

Network Working Group
Request for Comments: 1723
Obsoletes: 1388
Updates: 1058
Category: Standards Track

G. Malkin
Xylogics, Inc.
November 1994

RIP Version 2 Carrying Additional Information

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Abstract

This document specifies an extension of the Routing Information Protocol (RIP), as defined in [1,2], to expand the amount of useful information carried in RIP messages and to add a measure of security. This memo obsoletes RFC 1388, which specifies an update to the "Routing Information Protocol" STD 34, RFC 1058.

The RIP-2 protocol analysis is documented in RFC 1721 [4].

The RIP-2 applicability statement is document in RFC 1722 [5].

The RIP-2 MIB description is defined in RFC 1724 [3]. This memo obsoletes RFC 1389.

Acknowledgements

I would like to thank the IETF ripv2 Working Group for their help in improving the RIP-2 protocol.

Table of Contents

1.	Justification	2
2.	Current RIP	2
3.	Protocol Extensions	3
3.1	Authentication	4
3.2	Route Tag	4
3.3	Subnet Mask	5
3.4	Next Hop	5
3.5	Multicasting	5
3.6	Queries	6
4.	Compatibility	6
4.1	Compatibility Switch	6
4.2	Authentication	6
4.3	Larger Infinity	7
4.4	Addressless Links	7
5.	Security Considerations	7
	Appendix A	8
	References	8
	Author's Address	9

1. Justification

With the advent of OSPF and IS-IS, there are those who believe that RIP is obsolete. While it is true that the newer IGP routing protocols are far superior to RIP, RIP does have some advantages. Primarily, in a small network, RIP has very little overhead in terms of bandwidth used and configuration and management time. RIP is also very easy to implement, especially in relation to the newer IGPs.

Additionally, there are many, many more RIP implementations in the field than OSPF and IS-IS combined. It is likely to remain that way for some years yet.

Given that RIP will be useful in many environments for some period of time, it is reasonable to increase RIP's usefulness. This is especially true since the gain is far greater than the expense of the change.

2. Current RIP

The current RIP message contains the minimal amount of information necessary for routers to route messages through a network. It also contains a large amount of unused space, owing to its origins.

The current RIP protocol does not consider autonomous systems and IGP/EGP interactions, subnetting, and authentication since implementations of these postdate RIP. The lack of subnet masks is a

particularly serious problem for routers since they need a subnet mask to know how to determine a route. If a RIP route is a network route (all non-network bits 0), the subnet mask equals the network mask. However, if some of the non-network bits are set, the router cannot determine the subnet mask. Worse still, the router cannot determine if the RIP route is a subnet route or a host route. Currently, some routers simply choose the subnet mask of the interface over which the route was learned and determine the route type from that.

3. Protocol Extensions

This document does not change the RIP protocol per se. Rather, it provides extensions to the message format which allows routers to share important additional information.

The first four octets of a RIP message contain the RIP header. The remainder of the message is composed of 1 - 25 route entries (20 octets each). The new RIP message format is:

0										1										2										3		3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
+---+---+---+---+---+---+---+---+---+---+										+---+---+---+---+---+---+---+---+---+---+										+---+---+---+---+---+---+---+---+---+---+										+---+---		+
Command (1)										Version (1)										unused												
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+
Address Family Identifier (2)										Route Tag (2)																						
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+
										IP Address (4)																						
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+
										Subnet Mask (4)																						
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+
										Next Hop (4)																						
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+
										Metric (4)																						
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+										+-----+		+

The Command, Address Family Identifier (AFI), IP Address, and Metric all have the meanings defined in RFC 1058. The Version field will specify version number 2 for RIP messages which use authentication or carry information in any of the newly defined fields. The contents of the unused field (two octets) shall be ignored.

All fields are coded in IP network byte order (big-endian).

