ISSN 2278-7763

Analytical Study of different types Of network failure detection and possible remedies

Shikha Saxena[1], Somnath Chandra[2]

[1]Research Scholar, Mewar University ,Chittorgarh, India; [2]Dept of Electronics & Information Technology, Govt of India, NewDelhi, India.
Email: [1]shikhasaxena83@gmail.com,[2]somnath.chandra@gmail.com

ABSTRACT

Faults in a network have various causes,such as the failure of one or more routers, fiber-cuts, failure of physical elements at the optical layer, or extraneous causes like power outages. These faults are usually detected as failures of a set of dependent logical entities and the links affected by the failed components. A reliable control plane plays a crucial role in creating high-level services in the next-generation transport network based on the Generalized Multiprotocol Label Switching (GMPLS) or Automatically Switched Optical Networks (ASON) model. In this paper, approaches to control-plane survivability, based on protection and restoration mechanisms, are examined. Procedures for the control plane state recovery are also discussed, including link and node failure recovery and the concepts of monitoring paths (MPs) and monitoring cycles (MCs) for unique localization of shared risk linked group (SRLG) failures in all-optical networks. An SRLG failure is a failure of multiple links due to a failure of a common resource. MCs (MPs) start and end at same (distinct) monitoring location(s). They are constructed such that any SRLG failure results in the failure of a unique combination of paths and cycles. We derive necessary and sufficient conditions on the set of MCs and MPs needed for localizing an SRLG failure in an arbitrary graph. Procedure of Protection and Restoration of the SRLG failure by backup re-provisioning algorithm have also been discussed.

Keywords : MCs, MPs, MPLS, SRLG, Backup Reprovisioning , Graceful restart,RSVP-TE

1 Introduction

A network which contains many network components of both hardware and software can incur failures due to failure at one (or even multiple) of its contained components, ranging from the largest to the smallest and from hardware to software. The paper analyzes types of failure like Control plane failure, SRLG (shared risk link group failure), Sub network failure, Node failure, Link failure. Failure detection and failure notification and protection and restoration of control plane failure and SRLG failure.

2 Types of Failure in a network

There are many types of failure as link, node, SRLG, control plane failure as we can see in figures below.

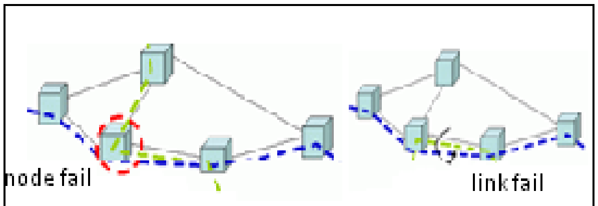


Fig 1 .NODE FAILURE AND LINK FAILURE

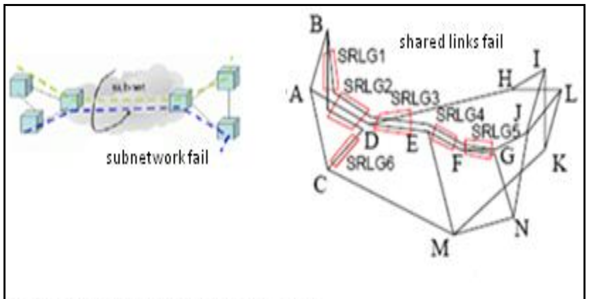


FIG 2. SUBNETWORK FAILURE AND SRLG FAILURE

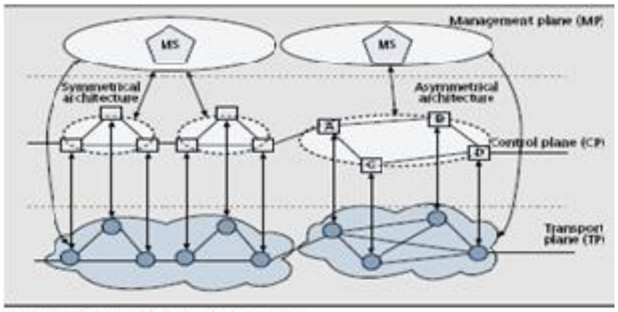


FIG 3. CONTROL PALNE FAILURE

Link (or conduit) failure(fig1): Link failures can be caused by equipment problems (e.g. a failed “blade” in a switch or router, power failure), a cable being unplugged or cut, a configuration change in the transport network or potentially a denial of service attack.(fig 1).

