RFC: 40008

Dynamic Routing Protocol

FILLING THE ROUTING TABLE DYNAMICALLY

PROTOCOL SPECIFICATION

April 2019

prepared for

Defense Distributed Applications

Programming Project

Creating Virtual Networks over TCP/IP layer

Lebanese University

1700 Nabatiyeh, Lebanon

by

Master 1 Students

Lebanese University

Faculty Of Sciences

1700 Nabatiyeh, Lebanon

Dynamic Routing Protocol

Abstract

This document specifies the protocol of dynamic routing (DRP)

that allows filling the routing table dynamically.

Maria Afara

Ali Fakih

Editor

Table of Contents

1 Introduction . . . . . . . . . . . . . . . . . . . . . . . 6

2 Limitations of the Protocol . . . . . . . . . . . . . . . . 6

3 Distance Vector Algorithm for DPR . . . . . . . . . . .. . 7

4 Protocol Specification . . . . . . . . . . . . . . . . . . 8

5 Message Format . . . . . . . . . . . . . . . . . . . . . . . 9

5.1 Dest IP Address-Hostname . . . . . . . . . . . .. .. . 11

5.2 Next IP Address-Hostname. . . . . . . . . . . . . . . . . 11

5.3 Next Hop . . . . . . . . . . . . . . . . . . . . . . . . . 11

5.4 Metric . . . . . . . . . . . . . . . . . . . . . . . . . . 11

6 Addressing Considerations . . . . . . . . . . . . . . . . . 11

7 Timers . . . . . . . . . . . . . . . . . . . . . . . . . . . 12

8 Routing table Updating . . . . . . . . . . . . . . . . . . . 13

9 Failed Nodes . . . . . . . . . . . . . . . . . . . . . . . . 13

References . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

1 Introduction

DRP is a dynamic routing protocol based on the Bellman-Ford (or distance vector) routing algorithm. Its single purpose is to direct data traffic down the optimal path toward a destination when given the choice between multiple paths. The “dynamic” part refers to the protocol's ability to recalculate and re-route traffic when more optimal paths become available or when links along the most optimal path fail.

DRP is intended for use within the IP-based Internet. The Internet is organized into a number of networks connected by routers. Hosts and routers are presented with IP datagrams addressed to some host. Routing is the method by which the host or router decides where to send the datagram. It may be able to send the datagram directly to the destination, if that destination is on one of the networks that are directly connected to the host or router.

However, the interesting case is when the destination is not directly reachable.

In this case, the host or router attempts to send the datagram to a router that is nearer the destination. The goal of a routing protocol is very simple: It is to supply the information that is needed to do routing i.e it is responsible for the creation, maintenance and updating of the dynamic routing table.

2 Limitations of the Protocol

DPR prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for DPR is 15(the newtork's diameter). This hop limit, however, also limits the size of networks that DPR can support thus it is inappropriate for larger networks.

3 Distance Vector Routing Protocol for DPR

A distance-vector routing protocol uses the Bellman-Ford algorithm to calculate paths.

A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically and, in some cases, when a change is detected in the topology of a network.

Distance Vector means that Routers are advertised as vector of distance and direction. 'Direction' is represented by next hop address,hostname and exit interface, whereas 'Distance' uses metrics such as hop count.Routers using distance vector protocol do not have knowledge of the entire path to a destination. Instead DV uses two methods:

1. Direction in which or interface to which a packet should be forwarded.

2. Distance from its destination.

Updates are performed periodically in a distance-vector protocol where all or part of a router's routing table is sent to all its neighbors that are configured to use the same routing protocol .Once a router has this information it is able to amend its own routing table to reflect the changes and then inform its neighbors of the changes. This process has been described as ‘routing by rumor’ because routers are relying on the information they receive from other routers and cannot determine if the information is actually valid and true.

4 Protocol Specification

DPR is intended to allow routers to exchange information for computing routes through an IPv4-based network.

Any router that uses DPR is assumed to have interfaces to one or more networks which are called directly connected networks, otherwise it isn’t really a router. The protocol relies on access to certain information about each of these networks, the most important of which is its metric. The DPR metric of a network is an integer between 1 and 15, inclusive. Thus the maximum path limit of 15. In addition to the metric, each network will have an IPv4 destination address and hostname associated with it. These are to be set by the system administrator.

Each router that implements DPR is assumed to have a routing table. This table has one entry for every destination that is reachable throughout the system operating DPR. Each entry contains at least the following information (the basics):

- The IPv4 address of the destination , hostname of the destination.

- A metric, which represents the number of routers data must pass from source network to reach the destination.

