Analysis of Routing Protocol RIP, EIGRP, OSPF and BGP

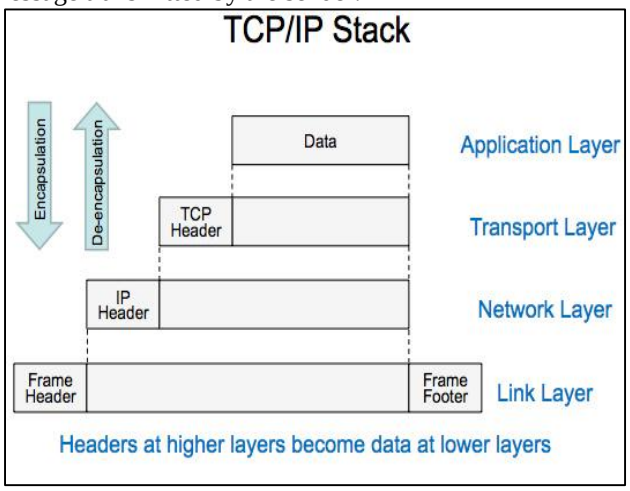
Keshav[1] Aryan Seth[2]
[1,2]Department of Computer Science and Engineering
[1,2]ABES Institute of Technology, Ghaziabad, Uttar Pradesh, India

Abstract— In a network topology packets are forwarded using various routing protocols. Routers have to maintain a routing table for a guaranteed delivery of the packets from a source device to the desired destined node. The amount of information stored about a network depends on the algorithm a router follows. Most of the Routing protocols that are widely used are RIP, OSPF, IGRP and EIGRP. In the connectivity of the networks, routing protocols performs a vital role and also determines how the communication is done between various network devices to forward the packets.

Keywords: Routing Protocols, Interior Gateway Protocol, Neighbour, Internet Service Provider, Border Gateway Protocol

I. INTRODUCTION

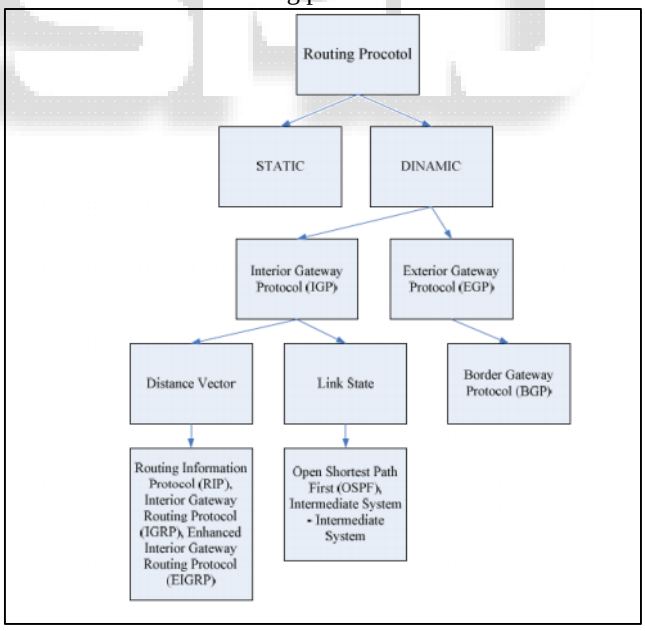
The internet works on the TCP/IP suite or the Internet protocol suite which helps in the communication for the networks and access the internet. TCP/IP provides end to end connectivity and also specifies how data should be formatted, addressed, transmitted, routed and received at the destination. TCP/IP model consists of four abstraction layers namely network access layer, internet layer, transport layer and application layer. Each layer has its own functions. The Link Layer contains communication technologies for a local network; Internet Layer connects local networks and establishes internetwork communication; Transport layer handles host to host communication and Application layer contains protocols specific for data communication services on various levels. Encapsulation of data that is enclosing of a set of data (code) into another set of code to protect its integrity when transferring it between non-compatible systems, or to secure it from unauthorized access during transmission. The figure below shows data encapsulation; it shows how the data is encapsulated from application layer to network access layer via transport and internet layers. At each layer a set of header and footer are added and at the receiver side it is unwrapped. The header and footer are removed right from link layer first to application layer to get the data or message transmitted by the sender.



The routing protocols which are used for the internetworking, function under the layer 3 or the internet layer of the TCP/IP suite. These routing protocols are enabled on a router which is a device that forwards data packets between computer networks. It is connected to two or more devices or different networks. When a data packet is forwarded in a network, the router reads the IP address information in the packet to determine its desired destination. Then, using information in its routing table or routing policy, it directs or forwards the packet to the next device or network on its journey. It is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. These routing tables contain information about the topology of the network. The primary goal of routing protocols is to construct a routing table for the router.

