Fast Convergence IP Routing Scheme based on Special Nodes using 2-Port Router in Campus Network

Sanjib Halder
Assistant Professor
Department of Computer Science
The Bhawanipur Education Society College
Kolkata, India

Siddhartha Roy
Assistant Professor
Department of Computer Science
Shree Agrasain College
Liluah Howrah, India

***Abstract*—Failure recovery in the internet is most crucial factor. Failure of an IP router cannot be completely avoided. Due to failure, many events are associated with the network, topological changes, loss of packet, recovery the routing table, local reconfiguration of the network followed by the global reconfiguration of the network are required. Network failure can be caused by a variety of reasons such as a router fails, one of its connecting cables snaps or a router is deliberately withdrawn (disconnected). Under such a failure condition, a router does not perform its forwarding and delivery function. A fast convergence scheme to this problem is extremely important for the smooth operation of the network. The main approach used by today's IP routers is route recalculation and routing table update to recover from failure. However, route recalculation and routing table build up could take considerable amount of time during which a large number of packets will be routed wrongly. The strategy we have taken is to pre-calculate and store back-up routes in advance and to automatically switch to the backup routes when a failure occurs. More over study of special neighbourhood concept detecting by the router make the recovery of the IP network reasonably fast and recovers immediately from the router failure. Detecting special neighbor reduce the unnecessary recalculate of routing table. We propose a very simple design scheme how router detects a special neighbor and quickly converge due to failure of a router.**

Index Terms* — *2-port router, campus network, fast convergence, network failure recovery, special neighbour.

I. INTRODUCTION

A computer network is a collection of multiple autonomous computers which are interconnected by communication links and can thus exchange messages between themselves. A computer network allows its users to share the resources available on the various computers connected to the network[1],[3]. The early activities in the area of computer networking were developed by the ARPANET and Digital Equipment Corporation's DECNET, etc., in the late sixties and early seventies. Due to reduce cost of hardware, an increasing number of networks were built and installed worldwide during the decade of the seventies [2]. All these networks were wide area networks (WAN), i.e. they covered wide areas. In the late seventies, technology of the first local area network (LAN) was invented and it was called Ethernet. Though many WAN technologies, LAN technologies exists, Ethernet has become so widely used due to simplicity, low-cost, high reliability [4],[5].

In our thesis we have designed an alternative approach to build an IP-based internetwork of Ethernet LANs in a campus using 2-port IP routers" as the internetworking relays. Basically, the routing scheme itself has utilized the fundamental philosophy in the design of the IP addresses and IP routing. Packets have been hopped from one LAN to a neighbouring LAN, from there to another neighbouring LAN, and so on by routers. Routers on a network have been assumed to run a distributed algorithm among them to decide who should forward the packet by checking whether the net-id of the destination LAN is included in the Routing Table. The simple and widely used DVR algorithm (DVRA) has been basically employed as the basis of the routing protocol, but it has various drawbacks, like poor convergence problem, Count To Infinity problem following a router [1],[3]failure, etc. In this paper we design the scheme of 2-port router to quickly converge the routing table from its backup route without recalculating its routing table.We design the scheme in such a way that router will save two back up routes in addition with its shortest path route in its routing table. Moreover, use of the concept of utilizing special neighbours has made the internetwork quickly converge following a router failure.

