RIPNG – A NEXT GENERATION ROUTING PROTOCOL *(IPv6)*

Adeyinka Adesuyi Falaye
Department of Mathematics and Computer Science
Federal University of Technology, Minna, Nigeria
E-mail: **falayemike@yahoo.com**

Abstract

This paper describes the future routing protocol called the Routing Information Protocol Next Generation (RIPng) owing to the current depletion rate of IPv4. The term Next Generation (NG), is used to describe protocols that support the Internet Protocol Version 6 (IPv6).addressing scheme. It starts up with a brief background to internetworking, internetwork models, Internet Protocols and IP addressing. IP version 4 address depletion is discussed; as well as methods available for slowing the depletion rate. It then introduces the IPv6 and highlighting the reasons for the drive towards it. IP packet routing and routing protocols are also discussed, with emphasis on the Routing Information Protocol (RIP). A brief history is given; its various versions are discussed, and detailed discussion on RIPv6 or RIPng are presented .

Keywords: Internetworking, network architecture router, ripng**,** internet protocol, ipv6.

Introduction

A network is a group of computers and associated peripheral devices connected by a communications channel capable of sharing files and other resources among several users (Dyson, 1999). A reference model is thus a conceptual blueprint of how communications should take place. The organization of a network in such a way as to conform to the reference model is known as network architecture. There are two common and widely accepted models of internetworking, namely: the OSI Model and the TCP/IP Model (Todd, 2007).

Internetwork models

THE TCP/IP MODEL

Fundamentally, this is a model defined by the Department of Defense (DoD) as a resilient protocol suite for interconnectivity amongst devices.

The TCP/IP specifies a four (4) layered model

Table 1: The TCP/IP Model

TCP/IP LAYER	*OSI EQUIVALENT*
Process/Application	Application, Presentation and Session Layers
Host-to-Host	Transport Layer
Internet	Network
Network Access	Data link and Physical

Each of these layers have protocols that run on them, a few of them are listed below

Table 2: Protocols on the TCP/IP layers

Application/ Process	*Telnet, FTP, TFTP, SNMP, NFS*
Host-to-Host	TCP and UDP

Internet	ICMP, ARP, RARP, IP
Network Access	Ethernet, FDDI, Token Ring

IP addressing

It operates at the internet layer of the TCP/IP model and has the task of delivering distinguished protocol packets from the source host to the destination host solely based on their addresses. It only provides best effort services as it does not provide any means of tracking packets, protecting packets from corruption, preventing packet replay etc. These services can be provided at the end nodes of each data transmission and are not necessary along the transmission path. This has the benefit of reducing network complexity (IP Addressing, 2010).

IP address

An IP Address is numeric identifier assigned to each machine on an IP network. It designates the exact location of a device on the network (Todd, 2007).There are two versions of the IP addresses available, namely the IPv4 and IPv6 (or IP next generation, IPng which is the future (Todd, 2007).

IP version 4 (IPV4)

This is the classic and most widely used address scheme on the internet. It consists of 32 bits of information, divided into four referred to as octets or bytes each divided by a dot.

IPv4 addresses are usually hierarchical in nature; consisting of a Network Address, an optional Subnet Address and a Host Address. This hierarchy is what defines the grouping of IP addresses into classes.

Table 4: A Summary of IPv4 Addressing Hierarchy

	8 Bits	8 Bits	8 Bits	8 Bits	Address Range
CLASS A	Network	Host	Host	Host	0 – 127
CLASS B	Network	Network	Host	Host	128 – 191
CLASS C	Network	Network	Network	Host	192 – 223
CLASS D	Multicast				224 – 239
CLASS E	Research				240 – 255

Sample IPv4 Addresses

10.10.11.15	*a 10... network class A address*
174.45.1.1	*174.45.. network class B address*
192.168.10.160	*192.168.10. network class C address*

It is can be concluded that if every system in the world were to be assigned a unique IP address based on IPv4 scheme, then we would have ran out of unique addresses. To deal with this unavoidable challenge a few concepts were developed, these included but not limited to Network Address Translation (NAT), Classless Inter-Domain Routing, Subnetting, and Variable Length Subnet Masks (VLSM). Only the NAT would be addressed.

