Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Fast Restoration Mechanisms in ATM Networks

Dr. M. Usha Rani[1]
Associate Professor
Dept. of Computer Science & Spmvv, India

K. Sailaja[2]
Research Scholar
Dept. of Computer Science & Spmvv, India

***Abstract :** Automatic and rapid network service restoration (self-healing) when failures occur is of increasing importance for network operations and management as network speed and bandwidth increase. In this paper, I presented the implementation of self healing functions of the REFORM system. The REFORM system is to ensure network performance and availability within acceptable levels under normal and fault conditions. The specifications of this system covers both the functional and architectural aspects. The REFORM system provides self-healing mechanisms at both the control and management planes. Self-healing implies resource restoration by means of a distributed mechanism. The term self- healing refers to the ability of the network to reconFig. itself around failures quickly and gracefully with the goal of restoring service availability within acceptable levels for existing as well as future connections. The implementation approach was presented based on real experiments performed in the REFORM/EXPERT testbed in Basle, Swiss.*

KEYWORDS:ATM, EXPERT, REFORM,SELF-HEALING, TESTBED,RESTORATION.

1. Introduction

An ATM (asynchronous transfer mode) network [l] is a high-capacity optical fiber network, which transports signals of various services such as voice, data, image, and video. As an ATM-based network offers a high transimission capacity of integrated services, the failure of a network element (NE)such as a link or a node can cause a significant loss of 2 services to users and a loss of revenue to the network operating companies. It is estimated that if the network is disabled for one hour, up to $6,000,000 loss of revenue may occur in the trading and investment banking industries **[2].** Therefore, automatic and rapid network service restoration (self-healing) when failures occur is of increasing importance for network operations and management.

2. Analysis Of Self-Healing Concept

The system incorporates rapid and reliable ATM network layer self healing mechanisms, intelligent load balancing, dynamic routing and resource management functions all interworking together with the overall goal to ensure cost-effective network performance and availability under normal and fault situations. Restoration mechanisms in the ATM network layer are integrated with the control and management plane functionality, aiming at providing an integral and network-wide treatment to the problem of fault recovery. In order to meet the simplicity, fastness and cost effectiveness criteria, the REFORM system implements the so-called static shared VP Connection (VPC) restoration scheme.Static, while the protection VPCs that protect working VPCs on disjoint physical links are pre-conFig.d by the operation system. Shared, while restoration resources are jointly shared among a number of protection VPCs, that protect working VPCs on disjoint physical paths. These protection VPCs are potentially activated due to different failures. Depending on the network planning, a predefined level of restoration capability can be introduced within the network. Although the scheme might become slightly slower than its dedicated counterpart, where the restoration resources along a physical path are reserved for the protection VPC, it is considered as more cost-effective in terms of restoration bandwidth.

On Fig. 1, the drawn bi-directional working and protection VPCs consist of two distinct unidirectional VP connections. ITU prescribes that the unidirectional connections of a bidirectional VP should follow the same physical route. Based on this paradigm, a single unidirectional link failure must lead to the bidirectional switch over of traffic between working and protection VPC, while principally, a failure occurring at a single direction of a bi-directional One node (A) can upon determination of a failure in the ingress direction, trigger the reservation of restoration resources along the protection VPC (along nodes B and C), and force the peer node (Z) by means of a confirm message to switch over the active traffic in the direction of the failure. The receipt of the confirmation message by node Z guarantees the reservation of resources along the protection path. independently, node Z sends the same reservation message in opposite direction (C-B), thereby forcing the switch over by node A. This accomplishes the bi-directional switch over. All connecting nodes should be made aware by information in the message, that this reservation is about the same protection VPC, thereby avoiding contention problems. The VPC restoration reservation protocol has first been described by Kawamura in [9], and has been extended in the

REFORM system with the necessary messages to make the scheme more robust, both in terms of unavailability of restoration resources, as well as towards the loss of protocol messages

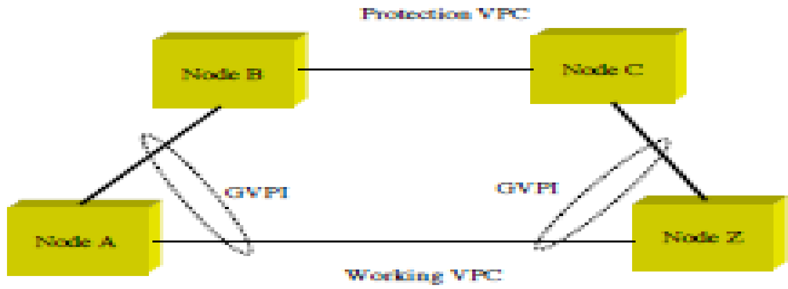

Fig 1: Working and protection VPCs

One of the choices to be made at the time of traffic restoration, is how much bandwidth will be allocated along the restoration path. One has the choice amongst the fully allocated bandwidth associated with the (failed) working VPC, which includes both used and unused portions of working VPC, or merely the used bandwidth at the time of failure. By applying the former, the switch over from working to protection VPC does not result in any decreased availability of unused bandwidth, and as such, no topology update in the VP layer network .

