IMPLEMENTING OSPF PROTOCOL IN CISCO 2800 SERIES ROUTER

P. Ramya

Assistant Professor
SNS College of Engineering, Coimbatore

Gowtham.N, Sri Guruprassad.N, Suresh Kumar.S, Vinoth.K,
Vishnu Vinod
Student, Final Year ECE
SNS College Of Engineering, Coimbatore

Abstract-   The Routing Information Protocol is a Distance vector protocol, which employs the hop count as a routing metric. RIP 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 RIP is 15. Originally each RIP router transmits full updates every 30 seconds. As the network grew in size, however, it became evident there could be a massive time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability is poor compared to EIRGP and OSPF, Because RIP based on Distance vector routing protocol, But OSPF based on Link State Routing Protocol. So we are using the OSPF protocol in CISCO 2800 series Router to overcome the above mentioned problem.

Key-words: - RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Protocol), interior gateway protocol (IGP)

I.   INTRODUCTION

A Routing Protocol is a protocol that specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. While routing, the choice of the route being done by routing algorithms. Each router has a priori knowledge about networks attached to it directly.
A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. The term Routing Protocol refers specifically to one of the operating layers of the OSI model, which similarly disseminates topology information between routers.
The specific characteristics [33] of routing protocols include:

- Routing path
- Hop count
- Convergence time
- Scale up factor

1.1 OSI REFERENCE MODEL
A protocol is a set of rules that governs the communications between computers on a network.
These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer [14]. A protocol may have a formal description. Protocols may include signaling, authentication and error detection and correction capabilities. A protocol definition defines the syntax, semantics, and synchronization of communication; the specified behavior is typically independent of how it is to be implemented. A protocol can therefore be implemented as hardware or software or both.
One of the greatest functions of the OSI specification is to assist in data transfer between disparate hosts, that they can enable us to transfer data between a UNIX host and a PC or a MAC.
OSI has seven layers, divided into two groups namely, Host group and Media group. The host group explains how data is transmitted end to end and the Media group explains how the applications within the end station will communicate with each other and with users. These groups are further divided into layers as shown below:

- Host Layer:
    - Physical layer
    - Data link layer
    - Network layer
    - Transport layer

- Media Layer:
    - Session layer
    - Presentation layer
    - Application layer

II. ROUTING INFORMATION PROTOCOL

Distance vector Routing protocols uses frequent broadcasts (255.255.255.255 or FF.FF.FF.FF) of their entire routing table every 30 Sec, on all their interfaces in order to communicate with their neighbors. The bigger the routing tables, the more broadcasts. This methodology limits significantly the size of the network on which distance Vector can be used.

Routing Information Protocol and Interior Gateway Routing Protocol (IGRP) are two very popular distance Vector routing protocols. You can find links to more information on these protocols at the bottom of the page.

Distance Vector routing protocols view networks in terms of adjacent routers and hop counts, which also happens to be the metric used. The "hop" count (max of 15 for RIP, 16 is deemed unreachable and 255 for IGMP), will increase by one every time the packet transits through a router. So the router makes decisions about the way a packet will travel, based on the amount of hops it takes to reach the destination and if it had 2 different ways to get there, it will simply send it via the shortest path, regardless of the connection speed. This is known as pinhole congestion.

2.1 MAXIMUM HOP COUNT

The routing loop that must be noticed at is called "counting to infinity" and it is caused by gossip and wrong information being communicated between the routers. Without something to protect against this type of loop, the hop count will keep on increasing each time the packet goes through a router! One way of solving this problem is to define a maximum hop count. Distance Vector (RIP) permits. The hop count of up to 15, so anything that needs 16 hops is unreachable. So, if a loop occurred, it would go around the network until the packet reached a hop count of 15 and the next router would simply discard the packet.

2.2 SPLIT HORIZON

Works on the principle that it's never useful to send information about a router back to the destination from which the original packet came. As explained in the earlier subsection, it would have prevented Router A from sending the updated information it received from router B back to Router B.

2.3 HOLD-DOWN TIMERS

Routers keep an entry for the network-down state, allowing time for other routers to be recomputed for this topology change, this way, allowing time for either the downed router to come back or the network to stabilize somewhat before changing to the next base router.