- The IPv4 address,hostname of the next router along the path to the destination (i.e., the next hop).

The entries for the directly-connected networks are set up by the router using information gathered by means not specified in this protocol. The metric for a directly-connected network is set to the cost of that network. As mentioned, 1 is the usual cost. In that case, the DPR metric reduces to a simple hop-count. More complex metrics may be used when it is desirable to show preference for some networks over others (e.g., to indicate of differences in bandwidth or reliability).

Implementers may also choose to allow the system administrator to enter additional routes. These would most likely be routes to hosts or networks outside the scope of the routing system. They are referred to as "static routes." Entries for destinations other than these initial ones are added and updated by the algorithms described in the following sections.

In order for the protocol to provide complete information on routing, every router in the AS must participate in the protocol.

5 Message Format

DPR is a UDP-based protocol. Each router that uses DPR has a routing process that sends and receives datagrams on UDP port number 520, the

DPR port. All communications intended for another routers’s DPR process are sent to the DPR port. All routing update messages are sent from the DPR port. Unsolicited routing update messages have both the source and destination port equal to the DPR port. Update messages sent in response to a request are sent to the port from which the request came. Specific queries may be sent from ports other than the DPR port, but they must be directed to the DPR port on the target machine.The DPR packet format is:

0 1 2 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) | must be zero (2) |

+---------------+---------------+-------------------------------+

| |

~ DPR Entry (20) ~

| |

+---------------+---------------+---------------+---------------+

The format for the 20-octet route entry (RTE):

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

+-------------------------------+-------------------------------+

| Dest IP Address-Hostname (4) |

+---------------------------------------------------------------+

| NextIP Address-Hostname (4) |

+---------------------------------------------------------------+

| Next Hop (4) |

+---------------------------------------------------------------+

| Metric (4) |

+---------------------------------------------------------------+

5.1 - Dest IP Address-Hostname

This will be the IP address and hostname of the host or network.

5.2 Next IP Address-Hostname

This will be the IP address and hostname of the next host or network.

5.3 Next Hop

The immediate next hop IP address to which packets to the destination specified by this route entry should be forwarded. 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.

5.4 Metric

A number, indicating the distance to the destination.

6 Addressing Considerations

Distance vector routing can be used to describe routes to individual hosts or to networks. The DPR protocol allows either of these possibilities. The destinations appearing in request and response messages can be networks, hosts. In general, the kinds of routes actually used will depend upon the routing strategy used for the particular network.

Many networks are set up so that routing information for individual hosts is not needed. If every node on a given network or subnet is accessible through the same routers, then there is no reason to mention individual hosts in the routing tables. However, networks that include point-to-point lines sometimes require routers to keep track of routes to certain nodes. Whether this feature is required depends upon the addressing and routing approach used in the system.Thus, some implementations may choose not to support host routes

7 Timers

This section describes all events that are triggered by timers.

Every 10 seconds, DPR process is awakened to send an unsolicited

Response message containing the complete routing table to every

neighboring router. When there are many routers on a single network,

there is a tendency for them to synchronize with each other such that

they all issue updates at the same time. This can happen whenever

the 10 second timer is affected by the processing load on the system.

It is undesirable for the update messages to become synchronized,

since it can lead to unnecessary collisions on broadcast networks.

Therefore, implementations are required to take one of

two precautions:

8-Routing table updating

if an entry is present in the routing table,checks for the cost if it is less than what the cost was plus 1 , then update the cost to the new one. else add the new entry with updating the next ip address and hostame.

- Setting the destination address to the destination address in the RTE

- Setting the metric to the newly calculated metric (as described above)

- Set the next hop address to be the address of the router from which the packet came

If there is an existing route, compare the next hop address to the address of the router from which the packet came. If this packet is from the same router as the existing route. Next, compare the metrics. If the packet is from the same router as the existing route, and the new metric is different than the old one; or, if the new metric is lower than the old one; do the following actions:

- Adopt the route from the packet (i.e., put the new metric in and adjust the next hop address, if necessary).

9-Failed Nodes

when a router failes it sends itself as a failed node to its directly connected networks and then sends al the routes that it has in the routing table as a failed node.when a router recieves a failed node it checks if there is any destination in its router that reaches it through the failed node.In this case it sends to its neighbors also that it deleted it.each time failed node is recieved there is a timer of 15 sec set to the router to stop recieving any routing table.

References

[1] RFC 2453 RIP V2

[2] Wikipedia

[3] Info 402 Inter Network and Network Security Course in

Lebanese University Faculty of Science.