NAT

NAT is an interim solution and was meant to help slow down the depletion of available IP address space by allowing many private IP addresses to be represented by some smaller number of public IP addresses.Private IP addresses are addresses that can be used on a private network, but are not routable through the Internet (Todd, 2007).

Public IP addresses on the other hand are addresses that are routable through the internet.

NAT basically takes a private IP address and converts it to one that can be used on the internet. With NAT, it is possible for multiple devices to have the same IP addresses*.

There are three types of NAT namely:

Static NAT

This type of NAT is designed to allow one-to-one mapping between local and global addresses.

Dynamic NAT

In this type of NAT a private IP address is mapped to a registered public IP address from a pool of registered IP addresses (Todd, 2007).

Overloading or Port Addressing Translation (PAT)

This is the most popular type of NAT configuration. This allows for thousands of users to be connected to the Internet using only one real global IP address (Todd, 2007).

*The devices should not be on the same network; else an IP conflict would result.

IP Version 6 (IPV6)

This is the next version of the Internet Protocol after IPv4. It is also called IPv6 or IP next generation (IPng). Unlike IPv4, IPv6 uses a 128-bit address space rather than the 32-bit. ‘This provides for a truly astronomical number of possible addresses’ (Dyson, 1999).

Why 1s IPv6 the future?

1. Scarcity of IPv4 addresses: This was majorly as a result of inefficient assigned allocation. Class A addresses which support about 16,777,214 host addresses are usually too big for most organizations. While Class C addresses (supporting 254 host addresses) are too small and not easily extensible. As a result, most organizations request Class B addresses (supporting 65,534 host addresses), but they use only a fraction of their assigned space.

2. Initially, every IP device required a unique public address and allowing this would lead to a rapid depletion of the available addresses. Some of the concepts for slowing depletion rate discussed above actually go against the design of the Internet. The internet was designed for best effort; therefore allowing intermediary devices manipulate packets is actually counterproductive.

3. Organizations and individuals requiring more than 1 public IP address

4. IPv4 only allows about 250 million assignable addresses, most of which have been allocated. IPv6 however offers over 3.4 x 10^38 addresses.

The IPv6 was developed to address these aforementioned shortcomings and other related issues with the IPv4.A typical IPv6 address consists of 8 sections, each separated by colons; with each of these sections containing 16 bits expressed as 4 hexadecimal numbers.

IPv6 addresses might look like this:*1234:5678:9ABC:DEF0:1234:5678:9ABC:DEF0*
2001:0000:0000:0012:0000:0000:1234:56AB, which can be rewritten as
2001::12:0:0:1234:56AB

It is interesting to note that IPv6 supports three types of addresses: One, **Unicast** which is the unique address of a device. Two, **Multicast**— Used For sending packets to all of the interfaces in a group. Three, **Anycast—** Used For sending to the nearest interface in a group. It is an established fact that IPv6 does not have broadcast addresses (IP Addressing, 2010).

Routing and routing protocols

A router is thus a device that routes / directs traffic to and from all the networks in an internetwork. A routing table is essentially a map that describes how to find remote networks (Todd, 2007). A router's routing table is populated automatically by the router itself, as is the case with networks directly connected to the routers interface. Hence, Routing Protocols in use today include: Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), and Intermediate System-to-Intermediate System (IS-IS) amongst others. Routing Protocols which are either Distant Vector or Link State (Todd, 2007).