When a router receives an update from a neighbor indicating that a previously accessible network is not working and is inaccessible, the hold-down timer will start. If a new update arrives from a neighbor with a better metric than the original network entry, the hold-down is removed and date is passed. But an update is received from a neighbor router before the hold-down timer expires and it has a lower metric than the previous route, therefore the update is ignored and the hold-down timer keeps ticking. This allows more time for the network to converge.

There are three instances when triggered updates will reset the hold-down timer:
- The hold-down timer expires
- The router receives a processing task proportional to the number of links in the internetwork.
- Another update is received indicating the network status has changed.

2.4 ROUTING INFORMATION PROTOCOL

Routing Information Protocol is a true Distance Vector Routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable. RIP works well in small networks, but it is inefficient on large networks with slow WAN links or on networks with large number of routers installed.

The basic concepts about the RIP virtual diagram is shown in Fig 2.1. RIP comes in two different versions. RIP uses only Classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP does not include the subnet mask when it sends updates. RIP uses broadcasts (255.255.255.255). The disadvantages of RIP are:

- More utilization of Bandwidth
- Work with only 15 hop count
- Slow Convergence
- Formation of Routing loop
- Classful routing is followed
- Maximum router can be connected is 16
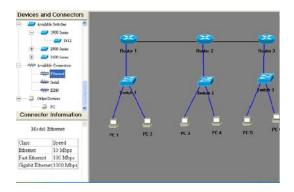- Load balancing is of 4 paths

Fig 2.1 RIP Virtual Diagram

2.5 OSPF PROTOCOL

Link State protocols, unlike Distance Vector broadcasts, use multicast. Multicast is a "broadcast" to a group of hosts, in this case routers. Let us assume there are 10 routers of which 4 were part of a "multicast group" then, when sending out a multicast packet to this group, only these routers will receive the updates, while the rest of them will simply ignore the data. The multicast address is usually 224.0.0.5 & 224.0.0.6, this address is defined by the IGRP (Interior Gateway Protocol).

Link State routing protocols do not view networks in terms of adjacent routers sand hop counts, but they build a comprehensive view of the overall network which fully describes the all possible routes along with their costs. Using the SPF (Shortest Path First) algorithm, the router creates a "topological database" which is a hierarchy reflecting the network routers it knows about. It then puts its self on the top of this hierarchy, and has a complete picture from its own perspective.

When a router using a Link State protocol, such an OSPF (Open Shortest Path First) knows about a change in the network, it will multicast this change instantly, there for flooding the network with this information. The information routers require to build their databases is provided in the form of Link State advertisement packets (LSAP). Routers do not advertise their entire routing tables; instead each router advertises only its information regarding immediately adjacent routers.
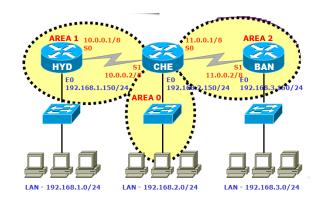
Fig 2.2 OSPF virtual Diagram

The Virtual diagram of OSPF is shown in Fig 2.2. Open Shortest Path First (OSPF) is routing protocol developed for Internet Protocol(IP) networks by the interior gateway protocol(IGP) working group of the Internet Engineering Task Force(IETF). The working group was formed in 1988 to design an IGP based on the shortest path first (SPF) algorithm for use in the Internet. Similar to the Interior Gateway Routing Protocol (IGRP), OSPF was created because in the mid-1980s, the Routing Information Protocol (RIP) was increasingly unable to serve large, heterogeneous internet works.

OSPF is a classless routing protocol, which means that in its updates, it includes the subnet of each route it knows about, thus, enabling variable-length subnet masks. With variable-length subnet masks, an IP network can be broken into many subnets of various sizes. This provides network administrators with extra network-configuration flexibility. These updates are multicasts of specific addresses (224.0.0.5 and 224.0.0.6).