II. LITERATURE SURVEY

In a computer network, a message from the source host to the destination host is almost always transported across the subnet as a sequence of packets and such networks are called packet-switched networks. For this purpose, the original message of the sender (i.e, the source host) is fragmented into multiple packets which are transported across the packet-switched network by devices which are called switches or routers and the packets are delivered to the receiver (i.e., the destination host). Efficient transportation of a packet requires choosing the optimal route or the shortest path which is the best sequence of links for the packet to traverse in reaching the destination host from the source host[6]. Obviously, all the packets belonging to a message or a session will then reach their destination in order because the route remains unchanged for all packets in the message or a session. Some commonly used routing algorithms. The Distance Vector Routing Algorithm (DVRA) is a dynamic (adaptive), distributed (decentralized), routing tables are continuously updated with the information received from the neighbouring routers. The DVRA requires each router to periodically compute its shortest path to every other router in the network and exchange these distance information, in the form of a DVT, with its neighbours and thereby update its own routing table (DVRT). This DVRT updation process is continued till a stable DVRT is obtained which the router can then use to forward packets to other routers. In case any change occurs in its DVRT, the router immediately sends its correspondingly changed DVT to all its neighbours. Receipt of this updated DVT triggers the neighbours to immediately recompute their respective DVRTs. If this triggered update (TU) brings about any change in the DVRT of any of the neighbours, the latter immediately sends its updated DVT to all its neighbours which may, in turn, result in further TUs. Though DVRA is a simple technique, it suffers from various problems like Count-To-Infinity (CTI) Problem, Slow Convergence Problem and Oscillation Problem [1],[3]. Specially, DVRA suffers from the serious CTI problem following a link or router failure, due to unending loops involving two or more routers. The basic problem that gives rise to the CTI problem is that two or more routers mutually believe each other or one another when each claims to provide a route to a destination, the reality being that none has a route to that destination[2]. The slow convergence phenomenon actually results from the propagation of bad news and never from a propagation of good news. A bad news implies a loss or increased distance of a route; where as a good news implies the gain (joining of a new router) or reduced distance of a route. In the DVRA, the bad news travel slowly unlike the good news. If a router advertises a shorter route to some destination, all receiving routers respond quickly to install that route. But if a router stops advertising a route, the protocol has to look for the new shortest path and must depend on a time out mechanism before it can declare the route is unreachable. Besides slow convergence, another important problem of the DVR or compatible shortest path routing protocols is that because of the need to always use the shortest path, there may be frequent switching of routes caused by even small increase or decrease in the link costs. This frequent route switching gives rise to instability in routing and this problem is known as the route oscillation problem. The route oscillation problem degrades overall performance of a network and hence some mechanism is required to dampen the oscillation, i.e., to reduce the frequency of route switching. It should be noted in this context that if hop count is used as the metric in the DVR, then the route oscillation problem does not arise at all because the traffic changes which cause changes in the link delays are ignored.

Since CTI, is a serious problem of the DVRA, various ways to modify the DVRA has been proposed for solving the CTI problem under all conditions."Hold-down" or delaying, with the help of a timer, the process of switching to an alternative path following a link failure or a router failure, does not often prevent the CTI[7]; it further slows down the process of convergence in case CTI does not occur. "Split Horizon" requires a router R_j not to include the entry for a destination R_i while sending its DVT to the neighbor R_k if R_j presently reaches R_i via R_k itself. In a slightly different version of Split Horizon, called "Split Horizon with Poisoned Reverse", R_j does send the distance to R_k in case R_k loses communication with Ri. The purpose in both the versions of Split Horizon is to prevent R_k from ever sending packet destined to R_i via R_j itself so that looping does not occur.

Only two algorithms really make the DVRA free from looping, the first one is the Diffusing Update Algorithm (DUAL) It uses the concept of upstream neighbor (predecessor) and downstream neighbor (successor) but due to extremely complex algorithm , DUAL is not well accepted. The other algorithm that avoids the looping problem and the CTI problem is the path vector routing algorithm that is used in Border Gateway Protocol (BGP). A router R_j in the BGP reports its entire path for reaching a certain destination R_i to all its neighbours along with the distance (in hops) so that each neighbor can check this path vector and avoid any possible looping by ignoring this entire path if its own identity is included in the path. Though relatively simple in idea, the implementation is obviously much expensive in respect of storage, computation and communication costs if the network is large.

In a relatively recent research, 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 employed in designing a new routing algorithm for MANET [9],[10], and in designing a modified BGP for achieving a faster convergence. In the MDVRA, as the first modification, instead of the DVT each router sends to its every neighbor its DVRT itself which, additionally contains the Next-Hop (NH) information of the router to reach every destination.