The routing can be classified into two categories namely static routing and dynamic routing. Static routing is used to manually configure a router. Changes in a network will affect the routing table of the router so every time there is a change the router has to be updated manually. Whereas in the case of dynamic routing, routing table is automatically configured.

The classification of routing protocols:



Dynamic Routing Protocols are divided into two categories: IGP and EGP. Interior Gateway Protocol (IGP) is used for the routers in same domain network such as Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Intermediate System – Intermediate System (ISIS). And for the routers in different domain network, Exterior Gateway Protocol (EGP) is used such as Border Gateway Protocol (BGP). For the router in the same domain network, dynamic routing protocols that can be used on computer networks are further

divided into three categories, namely distance vector, link-state and hybrid routing protocols. These types of routing protocols have their own advantages and disadvantages. For the distance vector type, RIP (Routing Information Protocol) will be used. For the link-state type, OSPF (Open Shortest Path First) will be used. And for the hybrid type EIGRP (Enhanced Interior Gateway Routing Protocol) will be used. These dynamic routing protocols can be used in both IPv4 and IPv6 networks.

II. ROUTING PROTOCOLS

A. RIP

The Routing Information Protocol (RIP) is a dynamic routing protocol it uses UDP port 520 for transmission of message.
The Routing Information Protocol (RIP) is one of the most often used interior gateway protocol (IGP) routing protocols on internetworks (and to a lesser extent, networks connected to the Internet), which enables routers to adapt in different type of networks dynamically by communicating information about changes in the network how each router can reach a network and how far the network is from the source with the best path to follow

The Routing Information Protocol, also known as RIP, is one of the most lasted routing protocols of all. RIP is easy to configure and demand very fewer resources as compared to other routing protocols. Its popular beacause of its simplicity to configure and a long-lasting history. RIP emerged from research that dates back to 1957.

For Request for Comments check out (RFC) 1058 and 1723. RFC 1058 (1988) is based on the first implementation of RIP, while RFC 1723 (1994) is an updated RFC1058. RFC 1058 allows RIP messages to send out more information and give additional security options.

RIPv1 does not Variable Length Subnet Mask. It cannot operate classless routing. RIP v1 advertises all networks it knows as classful networks, so it is not possible to subnet a network by VLSM if you are using RIP v1, It must be noted that RIP is the only routing protocol that is supported by all network devices and softwares, so in a complex environment, RIP may be your only option for dynamic routing.

B. RIP Updates

Routing Information Protocol sends routing-update messages after every fixed interval of time and when there is a change in the network topology. Then an update message is rolled out to inform all the other routers in the network, then all the routers update its routing table to according to the new path. The metric value is the increase for every next hop it is increased by one and its sender indicates as next hop. Routing Information Protocol routers only maintain

The best route to reach a destined node it select the best path using the hop count as metric. After updating its routing table, the router starts sending out the in the network so that other routers in the can also make changes according to the changes in the network.

C. RIP Problems

RIP is a routing protocol with slow convergence time and computes best path using number of hops. Router configured to use RIP, sends updates to its neighbours every thirty seconds. If any change happen in the network, which is very much common in network devices, then every time route updates are used to reconfigure it, changes happen for unimaginable period of time. In worst case scenario each and every router waits for about thirty seconds to send out an update to the next hop in a network. Network failures are common make things even difficult for dynamic routing protocols. Router considers link as down if it doesn't receive any updates from neighbor for 180 seconds. Then RIP uses loop avoidance techniques to advertise to its neighbor the down route. For the end node it is like network is down/unreachable. Critical networks cannot tolerate such delays. Additionally, RIP calculates best route using hop count and the no of hop is also fixed to 16 because of loop avoidance there is no parameter to calculate the best path using link bandwidth or using link delays which play an important factor in case of transmission of data.

D. RIPv2

Routing Information Protocol version 2 (RIPv2), was a common LAN routing protocol in the '90s, but is rapidly fading away in production networks. RIPv2 suffered from scalability issues due to a relatively low maximum hop count of 15 routing devices. Compared to more modern dynamic routing protocols, RIPv2's methods for selecting optimal routes and the substantial convergence time it takes to recalculate paths renders it nearly obsolete. Today, the only reason you might run across a network running RIPv2 is either that the network is very old and in serious need of an upgrade or the network is running cheaper, consumer-grade routing hardware that can only support RIP.

