International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

A Novel Re-Route Method on Network topology

Sable Arjun Shivajirao[1]; Pawar Prashant Balasaheb[2]; Rohom Nilesh Bhausaheb[3]; Shinde Yogesh Arjun [4] & K. U. Rahane[5]

[1]B.E. Dept. of Computer Science Amrutvahini College of Engineering, Sangamner Amrutanagar, Ghulewadi. Ahmedanagar.

[2]B.E. Dept. of Computer Science Amrutvahini College of Engineering, Sangamner Amrutanagar, Ghulewadi. Ahmedanagar

[3]B.E. Dept. of Computer Science Amrutvahini College of Engineering, Sangamner Amrutanagar, Ghulewadi. Ahmedanagar

[4]B.E. Dept. of Computer Science Amrutvahini College of Engineering, Sangamner Amrutanagar, Ghulewadi. Ahmedanagar

[5]M.E. Dept. of Computer Science Amrutvahini College of Engineering, Sangamner Amrutanagar, Ghulewadi. Ahmedanagar

A Fast Abstract

Today the world is rapidly transmuting and technology is zooming exponentially, the number of users of internet is additionally incrementing rapidly which cause increase in traffic and causes more no of failures in transmission of packets. The backbone process of the ecumenical internet or any internal network is Routing. Subsisting routing techniques includes static and dynamic routing which are implemented utilizing routing algorithms like RIP, EIGRP, OSPF, and IS-IS. These routing algorithms perspicaciously route the packets on the network. There are many scenarios where a packet is sent, the routing algorithm finds a felicitous path for the packet, routes it and it is distributed. There are cases where packets do not get distributed because of many reasons like link failures. A method to find an alternate path, after a link failure, from a source node to a destination node, afore the Interior Gateway Protocol (e.g., OSPF or IS-IS) reroutes the packet by notifying the sender which takes about 100ms. A more perspicacious way to distribute the packet is to reroute the packets from the last prosperous node. In this method an alternate route is ascertained instantly after a node failure, and updating the routing table of other nodes according to the incipient route. The target application (up to tens of nodes) accesses the sub-network of an accommodation provider's network, which is a typical scale, encountered in practice; an accommodation provider typically has many such minute regional access networks. The expeditious reroute method would establish an incipient path from the source to destination in a much lesser time than the subsisting system i.e. IGP (OSPF).

Keyword: OSPF; Re-Routing; Routing; IS-IS; Reconvergence.

1. Introduction

Multiprotocol Label Switching (MPLS) is the backbone network for IP domain and it is the incipient most expeditious growing communication network to enhance the haste, scalability of network. MPLS network has feature is that it support traffic engineering tunnels by eschewing congestion and utilizing all the available network bandwidth with an efficient way. The main functionality of Traffic

Engineering [13] of MPLS network is resource reservation, faulttolerance and optimal Resources utilization. Multiprotocol Label Switching technology (MPLS) sanctions traffic engineering (TE) and enhances the performance of the subsisting protocols over the traditional IPv4 network. It is presaged that MPLS will be called as the bearer of IP network in future sizably voluminous backbone networks. The main focus of MPLS network is to affix a short fine-tuned-length label to packets at the ingress router of the MPLS domain. The packet forwarding in network depends on the tagged label, not on longest address match, as in traditional IP forwarding. A router or nodes placed on the edge of the MPLS network called Label Edge Router (LER) that is associated to a label on the substructure of a Forwarding Parity Class (FEC). In the MPLS network, internal routers that perform swapping and label-predicated packet forwarding are called Label Switching Routers (LSRs).

2. Related Work

Routing technique, "recursive Loop-Free Alternates (RLFAs)", to alleviate packet loss due to transient link failures. This technique consists of a backup path calculation with corresponding re-routing scheme predicated on the Loop-Free Condition (LFC) as mentioned in the rudimentary designation for IP Expeditious Re-Route (IPFRR)[9]. Under this routing strategy, nodes calculate backup paths by making modification on the weights of links in the primary shortest path tree. If a failure transpires , the detecting node determines the number of recursions, which denotes the number of times packets must be moved along the alternate next hops to bypass the failed link. This technique guarantees full repair coverage for single link failures. We calculate the performance of our proposed technique through simulations and show that the overheads, the stretch of its pre-computed alternate paths, and the failure-state Maximum Link Utilisation (MLU) are minimal.

