Online Publication Date: 19 April 2012
Publisher: Asian Economic and Social Society

Network Resilience in Multiprotocol Label Switching

Afzaal Hussain (Government College University Faisalabad)

Shahbaz Nazeer(Government College University Faisalabad)

Tahir Abdullah(Government College University Faisalabad)

Beenish Yaseen(Government College University Faisalabad)

Asim Salam (Govt. College of Technology Faisalabad)

Citation: Afzaal Hussain, Shahbaz Nazeer, Tahir Abdullah, Beenish Yaseen, Asim Salam (2012): "Network Resilience in Multiprotocol Label Switching" Journal of Asian Scientific Research Vol.2, No.4, pp.221-227.

Author (s)

Afzaal Hussain
Government College University
Faisalabad.
E-mail: afzaalasn@hotmail.com

Shahbaz Nazeer
Government College University
Faisalabad.
E-mail:
shahbaz_nazir1@yahoo.com

Tahir Abdullah
Government College University
Faisalabad
E-mail:
tahir_wains@hotmail.com

.Beenish Yaseen
Government College University
Faisalabad.
E-mail: gr8_bini@yahoo.com

Asim Salam
Govt. College of Technology
Faisalabad
Email: asim_salam2003@yahoo.com

Network Resilience in Multiprotocol Label Switching

Abstract

The ability of a network which keeps services running regardless of a link or node failure is called Network resilience. In this research the provisioning of resilience against network failures in Multiprotocol Label Switching (MPLS) based networks is investigated. Due to the ever increasing amount of data transported over a single link failures can cause tremendous loss of data, loss of reputation, and loss of revenue for the network operators. Therefore the network has to be resilient against failures. It must be capable to detect the failure and recover affected services in an efficient manner, ideally without the services realizing the outage and disconnecting. Due to the complexity of the transport network architectures sophisticated resilience mechanisms are needed. This research is focused on techniques that can be used to reroute traffic faster in case of a failure in a network with respect to network topology, available resources, requirements of the network and the requirements of users.

Introduction

Multiprotocol Label Switching (MPLS) is emerged from the Internet Engineering Task Force's (IETF)effort to standardize a number of proprietary multilayer switching solutions

that were initially proposed in the mid-1990s. MPLS integrates layer 3 routing and layer 2 switching functionalities [5]. MPLS introduces connection-oriented forwarding paradigm by replacing the routing of IP packets based on the IP header information with short four-byte Label based switching. The mechanism does not build forwarding decision based on traditional destination IP address on complex routing table lookup. This fixed-length switching concept is similar as in ATM and Frame Relay networks, but not the same. The technology is independent from the layer 2 technology used, and several implementation proposals have been made, e.g. for ATM, Frame Relay, and SDH/SONET. Multiprotocol Label Switching (MPLS) is designed to provide an elegant solution to present shortcomings of IP routing in the area of traffic engineering, QoS, virtual private networks (VPN) and DiffServ [1].

In seven-layer OSI reference model, MPLS resides somewhere between the Data Link Layer (Layer 2) and the Network Layer (Layer 3). MPLS introduces the concept of connection-oriented mechanisms in connectionless IP-based networks. It also introduces new methods for Traffic Engineering (TE) and traffic management in these networks. The circuit-switching or virtual circuit model, such as that used in ATM, possesses advantages like performance management, bandwidth reservation, and traffic management. MPLS provides IP networks with such advantages of the circuit switching model in addition to the scalability and flexibility merits that are already available in IP-based networks. MPLS provides simpler mechanisms for packet-oriented Traffic Engineering (TE) and multiservice functionality with the added benefit of greater scalability.

The basis of MPLS operation is the classification and identification of IP packets with a short, fixed-length, and locally significant identifier known as a Label and forwarding the packets to a switch or router that is modified to operate with such labels. The modified Routers and switches do not use the network layer addresses they only use these labels to switch or forward the packets through the Network [5].
Router which assigns such labels to the packets, are called Label Edge Routers (LERs) and the Routers and Switches that use these labels to forward traffic are called Label Switch Routers (LSRs). A particular path that a packet or flow traverses through the network based on the labels assigned to that packet or flow is know as Label Switched Path (LSP). Group of IP packets which are forwarded in the same manner, over the same LSP, with the same forwarding treatment is called Forward Equivalence Class (FEC). The MPLS domain is a portion of a network that contains such devices that understand MPLS.

Fault Indication Signal (FIS) is a message that indicates that a fault on the working path has occurred. This FIS is sent back upstream to the Path Switch Label switch router (PSL) which is responsible for switching the traffic between the working path and the recovery path.