The routing information protocol

Routing rnformation protocol version 1

RIPv1 was the first version of RIP developed. It is a distant-vector routing protocol using the Bellman-Ford algorithm for path selection. Being a Distant-Vector Routing Protocol (DV-RP), RIP sends its entire routing table to its neighbors periodically (30 seconds interval). RIP uses the number of routers between a source and destination as a route metric. Each router along the path is called a HOP. A maximum of 15 Hops are allowed, above that is flagged as an unreachable route. RIP routers communicate on port 520 (Hedrick, 1988).

Path Selection In Rip – The Bellman-Ford Algorithm

RIP routes by rumor, meaning that a RIP enabled router fills its Routing Table with information received from its neighbor (Hedrick, 1988).

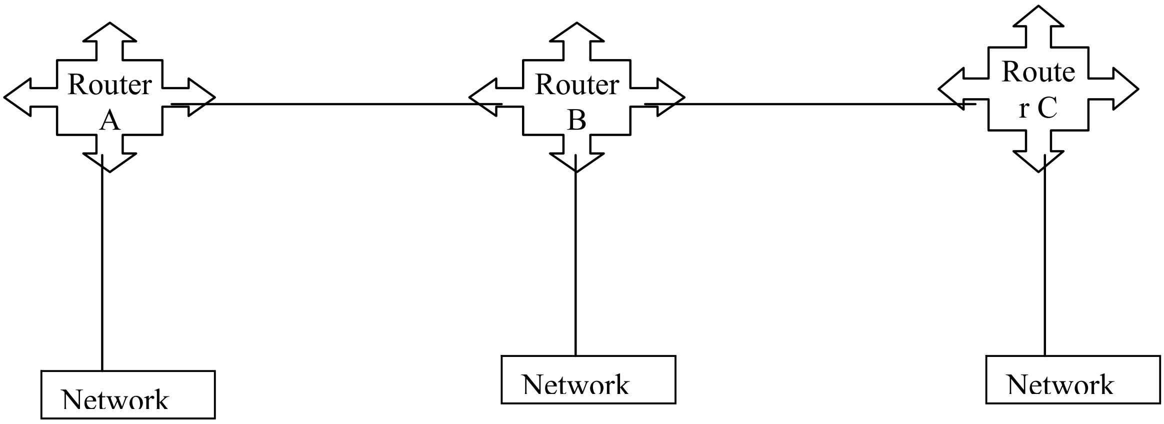


Figure 1: A simple RIP enabled Network

In the sample RIP enabled network above, RIP's algorithm is highlighted below:

1. RIP is enabled on Router A (RA)
2. RA sends a Request Message out all interfaces, but since no other router is on yet, it receives no response.
3. Router B is now enabled and its sends out (broadcast) a Request Message.

4. RA replies with its Routing Table, which contains only an entry for its directly connected network (Network A - NA), with a Hop Count of 1
5. RB then adds this to its Routing Table: NA via RA, Cost (Hop Count) 2
6. After 30 seconds (from the enable time), each router sends out its entire Routing Table to its rumor. RA's Routing Table would look like this:

NA	*Cost = 1*	*Interface 1*
NB	*Cost = 2*	*RB*

While RB's would look like this:

NB	*Cost = 1*	*Interface 1*
NA	*Cost = 2*	*RA*

7. Although when RB, sends its update after 30seconds, it would contain NA, Cost 2. This entry is ignored by RA, because it has a higher cost than what it already has; Cost = 1
8. When Router C (RC) is brought up, steps 3 to 6 are repeated
9. The process is repeated for subsequent routers, up to 15, beyond that the 16th network would be regarded by RA as unreachable or infinity (Hedrick, 1988).

Routing information protocol version 2 (Ripv2)

This is the second version of the RIP. It is essentially an improvement on RIP as it still runs/operates like RIPv1 but with a few tweaks and additions. These additions are highlighted below:

1. Classless Addressing and Subnetting: Prior to the development of RIPv1, subnetting did not exist and as such no provision was made for it in RIPv1. However as time went on, subnetting was introduced as one of the ways of slowing down the rapid depletion of IPv4 addresses (Todd, 2007).

