IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 50-53

Survey of Network Routing Protocols

Ditixa Vyas[1]

[1](*Assistant Professor, Computer, Atharva College of Engineering/Mumbai University, India)*

Abstract: *The purpose of routing protocols is to learn of available routes that exist on the enterprise network, build routing tables and make routing decisions. Some of the most common routing protocols include RIP, IGRP, EIGRP, OSPF, IS-IS and BGP. There are two primary routing protocol types although many different routing protocols defined with those two types. Link state and distance vector protocols comprise the primary types.* ***Distance vector protocols*** *advertise their routing table to all directly connected neighbors at regular frequent intervals using a lot of bandwidth and are slow to converge.* ***Link state protocols*** *advertise routing updates only when they occur which uses bandwidth more effectively. This paper describes various Routing protocols in brief and at the ebnd of the paper the protocols are compared with different factors.*

I. Introduction

Hundreds of different network protocols have been created for supporting communication between computers and other types of electronic devices. So-called routing protocols are the family of network protocols that enable computer routers to communicate with each other and in turn to intelligently forward traffic between their respective networks. The protocols described below each enable this critical function of routers and computer networking.

How Routing Protocols Work

Every network routing protocol performs three basic functions:

1. discovery – identify other routers on the network
2. route management – keep track of all the possible destinations (for network messages) along with some data describing the pathway of each
3. path determination – make dynamic decisions for where to send each network message

A few routing protocols enable a router to build and track a full map of all network links in a region while others (called distance vector protocols) allow routers to work with less information about the network area.

The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors.

The chief advantage of dynamic routing over static routing is scalability and adaptability [1]. A dynamically routed network can grow more quickly and larger, and is able to adapt to changes in the network topology brought about by this growth or by the failure of one or more network components. With a dynamic routing protocol, routers learn about the network topology by communicating with other routers. Each router announces its presence, and the routes it has available, to the other routers on the network. Therefore, if a new router or an additional segment is added to an existing router, the other routers will learn about the addition and adjust their routing tables accordingly. The ability to learn about changes to the network's configuration has implications beyond adding new segments or moving old ones [2]. It also means that the network can adjust to failures. If a network has redundant paths, then a partial network failure appears to the routers as if some segments got moved and some segments have been removed from the network. In short, there's no real difference between a network failure and a configuration change. Dynamic routing allows the network to continue functioning, in a degraded fashion, when a partial failure occurs. The terms distance vector and link state are used to group routing protocols based on whether the routing protocol selects the best routing path based on a distance metric and an interface, or selects the best routing path by calculating the state of each link in a path and finding the path that has the lowest total metric to reach the destination . Distance vector protocols use a distance calculation plus an outgoing network interface to choose the best path to a destination network. Routers that use distance vector routing share information or a routing map with other routers on the network. When a change in the network occurs, the router with the change propagates the new routing information to all neighboring routers. Each recipient on this information adds a distance vector to the routing table before it forwards it on to its neighbors. Link State protocols track the status and connection type of each link and produces a calculated metric based on these and other factors, including some set by the network administrator.

In link state routing the best route for data is calculated based on cost and once the network is converged, protocol traffic is limited to changes in specific links.

II. Routing Information Protocol (RIP)

RIP version1 is a DV protocol that is easy to comprehend and deploy within an AS. Although superseded by more complex routing algorithms, RIP is still widely in smaller Ass thanks to its simplicity. RIP makes no formal distinction between networks and hosts. Routers typically provide a gateway for datagram to leave one network or AS and to be forwarded onward to another network. Routers therefore, have to make decisions if there is a choice of forwarding path on offer. The metric system RIP networks use is the hop count, which has a maximum value of 15. Every time a router passes the routing table to other routers a value of 1 is added to the metric inside the routing update. The maximum number of hop count is to solve the routing loops problem. Routing loops are basically confusions in a network topology that occur when the update/age out timers can be inefficient. With the hop count set to 15 the packet can be passed through a maximum of 15 routers before being discarded, without which the packets can be passed indefinitely until either the network crashes or the routers are switched off. RIP supports up to a maximum of 6 equal-cost path to a destination, this means that is a destination is reachable over different routes that have the same amount of hops, the router will hold all routes in memory up to a maximum of six (four is the default). The paths are all placed into the routers table and can be used to load balance when sending data. The main features of RIP can also lead to its disadvantages, such as information flooding, ineffectiveness of metrics system, and classful routing algorithm, explanations of which follow.