Mpls Recovery Mechanisms

Protection switching and Restoration (rerouting) are two most common techniques used in MPLS recovery both can be used together. Protection switching to a recovery path can be used for rapid restoration of connectivity while rerouting determines a new optimal network configuration, rearranging paths, as required, at a later time [6]. Both protections switching and rerouting supports Local and Global repair. In protection switching, the alternative LSP (Protected Path) is pre-established and pre-reserved (pre-provisioned). That is the reason that protection switching realizes the shortest disruption of traffic.

Several options are possible for the resource usage of the recovery path [1]. In 1+1 ("one plus one") protection switching scheme a copy of the working traffic is always transported over the recovery path. To recover from a failure the egress LSP must only select the incoming traffic from the protection LSP instead of the working LSP. No signaling is required in this case. In 1:1 ("one for one") protection scheme, the working traffic is only switched to the recovery LSP if a failure occurred on the working LSP. Depending on the selected resource usage, dedicated or shared, the recovery LSP may be used only to recover a single working LSP or it may be used to recover different LSPs with the same LSP end points. If a 1:1 resource allocation is used the recovery LSP may additionally carry low-priority, pre-emptible traffic (extra-traffic) when no failure is present in the network. The recovery path is unused by working path traffic until the Path Switch LSR (PSL) receives a Fault Indication Signal, then traffic is switched over to the recovery path and lower priority traffic is no longer allowed to use the reserved resources on the recovery path. This concept can be extended to 1:N (one for N) and M:N (M for N) protection.

First proposed models for MPLS recovery which was presented in [4] and it is often referred to as Makam's model. The model provides end-to-end protection for a LSP by setting up a global recovery path between the Path Switch LSR (PSL) and egress LSR. This recovery path is totally link and node disjoint with the working path. When a failure is detected on the working path, a fault indication signal (FIS) is used to convey information about the occurrence of the failure to the Path Switch Label Switch Router (PSL). The PSL is then responsible for switching traffic over to the recovery path. One of the drawbacks of Makam's Model is when global recovery is used the PSL has to be informed about a failure in the working path with the help of FIS before traffic can be switched over to the recovery path. When this is done with a FIS, PSL will continue sending traffic down the failed working path until this FIS has been received. This will result in dropped packages at the LSR that is upstream of the failure, as this node does not have any forwarding information for these packages since the downstream node is not reachable. If the transmission rate is high and the failure is situated far away from the point of repair, the number of packets dropped can be very high.

In Haskin's Model the idea of reverse backup

technique is used to reverse traffic at the point of failure in the working path, back to the PSL. As soon as a LSR detects a failure on the working path, it redirects the incoming traffic on to an alternative LSP that is setup in the reverse direction of the working path. When PSL receives the reversed traffic, it forwards this traffic on to a global protection path. Both the reverse path and the global protection path are pre reserved. This scheme was introduced by Haskin [2] and is therefore often called Haskin's model.

Fast Re-route is a protection switching scheme in which recovery LSPs are pre-established for each link. The basic advantage of such a fast rerouting scheme is that no end-to-end failure notification and signaling are required for the protection switching. A node detecting a physical failure at its port may immediately switch the affected traffic to the recovery path. A single recovery LSP could be configured to protect several LSPs running over the link to reduce the number of recovery LSPs a node has to configure and belonging to the same FEC.

In fast reroute one-to-one backup technique a separate backup LSP, known as detour LSP is computed for each LSR in a protected path. These detour LSPs are set up to use node recovery (if possible) otherwise link recovery. In case a failure occurs anywhere along the protected path, the LSP which detects the failure can always switch traffic onto a local detour. There is no need to send a FIS upstream. So, the recovery operation becomes a local decision for the LSP that detects the failure.

In this research Network resiliency comparisons are made for each model on the basis of.

- Packets Dropped when Failure occurred
- Service Disruption Time
- Reserved Resources

Results

Table-1 illustrates Packets Dropped when Failure occurred, Service Disruption Time and Reserved Resources for backup operation.

Recovery Model	Service Disruption time	Reserved Resources	Packet Dropped
Makam's Model	0.02441s	5	69
Haskin's Model	0.02456	8	59
Global Protection with rerouting	0.03686s	0	108
Local Rerouting	0.02839s	0	82
Fast reroute one-to-one backup	0.02033s	8	58

Table 1: Comparison of Recovery Models

Packets Dropped

Rerouting mechanism causes the most packet loss during recovery, because in rerouting mechanism packets can be dropped during the time of

- Failure Detection
- Failure Notification

- Recovery Path Calculations
- Setup Of Recovery Path

If we minimize these intervals given above, the packet loss during rerouting can also be minimized. Failure detection time depends on the mechanism used for failure detection. As RSVP-TE hello mechanism is used in MPLS for failure detection; we can optimize the RSVP-TE hello mechanism by setting the most optimal values for this hello interval and the failure check multiplier.

