Routing Area Working Group
Internet-Draft
Updates: 9568 (if approved)
Intended status: Standards Track
Expires: 29 November 2026

A. Dogra
A. Abraham
Cisco Systems
S. Krishnamurthy
Independent

28 May 2026

Unicast Support for the Virtual Router Redundancy Protocol (VRRP) draft-abinabraham-vrrp-unicast-01

Abstract

The Virtual Router Redundancy Protocol (VRRP) Version 3 as specified in RFC 9568 assumes multicast operation on a shared LAN. Some deployments require the VRRP first-hop redundancy function but cannot use multicast delivery for VRRP advertisements. This document updates RFC 9568 by defining an optional configured unicast mode for VRRP Version 3 in which advertisements are sent to configured peer addresses rather than to the VRRP multicast group. The VRRP packet format, state machine, protocol number, virtual IP semantics, and Virtual Router MAC behavior remain unchanged from RFC 9568.

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 29 November 2026.

Copyright Notice

Table of Contents

1. Introduction

[RFC9568] specifies VRRP Version 3 for IPv4 and IPv6 and assumes multicast operation on a shared LAN. In a number of 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 VRRPv3 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.

Multiple implementations already support some form of unicast VRRP advertisement delivery, including Cisco IOS XR, Keepalived, VyOS, and Juniper Cloud-Native Router. This document provides a common specification for the most conservative unicast extension: replace multicast advertisement delivery with configured unicast peers while preserving the rest of the VRRP protocol.

The intended use case for this document is not a generic active/backup role-election mechanism. Rather, it is a narrow extension of VRRPv3 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 using a different advertisement delivery mode.

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 configured unicast mode of operation for VRRPv3. Multicast mode remains the default mode of operation. 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 unicast packets with IPv4 TTL or IPv6 Hop Limit arriving at 255 at the receiver. This preserves the receive-side validation model of [RFC9568] and the GTSM [RFC5082] protection against remote injection. In practice, this means the VRRP Routers must be reachable without traversing any device that decrements the TTL or Hop Limit.

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.

This document does not update VRRP Version 2.

4. 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. This list serves as both a destination list for transmission and an allow-list for reception.

5. Unicast VRRP Overview

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

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

* unicast mode, as specified in this document.

Multicast mode is the default mode. A VRRP Router MUST use multicast mode unless unicast mode is explicitly configured for the Virtual Router.

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, Priority 0 advertisements, Address Owner behavior, Accept_Mode, 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.

6. 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. Symmetric peer-list configuration is essential for correct protocol operation, including Active/Backup election, preemption, and advertisement-interval learning.

For IPv4 operation, each configured peer address MUST be an IPv4 address that the peer uses as the source address for VRRP advertisements, as described in Section 7.3. For IPv6 operation, each configured peer address MUST be an IPv6 link-local address that the peer uses as the source address for VRRP advertisements, as described in Section 7.4. For IPv6, the configured link-local address must be reachable on the interface associated with the Virtual Router.

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

A conforming implementation MUST support at least one configured Unicast Peer. Implementations SHOULD support multiple peers for deployments with more than two VRRP Routers in a Virtual Router group.

7. Updates to RFC 9568

7.1. 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.

7.2. 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.

7.3. 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 address configured in the Unicast Peer List for the 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.

7.4. 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 IPv6 link-local address configured in the Unicast Peer List for the 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.

7.5. Checksum Computation

Unicast mode does not define a new VRRP checksum algorithm. A VRRP Router operating in unicast mode computes and verifies the checksum as specified in Section 5.2.8 of [RFC9568].

7.6. 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 (and, for IPv6, the resulting checksum), the packet contents MUST be the same for each transmitted copy.

The source MAC address MUST be the Virtual Router MAC address as specified in Section 7.2 of [RFC9568]. This is unchanged from multicast mode.

Priority 0 advertisements (indicating that the Active Router is relinquishing the active role) are sent to all configured Unicast Peers, exactly as regular advertisements are sent.

7.7. 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 in the configured Unicast Peer List,

* 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 (i.e., advertisements whose destination address is the VRRP multicast group address).

A VRRP Router operating a Virtual Router in multicast mode MUST ignore unicast-delivered VRRP advertisements for that same Virtual Router.

These mode-isolation rules ensure that misconfigured peers operating in different modes for the same VRID do not interfere with each other’s state machines.

7.8. State Machine

Unicast mode does not change the VRRP state machine defined in Section 6 of [RFC9568]. The states, state transitions, timer calculations, preemption behavior, Priority 0 processing, Address Owner behavior, and Accept_Mode behavior remain unchanged.

A Virtual Router operating in unicast mode applies the transmit and receive rules in Section 7.6 and Section 7.7 when the state machine sends or processes VRRP advertisements.

7.9. 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 change the Virtual Router MAC address. The Virtual Router MAC remains the well-known unicast VRRP MAC associated with the VRID (00-00-5E-00-01-{VRID} for IPv4 and 00-00-5E-00-02-{VRID} for IPv6), as specified in [RFC9568].