RIPv2 brought with it support for subnetting, by allowing subnet information to be included within Route Entries on its Routing Table. With this also came support for Classless Inter-Domain Routing (CIDR) and Variable Length Subnet Mask (VLSM) (Todd, 2007).

2. Next Hop Specification: This meant that the exit interface for a packet can explicitly be specified by entering the IP address of the next hop router. This is very useful in cases where the next hop router is not running RIP and would normally not be selected by RIP as the next hop for any network (Todd, 2007).
3. Authentication and Security: RIPv2 came with a basic authentication scheme, which allowed routers to ascertain the identity of peer routers before accepting RIP messages from them (Todd, 2007).
4. Use of Multicast: Broadcasting of RIPv1 unsolicited Messages around the network had a negative effect on the network, by introducing excess network load. This was addressed in RIPv2 by the use of Multicasts rather than Broadcast messages. Multicast address 224.0.0.9 was used instead (Todd, 2007).
5. Route Tags: Route tags where introduced in RIPv2, to convey additional information to be carried with the route (Todd, 2007).

Barring these additions/modifications both versions of RIP can work together, as RIPv1 would simply ignore the additional entries it does not understand. Thus RIPv2 is backward compatible with RIPv1 (Todd, 2007)..

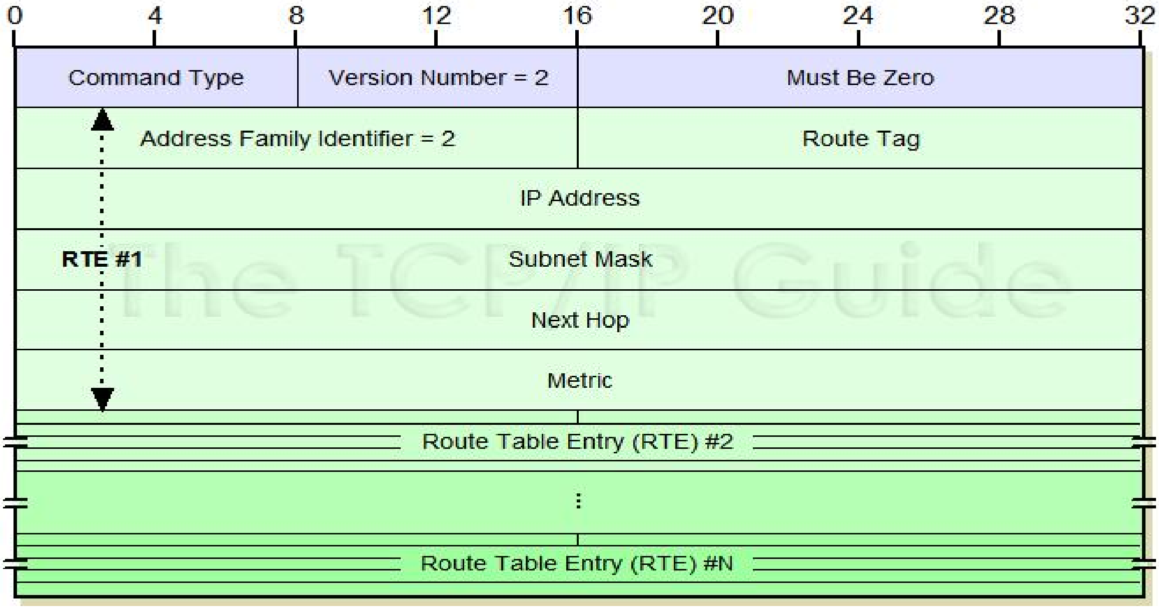
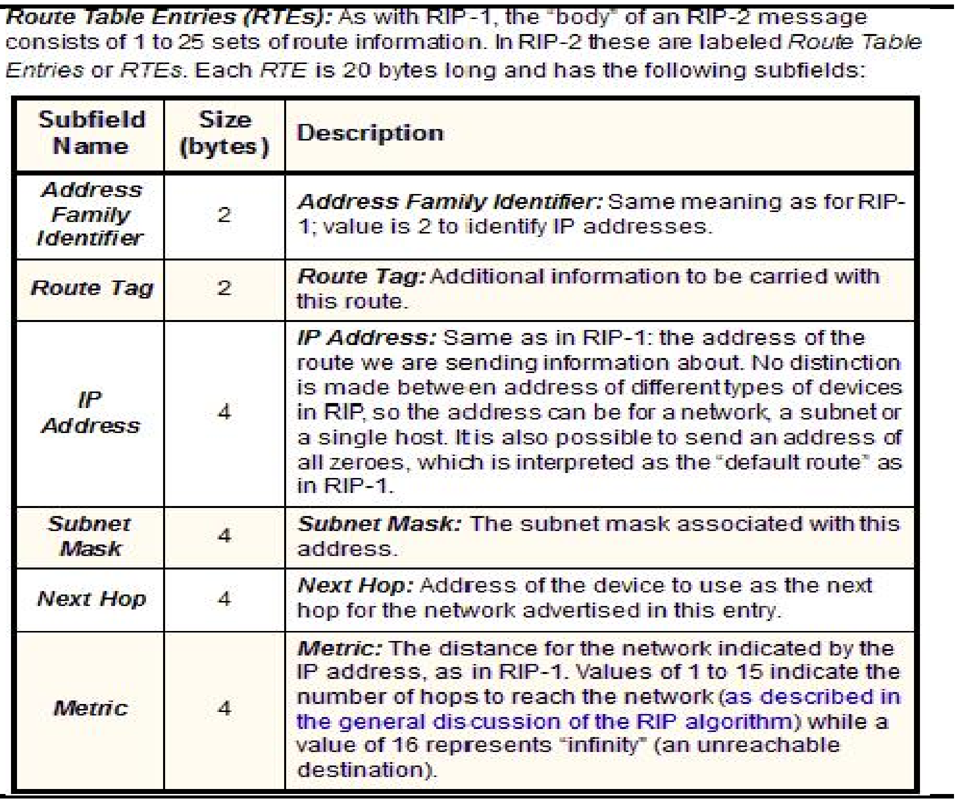