Node failure (fig1): Node failure is a type of failure with a single network node. If a node suffers an unrecoverable problem or permanent destruction.

sub network failure(fig2), is a type failure occurred with a regional sub network t hat commonly shares a risk, e.g., a region that has high occurring frequency of earthquake.

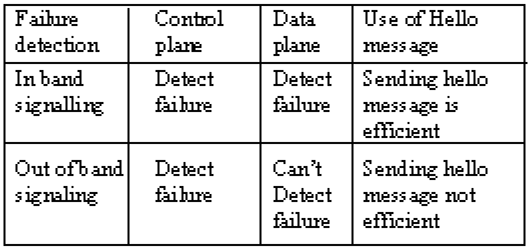
SRLG failure (fig2): It defines a concept that multiple different services may suffer from a common network failure if they are sharing a common failure risk [2].

Control plane Failure (fig3): The control plane failure would lose the control of the data plane, which means that we cannot establish new service connections, or terminate or modify an existing service connections within the data plane, even though the existing connections can still perform normally to carry user's data Control plane failure [1].

3. FAILURE DETECTION:

3.1. A In Control Plane failure detection:

By RSVP HELLO Protocol: Hello extension for RSVP has been proposed in RFC3209.[7]



Failure detection	Contol plane	Data plane	Use of Hello message
In band signalling	Detect failure	Detect failure	Sending hello message is efficient
Out of band signaling	Detect failure	Can't Detect failure	Sending hello message not efficient

Table1.Failure detection in control plane failure

As mentioned in above table1 , in out-of band signalling the use of this method can be ineffective, especially for the asymmetrical architecture(fig.4). There are two situations in which exchanging Hello messages between direct neighbours is not efficient [3]. The first case occurs when RSVP nodes are separated by a non RSVP host. The failure detection is limited in this case due to Time to Live set to 1. The second case occurs when RSVP nodes are separated by other RSVP nodes. This situation is presented in Figure 4. a)If the Label Switched Path is created through Label Switch Router1 and Label Switch Router 3, signalling messages are passed through R1, R2 and R3. b)Therefore, the failure of the link R2–R3 cannot be discovered by R1. This happens because hello packets are still exchanged between R1 and R2. SO the use of RSVP Hello for failure detection in the control plane requires additional modification of signalling procedures triggered by failures in this plane. The solution is to allow for multi-hop hello exchange. This solution can be performed by a direct logical connection created by some technology like IP or MPLS tunneling. In order to allow time for protection or convergence, a solution, like graceful restart mechanism can be used.

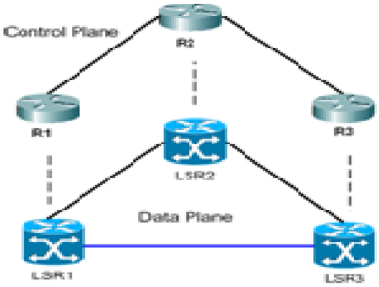


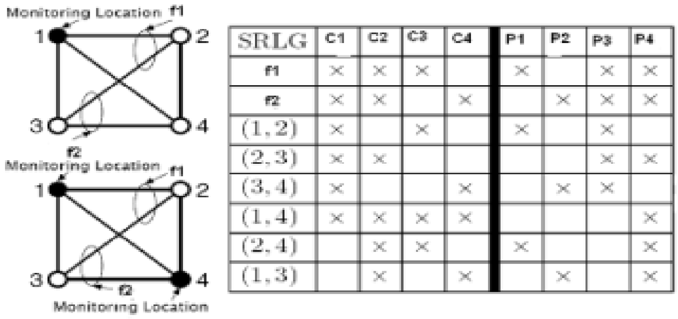
fig 4. Asymmetrical architecture of control plane

3.1.B IN SRLG failure DETECTION:

Links in an optical network may share a common resource, such as a duct or conduit through which they are laid out. The failure of this resource results in the simultaneous failure of multiple links. Such failures are referred to as Shared Risk Link Group (SRLG) failures [8]. A practical approach to fault detection and localization to equip only a few nodes in the network with monitors, referred to as monitoring locations. In such networks, SRLG failures may be uniquely localized using monitoring paths (MPs) and monitoring cycles (MCs). An MP starts and ends at distinct monitoring locations, whereas an MC starts and ends at the same monitoring location. The MPs and MCs should be selected such that the failure of any SRLG results in the failure of a unique combination of MPs and MCs [3].