III. ENHANCED INTERIOR ROUTING PROTOCOL

Enhanced Interior Gateway Routing Protocol (EIGRP) or Enhanced IGRP is a Cisco proprietary routing protocol. EIGRP works on Diffusing Update Algorithm (DUAL). EIGRP is a hybrid protocol as it integrates features of a Distance Vector routing protocol and features of a Link State routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of IGRP. EIGRP is used as an interior gateway protocol (IGP) but can also been used broadly as an exterior gateway protocol for inter-domain routing. Key capabilities that distinguish Enhanced IGRP (EIGRP) from other routing protocols include fast convergence, support for variable length subnet mask, support for partial updates, and support for multiple network layer protocols. A router running EIGRP stores all its neighbours' routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbours to discover an alternate route. These queries generate until an alternate route is found. EIGRP supports VLSM i.e., variable-length subnet masks therefore it permits routes to be automatically summarized on a network number boundary. EIGRP can also be configured to summarize at any interface on any bit boundary.

Like RIPv2, Enhanced Interior Gateway Routing Protocol (EIGRP) is a hybrid distance vector protocol. But in terms of scalability and convergence times, EIGRP blows RIPv2 out of the water. EIGRP is a popular choice for routing

within campus networks both big and small. Many network engineers believe that EIGRP is the best choice for a routing protocol on private networks because it offers the best balance between speed, scalability and ease of management. One drawback with EIGRP is that for a long time, it was a Cisco proprietary routing protocol that only ran on Cisco hardware and software. That limited deployment to networks that only ran Cisco gear. In 2013, Cisco opened EIGRP up as an IETF draft and some vendors have adopted EIGRP and offer it on their routers, switches, and associated gear. Regardless, you still need to be careful that every piece of equipment on your network that you want to run EIGRP on supports the protocol. Even Cisco's own Meraki line of layer 3 switches and security appliances offer no support for EIGRP. So this may be yet another once-popular routing protocol that will end up fading away.

IV. WORKING

In EIGRP router maintains a Neighbour Table in which router keeps state information about adjacent neighbours. When a new device or a network is discovered, neighbours are learned, i.e., the address and interface of the neighbour is recorded. This information is stored in the neighbour table. The neighbour table holds these entries. When a neighbour sends a hello, it advertises a HoldTime. The HoldTime is the amount of time a router treats a neighbour as reachable and operational. The HoldTime expires if a hello packet isn't heard within that time. When the HoldTime expires, DUAL is informed of the topology change.

The neighbour table entry also includes information required by the reliable transport mechanism. Data packets are sent with sequence numbers so as to match the acknowledgments. The last sequence number received from the neighbour is recorded so out of order packets can be detected. A transmission list is used to queue packets for possible retransmission on a per neighbour basis. Round trip timers are kept in the neighbour table to estimate an optimal retransmission interval. The topology table is occupied by the protocol dependent modules and acted upon by the DUAL finite state machine. All destinations advertised by neighbouring routers are in the topology table. Each entry in the table is associated with the destination address and with a list of neighbours that have advertised the destination. The advertised metric is recorded for each neighbour. This metric is stored in the routing table by the neighbours. If the neighbour is advertising this destination, it must be using the route to forward packets. This is one of the important rule that must be followed by distance vector protocols. A router uses metric to reach the destination. It is the sum of the best advertised metric from all neighbours and the link cost to the best neighbour. The router uses this metric in the routing table to advertise to other routers. When there is a feasible successor, the destination entry is moved from the topology table to the routing table. The neighbours that have an advertised metric less than the current routing table metric are considered feasible successors. Feasible successors are viewed by a router as neighbours that are downstream with respect to the destination. These neighbours and the associated metrics are placed in the forwarding table. When a metric or a topology change occurs in the network, the set of feasible successors may have to be re-evaluated. However, this should not categorized as a route re-computation. When a feasible successor goes down, all routes through that neighbour commence a route re-computation and enter the active state.

A. OSPF

The OSPF (Open Shortest Path First) protocol is an Interior Gateway Protocol (IGP). It is used to distribute IP routing information throughout a single or within the same Autonomous System (AS) in an IP network.

The OSPF protocol is a link-state routing protocol. Information in the topology of a router are shared with their nearest neighbours. The topology information is flooded throughout the AS. Therefore, every router within the AS has a complete picture of the topology of the AS. With the use of a variant of the Dijkstra algorithm end-to-end paths through the AS is calculated. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the desired destination.

The main advantage of a link state routing protocol like OSPF is that it allows routers to calculate routes that satisfy particular criteria and have the complete knowledge of topology. This can be applicable for traffic engineering goals, where routes can be compelled to meet particular quality of service requirements. One of the main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. The size and frequency of the topology updates increases on increasing the number of routers, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link state routing protocol is inappropriate for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS.

Information in each OSPF router is distributed about its local state (usable interfaces and reachable neighbours, and the cost of using each interface) to other routers using a Link State Advertisement (LSA) message. The received messages are used by each router to build up an identical database that describes the topology of the AS.

