Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Interior Gateway Protocols

P. Priyadhivya*
PG Scholar,
Department of ECE,
SNS College of Technology,
India

S. Vanitha
Assistant Professor,
Department of ECE,
SNS College of Technology,
India

Abstract— Routing is usually performed by a device called router. Routing is the significant characteristics of the internet since it enables messages to pass from one computer to another and eventually reach the destination. Each computer in the network performs routing by passing the message to the next computer. The commonly used routing protocols are RIP (Routing Information Protocol), OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol). These are the interior gateway protocols that have been developed for IP networks and it is used to exchange routing information within an administrative network. This paper explains briefly about Interior gateway routing protocols.

Keywords— RIP, OSPF, EIGRP, IGP, Autonomous system, Routing protocols

I. INTRODUCTION

The term IGP (Interior Gateway Protocol) is used to describe any routing protocol operating as a separate routing domain within a single administrative network. IGPs have knowledge about routes to networks that are internal to AS; hence it is named as Interior [1]. Within an organization's network there may be one or more routing protocols (IGPs) keeping track of the routes to subnets within the AS. Routers running a single IGP (routing protocol) only share route information with other routers running the same routing protocol. Routers working with more than one interior gateway protocols like RIP and OSPF are participants of two different routing domains. These routers are known as border routers because they are in the border between two IGP routing domains. The IGP is classified into Distance vector routing protocol, Link state routing protocol, Hybrid routing protocol.

A. Distance vector routing protocol

The distance-vector routing is a type of algorithm used by routing protocols to discover routes on an interconnected network. The distance-vector routing protocol uses Bellman-Ford algorithm. Distance-vector routing refers to a method for exchanging route information. A router will announce a route as a vector of direction and distance. Direction sends to a port that guides to the next router along the path to the destination, and distance is a metric that point out the number of hops to the destination, even though it may also be an unsupported value that gives one route precedence over another. Internetwork routers exchanges this vector information and build route lookup tables from it. Distance vector as the name suggests uses distance between remote networks to determine the best path to a remote network.

The distance vector metric is represented by hop [1]. It's not a measure of distance rather the number of routers in between the router and the destination network. The examples of Distance vector routing protocols are RIPv1 (version1), RIPv2 (version2), RIPng (Next generation), IGRP (Interior Gateway Routing Protocol).

B. Link state routing protocol

Link state protocols are based on Shortest Path First (SPF) algorithm to find the best path to a destination. Shortest Path First (SPF) algorithm is also known as Dijkstra algorithm, since it is conceptualized by Dijkstra. Link state routing always try to maintain full networks topology by updating itself incrementally whenever a change happen in network. In Shortest Path First (SPF) algorithm, whenever a link's state alters, a routing update referred as Link-State Advertisement (LSA) is exchanged between routers. When a router gets an LSA routing update, the link-state algorithm is used to recompute the shortest path to affected destinations [2]. Each router constructs a map of the complete network. The examples of Link state routing are Open Shortest Path First (OSPF), Intermediate system to intermediate system (IS-IS).

C. Hybrid routing protocol

Hybrid routing protocols have both the features of distance vector routing protocols and linked state routing protocols. The example is Enhanced Interior Gateway Routing Protocol (EIGRP).

II. RIP

The Routing Information Protocol (RIP) is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) designed to distribute routing information within an Autonomous System (AS).RIP is a simple vector routing protocol with many existing implementations. In distance vector routing protocol, the routers exchanges the

network information with their closest neighbours. In other words, the routers transmit to each other the sets of destinations ("address prefixes") that they can arrive, and the next hop address to which data should be sent in order to reach those destinations [2]. This contrasts with link-state IGPs; vectoring protocols exchange routes with other, whereas link state routers exchanges the topology information, and calculate their own routes locally. A vector routing protocol floods reachability information throughout all routers participating in the protocol, so that all routers maintains a routing table containing the complete set of destinations known to the participating routers.

A. RIP Version 1

RIP uses classful routing. The periodic routing updates do not carry subnet information and it lacks support for variable length subnet masks (VLSM). In other words, all subnets in a network class must have the same size. There is also no support for router authentication.

B. RIP Version 2

Due to the some deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed. It includes the ability to carry subnet information and hence it supports Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. It uses MD5 mechanism for authentication.

