An Efficient Approach towards Failure Recovery in IP Networks using Binary Router

Sanjib Halder
Asst. Professor, Department of Computer Science
The Bhawanipur Education Society College, West Bengal, India

Siddhartha Roy
Asst. Professor, Department of Computer Science
The Bhawanipur Education Society College, West Bengal, India

Abstract— It has been observed that failures of routers and its connecting links in Ethernet LAN cannot be completely avoided even in well maintained networks. Due to failure, many events occur in the affected network, such as topological changes, loss of packets, recovery of the routing table etc. There are various causes of network failure such as the failure of a router, failure of one of its connecting link or when a router is deliberately withdrawn etc. Under such failed conditions, a quick convergence scheme is extremely essential for the packet transmission of the network. Route recalculation and rebuilding of routing tables, for the recovery of network failure, is the main approach used by today's IP router. However, route recalculation and routing tables building up are time consuming. Mean while, a large number of packets may be dropped due to failure of link. In this paper, we have proposed an alternate efficient IP rerouting scheme based on Steady State Routing Table (SSRT), using binary Router (having 2 ports only), which automatically switches to the pre-calculated backup routes following a network failure. Consequently, the Ethernet LAN can recover immediately as recalculation of routes or rebuilding of routing tables are not needed.

Keywords - binary router, quick convergence, network failure, SSRT.

I. INTRODUCTION

A computer network is a collection of autonomous computers, interconnected by communication links and can exchange messages among themselves. It allows its users to share the available resources among the various computers of the network. In the late sixties and early seventies, the design in the area of computer networking was developed by the ARPANET, DECNET, etc. Due to the reduced hardware cost, an increasing number of networks were developed and used worldwide in the early seventies. All these networks were wide area networks (WAN). The technology of the first local area network (LAN), also called Ethernet, was invented in the late seventies. Among the various network technologies, Ethernet gained its popularity due to simplicity, low-cost and high reliability. Now-a-days, most of the networks are using Ethernet LAN. The relay device which is used to transmit a message from one network to another is a router or Layer 3 switches. For large message transmission, non-interrupted service is very much essential. Also quick failure recovery schemes are utmost essential for smooth service of the Network. Network failures can be caused by a variety of reasons such as connecting cable fault, malfunctioning of any of the port of the router, software bugs etc. Despite continuous technological advances, failures cannot be completely avoided even in well maintained networks [3]. The main approaches used by today's IP networks are route recalculation and lower layer protection [4], [5]. Most of the routing protocols are designed to perform failure advertising, route recalculation and routing tables modification to recover from failures. Although these mechanisms are capable of dealing with any type of failures, the process is very slow. From this point of view, the original objective of packet switching, to design a highly survivable network where packet forwarding in each router is adaptive to the network status, is yet to be achieved [9]. In this paper we propose an alternative approach to re-build routing tables of the 2-port router based on SSRT on an IP-based Ethernet LANs. Here we considered the case only for Ethernet LAN over IP network. Routers on a network have been assumed to run a distributed algorithm among them to decide who should forward the packet by checking the net-id of the destination LAN. The simple and widely used DVR algorithm (DVRA) has been used as the basis of the routing protocol. However, various drawbacks of DVRA, like poor convergence problem, Count to Infinity problem, following a router failure, have been removed in our proposed algorithm. After the introductory section, we discussed the literature survey in section 2 and recovery scheme due to router failure is discussed in Section 3.

II. LITERATURE SURVEY

In a computer network, a message from the source host to the destination host is transmitted across the network as a sequence of packets. Such networks are called packet-switched networks. For the transport of this packet, the original message of the sender is fragmented into multiple packets which are transmitted across the packet-switched network by relay devices such as switches or routers The packets are then delivered to the destination host. Efficient and quick transmission of a packet requires the optimal route or the shortest path for the packet to traverse in order to reach the destination host from the source host.