2.6 RESULT & DISCUSSION

The analysis of Routing Information Protocol has been made in this Project. Using Cisco Packet Tracer, the Protocol has been simulated. On analyzing the Protocol, there were various drawbacks in the Routing Information Protocol. The principal drawbacks include increased bandwidth utilization for sending updates. Also, the protocol does not consider the Bandwidth in metric calculation as it uses only hop count.

Let us assume two networks, both having the same class of IP. In this case, the Routing Information Protocol allows data transmission between two networks. But if the networks are configured with different Classes of IP, then the Protocol doesn't allow data transmission between the networks. This is the major drawback of the Routing Information Protocol and is shown in the fig. 3.3 and figs. 3.4.

Fig 2.3 shows the successful data transmission between the two networks on assigning the IP of the same class. The green dot on the router cable indicates the successful data transmission.
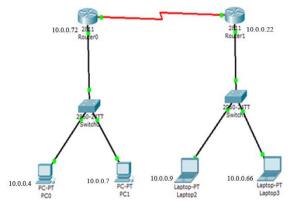

Fig 2.3 RIP configuration with same class of IP

Fig 2.4 shows that there is no data transmission on the assigned IP of different classes. The red dot on the router cable indicates that there is no data transmission.
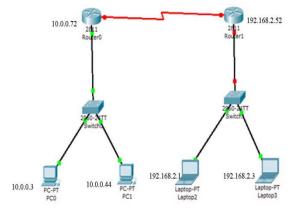

Fig 3.4 RIP configuration with different classes of IP

The major disadvantage of this configuration is that the networks which don't have the same IP cannot communicate with each other.

III. CONCLUSION AND FUTURE WORK

The study on earlier chapters shows that working with this OSPF protocol will have the following advantages:

- Classless routing protocol
- Updates are through multicast (244.0.0.5)
- The administrative distance is 110
- Metric cost is 10^8/bandwidth in bps
- Acknowledge is sent in every 30 Sec
- Hierarchical design in Multiple area
- First and foremost area is called as a backbone.

The results of this project indicate and enhance our understanding that all major disadvantages of RIP can be overcome using OSPF protocol, because it uses a link state algorithm and it maintain three tables for easy and convenient routing: - Neighbor table, Database table, and Routing information table.

The neighbor table contains information about directly connected OSPF neighbor. This forms a adjacency. Database table contains information about the entire view of topology with respect to each router. Routing table contains information about the best path calculated by the shortest path first algorithm.

Future research should therefore concentrate on the investigation of Routing in Ad-hoc network. In an Ad - hoc network the router without any access point (AP) will be used.

Extended Service Set can be provided which can connect the larger area network with multiple AP and cover a greater area will also be provided. Authentication for the router from the attack of foreign elements can be done by providing password and username for admin controller.

REFERENCES

[1] Ahmad Karim, Minhaj Ahmad Khan(2011). "Behaviour of Routing Protocols for Medium to Large Scale Networks", Australian Journal of Basic and Applied Sciences, 5(6): 1605-1613.
[2] Bertsekas.D and R. Gallager (1992), Data Network. Prentice-Hall .
[3] Bruno, Anthony & Kim, Jacqueline (2005), CCDA Self-Study: RIP, IGRP, and EIGRP Characteristics and Design .Retrieved.
[4] Bernard Fortz,Jennifer Rexford and MikkelThorup.(2002), Traffic Engineering With Traditional IP Routing Protocols." IEEE Communications Magazine.
[5] Cisco EIGRP: Enhanced Interior Gateway Routing Protocol Overview (2005). Retrieved
[6] Davis, David. (2005) Cisco administration 101: What you need to know about EIGRP.

[7] Guang Yang, "Introduction to TCP/IP Network Attacks" white paper available at seclab.cs.sunysb.edu/sekar/papers/netattacks.pdf.

[8] Garcia-Lunes-Aceves and Murthy.S,(1995) "A Loop-Free Path-Finding Algorithm: specification, Verification and Complexity," in Proceedings of the IEEE INFOCOM.