Firstly, routing information is passed to other routers in a RIP network by using a local broadcast. This broadcast is by default every 30 seconds and is held for a maximum of 180 seconds. The broadcast update contains the routers entire routing table; this is passed every 30 seconds among routers. These activities cause a fairly large amount of network traffic to be periodically sent throughout the network. This type of information flooding wastes network resources and cause network inefficiency and potential congestion problem.

Secondly, the metric system that RIP uses is to find the shortest paths through a network for the data delivery. The task is carried out merely based on the hop count measurements regardless the other aspects of the networks such as bandwidth, etc. This behavior cannot guarantee the discovery of the optimal route for the data packets.

Thirdly, RIP comes under the heading of classful routing protocol; meaning only one subnet mask for any class of subnet can be used for the routers, which in effect can be wasteful of IP addresses. For instance, if 192.168.1.0 is assigned to accommodate 6 subnets, subnet mask 255.255.255.224 should be used, which prevents the use of the default mask of 255.255.255.0, otherwise, the router will return errors in the configuration file, e.g. duplicate IP Address. Non-meticulous subnet mask formality can cause loss of router configuration information which provokes unstable network performance.

III. Interior Gateway Routing Protocol (IGRP)

The Interior Gateway Routing Protocol (IGRP) is a routing protocol to provide routing within an autonomous system (AS). Distance-vector routing protocols calls for each router to send all or a portion of its routing table in a routing update message at regular intervals to each of its neighboring routers. As routing information proliferates through the network, routers can calculate distances to all nodes within the internetwork. IGRP adheres to the following Distance-Vector characteristics: sends out periodic routing updates (every 90 seconds); sends out the full routing table every periodic update; uses a form of distance as its metric; uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination; supports only IP routing; utilizes IP protocol 9; routes have an administrative distance of 100; by default, supports a maximum of 100 hops. This value can be adjusted to a maximum of 255 hops; is a classful routing protocol; uses Bandwidth and Delay of the Line, by default, to calculate its distance metric. Reliability, Load, and MTU are optional attributes that can be used to calculate the distance metric; requires that you include an Autonomous System (AS) number in its configuration. Only routers in the same Autonomous system will send updates between each other [5].

IV. Exterior Gateway Protocol (EGP)

The Exterior Gateway Protocol (EGP) is a now obsolete routing protocol for the Internet originally specified in 1982 by Eric C. Rosen of Bolt, Beranek and Newman, and David L. Mills. It was first described in RFC 827 and formally specified in RFC 904 (1984). Not to be confused with exterior gateway protocols in general (of which EGP and Border Gateway Protocol (BGP) are examples), EGP is a simple reach ability protocol, and, unlike modern distance-vector and path-vector protocols, it is limited to tree-like topologies.

To get from place to place outside your network(s), i.e. on the Internet, you must use an Exterior Gateway Protocol. Exterior Gateway Protocols handle routing outside an Autonomous System and get you from your network, through your Internet provider's network and onto any other network. BGP is used by companies with more than one Internet provider to allow them to have redundancy and load balancing of their data transported to and from the Internet [6].

V. Open Shortest Path First (OSPF)

OSPF is based on open standards and has good compatibility on a wider range of equipment, which is a prevalent routing protocol in larger enterprise networks. It is a LS routing protocol which uses more complex metric system to give efficient pathways discovery solutions to remote networks. The cost to measure the metric is worked out by taking the inverse of the bandwidth of links. Essentially a faster link is lower in cost. The lowest cost paths to remote networks are the most preferred routes, and held in the routing table. OSPF can load balance across a maximum of six equal-cost path links, although doing this can cause difficulties. The serial interface of the router is configured with a clock rate and a bandwidth. The clock rate is the speed data can be sent across a link, and the bandwidth is used by the routing protocol in the metric calculations. By default the speed of a serial interface is set to 1544 Kbps . There is a potential hazard of this system. When different clock rates are set on a different link, the bandwidth has to be accordingly configured; otherwise OSPF will regard both connections as the same speed, which will cause problem with load balancing. When routers need to run OSPF frequently, lots of resources are dedicated to the process; this potential problem can dramatically slow down the network service speed [4].

VI. Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a Cisco proprietary distance-vector routing protocol based on its original IGRP. Unlike traditional distance-vector protocols such as RIP and IGRP, EIGRP does not rely on periodic updates: routing updates are sent only when there is a change in the network. EIGRP relies on small hello messages to establish neighbor relationships and to detect the loss of a neighbor. The rest of the messages, that is, the routing information and the disconnection queries and results, have a sequence number and must be acknowledged. Each router that implements EIGRP uses three tables to keep the information about the net: the neighbors table stores information about the adjacent routers, namely the cost to reach them, the time that we can wait for their hello messages, a queue of messages waiting for acknowledgment, and the sequence numbers for sending and receiving messages; the topology table contains, for each known destination, information about all the possible next routers to be followed to reach the destination together with the total cost of that concrete route, and the state of that information (active if it is being calculated and passive when it has been computed); and the routing table points for each destination the best next router that has to be followed in order to reach that destination.