C. RIPng

RIPng (RIP next generation) is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. While RIPv2 supports RIPv1 updates authentication, RIPng does not support. IPv6 routers at the time are supposed to use IPSec for authentication; RIPv2 allows attaching arbitrary tags to routes, where RIPng does not support [5]. RIPv2 encodes the next-hop into each route entry. RIPng requires unique encoding of the next hop for a set of route entries.

D. RIP Timers

The routing information protocol makes use of the following timers as part of its operation.

- **Update timer**
  The update timer controls the time between routing updates. By default the value is 30 seconds.
- **Invalid timer**
  The invalid timer specifies how long a routing entry can be in the routing table without being updated. The default value is 180 seconds.
- **Hold-down timer**
  The Hold Down timer tells the routers to hold down recently affected routes for some period. During this time no update can be done to that routing entry. The default value of this timer is 90 seconds.
- ***Flush timer***
  The flush timer controls how long before a route is completely flushed from the routing table. The default value is 120 seconds.

E. Operation of RIP

RIP uses two types of messages.

1. A request message is used to ask neighbouring routers to send an update.
2. A response message carries the update.

RIP protocol works as follows;

- Each router prepares its routing table with a list of locally connected networks.
- Periodically, each router advertises the entire contents of its routing table over all of its RIP-enabled interfaces.
- Whenever a RIP router receives such an advertisement, it puts all of the suitable routes into its routing table and begins using it to forward packets. This process guarantee that every network connected to every router eventually becomes known to all routers.
- If a router does not continue to receive advertisements for a distant route, it finally times out that route and stops forwarding packets over it. In other words, RIP is a "soft state" protocol.
- Every route has an attribute called a metric, which indicates the "distance" to the route's destination.
- Every time a router gets a route advertisement, it increments the metric.
- Routers give priority to shorter routes than longer routes when deciding which of two versions of a route to program in the routing table.
- The maximum metric permitted by RIP is 16, which means that a route cannot be reached. This means that the protocol cannot support networks where there may be more than 15 hops to a given destination.
  RIP includes optimization of this basic algorithm to improve stabilization of the routing database and to eliminate routing loops.
- When a router detects a change to its routing table, it sends an immediate "triggered" update. This makes the routing table stable and eliminates routing loops.
- When a route is determined to be not reachable, RIP routers do not remove it straightaway. Instead they continue to publicize the route with a metric of 16 (unreachable). This ensures that neighbors are quickly notified of not reachable routes, rather than to wait for timeout.

- When router A has learnt a route from router B, it publicizes the route back to B with a metric of 16 (unreachable). This ensures that B is never under the effect that A has a different way of getting to the same destination. This technique is known as "split horizon with poison reverse."
- A "Request" message allows a newly-started router to rapidly query all of its neighbour's routing tables.

F. RIP Advantages and Disadvantages

Routing Information Protocol has advantages in small networks. It is easy to understand, configure and is supported by mostly all the routers. Since its restricted to 15 hops, any router beyond that distance is considered as infinity, and hence unreachable. RIP has very slow network convergence in large networks. If implemented in a large network, RIP can create traffic by multicasting all the routing tables every 30 seconds, which is bandwidth intensive. The routing updates take up significant bandwidth leaving behind very limited resources.RIP doesn't support multiple paths on the same route and is likely to have more routing loops resulting in a loss of transferred data. RIP uses predetermined hop count metrics to compare available routes, which cannot be used when routes are chose based on real-time data. This results in an increased delay in transmitting packets and overloads network operations due to repeated processes.

III. OSPF

The OSPF (Open Shortest Path First) protocol is one of a family of IP Routing protocols, and is an Interior Gateway Protocol (IGP) for the Internet, used to deliver IP routing information throughout a single Autonomous System (AS) in an IP network [3]. The OSPF protocol is a link-state routing protocol, because the routers exchanges topology information with their closest neighbours. The topology information is distributed throughout the AS, so that all routers within the AS have a complete picture of the topology of the AS. This picture is then used to estimate end-to-end paths through the AS, usually using a variant of the Dijkstra algorithm. OSPF supports a variable network subnet mask so that a network can be subdivided.

A. Protocol Messages

Unlike other routing protocols, OSPF does not carry data via a transport protocol, such as the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP). Instead, OSPF forms IP datagram directly. OSPF defines five different message types, for different types of communication.

- ***Hello***

As the name suggests, these messages are used as a form of greeting, to permit a router to discover other adjacent routers on its local links and networks. The messages establish relationships between neighbouring devices (called adjacencies) and communicate key parameters about how OSPF is to be used in the autonomous system or area.

- ***Database description***

These messages contain descriptions of the topology of the AS or area. That is, they carry the contents of the link-state database for the autonomous system or area from one router to another. Transferring large LSDB may need several messages to be sent; this is done by having the sending device designated as a master device and sending messages in sequence, with the slave (recipient of the LSDB information) responding with acknowledgements.

- ***Link state request***

These messages are used by one router to request updated information about a portion of the LSDB from another router. The messages clearly describe which link(s) about which the requesting device wants more current information.

- ***Link state update***

These messages contain updated information about the state of certain links on the LSDB. They are received in response to a Link State Request message, and it is also broadcasted or multicasted by routers on a regular basis. Their contents are used to update the information in the LSDBs of routers that receive them.

- ***Link state acknowledgement***

These messages provide credibility to the link-state exchange process, by explicitly acknowledging receipt of a Link State Update message.

B. Router Types

OSPF defines the following categories of Routers.

- ***Internal router(IR)***

An Internal Router has only OSPF neighbour relationships with routers in the same area.

- ***Area border router(ABR)***

Routing devices that belong to more than one area and connect one or more OSPF areas to the backbone area are called area border routers (ABRs). At least one interface is within the backbone while another interface is in another area. ABRs also preserve an individual topological database for each area to which they are connected.

- ***Backbone router(BR)***

Backbone Routers are part of the OSPF backbone. This includes all area border routers and also routers connecting different areas.

- ***Autonomous system boundary router(ASBR)***

Routing devices that exchange routing information with routing devices in non-OSPF networks are called AS boundary routers. They publicise externally learned routes throughout the OSPF AS. Depending on the position of the

AS boundary router in the network, it may be an ABR and it is also a backbone router, or an internal router (with the exception of stub areas). Routing devices within the area where the AS boundary router resides know the path to that AS boundary router. Any routing device external to the area only knows the path to the nearest ABR that is in the same area where the AS boundary router resides.

C. Router Attributes

In addition to the four router types, OSPF uses the terms designated router (DR) and backup designated router (BDR), which is attributes of a router interface.

- ***Designated router and Backup designated router***

A Designated Router (DR) is the router interface elected among all routers on a network segment, and Backup designated (BDR) is a backup for the Designated Router. Designated Routers are used for reducing network traffic by providing a source for routing updates [4]. The Designated Router maintains a complete topology table of the network and sends the updates to the other routers via multicast. All routers within an area forms slave/master relationship with the Designated Router.

D. OSPF advantages and disadvantages

OSPF routing protocol has a complete knowledge of net work topology allowing routers to calculate routes based on incoming requests. Additionally, OSPF has no restrictions in hop count, it will converge faster than RIP, and has better load balancing. OSPF doesn't scale when there are more routers added to the network. This is because it maintains many copies of routing information. An OSPF enabled network with intermittent links may increase traffic every time a router sends information [4]. This lack of scalability in OSPF makes it unsuitable for routing across the Internet.

IV. EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is considered as a Hybrid Routing Protocol because EIGRP has characteristics of both Distance Vector and Link State Routing Protocols. It is designed to give all the flexibility of routing protocols such as OSPF but with much faster convergence [5]. EIGRP shares routing table information that is not available in the neighbouring routers, which decreases unwanted traffic transmitted through routers. It uses Diffusing Update Algorithm (DUAL), which decreases the time taken for network convergence and improves operational efficiency. EIGRP is used on a router to share routes with other routers within the same autonomous system. Unlike RIP, EIGRP only sends incremental updates, decreasing the load on the router and the amount of data that needs to be transmitted. EIGRP calculates its metrics by using bandwidth, delay and load. By default, only bandwidth and delay are used when calculating metric, where reliability and load are assumed to zero. In addition to the routing table, EIGRP uses the tables to store information.

- ***Neighbour table***

Each router keeps state information about adjacent neighbours. When new neighbours are learned, the address and interface of the neighbour are stored. This information is also recorded in the neighbour table. When a neighbour sends a hello packet, it publicises a hold time, which is the amount of time that a router treats a neighbour as reachable and operational. In other words, if a hello packet isn't heard within the hold time, the hold time terminates and DUAL is informed of the topology change.

