Volume 2, Issue 12, December-2015, pp. 1100-1105 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Avoid Link Failure Using Novel Re-routing Method

[1] Batsala Balaraju, [2] Sahukaru Jayavardhana Rao

[1]M.Tech (CSE), Sri Vaishnavi College of Engineering at Srikakulam
[2]Assistant Professor, Department of Computer Science & Engineering, Sri Vaishnavi College of engineering at srikakulam
balu27772@gmail.com , jayavardhanarao.mca@gmail.com

Abstract : In this paper we present a method to find a path when a link is failure when the data is transmitted for source node to destination node when a link Is failure before entering to the gate way protocol and to recover the response of failure the target application Is tested on small network up to tens of nodes for regional access of the service providers network which is one of the most challenging Task We provide and effective method to find the existing path for the Set of nodes to send the data when the link is failure.

I. INTRODUCTION

VoIP and other real-time applications require un-interrupted service from the network. It is shown that the current backbone network can deliver PSTN quality voice service with regard to delay and loss during normal condition [1]. However, it also shows that link and router failures can significantly impact a VoIP service, though infrequently. . Since reconvergence of an Interior Gateway Protocol (IGP) (e.g., OSPF or IS-IS) can take hundreds of milliseconds, there is a need for a method that will find an alternate path in less time than this. The target application is a small (up to tens of nodes) access sub network of a service provider's network, which is a typical scale encountered in practice; a service provider typically has many such small regional accessnetworks.Consider a source nodes sending data to destination noded.Suppose some link(i, j)on the shortest path from s to d fails. An IGP will find an alternate path from s to d that avoids (i, j)(assume such a path exists). However, IGP re-convergence may take hundreds of milliseconds or even seconds, and the packet loss during this time period may be unacceptable.FastRe-Route(FRR) methods establish a new path from to din much less time than required for IGP re-convergence. There are several available FRR methods. One method, used in conjunction with label-based forwarding (e.g., LDP), Creates an RSVP [6] primary tunnel between each pair of nodes. In addition, a bypass tunnel is pre-defined for each arc (i, j); the bypass tunnel for (i, j) is a path from i toj that is physically disjoint from the link (i, j). When the packet reaches nodeiandlink (i, j) has failed, a local repair forwards the traffic along the bypass tunnel for (i, j); when the packet reaches node j, it continues on the path defined by the RSVP primary tunnel. The disadvantage of this approaches that, for a network of NnodesandAarcs, N (N−1) unidirectional primary tunnels and2Auni-directional bypass tunnels are required. An alternative to building tunnels is to use aLoopFreeAlternative (LFA) method ([2], [4]). For any two nodesiandj, let c (i, j) be the minimal distance betweeniandj. Supposenodenis a neighbor of s(i.e., they are connected by a single arc). Then the neighbornofsis an LFA for destination (1) Thatis, nis an LFA if the shortest path from ntoddoesnot return to son the arc(n, s). To ascertain whether an Flautists for a givensanddit suffices to determine if (1) holds for some neighbornofs.A simple example where LFAs always exist is a three node network whose arc lengths satisfy the triangle inequality.

Most current backbone ISPs use Link-State pro-tocol, OSPF [2] or IS-IS [3], as their Intra-domain Routing Protocol (i.e. IGP, Interior Gateway Proto-col). When a link fails the adjacent routers flood Link State Advertisements (LSAs) through the net-work notifying the failure. Routers recalculate their routing tables to route around the failure. We call this procedure as *IGP*

convergence that usually takes seconds. During IGP convergence, packets originally routed along the link are likely to be dropped by the adjacent routers or by other routers because of transient routing loops.

To minimize the detrimental effect of link/node failures to real-time applications like VoIP, there is a requirement to provide a rerouting mechanism during IGP convergence. Compared to traditional IGP rerouting, i.e. LSA flooding and global recalculation of routing tables, we call rerouting during IGP convergence as *Fast Rerouting*. In this paper, we propose a Fast Rerouting ex-tension for Link State IGP protocols. By exploiting properties of shortest path trees, our approach has achieved a new tradeoff between complexity and response time to link failures.

II. RELATED WORK

The most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system. Tables.