As the Internet takes an increasingly central role in our communications infrastructure; the slow convergence of routing protocols becomes a growing quandary after a network failure. To assure resilient recuperation from link and node failures in IP networks, we show an incipient recuperation scheme called Multiple Routing Configurations (MRC)[7]. Our proposed scheme guarantees full instauration in all scenarios of failure, utilizing a single mechanism to handle both link and node failures, and without kenning the failure of root cause. MRC is rigorously connectionless, and postulates only destination predicated hop-by-hop forwarding. MRC is predicated on storing adscititious routing information in the routers, and sanctions packet forwarding to perpetuate on another output link immediately after the detection of a failure. It can be implemented with only minor changes to available solutions. In this paper we show MRC, and analyze its performance with deference to scalability, backup path lengths, and equal load distribution after a failure. We withal show how an estimate of the traffic demands in the network can be habituated to upgrade the distribution of the recuperated traffic, and thus reduce the chances of congestion when MRC is use

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

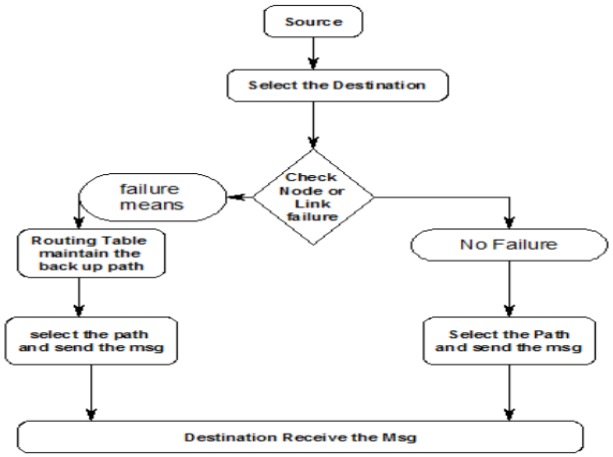

Fig 1: Multiple Routing Configurations.

MPLS[6] is a widely used technology in the accommodation providers and enterprise networks across the globe. MPLS-enabled infrastructure has the puissance to convey any type of payload (ATM, Frame Relay and Ethernet) over it, subsequently providing a multifarious architecture. An incoming packet is relegated only once as it enters into the MPLS domain and gets assigned labeldetails;[3] thereafter all decision processes along a designated path is predicated upon the affixed label rather than destination IP addresses. As network functions are becoming mission critical, the requisites for fault tolerant networks are growing , as a rudimental requisite for carrying sensitive traffic. Fault tolerance mechanisms as givenby an IP/MPLS network avails in giving end to culminate "Quality of Service" within a domain, by better handling blackouts and brownouts. This theory work reflects how MPLS increases the capability of deployed IP infrastructure to convey traffic in-between end contrivances with sudden failures in place. It additionally fixates on how MPLS converts a packet switched network to a circuit switched network, while owning the characteristics of packet switched technology. An incipient mechanism for MPLS fault tolerance is proposed.

LDP engenders an RSVP [1] primary tunnel between a dyad of nodes. In integration, a bypass tunnel is pre-defined for each arc(i, j); the tunnel which is bypassed for(i, j) is a path from i to j that is physically disjoint from the link(i, j).

When the packet reaches node i and link (i, j) is failed, a local repair forwards the traffic along the bypass tunnel for(i, j); when the packet reaches node j , it does not stop to move on the path defined by the RSVP primary tunnel. The disadvantage of this method is that, for a network of N nodes and A arcs,N(N−1) uni-directional primary tunnels and 2A uni-directional bypass tunnels are required. An another way to build tunnels is to utilize a Loop Free Alternative (LFA) method ([2], [4]). For nodes i and j let c*(i, j) be the minimal distance between i and j. Suppose node n is a neighbor of s(i.e., they are connected by a single arc.Then the neighbor n of source node s is an LFA for destination d if c*(n, d)<c*(n, s)+c*(s, d).