III. DESIGN PRINCIPLE FOR THE 2-PORT ROUTER

In order to achieve fast convergence we first explain the basic design features of 2 port router as follows.

i. Each router in the Campus Network has two ports which connect two different LANs. The two ports of thet router on its two adjacent LANs are called the "Conjugate_ Port" of each other while a port on any given LAN is called the adjacent_ port of every other port on that same LAN. Two routers are called Adjacent_Routers of each other if one port of each of these two routers are adjacent port on a LAN. The other two ports of the two routers will be connected to two other LANs, because parallel connection of two routers is ruled out in our design. Thus each router can have two sets of adjacent-Routers, one set for each adjacent LAN.

ii. Each router has one processor and a buffer to store its routing table. Being two-port router, it has no switching fabric and each port acts as an I/O port.

iii. Each router employs the concepts of the well known Distance Vector Routing Algorithm (DVRA) to build and maintain the Steady State Routing Table (SSRT) for its two adjacent LANs which are peer LANs by exchanging routing information with its adjacent-routers on each of the two adjacent LANs[8]. LAN-to-LAN hop count is used as the path distance metric for determining the shortest path. SSRT exchange is carried out between each port and its conjugate port on one hand and between adjacent port on eachhcp LAN, on the other. It should be noted that since hop count is used as the distance metric, the distances in the DVRA change only with topological changes like a new router joining the internet or an existing router fails or is withdrawn from the internet. Traffic changes have no effect on the routing.

iv. For each LAN, based on the SSRT of the LAN, a Forwarding Destination LAN List (FDLL) is created for each individual port on the LAN, i.e., effectively, for each incident router on the LAN. The goal of creating separate FDLL for each port on the LAN is to distribute the job of forwarding all packets from this LAN to all possible destination LANs among all the adjacent port (i.e., effectively, the adjacent-routers) on the LAN and this partitioning is done on the shortest path basis. When a packet arrives on the LAN for being forwarded then each router knows from its FDLL whether it has to forward the frame (via its conjugate_ port) or just discard the frame. The FDLLs thus ensure, in a distributed and cooperative manner, that each packet arriving at a LAN for being forwarded is actually forwarded and is forwarded via the shortest path computed by the DVRA.

v. For every LAN, the first joining router(FJR) act as a packet delivery agent to deliver each data packet, that arrives on the LAN for deliver, to the destination host on the LAN.

Each router self-assigns the static IP address of its two ports automatically [8]. In this context, it should be mentioned that when the first router joins a LAN it becomes both the FJR and the Most Recently Connected Router(MRCR) of the LAN. Similarly, each router self adjusts (i.e., self-reassigns) its IP address[8] for a port when any of its adjacent-routers on its either LAN fails or is deliberately withdrawn.

IV. RECOVERY SCHEME DUE TO ROUTER FAILURE

Network failure can be caused by one of the following reasons, like router failure (or one of its port failure) or link failure or a router is withdrawn deliberately (disconnected). Under one of the such condition, a router does not perform its forwarding and delivery function through its ports 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 recalculation of 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 will be routed wrongly. The strategy we have taken is to pre-calculate and store back-up routes in advance and to automatically switch to the backup routes when a failure occurs. Periodic monitoring is carried out in the campus network by the FJR to detect router failure or port failure automatically and to forward the affected packets immediately through the back up route.

In this section we study a special neighbour which may be very useful in the Campus Network in case of network failure. The concept of this special neighbour has been derived from the concept of special neighbours in the MDVRA[9],[10]. Unlike the MDVRA we assume that in the Campus Network each LAN is represented by a node and each router is represented by a link. For quick convergence of the campus network, we identify a special neighbour, namely Single connected Component LAN (SCCL) and illustrate its utilization. In the following section we first describe the concept of SCCL, then its identification and finally its utilization. This special neighbour can be utilized for quick convergence of the Campus Network following a router failure.

In a campus network having N nodes a router, at any time, views the entire network as being composed of exactly two partitions or components, as the router is a two port router.

In the Fig **(Fig 1.)** the router R2 views the whole network as two partitions or component named component R2L2 and component R2L3.

Now a component is a Single-Connected Component LAN (SCCL) with respect to a router $R_{i,}$ if the failure of the router R_i or the link from the either side, physically divides the entire network into two disjoint parts. Under such condition no LAN (a node) in one parts or component of the entire network will be able to communicate with the other parts of the network and vice a versa. In the fig below if the router R2 or any of its two links fail then the entire network is divided into two components namely component R2L2 and component R2L3. So the router R2 has two SCCLs are connected on its either side.