Figure 3: RIP Version 2 (RIPv2) Message Format. Malkin, (1998)

Table 7: RIP Version 2 (RIPv2) Message Format. Malkin, (1998)

Field Name	*Size (bytes)*	*Description*
Command	1	*Command Type:* Identifies the type of RIP message being sent. A value of 1 indicates an *RIP Request*, while 2 means an *RIP Response*.
Version	1	*Version Number:* Set to 2 for RIP version 2.
Must Be Zero	2	*Reserved:* Field reserved; value must be set to all zeroes.

Route Table Entries (RTEs)	20 to 500, in increments of 20	

Route Table Entries (RTEs): As with RIP-1, the "body" of an RIP-2 message consists of 1 to 25 sets of route information. In RIP-2 these are labeled *Route Table Entries* or *RTEs*. Each *RTE* is 20 bytes long and has the following subfields:

Subfield Name	Size (bytes)	Description
Address Family Identifier	2	***Address Family Identifier:*** Same meaning as for RIP-1; value is 2 to identify IP addresses.
Route Tag	2	***Route Tag:*** Additional information to be carried with this route.
IP Address	4	***IP Address:*** Same as in RIP-1: the address of the route we are sending information about. No distinction is made between address of different types of devices in RIP, so the address can be for a network, a subnet or a single host. It is also possible to send an address of all zeroes, which is interpreted as the "default route" as in RIP-1.
Subnet Mask	4	***Subnet Mask:*** The subnet mask associated with this address.
Next Hop	4	***Next Hop:*** Address of the device to use as the next hop for the network advertised in this entry.
Metric	4	***Metric:*** The distance for the network indicated by the IP address, as in RIP-1. Values of 1 to 15 indicate the number of hops to reach the network (as described in the general discussion of the RIP algorithm) while a value of 16 represents "infinity" (an unreachable destination).