A. Endpoint

The next Fig. shows the state diagram of the self-healer protocol at the endpoint nodes.

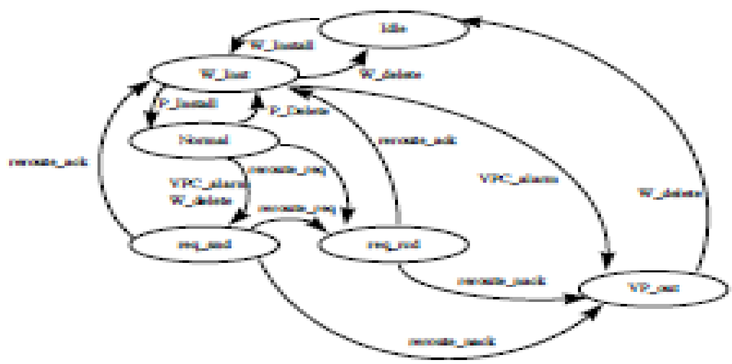

Fig.2: Endpoint node state diagram

The role of the endpoint node is to reroute the traffic to the protection VPC, after ensuring that the appropriate bandwidth has been allocated along the protection VPC. In order to be ready to operate, it has to be initialized. This initialization includes the installation of the working and its protection VPC. The protocol works for both kind of failure, at unidirectional or bi-directional failures. In both cases, the goal is to reroute the connections at both directions. It takes also under consideration the loss of protocol messages, as well as unavailability of restoration resources.

B. Connecting Point

The next Fig. shows the state diagram of the self-healer protocol at the connecting point nodes.

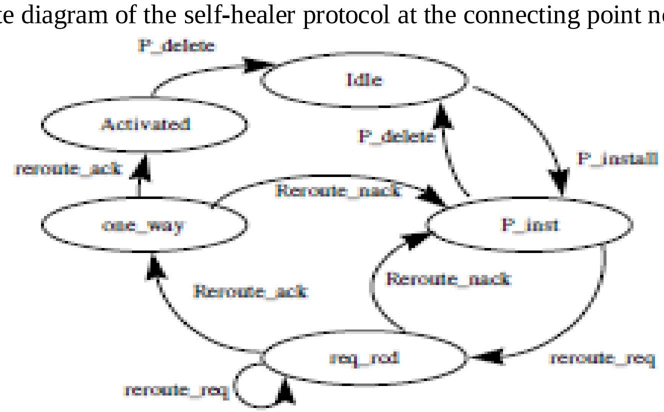

Fig. 3: Connecting point node state diagram

The role of this protocol is to allocate the bandwidth along the protection VPC and notify the endpoint nodes. It takes under consideration loss of protocol messages along the ATM control channel, as well as situations of unavailability of restoration resources.

3. THE REFORM NODE

Within the European Community's ACTS program, the REFORM project is dedicated to the investigation and demonstration of fully survivable ATM networks by exploring existing and new concepts, and implementing the required infrastructure on a real life ATM testbed. The REFORM system consists of a number of components that can be recognized either as control or as management plane entities. These are implemented in what is referred to as the REFORM node, a workstation attached to an ATM switch which undertakes all control and management plane functionality. The interaction of the control plane components is being achieved by means of a proprietary message infrastructure, based on IPC mechanisms, which is common to all control plane components.