The main alternative to EIGRP for most campus LAN routing deployments is the Open Shortest Path First (OSPF) dynamic routing protocol. Unlike EIGRP, OSPF was always an open standard protocol and is an available option on virtually any modern enterprise network hardware made in the past two decades. While some say that OSPF is a bit more complicated to set up and manage compared to EIGRP, it's relatively easy to run once you get the hang of things such as autonomous system routing domains. Odds are that unless a network is very small, old or primarily Cisco, the dynamic routing protocol in use on the LAN will be OSPF.

B. BGP

The dynamic routing protocol that is the most different from all the others is the Border Gateway Protocol (BGP). RIP, EIGRP and OSPF are all interior gateway protocols (IGP) while BGP is an exterior gateway protocol (EGP). Basically, interior protocols are meant to dynamically route data across a network that you fully control and maintain. Exterior routing protocols are used to exchange routes between

distinctly separate networks that you have no administrative control over. BGP is the routing protocol used on the internet; therefore, the most common enterprise use is to run BGP on your internet edge when connecting to your ISP.

Now, why use a dynamic routing protocol such as BGP for routing to the Internet as opposed to simply creating a static default route? The reason would be if you have multiple internet connections to multiple providers and want to provide automatic failover and load balancing capabilities. That means you have multiple paths or choices on which ISP is the best path in and out for specific destinations on the internet. BGP can be used to either dynamically fail over from one ISP link to another when the primary connection fails. BGP also can be configured to learn either full or partial routing tables to make better routing decisions based on the optimal outbound internet path to the destination router.

An AS can be an Internet Service Provider, a university or an entire corporate network, including multiple locations (IP addresses). Each AS is represented by a unique number called an ASN.

In this type of network architecture, each autonomous system controls a collection of connected routing prefixes, representing a range of IP addresses. It then determines the routing policy inside the network.

As the number of autonomous systems in the internet grew, the drawbacks of EGP became more pronounced. Its hierarchical structure hampered scalability and made it difficult to connect new networks in an efficient manner. Consequently, it was necessary to define a new exterior routing protocol that would provide enhanced and more scalable capabilities.

In June 1989, the first version of this new routing protocol, known as the Border Gateway Protocol, was formalized.

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

The main purpose of BGP is to exchange routing updates like other routing protocols, but BGP typically does not exchange individual network routes (but it technically can), it exchanges summaries of network routes. This is because the typical use of BGP is over very large networks including the Internet.

Without BGP the Internet as we know it would be quite a bit more inefficient. As it is today the Internet BGP routing tables have over 300,000 active forwarding entries and this is with summarization of over 2 billion addresses. Imagine what these tables would be like without summarization.

What makes eBGP configuration obvious from iBGP configuration is that the AS-number which is used in the neighbor command is different than the AS-number configured with the router bgp command.

It must also be known that with eBGP by default there is a direct connection requirement which is enforced by an advertised TTL of 1. Now when configuring BGP using loopback interfaces this can become an issue as the packet actually takes two hops from the remote device to the physical interface and from the physical interface to the loopback interface.

iBGP configuration is very similar to eBGP configuration but requires a little understanding of iBGP requirements. By default, iBGP requires that all iBGP devices being used are fully meshed (although there are ways of getting around this). This does not however mean that a direct connection is required but that each iBGP peer must neighbor with each other iBGP router.

V. Conclusion

All dynamic routing protocols serve a single purpose: 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. That said, not all dynamic routing protocols are alike.

As you can see, routing protocols have their own pros and cons and situations where they work best. Because of this, many organizations run multiple routing protocols on the same network and use route redistribution techniques. So, in the end it all comes down to the usage of the user and decide accordingly what fits best for him.

References

[1] Chandra Wijaya "Performance Analysis of Dynamic Routing Protocol EIGRP and OSPF in IPv4 and IPv6 Network", 2011 First International Conference on Informatics and Computational Intelligence.
[2] Sheela Ganesh Thorenoor"Dynamic Routing Protocol Implementation Decision Between EIGRP, OSPF And RIP Based On Technical Background Using OPNET Modeler",
[3] Yao Zhao, Jian Liang Yan, Hua Zou"Study On Network Topology Discovery in IP Network", Proceedings of IC-BNMT2010.
[4] IoanFitigau, Gavril Toderean"Network Performance Evaluation for RIP, OSPF and EIGRP Routing Protocols", IEEE, 2013
[5] Pankaj Rakheja, Prabhjot kaur, Anjali gupta, Aditi Sharma "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network" International Journal of Computer Applications, June 2012.
[6] V.Vetriselvan, Pravin R.Patil, M.Mahendran, Survey on the RIP, OSPF, EIGRP Routing Protocols, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1058-1065.
[7] Guang Yang, "Introduction to TCP/IP Network Attacks" white paper available at seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf

