Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Study on Causes and Effects of Link Failures in TCP/IP Network

Asma Parveen
Research Scholar
Computer Science & Engineering
JJT University, jhunjhunu, Rajasthan, India,

Dr. Mohammed Abdul Waheed
Associate Professor
Computer Science & Engineering
VTU Regional office, Gulbarga, Karnataka, India

Abstract— In recent years the Internet has been transformed from a special purpose network to a ubiquitous platform for a wide range of everyday communication services. It is observed that link failures occur as part of everyday operation, and the majority of them are short-lived (less than 10 minutes). This paper presents a detailed study of effects and causes and impact of link failures in TCP/IP network. We also discuss various statistics such as the, distribution of inter-failure time, distribution of link failure durations, classification of link failures etc. which are essential for constructing a realistic no- link failure model.

Keywords—Link failure, TCP/IP network, Transmission, packet loss, Protection.

I. INTRODUCTION

FAILURE in a system is a very common scenario to face. Since networking system is very much sophisticated, the failure is somewhat very natural and high in this case. Failure may occur between two nodes in a transmitted path; again total path can be failed by at situation. Thus a network failure in such system may seriously impair service continuity to a countless number of users. So, network survivability is essential.

The first step towards defining and measuring internet service availability is to develop a detailed understanding the reason for the failures in a network, how often failures occur, how long they last, and how each such failure leaves an impact on the service.

TCP has received tremendous attention due to its use as the reliable data transfer on the Internet. An underlying assumption about TCP is very low packet loss. Further, it is assumed that loss indicates congestion. As such, congestion control mechanisms are triggered to keep the throughput high so as to minimize the impact of packet loss. Most of the current work focuses on improvements to TCP performance using this paradigm. On the other hand, packet loss and/or congestion (or perceived congestion) can be manifested in a variety of ways. An example is the congested situation that can arise due to a network link failure. When a link fails in a network, the traffic is rerouted around the failure leading to congestion on a link (or multiple links) which will suddenly see heavier traffic than before. In the case of TCP, it can also cause out of sequence arrival at the destination, and/or unusual packet loss (which can then be”seen” by TCP as a congestion). To which links the traffic will be rerouted primarily depends on the network layer handling, mainly on the routing algorithm and the routing protocol in place [1].

II. LITERATURE REVIEW

In [2], Tipper *et al* have presented an excellent discussion on the transient effect of a link failure in a generic virtual-circuit based packet network. While the impact on the traffic performance due to a failure in the *presence* of routing has received considerable attention in circuit-switched networks (that employ dynamic routing) and virtual-circuit based packet networks [2], [3], 4], it has received little attention in the case of TCP/IP network. Labovitz et. *al.* [5] have shown that network instability on the Internet, caused mainly by the underlying transient physical and data link problems, can affect the routing protocols leading to routing instability. Examples of routing instability are route loops, routing fluctuations, route oscillations, synchronization and so on.

Whenever connectivity between two directly connected routers is lost, each router independently broadcasts an “adjacency down” LSP (Link State PDUs) through the network. When the connectivity is restored, each router broadcasts an “adjacency up” LSP. Note that the loss of connectivity at the IP level may be triggered by a variety of causes such as an optical fiber cut, router interface failure, IS-IS protocol malfunction, etc. We refer to each such event as a *failure event*.