That is, node n is an LFA if the path which is shortest from n to d does not return to s on the arc(n, s). To ascertain whether an LFA subsists for a given s and d it suffices to determine if (1) holds for some neighbor n of s.

Proposed System:

The subsisting system describes the concept of routing from the source to destination within the network. It deals with many available techniques to handle data loss, delayed timing, loss of cognizance , but it does not describe how the packet should be forwarded once node within the

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

path is unavailable or corrupted. The subsisting system faces link and node failure in IP networks. The convergence of routing protocol becomes a growing quandary after a link failure. Due to congestion packet loss or packet delay can be occured. Time consumed to send the data is incremented due to resending of lost data. There is no back-up path and it has no precise cognizance of failure location.

The proposed system would be fixated on the Expeditious Re Route module where an alogorithm finds an alternative path after a link failure afore the Interior Gateway Protocol had a chance to reconverge in replication to failure.This module will consider a source node (s) for sending data to destination node (d). Suppose some link(i,j) on the shortest path s to d fails.An IGP will an alternate path from s to d that eschews(i,j).When a failure occurs in an IP network, the routers adjacent to the failing resource must react by distributing incipient routing information to make each router of the network to update its routing table.

3. Implementation

3.1 The method

Domain of this project is networking. The technology utilized in this project is Java swings the most prevalent IGP's utilized by ISP networks today are OSPF which is Link State Routing Protocol but OSPF can take hundred of milliseconds for reconvergence. Fast Re-Route methods engender an incipient path from source to destination in much less time than required for IGP re-convergence. Thedetails of this method is described below.

3.2 Algorithm steps:

1. Select source node and destination node. Send packet from source node, set P(ordered list of node that has beenvisited) to zero and node n belongs to the set of neighbors (N). Let source node (s) set to (x).Set delta(n)=0delta(x) means multiplicity of node x indicating how many times n has been visited by packet.
2. Check for the condition if source node is not equal to destination node, if this condition satisfies then proceedssending the packet.
3. Set Y to y belongs to set of neighbor of x and multiplicity of node y equal to minimum of multiplicity of node nwhere n belong to set of neighbor of x.
4. From all neighbor of x select any y belong to Y that satisfies the condition. c(x,y)+c*(y,d) is smallest among all neighbor of x.
5. After selecting the neighbor augument multiplicity of node x by 1 ie. increment delta(x) by 1.And P belong to{P,x} ie,x is inserted after rightmost element in P. And send packet and P from x to y.
6. Set x to y.
7. Goto step 2 until packet reaches the Destination.

Algorithm:For sending packet to destination

```
procedure  Route(s, d)
1:  initialize P=Ø, Δ(n)=0 for n∈N , and x=s ;

2:  while(x=d)
{

3:  LetY={y∈N(x)|Δ(y)=minn∈N(x)(n)}

4:  Pick any y ∈Y for which the sum
c(x, y)+c*(y, d) is smallest;

5:  Set Δ(x)←Δ(x)+1,P←{P,x},and send the packet
and P from x to y;

6:  Set x ← y;

7:  }
```

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

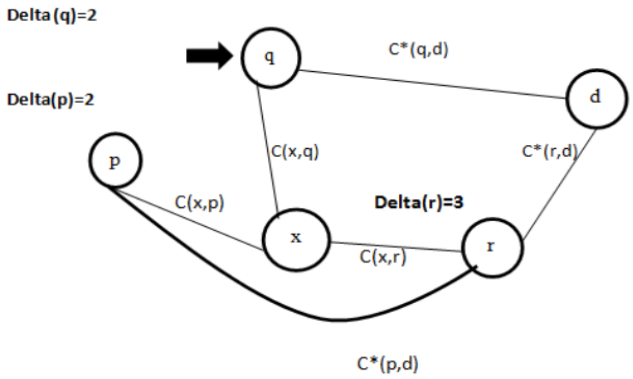

Fig 2: Picking the Next Node.

The neighbor of x from the above figure are p,q and r of these, p and q have the lowest multipl exityi.e:delta(p)=2and delta(q)=2. Since c(x,q)+c*(q,d) < c(x,p)+c*(p,d), the packet is next forwarded to q.