The calculation of routing table **Network topology** is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological [3] structure of a network and may be depicted physically or logically. *Physical topology* is the placement of the various components of a network, including device location and cable installation, while *logical topology* illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

An example is a local area network (LAN): Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

Link protection is designed to safeguard networks from failure. Failures in high-speed networks have always been a concern of utmost importance. A single fiber cut can lead to heavy losses of traffic and protection-switching techniques have been used as the key source to ensure survivability in such networks. Survivability can be addressed in many layers in a network and protection can be performed at the physical layer (SONET/SDH, Optical Transport Network), Layer 2 (Ethernet, MPLS) and Layer 3 (IP).

Protection architectures like Path protection and Link protection safeguard the above-mentioned networks from different kinds of failures. In path protection, a backup path is used from the source to its destination to bypass the failure. In Link protection, the end nodes of the failed link initiate the protection. These nodes detect the fault and are responsible to initiate the protection mechanisms in order to detour the affected traffic from the failed link onto predetermined reserved paths. Other types of protection are channel-, segment- and p-cycle protection.

Link State Packet (LSP) is a packet of information generated by a network router in a link state routing protocol that lists the router's neighbors. Link state packet can also be further defined as special datagram's that determine the names of and the cost or distance to any neighboring routers and associated networks. They are used to efficiently determine what the new neighbor is, if a link failure occurs, and the cost of changing a link if the need arises. LSPs are queued for transmission, and must time out at about the same time. They must be acknowledged, and can be distributed throughout the network, but cannot use the routing database. An Interior Gateway Protocol (IGP) is a type of protocol used for exchanging routing information between gateways (commonly routers) within an Autonomous System (for example, a system of corporate local area networks). This routing information can then be used to route network-level protocols like IP.

Interior gateway protocols can be divided into two categories: distance-vector routing protocols and link-state routing protocols. Specific examples of IGP protocols include Open Shortest Path First (OSPF),

Routing Information Protocol (RIP) and Intermediate System to Intermediate System (IS-IS).

Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet. For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network .[14]

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of sub networks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully-connected IP overlay network to the underlying ones. Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually map) indexed by keys. Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as Insert, Diffuser, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination. And the update of forwarding tables increase the response time of the algorithm to link failures and increases the work load of the router. In contrast, our scheme calculates rerouting paths beforehand and does not need to update forwarding tables, thus has faster response to link failures. One advantage of the above two approaches is that they do not require data plane changes. Our approach needs to modify the data plane, but the added overhead is not high.

III. FAST REROUTING SCHEME

Fast Reroute Method:

We now present the details of the method. Let $G = (N,A)$ be an undirected connected graph with node set N and arc set A. For $x \in N$, let $N(x)$ is the set of neighbors of x, where a neighbor of x is a node one arc away from x. We associate with each undirected arc $(i, j) \in A$ a cost $c(i, j)$, and require each $c(i, j)$ to be a positive integer. (The integer valued restriction can always be met by approximating, to the desired accuracy, each arc cost by an improper fraction, and then multiplying all the fractions by the least common multiple of the fraction denominators.) For $i, j \in N$, let $c\_(i, j)$ be the cost of the shortest path in G between i and j. When using *Route*(s, d) for fast re-route in the event of an arc failure, which is the target application, $c\_(i, j)$ represents the shortest path cost *before* the IGP has reconverted in response to the link failure

Multipath Routing:

Multipath routing is a promising routing scheme to accommodate these requirements by using multiple pairs of routes between a source and a destination. Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Extensive research has been done on multipath routing techniques.

Failure Recovery:

Techniques developed for fast recovery from single-link failures provide more than one forwarding edge to route a packet to a destination. Whenever the default forwarding edge fails or a packet is received from the node attached to the default forwarding edge for the destination, the packets are rerouted on the backup ports. In the authors present a framework for IP fast reroute detailing three candidate solutions for IP fast reroute that have all gained considerable attention. When a forwarding link on a tree fails, the packet may be switched to the other tree. Affected by the failure of (*a, b*) to *h*. Since RPs is usually very short, as shown in Section IV, the cost to setup a RP is not significant.