3.1 Authentication

Since authentication is a per message function, and since there is only one 2-octet field available in the message header, and since any reasonable authentication scheme will require more than two octets, the authentication scheme for RIP version 2 will use the space of an entire RIP entry. If the Address Family Identifier of the first (and only the first) entry in the message is 0xFFFF, then the remainder of the entry contains the authentication. This means that there can be, at most, 24 RIP entries in the remainder of the message. If authentication is not in use, then no entries in the message should have an Address Family Identifier of 0xFFFF. A RIP message which contains an authentication entry would begin with the following format:

```

      0               1               2               3 3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Command (1) | Version (1) | | unused | |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| | 0xFFFF | Authentication Type (2) | |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
~ Authentication (16) ~
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Currently, the only Authentication Type is simple password and it is type 2. The remaining 16 octets contain the plain text password. If the password is under 16 octets, it must be left-justified and padded to the right with nulls (0x00).

3.2 Route Tag

The Route Tag (RT) field is an attribute assigned to a route which must be preserved and readvertised with a route. The intended use of the Route Tag is to provide a method of separating "internal" RIP routes (routes for networks within the RIP routing domain) from "external" RIP routes, which may have been imported from an EGP or another IGP.

Routers supporting protocols other than RIP should be configurable to allow the Route Tag to be configured for routes imported from different sources. For example, routes imported from EGP or BGP should be able to have their Route Tag either set to an arbitrary value, or at least to the number of the Autonomous System from which the routes were learned.

Other uses of the Route Tag are valid, as long as all routers in the RIP domain use it consistently. This allows for the possibility of a

BGP-RIP protocol interactions document, which would describe methods for synchronizing routing in a transit network.

3.3 Subnet mask

The Subnet Mask field contains the subnet mask which is applied to the IP address to yield the non-host portion of the address. If this field is zero, then no subnet mask has been included for this entry.

On an interface where a RIP-1 router may hear and operate on the information in a RIP-2 routing entry the following rules apply:

- 1) information internal to one network must never be advertised into another network,
- 2) information about a more specific subnet may not be advertised where RIP-1 routers would consider it a host route, and
- 3) supernet routes (routes with a netmask less specific than the "natural" network mask) must not be advertised where they could be misinterpreted by RIP-1 routers.

3.4 Next Hop

The immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded. Specifying a value of 0.0.0.0 in this field indicates that routing should be via the originator of the RIP advertisement. An address specified as a next hop must, per force, be directly reachable on the logical subnet over which the advertisement is made.

The purpose of the Next Hop field is to eliminate packets being routed through extra hops in the system. It is particularly useful when RIP is not being run on all of the routers on a network. A simple example is given in Appendix A. Note that Next Hop is an "advisory" field. That is, if the provided information is ignored, a possibly sub-optimal, but absolutely valid, route may be taken. If the received Next Hop is not directly reachable, it should be treated as 0.0.0.0.

3.5 Multicasting

In order to reduce unnecessary load on those hosts which are not listening to RIP-2 messages, an IP multicast address will be used for periodic broadcasts. The IP multicast address is 224.0.0.9. Note that IGMP is not needed since these are inter-router messages which are not forwarded.

In order to maintain backwards compatibility, the use of the multicast address will be configurable, as described in section 4.1. If multicasting is used, it should be used on all interfaces which support it.

3.6 Queries

If a RIP-2 router receives a RIP-1 Request, it should respond with a RIP-1 Response. If the router is configured to send only RIP-2 messages, it should not respond to a RIP-1 Request.

4. Compatibility

RFC 1058 showed considerable forethought in its specification of the handling of version numbers. It specifies that RIP messages of version 0 are to be discarded, that RIP messages of version 1 are to be discarded if any Must Be Zero (MBZ) field is non-zero, and that RIP messages of any version greater than 1 should not be discarded simply because an MBZ field contains a value other than zero. This means that the new version of RIP is totally backwards compatible with existing RIP implementations which adhere to this part of the specification.

4.1 Compatibility Switch

A compatibility switch is necessary for two reasons. First, there are implementations of RIP-1 in the field which do not follow RFC 1058 as described above. Second, the use of multicasting would prevent RIP-1 systems from receiving RIP-2 updates (which may be a desired feature in some cases). This switch should be configurable on a per-interface basis.

The switch has four settings: RIP-1, in which only RIP-1 messages are sent; RIP-1 compatibility, in which RIP-2 messages are broadcast; RIP-2, in which RIP-2 messages are multicast; and "none", which disables the sending of RIP messages. The recommended default for this switch is RIP-1 compatibility.

For completeness, routers should also implement a receive control switch which would determine whether to accept, RIP-1 only, RIP-2 only, both, or none. It should also be configurable on a per-interface basis.

4.2 Authentication

The following algorithm should be used to authenticate a RIP message. If the router is not configured to authenticate RIP-2 messages, then RIP-1 and unauthenticated RIP-2 messages will be accepted;

authenticated RIP-2 messages shall be discarded. If the router is configured to authenticate RIP-2 messages, then RIP-1 messages and RIP-2 messages which pass authentication testing shall be accepted; unauthenticated and failed authentication RIP-2 messages shall be discarded. For maximum security, RIP-1 messages should be ignored when authentication is in use (see section 4.1).

Since an authentication entry is marked with an Address Family Identifier of 0xFFFF, a RIP-1 system would ignore this entry since it would belong to an address family other than IP. It should be noted, therefore, that use of authentication will not prevent RIP-1 systems from seeing RIP-2 messages. If desired, this may be done using multicasting, as described in sections 3.5 and 4.1.

4.3 Larger Infinity

While on the subject of compatibility, there is one item which people have requested: increasing infinity. The primary reason that this cannot be done is that it would violate backwards compatibility. A larger infinity would obviously confuse older versions of rip. At best, they would ignore the route as they would ignore a metric of 16. There was also a proposal to make the Metric a single octet and reuse the high three octets, but this would break any implementations which treat the metric as a 4-octet entity.

4.4 Addressless Links

As in RIP-1, addressless links will not be supported by RIP-2.

5. Security Considerations

The basic RIP protocol is not a secure protocol. To bring RIP-2 in line with more modern routing protocols, an extensible authentication mechanism has been incorporated into the protocol enhancements. This mechanism is described in sections 3.1 and 4.2.

Appendix A

This is a simple example of the use of the next hop field in a rip entry.