NECESSARY AND SUFFICIENCY CONDITIONS FOR LOCALIZING SRLG FAILURES

Consider an all-optical network whose topology is modelled as a graph G(N<L), where N is the set of nodes and L is the set of links. Let F denote the set of SRLG failures in the network. An element f ∊ F is a subset of L. It denotes the set of links that may fail due to a failure in a shared resource. Given a certain placement of monitors, the objective is to localize an SRLG failure by observing failed MPs and MCs. We refer to a set of monitoring paths and cycles that can uniquely localize all SRLG failures as a fault localization (FL) set. The default case of no SRLG failure is indicated by no failures in any of the paths or cycles in the FL set. Every SRLG failure affects at least one MP or MC. In addition, an SRLG failure results in a unique syndrome – a combination of failed MPs and MCs. Consider the example in Figure 5,



SRLG	C1	C2	C3	C4	P1	P2	P3	P4
f1	×	×	×		×		×	×
f2	×	×		×		×	×	×
(1, 2)	×		×		×		×	
(2, 3)	×	×					×	×
(3, 4)	×			×		×	×	
(1, 4)	×	×	×	×				×
(2, 4)		×	×		×			×
(1, 3)		×		×		×		×

Fig 5. Example network topology. SRLG failures, and associated syndromes

where f1 ={(1, 2), (2, 3)} and f2 = {(2, 3), (3, 4)} are the two SRLG failures. When node 1 is the monitoring location, an FL set with four MCs is given by: c1 = (1–2–3–4–1), c2 = (1–3–2–4–1), c3 = (1–2–4–1), and c4 = (1–3–4–1). Similarly, if node 1 and 4 are both monitoring locations, an FL set with three MPs and one MC is given by: p1 =(1–2–4), p2 = (1– 3–4), p3 = (1–2–3–4), and p4 = (1–3–2–4–1). The associated syndromes are shown in Figure 5. An MC/MP is affected by an SRLG f if it passes through at least one link l∈ f.

Theorem: The necessary and sufficient conditions for the existence of an FL set to monitor any given set F of SRLG failures in an arbitrary network are:

1) Each SRLG failure affects at least one monitoring path or cycle; and

2) For any two SRLGs f1 and f2 in F, there exists a path or cycle in the FL set that is affected by f1 and not f2 or vice versa.

Proof: The necessity part is proved by contradiction. Assume to the contrary that there is a feasible solution but at least one of the two conditions presented are not satisfied. First assume that condition 1 is not satisfied. If condition 1 is not satisfied for an SRLG fi, then no cycle or path passes through it, and hence the failure of fi cannot be monitored. Thus, any feasible solution must satisfy condition 1. If condition 2 is not satisfied for a pair of SRLGs f1 and f2, then every cycle or path that is affected by f1 is also affected by f2, contributing to the syndromes of both f1 and f2. Thus, the failure of these two SRLGs cannot be uniquely identified, leading to a contradiction. Therefore, a feasible solution may be obtained only if the two conditions presented are satisfied. We prove the sufficiency part by construction. For any two SRLGs f1 and f2 in the network, we define three types of paths and cycles:

- T1: Set of paths and cycles affected by f1 and not f2.
- T2: Set of paths and cycles affected by f2 and not f1.
- T3: Set of paths and cycles affected by both f1 and f2.

To distinguish a failure between f1 and f2, an FL set must have paths and/or cycles that fall in at least two of these three types. For example, if the FL set contains a path or cycle c1∈ T1 and path or cycle c2 ∈ T3, then a failure of f1 will result in a failure of c1 and c2 and a failure of f2 will result in a failure of c2 only. Based on condition 2, we know that cycles or paths of type T1 or T2 must exist. Assume that a monitoring path/cycle of type T1 exists for SRLGs f1 and f2. For given monitoring locations, a path or cycle of type T1 may be obtained as follows: First, merge all the monitoring nodes to form one super-node m. This transformation may result in multiple links from a node to the super-node m. In addition, any link between two monitoring locations will transform into loops at node m. Second, remove links of SRLG f2 from the network. Third, if any of the remaining links of f1 \ f2 is among the loops at node m, then the loop is a (one link) path of type T1.Otherwise, construct a cycle traversing node m and link ≡ (xl, yl) ∈ f1 \ f2, as shown in table 2.

1) Add a virtual node vand two virtual links(v,xl) and (v,yl).remove link l.
2) Obtain two link disjoint path p1 and p2 from v to m.
3) From a cycle c by joining p1 and p2 after removing a virtual link and adding the link l.