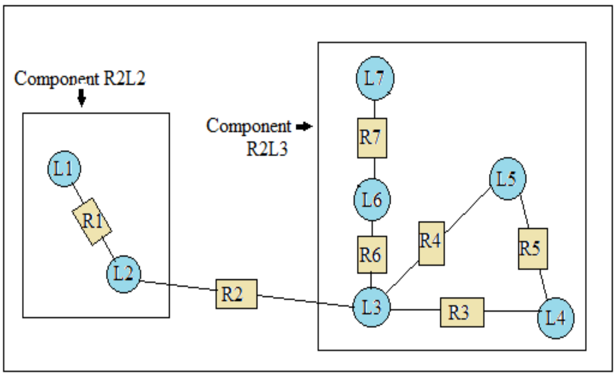

Fig 1: An example network to illustrate the failure of a link between L2 and L3.

A. Identifications

Unlike Campus Network here all the routers maintain one more table, apart from SSRT, containing the information regarding SSCL. While a new router fills up its SSRT, it will identify whether the destination LANs passing through it, are single connected component LAN (SCCL) or multi connected component LAN (MCCL) by consulting its backup entry.

Empty back up in the SSRT signifies that the destination LAN is SCCL. In that case it sends a special augmented message, namely single connected component members (SCCM) containing the member of the identified SCCL along with the updated SSRT to its adjacent LANs. On receiving the message SCCM, all routers connected to that adjoining LAN store the information about SCCL

B. Utilization

While failure occurs, the router owning the MRCR in the victim LAN first check whether SCCL flag is set for the failed router (or link) or not.

If SCCL flag is set, it 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.

In order to illustrate the utilization of an SCCL, let us consider the Fig 1. having 7 LANs and 7 two port routers namely L1, L2, L3………L7 and R1, R2, R3……………R7 . The component R2L2 (containing 2 LANs namely L1 & L2, and 1 router namely R1), and the component R2L3 (containing 5 LANs namely L3, L4, L5, L6 & L7, and 5 routers namely R3, R4, R5, R6, R7) are two SCCLs with respect to router R2. The router R2 detects this fact and send the information to its corresponding adjacent LANs L2 and L3. So that the routers R1, R3, R4 and R6 are kept informed about this fact.

Table 1 shows the contents of both the tables 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> signifies the 1st order back path and corresponding forwarding port. For example, the router R2 maintains table c1, c2 for one port and d1, d2 for another port. Table c1 contains the distance (hop count) and forwarding ports to reach different destination LANs. It also contains backup routes (if any) in terms of hop count and forwarding port. Another table ie c2 contains the information regarding SCCL. The value in the column SCCL_FLAG is 1 if there exists a SCCL through the corresponding router. The next column ie L# contains the list of LANs that are included in the SCCL. If the column SCCL_FLAG contains 0 signifies that there is no SCCL through the corresponding router. In case of table c2 there exists two SCCL. One through R2 and another through R6.

TABLE 1 SSRT AND SCCM OF ALL LANS AT A STABLE STATE.

SSRT(L1)

L#	*d*	*FI*	*1d*	*1FI*
L1	-	-	-	-
L2	1	FI11	-	-
L3	2	FI11	-	-
L4	3	FI11	-	-
L5	3	FI11	-	-
L6	3	FI11	-	-
L7	4	FI11	-	-

(a1)

SCCM(L1)

R#	*SCCL_FLAG*	*L#*
R1	1	L2, L3, L4, L5, L6, L7

(a2)

SSRT(L2)

L#	*D*	*FP*	*1d*	*1FP*
L1	1	FP12		
L2	-	-	-	-
L3	1	FP22	-	-
L4	2	FP22	-	-
L5	2	FP22	-	-
L6	2	FP22	-	-
L7	3	FP22	-	-

(b1)

SCCM(L2)

R#	*SCCL_FLAG*	*L#*
R1	1	L1
R2	1	L3, L4, L5, L6, L7

(b2)

SSRT(L3)

L#	*d*	*FP*	*1d*	*1FP*
L1	2	FP23	-	-
L2	1	FP23	-	-
L3	-	-	-	-
L4	1	FP33	2	FP43
L5	1	FP43	2	FP33
L6	1	FP63	-	-
L7	2	FP63	-	-

(c1)

SCCM(L3)

R#	*SCCL_FLAG*	*L#*
R2	1	L2, L1
R3	0	-
R4	0	-
R6	1	L6, L7

(c2)

SSRT(L4)