Each failure event is recorded with the MRTD timestamp of the *first* LSP received at our listener that reports the failure. Both the LSPs reporting the loss of IP connectivity may not reach every router (and our listener) at the same time. Our approach of determining a failure event based on the first LSP received is conformant with how the IS-IS protocol reacts to such failures. As soon as a router receives the first LSP reporting an adjacency down, it considers the IP connectivity to be lost without waiting for the second LSP. Hence the first LSP is sufficient to trigger a route re-computation, which may lead to a disruption in packet forwarding. A failure event ends when our listeners receive an LSP from both ends of the link. This is conformant with how routers handle “adjacency up” LSPs – both LSPs must be received by a router before it considers the IP connectivity to be restored. Our backbone is in constant evolution with new links being added and older ones being decommissioned every week. When a link is decommissioned, “adjacency down” LSPs are broadcast, but there is no subsequent "adjacency up" LSP. On the other hand, when IP connectivity is lost due to a problem with the optical fiber, restoration usually takes a few hours (and sometimes just a few minutes). Connectivity loss due to router or protocol problems is usually restored in less than an hour. In order to distinguish link decommissioning from valid failure events, we consider only those failure events for which we subsequently receive the two "adjacency up" LSPs within the next twenty-four hours.

In WDM (Wavelength Division Multiplexing) network, the failure of a single fiber link may lead to tremendous data loss since a single fiber link can carry a huge amount of data (on the order of terabits per second).Therefore, network survivability is an important problem in network design and its real-time operation. In order to reduce the data loss, various protection and restoration mechanisms have been proposed and studied in the literature to recover traffic after a failure occurs and before the failure is physically repaired [6], [7], [8], [9], [10]. Although the WDM network and wireless ad-hoc settings are quite different in nature, they share a number of problems and challenges. One of them is failures of network components. If a link failure is detected on the primary path (through which actual data transmission is taking place), the source can switch to an alternate path instead of initiating a route discovery/recovery process. A new discovery takes place only when all precomputed paths break. Since in a wireless ad-hoc network has no fixed infrastructure and there is no centralized control over the nodes ; no designated routers. So nodes serve as routers for each other, and data packets are forwarded from node to node in a multi-hop fashion. Protecting the circuits or connections established in such networks against single-link failures may be achieved in two ways: *path protection* or *link protection* [11]. Main focus of this paper is to protect end-to-end connections from dual-link failures using path protection and link protection.

III. CLASSIFICATION OF FAILURES

This section describes our methodology for classifying failures according to their causes and properties.

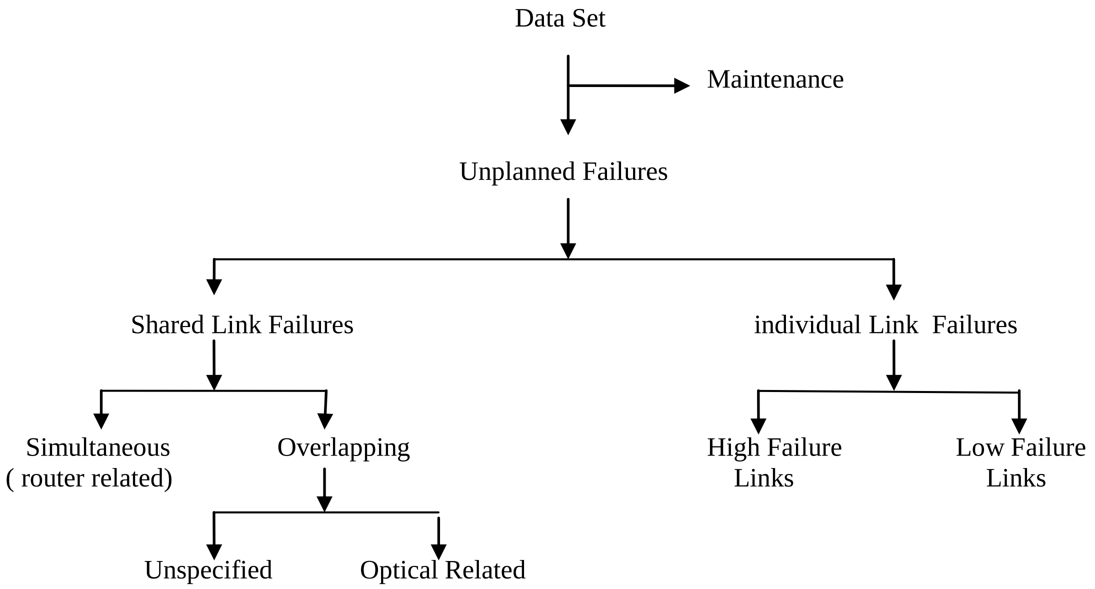


Fig. 1. Classification of failures

We attempt to infer the causes by leveraging patterns observed in the empirical data and by correlating them with the possible causes. we give an overview of our classification .