Table 2 procedure to compute a cycle traversing a given node m and link l

Such a cycle must exist for at least one link, as condition 2 is necessary. When the monitoring nodes are expanded, the cycle either remains a cycle or transforms into a monitoring path. Similarly, if the MC/MP of type T2 exists then it can be constructed using the above method by interchanging f1 and f2. We now have at least one cycle/path of type T1 or T2. Finally, assume that for SRLGs f1 and f2, we have a cycle/path of type T1 but not T2, then there must be a cycle/path of type T3 in order to satisfy condition 1 (otherwise f2 will not be covered by any MC/MP). An MC/MP of type T3 can be obtained using the procedure presented in Figure 2 by trying for all the links *l* ∈ f2. In this case, we do not remove the links in f1. By adding MCs/MPs of at least two of types T1, T2, and T3 for each SRLG pair (fi, fj) we can construct a feasible solution. The necessary and sufficient conditions are valid for an arbitrary topology, which may include multiple edges between two nodes and self-loops at a node. The placement of monitoring locations in the network must be able to generate MCs and MPs that satisfy the conditions in Theorem.

4 Protection and Restoration from failure

4.1 Protection and Restoration of the Control Plane

In order to allow time for protection or convergence, a solution, like graceful restart mechanism, is proposed. This procedure allows to avoid unnecessary switch-over in the data plane. After the control plane fails the restart time timer is activated. During this period of time the node waits for establishment of a new session with the neighbour. State information of both control and data planes is held. In this period, the data plane traffic can be sent successfully but signalling traffic is affected by the failure.

Procedures for Control-Plane State Recovery [5]

The RSVP-TE graceful restart capability is specified by two parameters: restart time, and recovery time. The restart time is the total time of a RSVP-TE signalling node to restart RSVP-TE and to re-establish Hello communication with its peer. The recovery time is the total time within which the relearning of the state of the data plane connections and resources should be completed, after the establishment of Hello communication. When an upstream RSVP-TE peer helps a downstream restarting RSVP-TE signalling node, the upstream RSVP-TE peer includes the Recovery Label object in the Path messages to the downstream restarting node. The Recovery Label is the stored label that was generated by the restarting downstream node, and was sent to the upstream node before the restart in a RSVP-TE Resv message. When a downstream RSVP-TE peer helps an upstream restarting RSVP-TE signalling node, the downstream RSVP-TE peer sends the Recovery Path messages to the upstream restarting node. The Recovery Path message is the same as the Path message that was generated by the restarting upstream node, and was sent to the downstream node before the restart in a RSVP-TE Path message. The RSVP-TE graceful restart mechanism is illustrated in Figure 6. After the a signalling plane failure, the RSVP-TE graceful restart mechanism re-establishes its Hello instance, then recovers lost state information, or re-confirms the preserved state information.

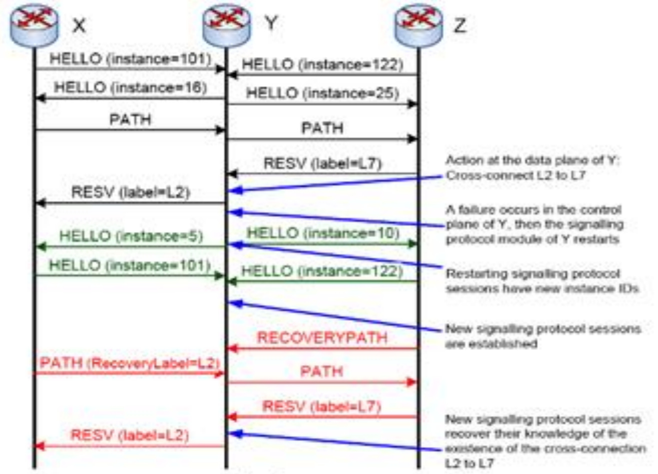

X
Y
Z
HELLO (instance=101)
HELLO (instance=122)
HELLO (instance=16)
HELLO (instance=25)
PATH
PATH
RESV (label=L7)
RESV (label=L2)
Action at the data plane of Y: Cross-connect L2 to L7
A failure occurs in the control plane of Y, then the signalling protocol module of Y restarts
HELLO (instance=5)
HELLO (instance=10)
HELLO (instance=101)
HELLO (instance=122)
Restarting signalling protocol sessions have new instance IDs
New signalling protocol sessions are established
RECOVERYPATH
PATH (RecoveryLabel=L2)
PATH
RESV (label=L7)
RESV (label=L2)
New signalling protocol sessions recover their knowledge of the existence of the cross-connection L2 to L7

fig 6.RSVP-TE graceful restart mechanism

4.2) Protection and Restoration of the SRLG failure by backup reprovisioning algorithm:

After SRLG failures, we need to modify traffic distribution and prune the network topology from G to G' as follows:

1) Eliminate all the links from the graph belonging to the failed SRLG.