As we have said above, routers implementing EIGRP send small hello messages periodically. When a router receives this message, it sets a timer to expire after a certain time interval, and each time the next hello is received, the timer is reset. Thus, a link is discovered when the first hello message from a new router is received. In this case, the routers interchange their routing tables and update all their tables accordingly; the changes are communicated to the neighbors by using the Diffusing Update Algorithm (DUAL). When the timer of hello messages expires, the link is declared down and DUAL is also used [3].

VII. Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is a routing protocol used on the edge of autonomous systems (AS). It is an routing protocol and calculates loop-free paths across the Internet. It is considered to use a path-vector routing algorithm. This means it tracks the path in terms of which AS it passes through, and does NOT track the 'route' through individual routers within an AS, and is not specifically capable of performing load balancing or packet forwarding itself. BGP is the routing protocol of choice and is used by all the Network Service Providers (NSPs) such as UUNet, Sprint, Cable & Wireless, Level3, Qwest etc. It is dynamic and handles outages and link failures fairly gracefully. To use BGP, you must have a router that supports BGP; register an AS Number and contact your provider to set up a BGP session. See the requirements page for more information.

BGP has gone through three revisions. The current version in use is BGP4 and is supported by most router manufacturers including Cisco, Lucent/Bay, Juniper and many others, as well as by Unix and Linux programs such as Zebra.

BGP uses a TCP connection to send routing updates using TCP port 179. BGP is therefore by definition a 'reliable' protocol. While BGP version 3 provides for the dynamic learning of routes, BGP 4 adds additional route dampening functionality, communities, MD5 and multicasting capability [7].

VIII. Comparison of Various Alcohols Sensing System

Table 1. Comparison of Routing Protocols [8]

	RIP	**OSPF**	**EIGRP**	**IGRP**	**EGP**	**BGP**
Nature	DV	LS	Hybrid	DV	Path Vector	Path Vector
Matrix	Number of hops	The inverse of the bandwidth of links	Available bandwidth, delay, load, MTU and the link reliability	Bandwidth	bandwidth, delay, load	Multiple Attribute
Convergence	Slow	Fast	Very Fast	Slow	Average	Average
Algorithm	Bellman-Ford	Dijkstra	DUAL	Bellman-Ford	Best Path Algorithm	Best Path Algorithm
Protocol	UDP	IP	IP	IP	TCP	TCP

IX. Conclusion

This paper compares the protocols based on various factors and as expected, RIP carries out low-efficient routing in the network with a bottleneck transmission link as it does not take bandwidth into consideration. In contrast, RIP and EIGRP perform with excellence as they are devoted to computing the fastest possible route. Results show that with the same network specifications it is likely that EIGRP and OSPF have chosen the same route for the VoIP application. The link failure has affected the performance of both EIGRP and OSPF. During the deliberate link failure and auto recovery process, OSPF acts consistently throughout the procedure, while EIGRP is seriously disrupted during the failure but restores to the original state after the failure recovery. OSPF updates the routing table upon network failure to re-calculate a new route, and does not alter the route for any existing traffic stream as long as there are no congestions or other new problems in its chosen route. Network based on OSPF maintains acceptable performance throughout the process, which indicates its flexibility and efficiency**.**

References

[1]. http://oreilly.com/

[2]. http://www.freesoft.org

[3]. Implementing and analyzing in Maude the Enhanced Interior Gateway Routing Protocol, Riesco A Verdejo A Electronic Notes in Theoretical Computer Science 2009

[4]. VoIP performance over different interior gateway protocols, Che X Cobley L, International Journal of Communication Networks and Information Security, 2009

[5]. Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network, Rakheja P, kaur P, gupta A, Sharma, A International Journal of Computer Applications, 2012

[6]. https://www.inetdaemon.com/tutorials/internet/ip/routing/interior_vs_exterior.shtml.

[7]. https://www.inetdaemon.com/tutorials/internet/ip/routing/bgp/whatis.shtml

[8]. Comparison of RIP, EIGRP, OSPF, IGRP Routing Protocols in Wireless Local Area Network (WLAN) by using PNET Simulator tool-A Practical Approach, Kalamani P, Venkatesh Kumar, M Chithambarathanu, M Thomas, R Lecturer, S vol: 16 (4) pp: 57-64