A. Overview

Our approach is to use several hints obtained from the ISIS failure data to identify groups of failures due to different causes.

Our classification of failures is summarized in Fig. 1 and consists of the following steps. We first separate failures due to scheduled *Maintenance* from *Unplanned* failures, these are the ones that an operator seeks to minimize. We distinguish between *Individual Link Failures* and *Shared Link Failures*, depending on whether only one or multiple links fail at the same time. Shared failures indicate that the involved links share a network component that fails. This component can be located either on a common router (e.g. a line card or route processor in the router) or in the underlying optical infrastructure (a common fiber or optical equipment). Therefore, we further classify shared failures into three categories according to their cause: *Router-Related*, *Optical-Related* and *Unspecified* (for shared failures where the cause cannot be clearly inferred). We divide links with individual failures into *High Failure* and *Low Failure Links* depending on the number of failures per link.

B. Maintenance

Failures resulting from scheduled maintenance activities are unavoidable in any network. Maintenance is usually scheduled during periods of low network usage, in order to minimize the impact on performance.

C. Simultaneous Failures

In the shared failures class, we first identify failures that happen simultaneously on two or more links. Failures on multiple links can start or finish at exactly the same time, when

a router reports them in the same LSP. For example, when a line card fails, a router may send a single LSP to report that all links connected to this line card are going down. When our listener receives this LSP, it will use the timestamp of this LSP as the start for all the reported failures. Similarly, when

a router reboots, it sends an LSP reporting that many of the links connected to it are going up. When our listener receives this LSP, it will use the same timestamp as the end for all the reported failures. (However, it still needs to receive an LSP from the other end to declare the end of a failure.)

D. Overlapping Failures

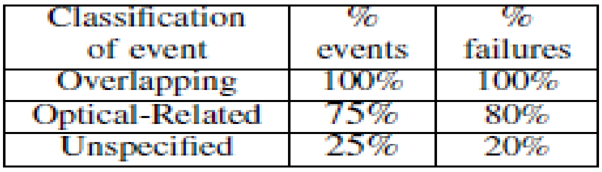
we look for events where all failures start and finish within a time window of a few seconds. Overlapping failures on multiple links can happen when these links share a network component that fails and our listener records the beginning and the end of the failures with some delays *Wstart* and *Wend*. For example, a fiber cut leads to the failure of all IP links over the fiber, but may lead to overlapping failures in our listener for several reasons. First, there are multiple protocol timers involved in the failure notification and in the generation of LSPs by the routers at the ends of the links. Most of these timers are typically on the order of tens of milli-seconds up to a few seconds.

E. Optical-Related

Among all overlapping events, we identify those that involve only inter-POP(Point-of-Presence) links and that do not share a common router. It turns out that 75% of all overlapping events and 80% of all overlapping failures are of this type, see Table I.

TABLE I

SUMMARY OF OVERLAPPING EVENTS



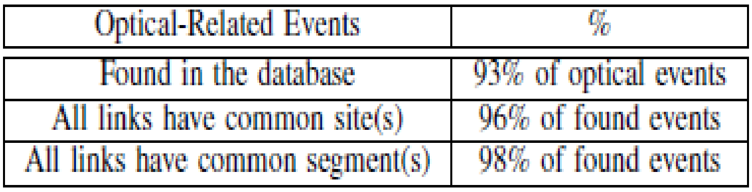
Classification of event	% events	% failures
Overlapping	100%	100%
Optical-Related	75%	80%
Unspecified	25%	20%

We consider those events to be *Optical-Related* for the following reason. Since the links in the same event have no router in common, an explanation for their overlapping failures is that they share some underlying optical component that fails, such as a fiber or another piece of optical equipment.