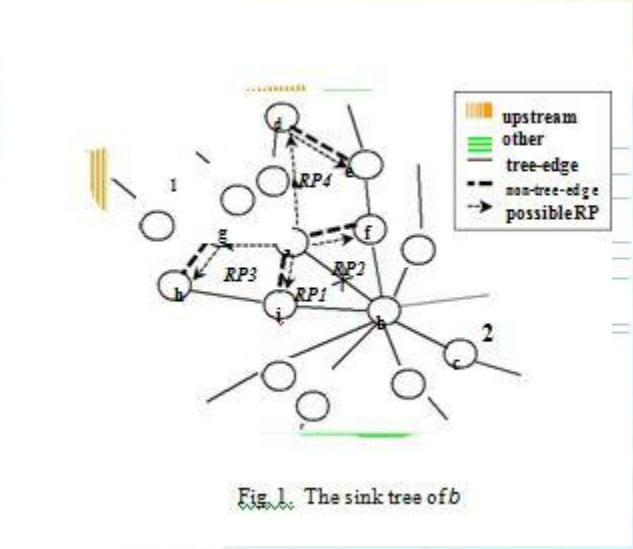

Fig. 1. The sink tree of *b*

B. Calculation of Rerouting Paths

In our scheme, each router calculates a RP based on its sink tree for each of its links on behalf of its neighbor. Its neighbor will use the RP to send affected traffic when the link fails. This choice of RP calculation requires routers to exchange RP information but can avoid routers to calculate sink tree for all its neighbors.

Without losing generality, we describe the algorithm for a router, *b*, to calculate a RP for a link between itself and one of its neighbors, *a*, as shown in Figure 1.

In the sink tree of *b*, we use BFS (Breadth First Search) in the sub-tree rooted at *a* to search for a RP for *a* and link (*a, b*). We call this sub-tree as the *upstream* area for link (*a, b*). During the search, at each node we check every neighbor of it. If the neighbor is not an upstream router, it is a FNH. As mentioned before, our scheme chooses the *nearest FNH* for rerouting. When there are ECMPs (Equal Cost Multi-Paths) between *a* and the *exit* node we use all of them as part of the RP. We can always find a RP for a given link as long as the network is not partitioned. (See [10] for the algorithm.)

Using this method we actually find a rerouting path for traffic with destination of *b*. But as Theo-rem 1 shows, this type of RPs can be safely used for all traffic originally forwarded to *b* by *a*.

Theorem 1: Once a packet originally forwarded from *a* to *b* is rerouted to a router outside the upstream area (the 1st part in Figure 1), the packet will be routed along a shortest path without link (*a, b*) to its destination.

Proof: It is obvious for packets that have *b* as its destination.

For a packet heading for a router below *b* , say *c*, it is also true. This can be proved as below: As shown in Figure 1, the shortest path from a nearest FNH, *e*, to *b*, (*e, f, b*), must be shorter than the shortest path from it via *a* to *b*, (*e, a, b*). So the shortest path from *e* to *a* to *b* to *c*, (*e, a, b, c*), is longer than the shortest path from *e* to *b* to *c*, (*e, f, b, c*), i.e. the shortest path from *e* to *a* to *b* to *c* is not the shortest path from *e* to *c*. Therefore, the shortest path from *e* to *c* must not include edge (*a, b*). And it is obvious that the path from *e* to *c* must not include edge (*b, a*).

C. Identification of Affected Traffic

In case there is no local RP, a router on the RP needs to efficiently identify traffic affected by a link failure.

Because there are ECMPs, when a link fails, it is also possible that a destination is not reachable via one next hop but reachable via another next hop. So our scheme decides whether a destination is reachable via a given next hop. In our scheme, a router identifies affected traffic using a simple range checking. It relies on an algorithm that assigns sequence numbers for all nodes in each *first level subtree* (i.e. the subtree under a first level child node) of the local routing tree. Sequence numbers for each subtree are independent. For each subtree, the sequence numbers are from 0 to the number of nodes in the subtree. The algorithm ensures: the sequence numbers of all nodes affected by a node failure and the sequence number of the failed node itself are continuous and thus can be represented as a simple range. In other words, when a node fails, only the nodes with sequence numbers within the *affected range* become unreachable from the root of the subtree. The start of the

affected range of a node is its sequence number. The end of the *affected range* is the largest sequence number of all nodes affected by this node. We call the end of the *affected range* of a node as the *seq end* number. We store the sequence number and the *seq end* number along with each node in the subtree.

A link failure either causes the downstream node of the link to become unreachable from the root of the subtree or does not affect reach ability of any destination. So the destinations affected by a link failure can also be identified using above sequence numbers. We will discuss this further in Section III-D.For a subtree without ECMPs, we can use DFS (Depth First Search) traversal order as the sequence numbers. This is because: in a tree without ECMPs, all descendant nodes are the nodes affected by this node; and they are traversed during the period when this node is traversed.