2) Release all the wavelengths used by failed paths as well as backup wavelengths blocked due to sharing of connections.

3) If a connection's working path fails, its backup path will become the working path.

Algorithm: Backup reprovisioning after SRLG failures[6]

Step 1) Sort unprotected connections to a list according to reprovision backup paths for connections whose working paths traverse more SRLGs first i.e., the highest BPAI connections first or The second policy is to reprovision backups for connections whose working paths traverse fewer SRLGs first (Policy II), i.e., the lowest BPAI connections first or random reprovisioning, depending on what policies will be used.

Step 2) Choose the working path Pw s,d,k accordingly from the list. To compute the backup path, prune G' to G'' by eliminating:

Step 2.1) All the links (including all the channels in these links) the working path Pw s,d,k traverses and the SRLG mates of these links.

Step 2.2) All the channels used by all the established working paths.

Step 2.3) If there is a working path Pw s',d',k' that traverses the same SRLG as the current working path Pw s,d,k, remove all the channels used by Pb s',d',k'.

Step 3) Compute the shortest paths on each wavelength layer from the pruned graph G'' in step 2). Compare the shortest paths from each wavelength layer and choose the shortest one as Pb s,d,k. If some of the shortest paths from different wavelength layers are equal, use the First-Fit algorithm to break the tie. If no backup path can be found, count this backup reprovisioning as an unsuccessful backup reprovisioning.

Step 4). Go back to Step 2) for more iteration.

NOTE: BPAI(backup path availability index) is defined as the total number of SRLGs that the unprotected connection belongs to the kth connection request from source node s to destination node d is represented as cs,d,k. In this study, every connection needs to be protected with shared-path protection against SRLG failures. Let Pw s,d,k and Pb s,d,k denote the working path and the backup path of cs,d,k, respectively.

5 Conclusion :

The paper presents an analysis for possible failure mechanisms in the different network topologies. The analysis could be corroborated through various simulation and mathematical techniques.

6 References:

[1] Andrzej Jajszczyk,Pawel Rozycki," Recovery of the Control Plane after

Failures inASON/GMPLS Networks” 0890-8044/06/$20.00 © 2006 IEEE Network • January/February 2006”

[2] Xu Shao, Luying Zhou, Xiaofei Cheng, Weiguo Zheng, Yixin Wang, “Best Effort Shared Risk Link Group (SRLG) Failure Protection in WDM Networks” IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

[3] Pawel Rozycki, Janusz Korniak “Failure Detection and Notification in GMPLS Control Plane”, GMPLS Performance Control Plane Resilience, 2007 Workshop on digital Object.

[4] Satyajeet S. Ahuja, Srinivasan Ramasubramanian, and Marwan Krunz,”SRLG Failure Localization in All-Optical NetworksUsing Monitoring Cycles and Paths”, proceedings of the IEEE INFOCOM 2008 IEEE Communications Society subject matter experts for publication

[5] Jing Wu, Michel Savoie,” Recovery from control plane failures in the RSVP-TE signaling protocol”,Communications Research Centre Canada, 3701 Carling Avenue, Ottawa, Ontario, Canada K2H 8S2 Crown Copyright 2011 Published by Elsevier

[6] Xu Shao; Yong Kee Yeo; Yuebin Bai; Jian Chen; Luying Zhou; Lek Heng Ngoh; , "Backup Reprovisioning After Shared Risk Link Group (SRLG) Failures in WDM Mesh Networks," Optical ‘Communications and Networking, IEEE/OSA Journal of , vol.2, no.8, pp.587-599, August 2010

[7] D. Awduche, Ed., “RSVP-TE: Extensions to RSVP for LSP Tunnels”,RFC3209

[8] A. Todimala and B. Ramamurthy. Survivable virtual topology routing under shared risk link groups in WDM networks. First International Conference on Broadband Networks (BROADNETS), pages 130–139, Oct. 2004.