QUANTITATIVE WORK STUDY ON MRC PROTOCOLS

Dr.V.Shanmukha Rao, M.Revanth, C.Chaitanya and P.Abhilash
*Professor and B.Tech students, Department of Information Technology, Andhra Loyola Institute of Engineering and Technology, Vijayawada - 520008, Andhra Pradesh, shanmukharao.v@gmail.com

Abstract— the **internet plays an indispensable role in our daily communication using computer network infrastructures and it can be online electronic related applications or online transactions, today internet becomes a heart of communication in the world. There are some problems still exists in internet network communication technologies, which gives slow reaction and espouse instability. In this paper, considered to ensure the fast recovery over the network failures, a several protocols are being implemented in MRC like OSPF, EIGRP, RIP, BGP, etc. A comparative study metrics was implemented to generate the suggested results from the existed protocols to enhance the communication stability in the network. The process was simulated by using Cisco packet tracer.**

Keywords—**Internet, MRC, OSPF, EIGRP, RIP, Network failure, Cisco packet tracer.**

I. INTRODUCTION

Internet has been transformed from a special purpose network to an omnipresent platform for a wide range of everyday communication services. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices which are inter-connected to one another to allow the sharing of data as well as resources.

The main motive of MRC is to use the network graph and the associated link weights to produce a small set of backup network configurations. The link weights in these backup configurations are manipulated so that for each link and node failure, and regardless of whether it is a link or node failure, the node that detects the failure can safely forward the incoming packets towards the destination on an alternate link. MRC assumes that the network uses shortest path routing and destination based hop-by-hop forwarding.

In the internet, [1].IP networks are intrinsically robust, since IGP routing protocols like OSPF [5] are designed to update the forwarding information based on the changed topology after a failure. This re-convergence assumes full distribution of the new link state to all routers in the network domain. When the new state information is distributed, each router individually calculates new valid routing tables. The IGP convergence [6] process is slow because it is reactive and global. It reacts to a failure after it has happened, and it involves all the routers in the domain [4].

The *Packet Tracer* is a network simulation tool will help you visualize your network configuration for innovative designs to build network topologies by you.

A complete set of valid backup configurations for a given topology can be constructed in different ways.[3] In the next subsection we present an efficient algorithm for this purpose. The number and internal structure of backup configurations in a complete set for a given topology may vary depending on the construction model. If more configurations are created, fewer links and nodes need to be isolated per configuration, giving a richer (more connected) backbone in each configuration. On the other hand, if fewer configurations are constructed, the state requirement for the backup routing information storage is reduced. However, calculating the minimum number of configurations for a given topology graph is computationally demanding

II. PROPOSED SYSTEM CONFIGURATIONS

Multiple Routing Configurations (MRC) [8] is a proactive and local protection mechanism that allows recovery in the range of milliseconds. MRC allows packet forwarding to continue over preconfigured alternative next-hops immediately after the detection of the failure. Using backup configuration algorithm it takes up the backup of nodes and links [9]. Using MRC as a first line of defense against network failures, the normal IP convergence process can be put on hold. The shifting of traffic to links bypassing the failure can lead to congestion and packet loss in parts of the network [10]. This limits the time that the proactive recovery scheme can be used to forward traffic before the global routing protocol is informed about the failure, and hence reduces the chance that a transient failure can be handled without a full global routing re-convergence. The following parameters are considered for the simulation of the protocols is as follows:

Parameters	OSPF	EIGRP	RIP
No. of nodes	27	27	27
Administrative distance	110	90	120
TTL	125	125	121
Load	0	0	0
Bandwidth	100000kb	100000kb	100000kb
Updating	3sec	5sec	30sec
MTU	1500	1500	1500
Hop count	∞	255	15
Time to complete	0.012	0.048	0.020

Table 1: considered parameters

OSPF Protocol [2]- OSPF stands for Open Shortest path first Standard protocol. It is a link state protocol. It uses SPF (shortest path first) or Dijkstra algorithm.It has Unlimited hop count. Metric is cost (cost=10 ^8/B.W.).Administrative distance is 110.It is a classless routing protocol. It supports VLSM and CIDR. It supports only equal cost load balancing.

Configuring OSPF [7]

Router# enable
Router# configure terminal
Router (conf) # router ospf <pid>
Router(config-router)#network <Network ID><wildcard mask> area <area id>

RIP Protocol –

It stands for Routing Information Protocol. It is an Open Standard Protocol. It is a Classful routing protocol. Updates are broadcasted via .255.255.255 Administrative distance is 120.Maximum hop count is 15.Maximum routers are16. Used for small organizations. Exchange entire routing table for every 30 seconds.

Update timer: 30 sec-Time between consecutive updates
Invalid timer: 180 sec-Time a router waits to hear updates. The route is marked unreachable if there is no update during this interval.

Flush time:- 240 sec-Time before the invalid route is purged from the routing table.

Configuration of RIP
Router# enable
Router # config t
Router (config) # router rip
Router (config-router) # network<network ID>
Router (config-router) # network <network ID>
Router (config-router) # exit
Router (config) # exit

EIGRP Protocol-

It is Cisco proprietary protocol. It includes all features of IGRP. The metric parameters are considered as follows: 32 bit IP Address, Composite Metric (BW + Delay + load + MTU + reliability). Administrative distance is 90. Multicast (224.0.0.10) updates for every 5 seconds, .Maximum Hop count is 255 (100 by default). It supports IP, IPX and Apple Talk protocols. In this protocol 'Hello' packets are sent for every 5 seconds.