Lower layer mechanism can be used for faster failure detection if available. By setting each LSR in the working path as PSL, the failure notification time can be minimized, in such case there is no need for failure notification message, the node that detects the failure can then start the rerouting mechanism. To further optimize the rerouting mechanism the path calculation time must be decreased, this optimization can be achieved if recovery paths are pre-calculated by each PSL whenever a new link state advertisement is received. In case of a failure the recovery path setup time depends upon the available resources in the network and the network topology, the longer the recovery path, the more packets will be dropped during the setup of recovery time.

In protection switching fewer packets can be dropped as the recovery path is pre-setup but Packets can be dropped during the time for failure detection and failure notification. With the use of local recovery failure notification time can be minimized which results in fewer packets drop, as in the fast reroute one-to-one [3]. Using traffic itself as a fault indication signal by establishing reverse recovery path is another alternative to even more reduce the number of packets dropped during the failure notification time.

Service Disruption

Service disruption time also depends on the time for failure detection, failure notification, recovery path calculations and recovery path setup just like the number of dropped packages. So it can be said that service disruption time will be high in rerouting mechanism as compared to protection switching, because in rerouting time is used for path calculations and path setup. These calculations are not required in protection switching because backup path is pre-calculated.

Local recovery with protection switching can be used to minimize the failure notification time, as in the fast reroute models. Service disruption time also depends on the length of the new path that traffic requires to traverse to reach at the egress node. When the recovery path is in use, the service disruption time will be short if the path from the point of failure to the egress node is short. If Haskins model is compared with Makam's model [4] the number of packets dropped in Haskins model [2] is less than the Makam's Model. Haskins model is an improvement over Makam's model. In case of service disruption time, both models will use the same time.

Pre-Reserved Backup Resources

No resources are reserved in Global Reroute Model and Local Reroute Model before the recovery operation starts; the resources are pre-reserved only in case of protection switching. In case of least amount of resources in the network Rerouting is the best alternative to consider. Pre-reserved resources used to

fully protect a working path end-to-end in protection switching, depends on the recovery model, network topology and kind of protection switching used. Both Haskin and Makam's Model uses global recovery path but Haskin Model uses a reverse backup path to send the packets back when failure occurs, so Haskins model will always use more resources as compared to Makam's model. In most cases Fast reroute will use more resources then Haskins model, but in the optimal topology the same amount of resources will be used by these models. If already established recovery path resources can be shared then a new recovery path in the network might not need to make any new backup reservations,

Conclusion

For the recovery of physical failures lower layer resilience is well suited, while resilience in higher layers can offer finer recovery granularity and higher protection selectivity. With the use of resilience mechanisms in multiple layers the recovery of multiple failures can be improved. Both techniques protection switching and rerouting can be used for the recovery operation locally around the failed link or node, or globally starting at the ingress to the egress LSP. Each has its own specific characteristics, merits and demerits so that the method(s) used must be chosen carefully with regard to the network topology, available resources, requirements of the network and the requirements of users.

1:N or M:N protection switching is more resource efficient where the reserved resources can be used by extra traffic. Local recovery shall be used to get the shortest service disruption time in 1:N or M:N protection switching. In such scenarios protection sharing should be used to decrease the amount of reserved resources.Fast re-route mechanism will probably provide the best solution if very rapid repair is needed, for example real time application like voice etc. 1+1 protection switching techniques is suitable where guaranteed data delivery is required in real time with least service disruption and data loss. Protection switching can be chosen if quick repair with the possibility of sharing backup resources is desired. Local repair can be used if repair time is not crucial and network resources are limited.

References

Autenrieth A. (2003) Differentiated Resilience in IP-Based Multilayer Transport Networks, http://www.aurit.de [1]

Haskin D. and R. Krishnan (2000) A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute, Internet Draft, Internet Society [2]

Kompella K. and G. Swallow (2006) Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, RFC 4379, Standard Track, Network Working Group [3]

Makam S., V.Sharma, K.Owens and C.Huang (1999) Protection/Restoration of MPLS Networks, Internet Draft, Internet Society [4]

Rosen E., A. Viswanathan and R.Callon (2001) Multiprotocol Label Switching Architecture, RFC 3031, Standard Track, Network Working Group[5]

Sharma V. and F. Hellstrand (2003)

Framework for Multi-Protocol Label Switching (MPLS)-based Recovery", RFC 3469, Informational, Network Working Group [6]

Hundessa L. and J. Pascual (2001) "Fast Rerouting mechanism for a protected label switched path," Proceedings of the IEEE International Conference on Computer Communications, vol: 10, pp: 527-530 [7]

Kompella K. and G. Swallow (2006) Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, RFC 4379, Standard Track, Network Working Group[8]

Raj A. and O. C. Ibe (2007) "A survey of IP and Multiprotocol label switching fast reroute schemes", Computer Networks, vol: 51, pp: 1882–1907 [9]

Virk A. P. S. and R. Boutaba (2006) "Economical protection in MPLS networks", Computer Communications, vol: 29, pp: 402–408. [10]

.