Routing information protocol next generation (Ripng)

With IPv4 almost completely depleted, IPv6 is fast becoming the emerging standard for device addressing. Unfortunately IPv6 uses an architecture that is completely different form that in the IPv4, thus devices and every other thing that works with IP addresses must change to function under IPv6, routing protocols inclusive.

With dynamic routing serving as almost the de facto standard for IP routing, routing protocols must be changed/upgraded to support IPv6. This is what led to the development of RIPv6 or RIPng (Malkin, 1997).

RIPng works essentially like its predecessor (RIPv2), but incorporates a few changes, prominent amongst which is the change from a 32-bit to a 128-bit addressing as used in IPv6.

From RIPV2 to Ripng

Though RIPng is a comparatively new protocol it is still based on its predecessors. RIPng also does not introduce any specific new features compared to RIPv2, except those needed to implement RIP for IPv6.

1. Metric: In RIPv2, metric was based on Hop counts. This hop count was always included in the route updates sent among RIPv2 enabled routers. This feature still remains albeit implemented in a slightly different way.

Due to the large size of IPv6 addresses, including a Next Hop field into a RIPng packet would almost double the size of every entry and since Next Hop is an optional feature it is sent in a separate routing update whenever it is needed.

2. Classless Addressing and Subnet Mask: IPng like RIPv2 is also a classless protocol (sends subnet mask information with route updates), but all IPv6 addresses are specified using an address and a prefix

length. Thus instead of a subnet mask as is the case in RIPv2, a prefix length is provided for each address entry.

3. Authentication and Encryption: RIPv2 uses Message Digest 5 (MD5) as its means of authentication. RIPng does not include any authentication but relies solely on IPSec features provided within the IPv6 protocol suite.
4. Route Update/ Messages: Like RIPv2, RIP Request and Response messages are also exchanged between routers.

When a Router running RIP is first initialized, it sends RIP Request messages out all interfaces on UDP port 520.
RIP Response packets are sent as response to Request messages. These messages can contain up to 25 routes and are only sent to direct neighbors. RIPng applies the same principle but uses UDP port 521 instead of port 520.

At regular intervals, unsolicited RIP Response messages (not in response to a request) are sent with both the source and destination ports set to 521.

In RIPng transmission of messages is done using a multicast address FF02::9, similar to RIPv2 that transmits to all peers on multicast address 224.0.0.9.

5. Route Table Entries: RIPv2 had a limit of 25 entries per message; this is not the case with RIPng. In RIPng route table entries can be unlimited*.

*Although the limitation of 25 entries in RIPv2 no longer exists in RIPng, practically it is not unlimited but limited by the Maximum Transmission Unit (MTU) of the network over which the message is being sent.

Ripv6 Message Format and Features

RIPng messages are similar to that of RIPv1 and RIPv2, except for the format of the routing table entries. The table below shows a summary of RIPng messages component and their description.