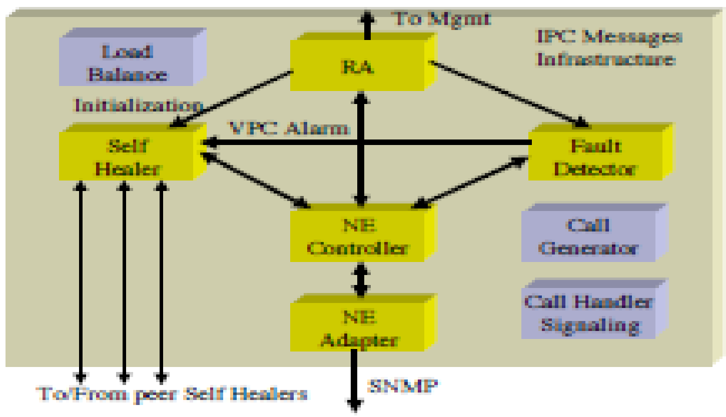

Fig. 4: The REFORM node

The REFORM control plane components that are interacting with the self-healer, are the following:

The RA (Resource Adapter) which is the heart of the REFORM node; it is responsible for managing the rest of the control plane components, for the communication between the control and the management plane components and for initializing the control plane components; The FD (Fault Detector) component, which is monitoring the VPCs and reports any (hard or soft) failures. This component emulates the OAM functionality, as at the testbed there was no uniform OAM capability among the different switches. The NEC (Network Element Controller) which has a general representation of the Network Elements (the switches) and is responsible for every action concerning them. Every component that needs to perform anything at the switches has to communicate with the NEC. A generic interface has been defined, which is independent on the vendor of the switch, and has no knowledge of the internals of the switches.

The NEA (Network Element Adaptation) is vendor specific and its primary task is to provide basic node functionality, such as VPC and VCC management. The component has been implemented by using the SNMP interface that the vendors offer as the only way to access each switch fabric.

4. IMPLEMENTATIONARCHITECTUE OF THE SELF HEALING COMPONENT

The Self-Healing component has been designed as a distributed, real time module. Self-healers are being activated across the nodes of the working as well as the protection VPC. The adjacent self-healing components communicate with their peers over a control channel with a predefined VPI-VCI value.

The architecture of the self-healing component is shown at the next Fig.:

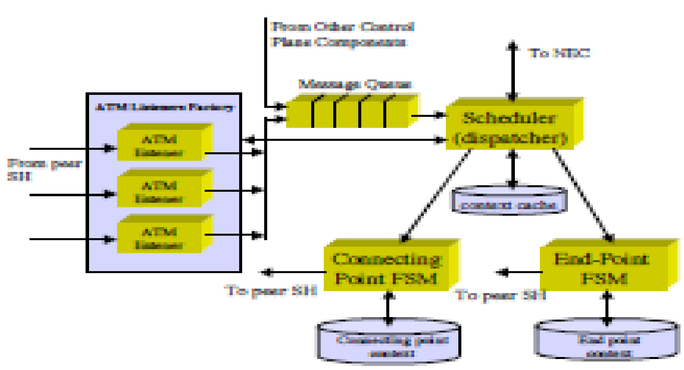

Fig. 5: The Self-healer architecture

The heart of the self-healer component is the scheduler. It gets input from the message queue and handles it according to the information that gets from the NEC about the GVPI for which this message is referring to. The context of all the messages that are exchanged is referred to the GVPI. Within the REFORM system, the GVPI (Global VP Identifier, see also Fig. 1) logically represents the connectivity between two VC switches. This connectivity, offers the basic infrastructure for VC switched service routing. Survivability has seamlessly been integrated in the routing function, by hiding the physical mapping of the working VPC and its associated The heart of the self-healer component is the scheduler. It gets input from the message queue and handles it according to the information that gets from the NEC about the GVPI for which this message is referring to. The context of all the messages that are exchanged (between the selfhealers in different nodes or between the control plane components) is referred to the GVPI. Within the REFORM system, the GVPI (Global VP Identifier, see also Fig. 1) logically represents the connectivity between two VC switches. This connectivity, offers the basic infrastructure for VC switched service routing. Survivability has seamlessly been integrated in the routing function, by hiding the physical mapping of the working VPC and its associated protection VPC. This way, protection switching performs its role without any reconfiguration needs in the overall system routing function. As such, all the messages that are exchanged between the peer self-healers as well as between the control plane components concerning a VPC are been identified by using this GVPI value only. All the information concerning this GVPI is being stored in the NEC component. So, every component that needs information about the GVPI value can get this information by asking the NEC.

The self-healer also, communicates with the NEC component for information about the VPC that are described by that GVPI. A caching mechanism is used, in order to minimize the effort continuously contacting the NEC about this info. Upon receiving of a message that contains a GVPI which is not currently at the self-healer's cache, the self-healer gets from NEC the appropriate information and adds it into its cache. In this cache, the scheduler keeps information about all the GVPIs that the self healer is handling, as an endpoint or a connecting node. Moreover, topological information is also been kept. This way, the scheduler can dispatch the message to the appropriate FSM. As the context of these FSMs varies dependent on the GVPI, these FSMs maintain their own context lists, where they keep information about the current state of the protocol for the specific GVPI, the file descriptor that they use in order to send a message to the peer self-healer etc.