Accept_Mode and Address Owner behavior are unchanged. An Address Owner (Priority 255) immediately transitions to Active state and sends advertisements to all configured Unicast Peers.

8. Misconfiguration Detection and Error Handling

Unicast mode relies on correct and symmetric peer-list configuration. Unlike multicast mode, where any router on the segment can hear all advertisements, unicast mode creates bilateral reachability dependencies. This section specifies error handling for common misconfiguration scenarios.

8.1. Source Validation Failures

Implementations MUST maintain a counter of VRRP advertisements discarded because the source address was not in the configured Unicast Peer List for the relevant Virtual Router and address family.

Implementations SHOULD log the first occurrence (subject to rate-limiting) of a source validation failure for a given Virtual Router, including the unexpected source address, the VRID, and the interface.

8.2. Mode Mismatch

A mode mismatch occurs when some routers for a given VRID are operating in unicast mode while others are in multicast mode. This can result in a dual-Active condition because routers in different modes will not hear each other’s advertisements.

Implementations SHOULD log a warning if the Virtual Router is in unicast mode and a VRRP multicast advertisement for the same VRID is received on the same interface (indicating a likely mode mismatch in the network).

8.3. Silent Peer Failure

When a Backup Router’s Active_Down_Timer fires and no advertisements were received from any configured peer during the timer period, this MAY indicate either Active Router failure (the correct failover case) or a connectivity or configuration problem.

Implementations SHOULD provide per-peer operational state showing the last-received advertisement timestamp for each configured Unicast Peer. This assists operators in distinguishing between Active Router failure and reachability/configuration issues.

8.4. Asymmetric Peer Lists

If Router A has Router B in its Unicast Peer List but Router B does not have Router A in its peer list, then Router A’s advertisements will be discarded by Router B. This can cause Router B to independently transition to Active, resulting in a dual-Active condition.

This specification does not define an in-band mechanism to detect or correct asymmetric peer configuration. Operators MUST ensure symmetric peer-list configuration across all routers participating in a unicast-mode Virtual Router. Management-plane tools (YANG model, configuration audit) are the intended mechanism for verifying symmetry.

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.

9.1. YANG Considerations

This document does not define a YANG module. The VRRP YANG data model is currently being revised by [I-D.ietf-rtgwg-vrrp-rfc8347bis], which is intended to obsolete [RFC8347]. Deferring the unicast VRRP YANG augmentation until that work is approved or published allows the augmentation to be based on the stable successor to [RFC8347], avoids unnecessary churn against a moving base model, and helps ensure alignment with the final VRRP YANG schema.

A future revision of this document, or a companion YANG document, is expected to define the management model for configuring the VRRP advertisement mode, the unicast peer list, and related operational state after [I-D.ietf-rtgwg-vrrp-rfc8347bis] has been approved or published as an RFC.

10. Security Considerations

The security considerations of [RFC9568] continue to apply. In particular, VRRP still provides no confidentiality and does not include cryptographic authentication of VRRP advertisements.

10.1. TTL/Hop Limit Protection

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] therefore continues to apply. An attacker must be on the same link (or logical link) as the VRRP Routers to inject or forge VRRP advertisements.

10.2. Security Recommendations

Deployments using unicast VRRP in environments with untrusted on-link neighbors SHOULD protect VRRP advertisement exchange using link-layer security (e.g., IEEE 802.1AE MACsec) or network-layer security (e.g., IPsec transport mode).

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

11. Implementation Status

[RFC Editor: This section is to be removed before publication.]

This section records the status of known implementations of the protocol behavior described in this specification at the time of posting, per [RFC7942].

Known implementations or products that support unicast VRRP include Cisco IOS XR, Keepalived, VyOS, and Juniper Cloud-Native Router.

12. IANA Considerations

This document requests no IANA actions.

13. Acknowledgements

The authors thank Acee Lindem for his work on RFC 9568 and draft-ietf-rtgwg-vrrp-rfc8347bis which provide the foundation for this extension. The Keepalived project’s mature unicast implementation provided valuable deployment evidence. The authors also thank the operators who provided feedback on unicast VRRP deployment requirements in cloud and overlay environments.

14. 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>.

15. Informative References

[I-D.ietf-rtgwg-vrrp-rfc8347bis] Lindem, A., "A YANG Data Model for the Virtual Router Redundancy Protocol (VRRP)", Work in Progress, Internet-Draft, draft-ietf-rtgwg-vrrp-rfc8347bis-15, 13 February 2026, <https://datatracker.ietf.org/doc/draft-ietf-rtgwg-vrrp-rfc8347bis/>.

[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>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[RFC8347] Liu, X., Ed., Kyparlis, A., Parikh, R., Lindem, A., and M. Zhang, "A YANG Data Model for the Virtual Router Redundancy Protocol (VRRP)", RFC 8347, DOI 10.17487/RFC8347, March 2018, <https://www.rfc-editor.org/info/rfc8347>.

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
Independent
Email: seskrish@gmail.com