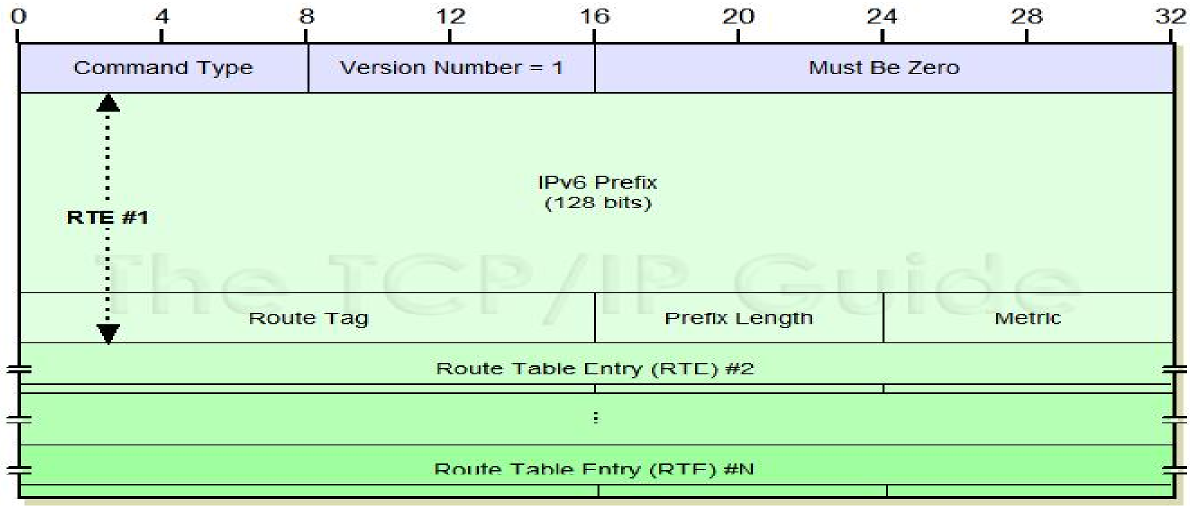
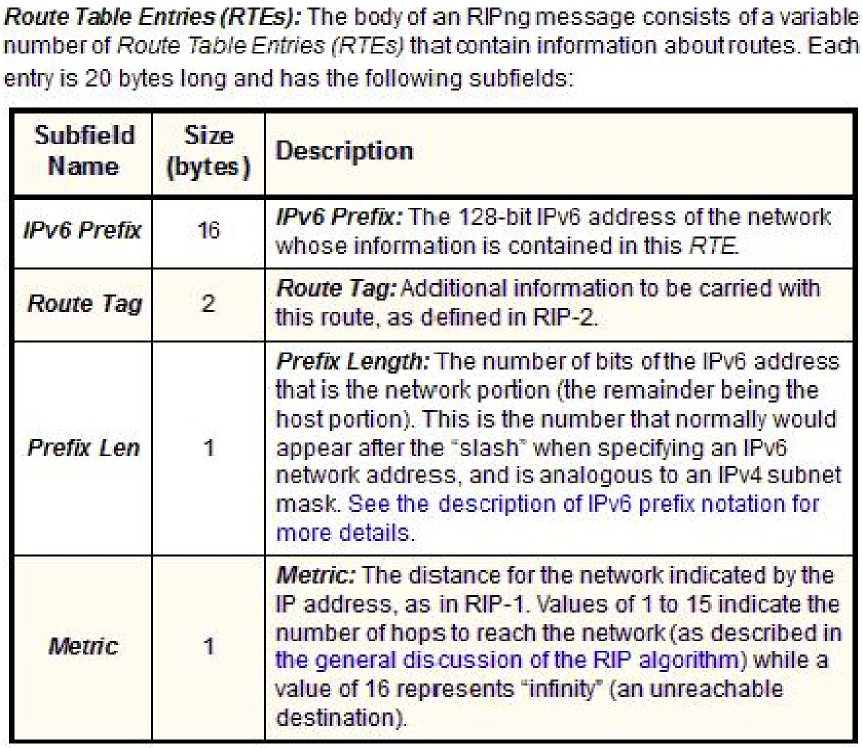


Figure 4: RIPng Message Format (Malkin, (1998)

Table 8: Fields within a RIPng message (Malkin, (1998)

Field Name	*Size (bytes)*	*Description*
Command	1	*Command Type:* Identifies the type of RIPng message being sent. A value of 1 indicates RIPng Request message. While 2 means RIPng Response message.
Version	1	Version Number*:* Set to a value of 1
Must Be Zero	2	Reserved: This field is reserved and usually set to a value zero.
Route Table Entries (RTEs)	Variable	

