

12. IANA Considerations

This document has no IANA actions.

13. References

13.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9568] Lindem, A. and A. Dogra, "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 9568, DOI 10.17487/RFC9568, April 2024, <https://www.rfc-editor.org/info/rfc9568>.

13.2. Informative References

[CISCO-XR-VRRP]
Cisco Systems, "Implementing VRRP on Cisco IOS XR", Includes a section on Unicast VRRP, <https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-9/ip-addresses/configuration/guide/b-ip-addresses-cg-asr9000-79x/implementing-vrrp.html>.

[FRR-SRC] FRRouting Project, "FRRouting vrrpd Source", Reviewed for Virtual Router MAC construction and advertisement transmission behavior, <https://github.com/FRRouting/frr/blob/master/vrrpd/vrrp.c>.

[FRR-VRRP] FRRouting Project, "FRRouting VRRP", <https://docs.frrouting.org/en/stable-7.5/vrrp.html>.

[HUAWEI-UC-VRRP]
Huawei, "VRRP in Unicast Mode", Huawei HedEx documentation, EDOC1100363264.

[HUAWEI-UC-VRRP-PORT]
Huawei, "unicast-vrrp port Command Reference", Huawei HedEx documentation, EDOC1100277644.

[JUNIPER-CNR-EKS]
Juniper Networks, "Cloud-Native Router Deployment on Amazon EKS", <https://www.juniper.net/documentation/us/en/software/cloud-native-router25.4/cloud-native-router-deployment-guide/topics/concept/system-resource-requirements-eks.html>.

[JUNIPER-CNR-VRRP]
Juniper Networks, "Cloud-Native Router VRRP Overview", <https://www.juniper.net/documentation/us/en/software/cloud-native-router23.4/cloud-native-router-user/topics/concept/l3-vrrp.html>.

[KEEPALIVED]
Keepalived Project, "keepalived.conf(5) Manpage", <https://www.keepalived.org/manpage.html>.

[KEEPALIVED-SRC]
Keepalived Project, "Keepalived VRRP VMAC Source", Reviewed together with vrrp_parser.c for VMAC construction and base-interface transmit behavior in unicast mode, <https://github.com/acassen/keepalived/blob/master/keepalived/vrrp/vrrp_vmac.c>.

[MIKROTIK-VRRP]
MikroTik, "RouterOS VRRP", <https://help.mikrotik.com/docs/spaces/ROS/pages/81362945/VRRP>.

[RFC5082] Gill, V., Heasley, J., and D. Meyer, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/info/rfc5082>.

[VYOS-HA] VyOS Project, "VyOS High Availability", <https://docs.vyos.io/en/1.4/configuration/highavailability/>.

Authors' Addresses

Aditya Dogra
Cisco Systems
Sarjapur Outer Ring Road
Bangalore 560103
Karnataka
India
Email: addogra@cisco.com

Abin Abraham
Cisco Systems
Sarjapur Outer Ring Road
Bangalore 560103
Karnataka
India
Email: abiabrah@cisco.com

Seshan Krishnamurthy
Cisco Systems
Sarjapur Outer Ring Road
Bangalore 560103
Karnataka
India
Email: seshakri@cisco.com