However, for a subtree with ECMPs, if a node becomes unreachable from the root of the subtree, some of its descendants may be still reachable, because there may be more than one path from the root to the later. We have developed a modified DFS algorithm (Algorithm 1) to assign sequence numbers for nodes in a general subtree (with or without ECMPs).

TABLE I
NOTATIONS

(a, b):	link from a to b
$RP(a, b)$:	Rerouting Path of link (a, b)
T_s:	routing tree of s
$ST(T_s, i)$:	subtree of T_s rooted at i
$P(T_s, n)$:	set of parents of n in T_s
$C(T_s, n)$:	set of children of n in T_s

Algorithm 1 can be described as follows: during the DFS traversal, whenever we encounter a child node having more than one parent, we find the nearest single upstream node whose failure will cause the child node unreachable from the root. We call this upstream node as the *nearest ancestor* of the child node. (The algorithm to find the *nearest ancestor* is a reverse DFS search from the node to the root. See [10] for details.) We enquire the child node to the *deferred DFS queue* of its *nearest ancestor*. After that we continue the DFS search for other children. After searching all its children, we call this modified DFS algorithm for the nodes in the local deferred DFS queue one by one. Similar to subtree without ECMPs, the sequence number of each node is its traversal order. Figure 2 shows the result of Algorithm 1 on a simple topology.

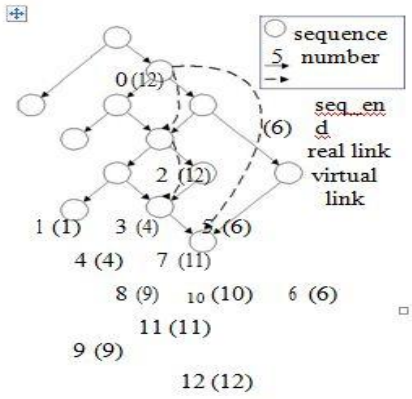

Fig. 2. Sequence numbers of nodes in a subtree tree

IV. FUTURE WORK

First, we plan to use more than one RPs to split rerouted traffic for load balancing. Second, we plan to enhance our algorithm to detect multiple link failures and node failures. In such cases we should avoid fast rerouting and rely on the original IGP convergence mechanism.

V. CONCLUSIONS

We have proposed a Fast Rerouting scheme for OSPF/IS-IS networks in this paper. We have developed efficient algorithms for calculation of Rerouting Path, and identification of affected traffic. The rerouting operation for each packet is comparable to basic IP forwarding. Simulation results show that, assuming there is one link failure at a time which accounts for a large portion of network failures, our scheme achieves fast response to link failures and the path elongation compared to optimal path is not significant.

REFERENCES

[1] C. Boutremans and G. Iannaccone and C. Diot, *Impact of link failures on VoIP performance*, NOSSDAV, 2002.
[2] J. Moy, *OSPF Version 2*, RFC 2328, Apr. 1998.

[3] D. Oran, *OSI IS-IS Intra-domain Routing Protocol*, RFC 1142, Feb. 1990.

[4] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. Chuah, C. Diot, *Characterization of Link Failures in an IP Backbone*, INFOCOM 2004.

[5] N. Dubois, B. Fondeviole, N. Michel, *Fast convergence project*, RIPE-47 presentation, Jan. 2004.

[6] P. Pan, G. Swallow, A. Atlas, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*, Internet Draft, Feb. 2004.

[7] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, *Failure Insensitive Routing for Ensuring Service Availability*, IWQoS 2003.

[8] P. Narvaez,´ K.-Y. Siu, and H.-Y. Tzeng, *Local Restoration Algorithm for Link-State Routing Protocols*, ICCCN 1999.

[9] A. Medina, A. Lakhina, I. Matta, and J. Byers, *BRITE: An Approach to Universal Topology Generation*, In Proceedings of MASCOTS 2001, Aug. 2001.

[10] Y. Liu, A. L. Narasimha Reddy, A Fast Rerouting Scheme for OSPF/IS-IS Networks, technical report available at http://ece.tamu.edu/techpubs, Dept. of Electrical Engineer-ing, Texas A&M University, 2004