L#	*d*	*FP*	*1d*	*1FP*
L1	3	FP34	4	FP54
L2	2	FP34	3	FP54
L3	1	FP34	2	FP54
L4	-	-	-	-
L5	1	FP54	2	FP34
L6	2	FP34	3	FP54
L7	3	FP34	4	FP54

(d1)

SCCM(L4)

R#	*SCCL_FLAG*	*L#*
R3	0	-
R5	0	-

(d2)

SSRT(L5)				
L#	***d***	***FP***	***1d***	***1FP***
L1		FP45	4	FP55
L2	2	FP45	3	FP55
L3	1	FP45	2	FP55
L4	1	FP55	2	FP45
L5	-	-	-	-
L6	2	FP45	3	FP55
L7	3	FP45	4	FP55

(e1)

SCCM(L5)		
R#	***SCCL_FLAG***	***L#***
R4	0	-
R5	0	-

(e2)

SSRT(L6)				
L#	***d***	***FP***	***1d***	***1FP***
L1	3	FP66	-	-
L2	2	FP66	-	-
L3	1	FP66	-	-
L4	2	FP66	-	-
L5	2	FP66	-	-
L6	-	-	-	-
L7	1	FP76	-	-

(f1)

SCCM(L6)		
R#	***SCCL_FLAG***	***L#***
R6	1	L1, L2, L3, L4, L5
R7	0	-

(f2)

SSRT(L7)				
L#	***d***	***FP***	***1d***	***1FP***
L1	4	FP77	-	-
L2	3	FP77	-	-
L3	2	FP77	-	-
L4	3	FP77	-	-
L5	3	FP77	-	-
L6	1	FP77	-	-
L7	-	-	-	-

(g1)

SCCM(L7)		
R#	***SCCL_FLAG***	***L#***
R7	1	L1, L2, L3, L4, L5, L6

(g2)

Now at any point of time during a monitoring cycle, if the router R6 owing the MRCR in L3 detects the failure of R2, 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 R1owning the MRCR FP_{12} in L2 and the router R6 owning the MRCR FP_{63} in L3detects the failure of the router R2, immediately check their SCCM table to find any SCCL through the router R2. By inspecting the SCCM (L2), the router R1 finds a SCCL (containing the LANs L3, L4, L5, L6, and L7) which is now lost destinations (LDs). Similarly by inspecting the SCCM (L3), the router R6 finds a SCCL (containing the LANs L1, L2) which is now lost destinations (LDs). So the entries related to LDs are deleted from the corresponding tables as shown in the table 2 below.

Step 2: The MRCR s will also broadcast a special message containing the list of LANs $\in$SCCL to all other routers. On receiving the message, all other routers, without further delay, update their SSRT and SCCM by deleting the corresponding entry to the SCCL. Thus ensures quick convergence and avoid count to infinity problem.

Table 2: Modification of SSRTs and SCCMs following the failure of the router R2.

SSRT(L2)				
L#	***D***	***FP***	***1d***	***1FP***
L1	1	FP12		
L2	-	-	-	-
L3	1	FP22	-	-
L4	2	FP22	-	-
L5	2	FP22	-	-
L6	2	FP22	-	-
L7	3	FI22	-	-

(a) Before failure

⇩

SSRT(L2)				
L#	***D***	***FI***	***1d***	***1FI***
L1	1	FI12		
L2	-	-	-	-

(b) After failure

SCCM(L2)		
R#	***SCCL_FLAG***	***L#***
R1	0	
R2	1	L3, L4, L5, L6, L7

(a1) Before failure

⇩

SCCM(L2)		
R#	***SCCL_FLAG***	***L#***
R1	0	-

(b1) After Failure

V.CONCLUSION

Fast convergence and re-routing, following a router failure in a campus network, is the main objective of this paper. Here we have designed a failure recovery scheme based on SSRT and SCCM to perform an immediate recovery from a router or link failure in a campus network. The scheme is free from CTI problem and Oscillation problem as in DVRA. A special neighbor SCCL has been considered for quick automatic failure recovery, but study of more special neighbours is likely to offer more benefits.

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] AudunFosselie Hansen, "Fast Reroute in IP Networks," Doctoral Dissertation at the University of Oslo, May 2007.

[12] S. Bryant, M. Shand,"IP Fast Reroute Framework," internetDraft , Internet Engineering Task Force, January, 2010.