```

-----
|IR1|  |IR2|  |IR3|          |XR1|  |XR2|  |XR3|
---+---+---+---+---+---+---+---+---+---+---+---+
|      |      |      |      |      |      |
+-----+-----+-----+-----+-----+-----+
<-----RIP-2----->

```

Assume that IR1, IR2, and IR3 are all "internal" routers which are under one administration (e.g. a campus) which has elected to use RIP-2 as its IGP. XR1, XR2, and XR3, on the other hand, are under separate administration (e.g. a regional network, of which the campus is a member) and are using some other routing protocol (e.g. OSPF). XR1, XR2, and XR3 exchange routing information among themselves such that they know that the best routes to networks N1 and N2 are via XR1, to N3, N4, and N5 are via XR2, and to N6 and N7 are via XR3. By setting the Next Hop field correctly (to XR2 for N3/N4/N5, to XR3 for N6/N7), only XR1 need exchange RIP-2 routes with IR1/IR2/IR3 for routing to occur without additional hops through XR1. Without the Next Hop (for example, if RIP-1 were used) it would be necessary for XR2 and XR3 to also participate in the RIP-2 protocol to eliminate extra hops.

References

- [1] Hedrick, C., "Routing Information Protocol", STD 34, RFC 1058, Rutgers University, June 1988.
- [2] Malkin, G., "RIP Version 2 - Carrying Additional Information", RFC 1388, Xylogics, Inc., January 1993.
- [3] Malkin, G., and F. Baker, "RIP Version 2 MIB Extension", RFC 1724, Xylogics, Inc., Cisco Systems, November 1994.
- [4] Malkin, G., "RIP Version 2 Protocol Analysis", RFC 1721, Xylogics, Inc., November 1994.
- [5] Malkin, G., "RIP Version 2 Protocol Applicability Statement", RFC 1722, Xylogics, Inc., November 1994.

Author's Address

Gary Scott Malkin
Xylogics, Inc.
53 Third Avenue
Burlington, MA 01803

Phone: (617) 272-8140
EMail: gmalkin@Xylogics.COM