[9] IP Routing: From Basic Principles to Link State Protocols. Retrieved November 27, (2005),

[10] Ittiphonkrinpayorm and SuwatPattaramalai, (2012)"Link Recovery Comparison Between OSPF & EIGRP ", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012) IACSIT Press, Singapore

[11] Malkin.G. (1998) Enhanced Interior Gateway Routing Protocol. (2005) . Retrieved

[12] Mehboob Nazism Shehzad, Najam-Ul-Sahar, "Simulation of OSPF Routing Protocol Using OPNET Module"(A Routing Protocol Based on the Link-State Algorithm).

[13] Malkin.G,(1998) "Routing Information Protocol Version 2," SRI Network Information Center, RFC 2453.

[14] McQuillan, G. Falk, and I. Richer,(1978) "A Review of the Development and Performance of the ARPANET Routing Algorithm," IEEE Transactions on Communications, vol. 26, no. 12, pp. 1802–1811

[15] Mittal.V and G. Vigna,(2002) "Sensor-Based Intrusion Detection for Intra- Domain Distance-Vector Routing," in ACM CCS's 02.

[16] Nordstr¨om and Dovrolis.C(2004), "Beware of BGP attacks," SIGCOMM Computer. Communication. Rev., vol. 34, no. 2, pp. 1–8.

[17] Office of the President of the United States, "Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program," 2004.

[18] Pethe.R.M., Miss S.R.Burnase (2011) TECHNICAL ERA LANGUAGE OF THE NETWORKING - EIGRP International Journal of Engineering Science and Technology (IJEST) NCICT Special Issue.

[19] Perlman.R, (1988) "Network layer protocols with byzantine robustness," Ph.D. dissertation, MIT Lab. for Computer Science.

[20] Pei.D, X. Zhao, L. Wang, D. Massey, A. Mankin, F. S. Wu, and L. Zhang,(2002) "Improving BGP Convergence Through Assertions Approach," in Proceedings of the IEEE INFOCOM.

[21] Pei.D, D. Massey, and L. Zhang,(2004) "A Framework for Resilient Internet Routing Protocols," IEEE Network Special Issue on Protection, Restoration and Disaster Recovery.

[22] Postel.J, "User Datagram Protocol, (1980)" SRI Network Information Center, RFC 768.

[23] Padmanabhan.V.N. and D. R. Simon,(2002) "Secure Trace route to Detect Faulty or Malicious Routing," in Proceeds of HOTNETS.

[24] Rajesh. R, Lakshmanan. M and Noor Mohammed(2011), ": Implementation of Networked Control Systems using TCP/IP", International Journal of Computer Applications 18(2):1-5.

[25] Rekhter.Y, Li.T, and Hares. S (2006), "A Border Gateway Protocol 4 (BGP- 4)," RFC 4271 (Draft Standard), Internet Engineering Task Force..

[26] Rekhter.Y, "Experience with the BGP Protocol," (1991) RFC 1266 (Informational), Internet Engineering Task Force.

[27] Rekhter.Y and T. Li,(1995) "Border Gateway Protocol 4," SRI Network Information Center, RFC 1771.

[28] RIP Version 2. Retrieved November 27, (2002), from http://rfc.net/std0056.html   Osterloh, Heather.

[29] Resource Reservation Protocol. (2002). Retrieved November 27, 2005.

[30] Smith.B. R, S. Murphy, and J. J. Garcia-Luna-Aceves,(1997) "Securing distance-vector routing protocol," in Global Internet'96.

[31] Terzis.A , K. Nikoloudakis, L. Wang, and L. Zhang,(2000) "IRLSim: A General Purpose Packet Level Network Simulator," in Proceedings of the 33rd ACM-SIAM Symposium on Discrete Algorithms..

[32] Vishal sharma, Rajneesh Narula and Sameer khullar(2012) "Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols" International Journal of Computer Applications (0975 – 8887)Volume 44– No13.

[33] Wu, Bing, "Simulation Based Performance Analyses on RIP, EIGRP and OSPF Using OPNET"

[34] YoungmiJoo, VinayRibeirot, AnjaFeldmannt,Anna C.Gilbertand Walter WillingerGuang Yang,", "TCP/IP traffic dynamics and network performance: A lesson in workload modeling, flow control and trace-driven simulations", ACMSIGCOM