Route Table Entries (RTEs): The body of an RIPng message consists of a variable number of *Route Table Entries (RTEs)* that contain information about routes. Each entry is 20 bytes long and has the following subfields:

Subfield Name	Size (bytes)	Description
IPv6 Prefix	16	***IPv6 Prefix:*** The 128-bit IPv6 address of the network whose information is contained in this *RTE*.
Route Tag	2	***Route Tag:*** Additional information to be carried with this route, as defined in RIP-2.
Prefix Len	1	***Prefix Length:*** The number of bits of the IPv6 address that is the network portion (the remainder being the host portion). This is the number that normally would appear after the "slash" when specifying an IPv6 network address, and is analogous to an IPv4 subnet mask. See the description of IPv6 prefix notation for more details.
Metric	1	***Metric:*** The distance for the network indicated by the IP address, as in RIP-1. Values of 1 to 15 indicate the number of hops to reach the network (as described in the general discussion of the RIP algorithm) while a value of 16 represents "infinity" (an unreachable destination).

The Bellman-Ford algorithm which RIP uses has a few inherent problems which are:

RIP timers

RIP uses four types of timers which are as follows:

Update timer

This is the interval between route updates (sending of complete copy of its routing table out to all RIP enabled neighbors). It's usually between **25-30 seconds** interval.

Invalid timer

The time frame for which a route is valid. If a RIP enabled router does not get any update about a route for a period of time = the invalid time, (usually about **3minutes or 180 seconds**) it concludes that the route has become invalid and announces same to its neighbors.

Holddown timer

A router upon receiving an update indicating that a route has become unreachable / invalid from its neighbors does not just delete the route from its routing table immediate, instead its waits for a period of about **180 seconds** known as the hold down time before deleting it.

Route flush timer

On expiration of the Hold down timer a router can then delete a route if no update about it is received yet. The router informs its neighbors about the route to be deleted before actually deleting it from its local routing table.
The time interval is usually (4 minutes or 240 seconds).

Conclusion

RIPng is the version of RIP that was developed for use on internetworks running on the IPv6. It is very similar to both its predecessors (RIPv1 and RIPv2) with only slight changes to their features to enable compatibility with IPv6.

1. Slow Convergence: It takes a long time for all routers to have the same information on their routing table. This is also very prominent when a topology change occurs.
2. Routing loops: A routing loop occurs when Router A has an entry telling it to send packets for a destination to Router B, and Router B has an entry saying that traffic for the same destination should be sent to Router A. RIP tries to deal with this situation by ensuring that updates sent from one router to its peer are not sent back; if they are such routes' hop count are set to 16 (unreachable).
3. Metric: RIP uses hop count as its metric for sending traffic between routers. When compared to other routing protocols hop count is a very poor metric as it does not take into consideration path costs, delays, bandwidth amongst others.
4. Scalability: RIP is limited to a stretch of 15 routers beyond which it becomes unstable. This is why RIP cannot be used on core / backbone networks.

Although RIPng might be a new protocol (relative to its predecessors), it is still based on the original RIP and as such by design it is limited to operating within a small network. For huge networks, Routing Protocols such as OSPFv3 (support for IPv6) should be considered.

Reference

Dyson, P. (1999). *Dictionary of Networking*, 3rd Edition USA: Sybex Publishing, Inc.

Hedrick C. (1988), RFC1058 "RIP Version 1" *Request for Comments*, International Engineering Task Force.

IP Addressing, (2010). Available at: http://en.wikipedia.org/wiki/IP_address

Malkin, G. (1997), RFC2080 "RIPng for IPv6" *Request for Comments*, International Engineering Task Force.

Malkin, G. (1998), RFC2453 "RIP Version 2" *Request for Comments*, International Engineering Task Force

Todd, L. (2007), *Cisco Certified Network Associate Study Guide*, 6th Edition, USA: Wiley Publishing, Inc,

.