An interruption caused due to network failure affects thousands of packet transmission over IP network, with obvious adverse effects. The ability to recover from failures has always been a key design issue in the Internet [1]. Distance Vector Routing Algorithm (DVRA) is one of the commonly used routing algorithms, which maintains a dynamic routing table that gets updated continuously with the information received from the neighbouring routers. Though DVRA is a simple technique, it suffers from various problems like Count-To-Infinity (CTI) Problem, Slow Convergence Problem and Oscillation Problem. Some modifications were incorporated in the DVRA to make it free from the CTI problem and to reduce the extent of its slow convergence and route oscillation problems. This modified DVRA (MDVRA) was used in designing a new routing algorithm for MANET [9][10], and in designing a modified BGP for achieving a faster convergence.

Interior Gateway Protocols (IGP), a routing scheme for intra-domain routing, is designed to recover from failures by updating the routing tables of routers. When a router detects a failure, it disseminates topology updates to the other routers in the same Autonomous System (AS). The topology updates trigger these routers to re-compute routing paths and update their routing tables. This IGP convergence process begins with the failure detection and finishes after routers update their routing tables. Unfortunately, the IGP convergence is a time consuming process, which usually takes several seconds even for a single link failure [1]. During IGP convergence, a large number of packets may be dropped due to invalid routes. A straightforward recovery method is to accelerate the IGP convergence [10]. However, fast triggering of the IGP convergence may cause route flapping and make networks more unstable [11].

Multiple Routing Configurations (MRC)[14] is another quick recovery scheme following a router failure. MRC allows packet forwarding to continue, based on pre-configured alternative next-hops, immediately after the detection of the failure. MRC guarantees recovery from any single link or node failure which constitutes a large majority of the failures experienced in a network [7]. The main idea of MRC is to use the network graph and the associated link weights to produce a small set of backup network configurations. Though the scheme used in MRC provides guaranteed connectivity after a failure, but load distribution problem is one of the major challenges for pre-calculated IP recovery schemes [14]. In case of IP network using binary router, the recent study shows that network failure on some special network topology like Single Connected Component LAN (SCCL) [13] is addressed. But the drawback is that they can handle only some special kind of network topology. In this paper, we have proposed an alternative simple routing scheme based on Steady State Routing Table(SSRT) using binary router[8] for fast convergence on network failure in the Ethernet LAN that address the above drawback.

III. PROPOSED RECOVERY SCHEME ON NETWORK FAILURE

Network failure can be caused due to different reasons, like router failure (or one of its port failure) or link failure or when a router is withdrawn deliberately (disconnected). Under one of such conditions, a router does not perform its task and the network must arrange for alternative ways to do the job. A fast and transparent solution to this problem is extremely important for the smooth operation of the campus network. The main approach used by today’s IP routers is to recalculate alternative routes [11],[12]. However, route recalculation and routing table build up could take considerable amount of time during which a large number of packets can be routed wrongly. The strategy we have taken is to pre-calculate and store, up to second degree back-up routes in advance and to use these backup routes information to switch to a new route as well as update the routing table quickly when a failure occurs. Periodic monitoring is carried out in the campus network by the Most Recently Connected Router (MRCR), to detect router failure or port failure automatically and to forward the affected packets immediately through the first level pre-computed back up route.

In this section we have studied the quick recovery of the Campus Network failure based on SSRT using 2-port router. Unlike the MDVRA, we assume that in the Campus Network each LAN is represented by a node and each 2-port router is represented by a link [9],[10]. In its SSRT a router maintains two backup paths apart from the shortest route. In the SSRT, if both the backup paths are empty for a destination LAN, then the corresponding LAN is single connected. Failure of this link (router) leaves the destination LAN as a lost destination.[13]. If backup path exists for a destination LAN, then failure of a link (router) needs modification of the SSRT. Here we describe the details of the quick modification scheme that achieve quick convergence and is free from CTI problem.

While failure occurs, the router owning the MRCR in the victim LAN, checks the SSRT corresponding to the failed router and does the following:

Step 1: If the SSRT doesn't contain backup path, then the corresponding LAN is a member of a Single Connected Component LAN (SCCL)[13] and becomes a lost destination. Then the MRCR will broadcast a special message containing the list of members belongs to SCCL as lost destinations. On receiving the message all the other routers, without further delay, just remove the entries corresponding to the lost destinations from their respective SSRTs and thus ensure quick convergence without CTI problem. [13]

Step 2: In case of local LANs -if the SSRT contains backup path corresponding to the failed router and the shortest path passes through the failed router, then replace the shortest path by its backup one. But if the failed path exists as a backup path then simply delete the backup one. Then exchange the updated routing table to all its adjacent routers.

Step 3: Prepare a list of affected LANs and updated hop count as <Destination LAN, hop count> and send to the affected routers.

Step 4: All routers at remote LAN, that were using the failed route, replace the existing hop count with the modified hop count + 1 and forward the modified <destination LAN, hop count> list to its immediate routers.
Routers stop forwarding when it finds that no modification occurs in hop count.

Illustration

In order to illustrate the quick recovery scheme in the Campus Network, let us consider the Fig 1 having 10 LANs and 13 two port routers namely L1, L2, L3………L10 and R1, R2, R3……………R13.

Table 1 shows the contents of the SSRT those are maintained by individual ports of each router. <L#, d, FP> signifies destination LAN, distance in terms of hop count and forwarding port. Whereas <1d, 1FP> signify the 1st order back path and corresponding forwarding port, and <2d, 2FP> signifies the 2nd order back path and corresponding forwarding port. For example, the router R5 maintains table (a) for one port and (e) for another port.

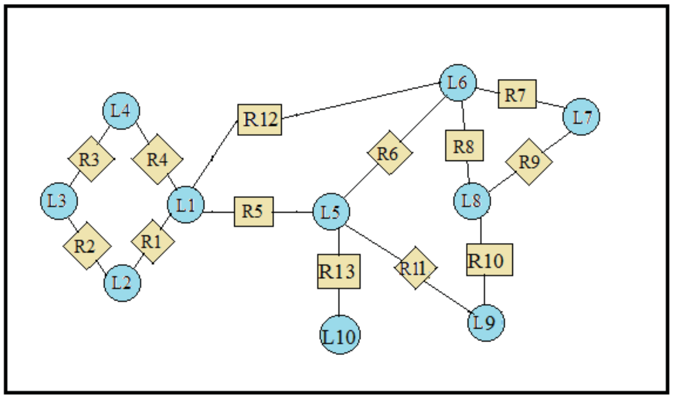

Fig 1: An example network to illustrate quick recovery.

Table (a) contains the distance (hop count) and forwarding ports to reach different destination LANs with backup path (if any) up to second order.

TABLE 1 SSRT OF ALL LANS AT A STABLE STATE.

SSRT(L1)						
L#	Fp	d	fp1	1d	fp2	2d
L1	-	-	-	-	-	-
L2	R11	1	R41	3	-	-
L3	R11	2	R41	2	-	-
L4	R41	1	R11	3	-	-
L5	R51	1	R12,1	2	-	-
L6	R12,1	1	R51	2	-	-
L7	R12,1	2	R51	3	-	-
L8	R12,1	2	R51	3	-	-
L9	R12,1	3	R51	3	-	-
L10	R51	2	R12,1	3	-	-

A

SSRT(L3)						
L#	Fp	d	fp1	1d	fp2	2d
L1	R23	2	R33	2	-	-
L2	R23	1	R33	3	-	-
L3	-	-	-	-	-	-
L4	R33	1	R13	3	-	-
L5	R23	3	R33	3	-	-
L6	R33	3	R13	3	-	-
L7	R33	4	R13	4	-	-
L8	R33	4	R13	4	-	-
L9	R33	5	R13	5	-	-
L10	R33	5	R13	5	-	-

C

SSRT(L2)						
L#	fp	D	fp1	1d	fp2	2d
L1	R12	1	R22	3	-	-
L2	-	-	-	-	-	-
L3	R22	1	R12	1	-	-
L4	R22	2	R12	2	-	-
L5	R12	2	R22	4	-	-
L6	R12	2	R22	4	-	-
L7	R12	3	R22	5	-	-
L8	R12	3	R22	5	-	-
L9	R12	4	R22	6	-	-
L10	R12	3	R22	5	-	-

B

SSRT(L4)						
L#	Fp	D	fp1	1d	fp2	2d
L1	R44	1	R34	3	-	-
L2	R44	2	R34	2	-	-
L3	R34	1	R44	3	-	-
L4	-	-	-	-	-	-
L5	R44	2	R34	4	-	-
L6	R44	2	R34	4	-	-
L7	R44	3	R34	5	-	-
L8	R44	3	R34	5	-	-
L9	R44	4	R34	6	-	-
L10	R44	3	R34	5	-	-

D

SSRT(L5)						
L#	Fp	d	fp1	1d	fp2	2d
L1	R55	1	R65	2	R11,5	4
L2	R55	2	R65	3	R11,5	5
L3	R55	3	R65	4	R11,5	5
L4	R55	2	R65	3	R11,5	6
L5	-	-	-	-		
L6	R65	1	R55	2	R11,5	3
L7	R65	2	R55	3	R11,5	3
L8	R65	2	R55	3	R11,5	3
L9	R12,5	2	R11,5	2	R6,5	3
L10	R13,5	1				

E

SSRT(L7)						
L#	Fp	D	fp1	1d	fp2	2d
L1	R77	2	R97	2	-	-
L2	R77	2	R97	2	-	-
L3	R77	2	R97	2	-	-
L4	R77	2	R97	2	-	-
L5	R77	2	R97	3	-	-
L6	R77	1	R97	2	-	-
L7	-	-	-	-	-	-
L8	R97	1	R77	2	-	-
L9	R97	2	R77	3	-	-
L10	R97	3	R77	4	-	-

G

SSRT(L9)						
L#	Fp	d	fp1	1d	fp2	2d
L1	R11,9	3	R10,9	3	-	-
L2	R11,9	4			-	-
L3	R11,9	5	R10,9	5	-	-
L4	R11,9	4	R10,9	4	-	-
L5	R11,9	2	R10,9	3	-	-
L6	R10,9	2	R11,9	3	-	-
L7	R10,9	2	R11,9	3	-	-
L8	R10,9	1	R11,9	4	-	-
L9	-	-	-	-	-	-
L10	R11,9	1	-	-	-	-

I

SSRT(L6)						
L#	Fp	D	fp1	1d	fp2	2d
L1	R12,6	1	R66	2	R86	4
L2	R12,6	2	R66	3	R86	5
L3	R12,6	3	R66	4	R86	6
L4	R12,6	2	R66	3	R86	5
L5	R66	1	R12,6	2	R86	3
L6	-	-	-	-	-	-
L7	R76	1	R86	2	R66	4
L8	R86	1	R76	2	R66	3
L9	R86	2	R86	2	R76	3
L10	R66	2				

f

SSRT(L8)						
L#	fp	d	fp1	1d	fp2	2d
L1	R88	2	R98	3	R10,8	3
L2	R88	3	R98	4	R10,8	4
L3	R88	4	R98	5	R10,8	5
L4	R88	3	R98	4	R10,8	4
L5	R88	2	R10,8	2	R98	3
L6	R88	1	R98	2	R10,8	3
L7	R98	1	R88	2	R10,8	4
L8	-	-	-	-	-	-
L9	R10,8	1	R88	4	R98	4
L10	R10,8	3				

h

SSRT(L10)						
L#	fp	D	fp1	1d	fp2	2d
L1	R13,10	2			-	-
L2	R13,10	3			-	-
L3	R13,10	4			-	-
L4	R13,10	3			-	-
L5	R13,10	1			-	-
L6	R13,10	2			-	-
L7	R13,10	3			-	-
L8	R13,10	2			-	-
L9	R13,10	1			-	-
L10	-	-			-	-

J

Now at any point of time during a monitoring cycle, if the router R_{12} owing the MRCR in L_1 detects the failure of R_5, the following sequence of steps will be performed in the network to obtain a steady state after the failure.

Step1: As soon as the router R_{12} owning the MRCR $FP_{12,1}$ in L_1 and the router R_{13} owning the MRCR $FP_{13,5}$ in L_5 detects the failure of the router R_5, immediately check their SSRT. By inspecting the SSRT(L1), the router R_{12} finds that the LANs L5, L6, L7, L8, L9 and L10 are affected. Out of these LANs L5, L9 and L10 lost their shortest path and rest of the LANs (L6, L7 and L8) lost their first order backup paths. The router R12 will just delete the first order backup for the LANs L6, L7 and L8. It doesn't require moving the second order backup to the first order backup entry as the second order backup is empty. The router R12 also move the first order backup to the shortest route entry for the LANs L5, L9 and L10 as they lost the shortest route. Then the router R12 exchanges the updated routing table to all its adjacent routers. Table 2 (a) and (b) show the SSRT(L1) and SSRT(L5) respectively after the failure of R5. Router R12 will share the table 2 (a) with R1 and R4. Whereas R13 will share the table 2(b) with R11 and R6.

TABLE 2 MODIFIED SSRT AFTER FAILURE RECOVERY OF ROUTER R5.

SSRT(L1)						
L#	Pi	D	1pi	1d	2pi	2d
L1	-	-	-	-	-	-
L2	R11	1	R41	3	-	-
L3	R11	2	R41	2	-	-
L4	R41	1	R11	3	-	-
L5	R12,1	2	-	-	-	-
L6	R12,1	1	R51	2	-	-
L7	R12,1	2	R51	3	-	-
L8	R12,1	2	R51	3	-	-
L9	R12,1	3	-	-	-	-
L10	R12,1	3	-	-	-	-

a

SSRT(L5)						
L#	Pi	D	1pi	1d	2pi	2d
L1	R65	2	R11,5	4	-	-
L2	R65	3	R55	4	-	-
L3	R65	4	-	-	-	-
L4	R65	3	-	-	-	-
L5	-	-	-	-	-	-
L6	R65	1	R55	2	-	-
L7	R65	2	R55	3	-	-
L8	R65	2	R55	3	-	-
L9	R12,5	2	R65	3	-	-
L10	R12,5	1	R65	4	-	-

b

On the other hand the router R_{13} finds that the LANs L1, L2, L3and L4 are affected. All routers lost their shortest path. The router R13 will move the first order backup to the shortest route entry for the LANs. Then the router R13 exchanges the updated routing table to all its adjacent routers.

Step 2: Both the MRCR in the LAN L1 (ie R12) and in the LAN L5 (ie R13) will prepare their own list of affected LANs and updated hop count, named Controll_Msg, as in the table 3 (a) and (b). Then send the Controll_Msg to the adjacent LANs.

TABLE 3 AFFECTED lANs WITH UPDATED HOP COUNT

Controll_Msg	
L#	Hop Count
L5	2
L9	3
L10	3

a

Controll_Msg	
L#	Hop Count
L1	2
L2	3
L3	4
L4	3

b

Step 3: On receiving the list Controll_Msg the routers update the hop count for the affected LANs. For example when the LAN L4 (actually R4L4 interface.) receive the table 3 (a), the router R4 checks that to reach L5, L9 and L10 it uses R44 interface. So it updates the SSRT(L4) as in the table 4 (a).