3.3 ARCHITECTURE OF PROPOSED SYSTEM:

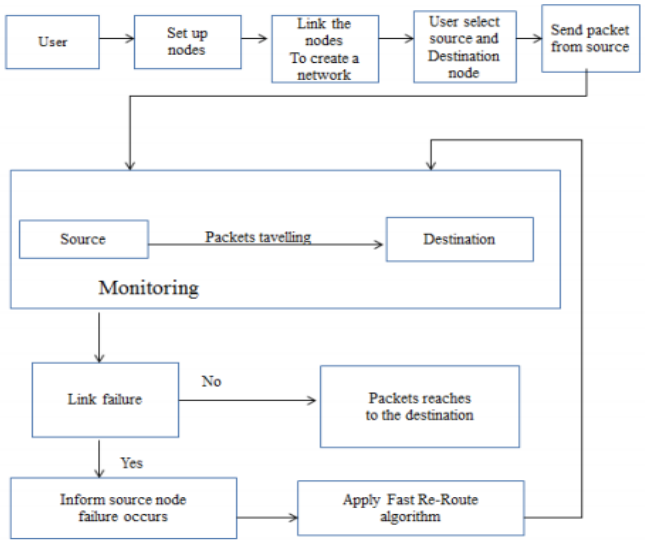

Fig 3:Architecture Diagram

Here we have describe the system architecture for our proposed system. In the commencement we require to require to establish different nodes in a wired network. The utilizer first cull the source node from where the packets are sent and destination node where we optate the packets should bedelievered. Once packets from source node are sent we monitor the packets perpetually in a network to ken the status of sent packet. If there is a link failure in the network then apprise the source node about link failure, and the source node apply expeditious re route method in replication to link failure.

Expeditious re route method cull neighbour of source node with minimized path cost and lowest multiplicity and send packet to destination. We engender an incipient protocol in NS2 and make utilization of Link state protocol for routing of packets. We additionally introduce the concept of lexicographically most diminutive node (closed to a in the alphabet) and lexicographically most immensely colossal node (most proximate to z in the alphabet) and forward the packet to next node. We apply expeditious re route method in replication to link failure until packet reaches the destination.

4. Experimental Results

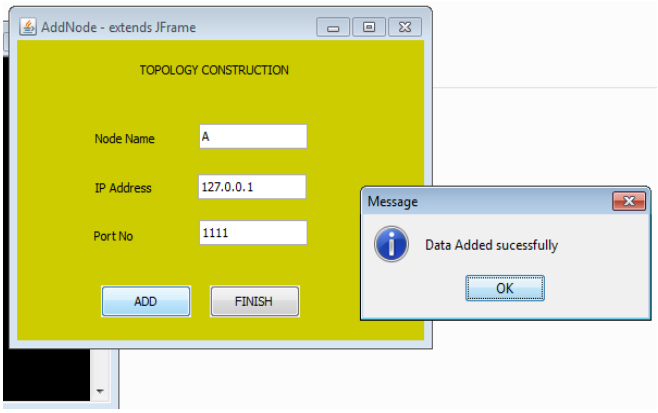

Fig 4: Add nodes.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 09
May 2016

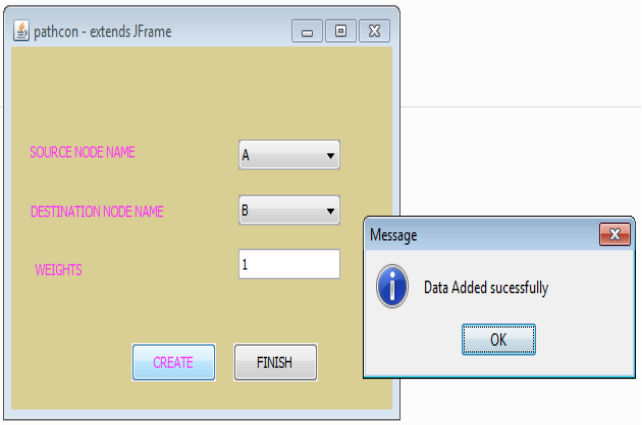

Fig 5: Path Connection.