Table II summarizes findings in the IP-to-Optical database.

TABLE II

USING THE IP-TO-OPTICAL MAPPING TO CONFIRM THAT LINKS IN THE SAME OPTICAL EVENT SHARE AN OPTICAL COMPONENT



Optical-Related Events	%
Found in the database	93% of optical events
All links have common site(s)	96% of found events
All links have common segment(s)	98% of found events

F. Unspecified.

All the overlapping failures that are not classified as optical-related fall in this class. These include overlapping failures on inter-POP links connected to the same router. The cause is ambiguous: they could be due to a problem at the router or to an optical problem. They also include overlapping failures of links in the same POP that could be due to a problem or operation in the POP. However, since we are not able to satisfactorily infer their cause, we call these events *Unspecified.*

They account for only 20% of the overlapping failures (see Table I), which is less than 3% of all the unplanned failures.

G. Individual Link Failures

After excluding all the above classes of failures from the data set, we refer to the remaining failures collectively as *Individual Failures* because they affect only one link at a time. It is difficult to determine the cause of individual failures. High failure links may be in an advanced stage of their lifetime and their components fail frequently; or they may be undergoing an upgrade or testing operation for a period of time. Unlike all previous failure classes, low failure links do not have a prominent pattern either in time or across links. Table III summarizes the contribution of each class to the total number of failures.

IV. CAUSES OF LINK FAILURES

The duration of failure may provide some hints about the possible cause. In Fig. 2, we plot the cumulative distribution of failure durations over the four-month period.

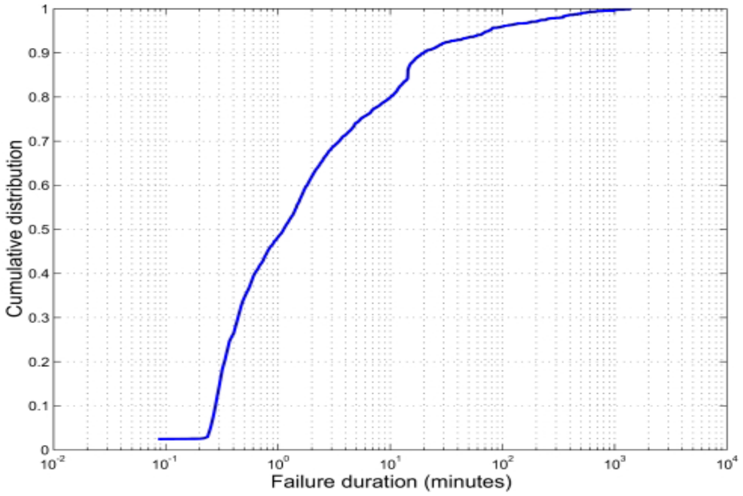


Fig. 2. Duration of failure events

We find that only 10% of failures last longer than 20 minutes. These are possibly caused by fiber cuts and/or equipment failures upgrades. Note that the longest duration for a failure is 24hours since we disregard all failure events where IP connectivity is not restored within 24 hours (Section II). About 40% of the failures last between one minute and 20minutes. These are possibly caused by router reboots, software problems, transient equipment problems, short maintenance operations on equipments or optical fiber, etc. Interestingly, about 50% of all failure events last less than a minute. While the cause behind this is still under investigation, one possible reason is for a router to mistakenly consider an adjacency to be down when it is not actually down. This could happen if the router CPU is overloaded and fails to process the IS-IS keep alive messages that are used to detect the loss of an adjacency. Furthermore, it is possible that multiple failure events on a single link within a short span of time could in fact be the oscillatory effect of a single fault or problem.