TABLE 4. UPDATED TABLE

SSRT(L4)						
L#	pi	D	1pi	1d	2pi	2d
L1	R44	1	R34	3	-	-
L2	R44	2	R34	2	-	-
L3	R34	1	R44	3	-	-
L4	-	-	-	-	-	-
L5	R44	3	R34	4	-	-
L6	R44	2	R34	4	-	-
L7	R44	3	R34	5	-	-
L8	R44	3	R34	5	-	-
L9	R44	4	R34	6	-	-
L10	R44	4	R34	5	-	-

A

The router also updates the Controll_Msg by incrementing the hop count by one. Table 3 (a) will be modified as

Controll_Msg	
L#	Hop Count
L5	2+1=3
L9	3+1=4
L10	3+1=4

This table will be sent to the interface of the LAN L3. Here interface R33 is used to reach L9 and L10. So hop count will be modified for L9 and L10. For the shortest path and for L5 backup path will be modified. And the Controll_msg will be modified as

Controll_Msg	
L#	Hop Count
L5	3+1=4
L9	4+1=5
L10	4+1=5

In turn this controll_Msg will be sent to L2. Here to reach L5, L9 and L10 interface R22 is used as backup path. So backup entry will be modified. Again the Controll_Msg will be modified in the same way and will be sent to L1. But from L1 to reach L5, L9 and L10 interface R11 is not used. So Controll_Msg is stopped here.
Thus ensures quick convergence and avoid count to infinity problem.

IV. CONCLUSION

Fast convergence and rerouting of packets, following a router failure based on SSRT in a campus network using 2-port router, is the main objective of this paper. Here we have proposed an algorithm that is capable of performing an immediate and transparent recovery from a router or link failure of the campus networks and converge very quickly. Building of routing tables based on the number of hop count has been considered but not on the link cost or congestion of the network which is the future research scope.

REFERENCES

[1] A.S. Tenenbaum,”Computer Networks”, 4th Ed., Pearson Education Asea,LPE,2003

[2] J.F. Kurose and K.W. Ross,”Computer Networking :A Top-Down Approach Featuring the nternet”,3rd Ed., Pearson Educatio Asea,LPE,2005.

[3] B. A. Forouzan, ” Data Communications ad Networking”, 4th Ed., Tata McGraw-Hill, New Delhi, 2004.

[4] Metcalfe, R.M ad Boggs, D.R, “Ethernet: Distributed Packet Switching for Local Computer Networks”, Communication of the ACM. Vol 19, pp 395-404, July 1976.

[5] Spurgeon, C.E., “Ethernet-The Definite Guide”, Orielly/Shroff Publishers and distributorsIndia, 2000.

[6] A Leon-Garcia ad Indra Widjaja, ”Communication Networks”, 2nd Ed., Tata McGraw-Hill, New Delhi, 2004.

[7] L. L. Peterson ad B.S. Davie, ”Computer Networks: A systems Approach”, 3rd Ed. Morgan Kaufman, 2003.

[8] S.K. Ray and S.Roy,”Building Large Private Networks with Plug-n-Play Binary IP 2-port routers”,Proc. NCC 2008 held at IIT, Bombay during Feb 01-03,2008, pp. 354-358

[9] S.K. Ray, J. Kumar, S. K. Sen ad J. Nath, ”Modified Distance Vector Routing Scheme for a MANET”, Proc. of the 13th National Conference on Communications (NCC) held at IIT, Kanpur during Jan 26-28, 2007, pp. 197-201.

[10] S. K. Sen, “An improved Network Routing Scheme Based on Distance Vector Routing”, Ph.D (Engg.) Thesis of Jadavpur University,2009.

[11] Audun Fosselie Hansen, “Fast Reroute in IP Networks,” Doctoral Dissertation at the University of Oslo, May 2007.

[12] S. Bryant, M. Shand,”IP Fast Reroute Framework,” internet Draft , Internet Engineering Task Force, January, 2010.

[13] S. Halder, S Roy, “Fast Convergence IP Routing Scheme Based on Special Nodes using 2-Port Router in Campus Network” International Journal of Engineering Research and Technology, Vol. 4 Issue 11, 2015, pp. 578-583.

[14] S. Bryant, M. Shand, and S. Previdi, “IP fast reroute using not-via addresses,” Internet Draft (work in progress), Oct. 2005, draft-bryantshand-IPFRR-notvia-addresses-01.txt.