- ***Topology table***

The topology table contains all destinations advertised by neighbouring routers. Associated with each entry are the destination address and a list of neighbours that have advertised the destination. For each neighbour, the publicised metric is stored. This is the metric that the neighbour records in its routing table. If the neighbour is publicising this destination, it uses the route to forward packets. Also associated with the destination is the metric that the router uses to reach the destination. This is the sum of the best-publicised metric from all neighbours and the link cost to the best neighbour. This is the metric, the router uses in the routing table and when advertising to other routers.

A. Features

EIGRP supports the following features.

- Support VLSM and non adjacent networks.
- Use Reliable Transport Protocol (RTP) to delivery and reception of EIGRP packets.
- Use the best path selection based on Diffusing Update Algorithm (DUAL), guaranteeing loop-free paths and backup paths throughout the routing domain [7].
- Finds neighboring devices using periodic Hello messages to discover and monitor connection status with its neighbors.
- It sends incremental updates when the state of a destination alters, instead of sending the entire contents of the routing table (Partial updates). This feature reduces the bandwidth required for EIGRP packets and also reduces CPU processing.
- It can exchange routes for IPv4, IPv6, AppleTalk and IPX/SPX networks.
- Supports unequal load balancing, which allows administrators to better distribute traffic flow in their networks.

B. EIGRP Packets

A different message type in EIGRP includes;

- ***Hello packet***

EIGRP hello packets are sent out every 5 seconds by default to maintain and discover neighbour relationships. On slower (T1 and below) and NBMA links, hellos are sent every 60 seconds to preserve bandwidth [5]. When a router receives a hello packet from another router with the same AS number, it automatically forms a neighbour relationship (also known as an adjacency).

- ***Update packet***

During the EIGRP start up process on a router, an update message is sent for its neighbours containing the contents of the router's routing table [7]. The only other time an update packet is sent is when network changes occur on a router and it then sends out an update message to its neighbours who the route change would affect.

- ***Acknowledgement***

Acknowledgement packets are received in response to update, query, or reply packets.

- ***Query***

When EIGRP loses its route, it sends out a query message to all of its neighbours asking if they know a path.

- ***Reply***

When a router responds to other router for a route (query), it sends it in the form of a reply.

C. EIGRP advantages and disadvantages

Speedy network convergence, low CPU utilization, and easy configuration are some advantages of EIGRP. The EIGRP router stores everything as routing table information so they can quickly adapt to alternate routes. The different length subnet mask decreases time to network convergence and increases scalability. EIGRP provides MD5 route authentication. Compared to RIP and OSPF, EIGRP have more adaptability and versatility in complex networks [8]. EIGRP combines many features of both link-state and distance-vector. Since EIGRP is mostly implemented in large networks, routers make delay of sending information during allotted time, which causes neighbouring routers to request the information again, thus increases the traffic.

V. CONCLUSION

This paper describes the different Interior gateway protocols that are used for communication among the network devices within a single administrative system. EIGRP protocol provides faster convergence, followed by OSPF. The worst convergence case is RIPv1. So, EIGRP protocol should be used when a critical network is being administered because the network becomes stable, fastest and the paths to the IP networks are found fastest when the network changes.

REFERENCES

[1] Vishal Sharma, Rajneesh Narula and Sameer Khullar "Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols" International Journal of Computer Applications(0975-8887) Volume 44-No13, April 2012.

[2] R.Rastogi, Y.Breitbart and M.Garofalakis, "Optimal configuration of ospf aggregates", IEEE/ACM transaction on networking , vol 11, April 2003.

[3] Cisco systems (2012), Enhanced Interior Gateway Routing Protocol (EIGRP) wide metrics, retrieved 14 March 2014.

[4] Ittiphon Krinpayorm and Suwat Pattaramalai, "Link recovery Comparison between OSPF & EIGRP", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT Vol. 27 (2012) IACSIT Press, Singapore.

[5] Ioan Fitigau, Gavril Toderean, " Network performance Evaluation of RIP, OSPF & EIGRP Routing protocols", IEEE, 2013.

[6] Pankaj Rakheja, Prabhjot kaur, Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network, International Journal of Computer Application, 2012.

[7] Dejan Spasov , Marjan Gushev, "On the Convergence of Distance Routing Protocols", ICT 2012.

[8] Poprzen, Nemanja, "Scaling and Convergence speed of EIGRPv4 and OSPFv2 dynamic routing protocols in hub and spoke network" IEEE 2009.

[9] Savage, Slice " Enhanced Interior Gateway Routing Protocol" Internet Engineering Task Force, 2013.

[10] Chandra Wijaya "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network", First International Conference on Informatics and Computational Intelligence, 2011.