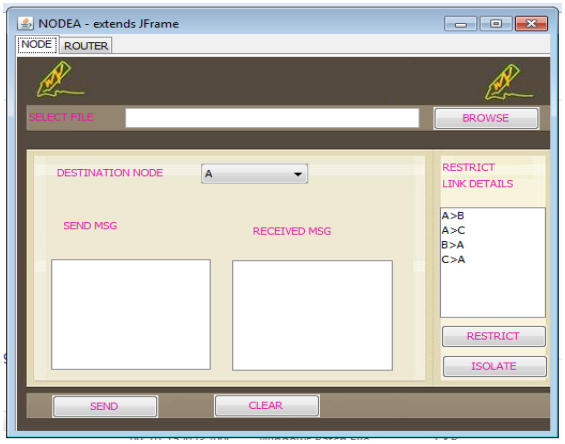

Fig 6: Node A details page.

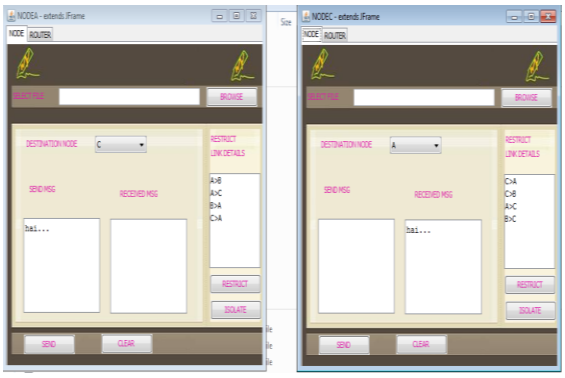

Fig 7: Between Nodes message information

5. Conclusion

IP Expeditious Re Route Framework takes very less time in finding an alternate path in replication to link failure as compared to other subsisting systems.And the reconvergence time is reduced to lower extent. Link state protocols proved to be very efficient in reducing reconvergence time as compared to non link states IGP protocol.

6. References

[1] A. Atlas, Ed., "U-turn alternates for IP/LDP fast-reroute," IETF draftatlas-ip-local-protect-uturn-03, Feb.2006.

[2] A. Atlas and A. Zinin, Eds., "Basic specification for IP fast reroute: loopfree alternative," IETF RFC 5286,Sept. 2008.

[3] S. Bryant, C. Filsfils, and M. Shand, "Remote LFA FRR," IETF Internet Draft draft-shand-remote-lfa-00,Oct. 2011.

[4] C. Filsfils and P. Francois, Eds., "Loop-free alternative (LFA) applicability in service provider (SP) networks," IETF RFC 6571, June 2012.

[5] E. M. Gafni and D. P. Bertsekas, "Distributed algorithms for generating loop-free routes in networks withfrequently changing topology," IEEE Trans. Commun., vol. COM-29, pp. 11–18, 1981.

[6] I. Hussain, Fault-Tolerant IP and MPLS Networks. Cisco Press, 2005.

[7] A. Kvalbein, A. F. Hansen, T. ˇCiˇci´c, S. Gjessing, and O. Lysne, "Multiple routing configurations for fast

IP network recovery," IEEE/ACM Trans. Netw., vol. 17, pp. 473–486, 2009.

[8] K. W. Kwong, L. Gao, R. A. Gue´rin, and Z. Zhang, "On the feasibility and efficacy of protection routing in IP networks," IEEE/ACM Trans. Netw., vol. 19, pp. 1543–1556, 2011.

[9] S. S. Lor, R. Ali, and M. Rio, "Recursive loop-free alternates for full protection against transient link failures," in Proc. 2010 IEEE Symp.onComput. andCommun., pp. 44–49.

[10] G. Re´tv´ari, J. Tapolcai, G. Enyedi, and A. Csa´sz´ar, "IP Fast ReRoute: loop free alternates revisited," in Proc. 2011 IEEE Int. Conf. on Comput.Commun., pp. 2948–2956.

[11] J. M. Welch and J. E. Walter, Link Reversal Algorithms. Morgan & Claypool Publishers, 2012