III. SIMULATION RESULTS

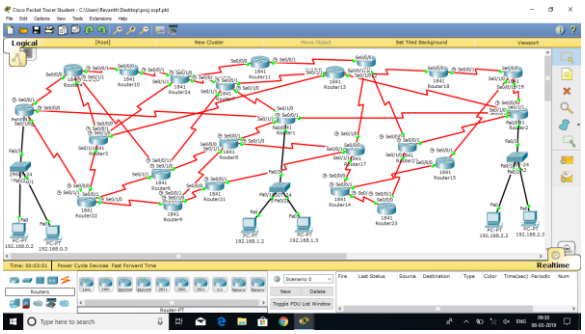

Figure 3.1 Considered topology for Simulation

OSPF Execution:

PC>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=2ms TTL=125
Reply from 192.168.2.3: bytes=32 time=2ms TTL=125
Reply from 192.168.2.3: bytes=32 time=3ms TTL=125
Reply from 192.168.2.3: bytes=32 time=4ms TTL=125
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 4ms, Average = 2ms

EIGRP Execution:

PC>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=2ms TTL=125
Reply from 192.168.2.3: bytes=32 time=2ms TTL=125
Reply from 192.168.2.3: bytes=32 time=3ms TTL=125
Reply from 192.168.2.3: bytes=32 time=4ms TTL=125
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 4ms, Average = 2ms

RIP Execution:

PC>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time=131ms TTL=121
Reply from 192.168.2.3: bytes=32 time=163ms TTL=121
Reply from 192.168.2.3: bytes=32 time=7ms TTL=121
Reply from 192.168.2.3: bytes=32 time=6ms TTL=121
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 163ms, Average = 76ms

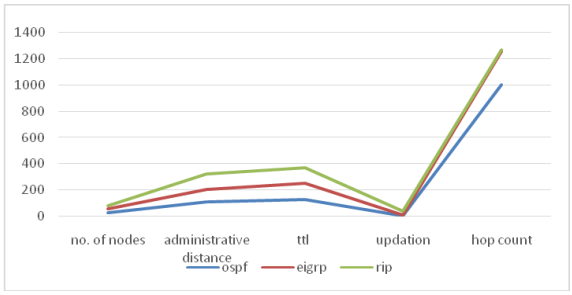

Figure 3.2 : Comparative study report of the protocols

IV. CONCLUSION

MRC provides the routers with additional routing configurations and allowing them to forward packets along with routing information, which will avoid failures in routes or links. MRC assures recovery from any single node or link failure in a randomly connected network. By calculating backup configurations in advance, and operating based on locally available information only, MRC can act promptly after failure discovery. MRC operates with or without knowing the root cause of failure, i.e., whether the forwarding disruption is caused by a node or link failure. This is achieved by using careful link weight assignment. The link weight assignment rules also provide basis for the specification of a forwarding procedure that successfully solves the last hop problem. The performance of the algorithm and the forwarding mechanism has been evaluated using simulations.

REFERENCES

[1] D. D. Clark, "The design philosophy of the DARPA internet protocols," SIGCOMM, Computer Communications Review, vol. 18, no. 4, pp. 106– 114, Aug. 1988.
[2] A. Basu and J. G. Riecke, "Stability issues in OSPF routing," in Proceedings of SIGCOMM, San Diego, California, USA, Aug. 2001, pp. 225–236.
[3] A. Kvalbein, T. Cici´c, and S. Gjessing, "Post-failure routing performance with multiple routing configurations," in Proceedings INFOCOM, May 2007.
[4] C. Boutremans, G. Iannaccone, and C. Diot, "Impact of link failures on VoIP performance," in Proceedings of International Workshop on Network and Operating System Support for Digital Audio and Video, 2002, pp. 63–71.
[5] D. Watson, F. Jahanian, and C. Labovitz, "Experiences with monitoring OSPF on a regional service provider network," in ICDCS '03: Proceedings of the 23rd International Conference on Distributed Computing Systems. Washington, DC, USA: IEEE Computer Society, 2003, pp. 204–213.
[6] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, "Achieving sub-second IGP convergence in large IP networks," ACM SIGCOMM Computer Communication Review, vol. 35, no. 2, pp. 35 – 44, July 2005.
[7] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an IP backbone network," in Proceedings INFOCOM, Mar. 2004.
[8] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah, "Fast local rerouting for handling transient link failures," IEEE/ACM Transactions on Networking, vol. 15, no. 2, pp. 359–372, April 2007.
[9] S. Iyer,S. Bhattacharyya, N. Taft, and C. Diot, "An approach to alleviate link overload as observed on an IP backbone," in Proceedings INFOCOM, Mar. 2003, pp. 406–416.
[10] S. Rai, B. Mukherjee, and O. Deshpande, "IP resilience within an autonomous system: Current approaches, challenges, and future directions," IEEE Communications Magazine, vol. 43, no. 10, pp. 142–149, Oct. 200

Dr.V.Shanmukha Rao presently working as a Associate Professor in the Department of Information Technology branch in Andhra Loyola Institute of Engineering and Technology, Vijayawada, affiliated to Jawaharlal Nehru Technological University, India. He has a total of 18 years of rich experience comprising teaching and research. He has published the papers in International and national journals. His current research interests are in the areas of Computer Networks, cloud computing, datamining, Web Mining and Semantic web technologies.