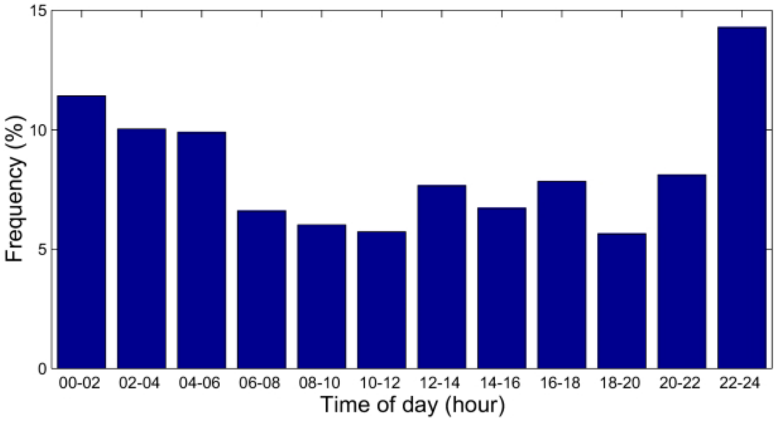


Fig. 3. Frequency of failures during 24 hours time windows

It is also interesting to compare the number of failure events due to scheduled maintenance and those that are unplanned or accidental, since it is desirable to eliminate (or at least minimize) the latter. Maintenance windows are scheduled during late night/early morning; hence a breakup of failure events by the time of day sheds light on this issue. Fig. 3 shows all the failures (over 4 months) grouped in two-hour bins by time of day. It is observed that about 47% of the failure events occur between 10 PM and 6 AM . The fact that this time period accounts for almost half of all failures indicates that maintenance activities do account for a significant portion of the failure events that we observe. Note also that failure events during this period are likely to have less of an impact on traffic, because the backbone is relatively lightly loaded at night.

The first step in analysis is to classify failures into different groups according to their underlying cause, i.e. the network component that is responsible. This is a necessary step for developing a failure model where the faults of each component can be addressed independently. In our classification, we proceed as follows. First, link failures resulting from scheduled maintenance activities are separated from unplanned failures. Then, among the unplanned failures, we identify shared failures, i.e. failures on multiple IP links at the same time due to a common cause. Among shared link failures, we further distinguish those that have IP routers in common and those that have optical equipment in common. The remaining

Failures represent individual link failures, i.e. faults that affect only one link at a time. For the individual failures, we further differentiate groups of links, based on the number of failures on each link.

Impact of a Failure
The following are the 7 steps require to re-route traffic after a failure has occurred with minimum time required:
1. Detect link down <100ms
2. Wait to filter out transient flaps ~2s
3. Wait before sending update out ~50ms
4. Processing & flooding the update
   ~10ms/hop
5. Wait before computing SPF ~5.5s
6. Compute shortest paths ~100-400 ms
7. Update the routing tables ~20 pfx/ms

VI. METHODOLOGY

We analyze how the network reacts to the following two categories of events:
A. LinkDown: A link is down, kicking off IS-IS convergence procedure to recompute the shortest paths for all route entries. Traffic may be lost due to unresolved routes in the interim until a new alternative path is found.
B. LinkUp: The link that previously failed has recovered. Again the routers have to recompute shortest paths to all destinations. The traffic originally carried by this link will be re-routed from the respective alternative paths to the primary shortest paths. Always it will maintain substitute path in buffer. As the primary path is failed, it will automatically connect to substitute path which is considered as second shortest path from source to destination. If a breakdown happens in node or path, it will pop up the notification to the users and will go for the second substitute path for transmitting the data.

In the scenario of node failure, we propose scheme that can be used to recover multiple node failures. The only difference is to find multiple disjoint backup paths instead of only one. Using this method, the memory overhead in the nodes is also dependent on the number of failures that is guaranteed to be recovered. This scheme allows to recover multiple failures as long as the two failing nodes are not adjacent. So it is also a future plan to recover multiple node failures in any location.

We propose two recovery methods for single link and node failure in greedy routing. We also propose a simple embedding based on the spanning tree of the network in order to perform the greedy routing. In the scenario of a link failure, backup trees are used and for node failure scenarios, backup paths will be considered. Using these techniques, there is no need to re-calculate the coordinates of the nodes. The proposed schemes are protection schemes which result into a fast switchover. In the experimental evaluation, both methods may show interesting stretch characteristics compared to the existing alternatives and the added overhead to the packets will be very low. The proposed methods can be used in large-scale networks due to their scalability, simplicity, low overhead and limited resource requirement.

VII. CONCLUSION

In this paper, we have studied the causes and effects of link failure so as build a model that provides the services which is free from link failures, we also studied classification and impact of link failure in TCP network. We classify failures according to their cause and describe the key characteristics of each class. Our findings indicate that failures are part of the everyday operation: 20% of them are due to scheduled maintenance operation, while 16% and 11% of the unplanned failures are shared among multiple links and can be attributed to router related and optical-related problems respectively. Our study not only provides a better understanding of the nature and the extent of link failures, but is also the first step towards developing a failure model. Directions for future work include (i) the modeling aspects (ii) more root-cause analysis, using correlation with different failure logs (iii) a better understanding of the impact of failures on network availability.

REFERENCES

[1] U. Ranadivey and D. Medhi, (2001), “Some Observations on the Effect of Route Fluctuation and Network Link Failure on TCP”, *Proc. of IEEE Intl. Conf on Comp. Communications & Networks (ICCCN),* Scottsdale, AZ, Oct 2001, pp. 460-467.

[2] D. Tipper *et. al.*, “An Analysis of the Congestion Effects of Link Failures in Wide Area Networks,” *IEEE Jrnl. Sel. Areas Comm.*, Vol. 12, pp. 179-192, 1994.

[3] G. R. Ash, *Dynamic Routing in Telecommunications Networks*, McGraw-Hill, 1998.

[4] W.-P.Wang, D. Tipper, B. Jaeger and D. Medhi, “Fault Recovery Routing in Wide Area Packet Networks,” *Proc. of 15th International Teletraffic Congress*, Washington, DC, pp. 1077-1086, June 1997.

[5] C. Labovitz, G. R. Malan and F. Jahanian, “Internet Routing Instability,” *IEEE/ACM Trans. Networking*, Vol. 6, pp. 515-528, 1998.

[6] B. Mukherjee, “WDM optical networks: progress and challenges,” IEEE J. Select. Areas Commun., vol. 18, pp. 1810–1824, (Oct. 2000).

[7] O. Gerstel and R. Ramaswami, “Optical layer survivability: a services perspective,” IEEE Commun. Mag., vol. 38, pp. 104–113, (March 2000).

[8] G. Mohan, C. S. R. Murthy, and A. K. Somani, “Efficient algorithms for routing dependable connections in WDM optical networks,” IEEE/ACM Trans. Networking, vol. 9, pp. 553–566, (Oct. 2001)

[9] M. Clouqueur and W. D. Grover, “Availability analysis of spanrestorable mesh networks,” *IEEE J. Select. Areas* Commun., vol. 20,no. 4, pp. 810–821, (May 2002).

[10] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, “Survivable WDM mesh networks,” *IEEE/OSA J.* Lightwave Technology, vol. 21,no. 4, pp. 870–883, (Apr. 2003).

[11] Chandak and S. Ramasubramanian, “Dual-link Failure resiliency through backup link mutual exclusion,” in Proc. IEEE Int. Conf. Broadband Networks, Boston, MA, (Oct. 2005), pp. 258– 267.

[12] Md.Saifur Rahman, Nargis Parvin, Md.Tofael Ahmed, Md. Selim Reza, Halida Homyara, Farhana Enam “Detection of multiple failures in wavelength division multiplexed optical network using graph based light path restoration method” ISSN: 2248-9622 Vol. 3, Issue 1, January -February 2013, pp.1398-1406