At the phase of initialization of the self-healer, the RA is informing the Self-Healer, about the topology of the node that it is running on. This means, that the self-healer gets information about the ports that the node has, and about the control channels that have been established in order to accommodate the peer to peer self-healer messages. When the self-healer gets this information, it uses the ATM listener threads factory, to prepare threads that listen to the ports for messages from the peer self-healer.

In order to prove the feasibility of the REFORM concept, a REFORM compliant system has been built on top of the EXPERT testbed in Basle, Swiss. The REFORM network used for experimentation and demonstration purposes was initially based on a fully interconnected network of 5 nodes.

The self-healing component, as any other component that is part of the REFORM system is running on each controlling workstation. For the purposes of the integration at the testbed three workstations were used to control five switches. Of those three workstations, two of them had 2 ATM adapters installed, each one connecting with a different switch. So, a workstation that was used to control 2 nodes had two different logical instances of the REFORM node running. Various scenarios were defined for demonstration and experimental purposes. The REFORM network is depicted in Fig. 2.

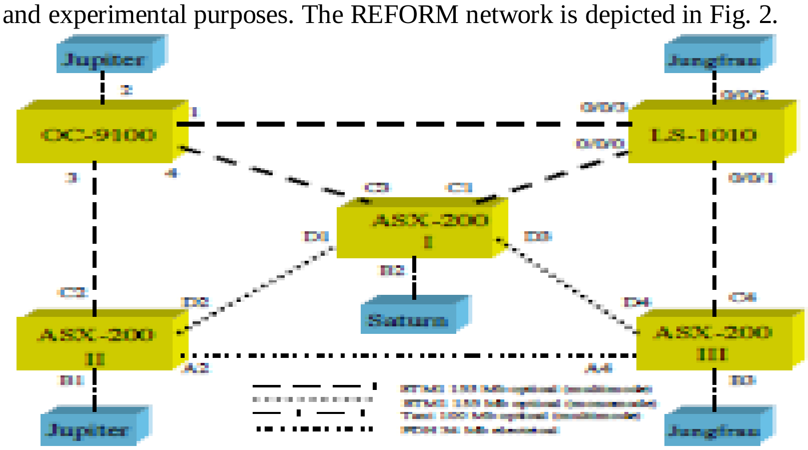

Fig. 6. The testbed configuration

Three switches from different vendors were used, (FORE ASX-200, CISCO LS-1010 and OLICOM OC-9100). As for the experiments five switches were needed, the FORE switch was divided into three logical switches by looping back two pairs of its ports. This had no implication at the experiments, (as the fiber of the switch was logically independent from switch to switch) except from the fact that a simple SNMP agent had to undertake in parallel requests from the two end-point switches. As endpoint switches at the experiments the two FORE switches were used. For our experiments, the following applications and test tools were available at the EXPERT testbed:

- the ISABEL application: video conferencing / video distribution application
- TPC/IP based (Internet) applications over ATM
- traffic generators and analyzers: for background traffic generation as well as traffic monitoring and analysis,
- Signaling load generator (call generator).

ISABEL is a video conferencing application with the capability of multiple concurrently active video windows. It uses the MJPEG standard for video coding. The application is executed under Solaris and is currently operated at the testbed within workstations with TAXI 100 interface attached to the FORE switch.

The signaling load generator (provided by NTUA) is capable of producing set-up requests for new calls based on user defined exponential probabilities. The tracing tool (provided by Solinet) system is a protocol analyzer that provides various features like time stamping, message filtering, performance measurements, statistics, etc. The system can be installed in the testbed and monitor the messages that sent between the REFORM components. The system can very efficiently be for the execution of the experiments and the analysis of the results.

5. EVALUATION

Due to the fact that the equipment supplied to the project does not explicitly and uniformly offer ATM OAM capabilities such as F4 AIS and RDI flows, the project had to rely on active supervision of the working VPCs by proprietary means. This implies that instead of having a fault detection of LOS at the physical layer resulting in an immediate sending of ATM AIS cells, a delay is introduced, arising from the active supervision of the VPC (between 30 and 300 ms, configurable). This delay has not been taken into account within the following analysis, where timing of events starts at the identification of the failure at the self healing processes. These SH processes run on workstations that have no dedicated resources for the restoration actions, that is to say, some of the results are influenced by the instantaneous load on the workstations CPU. This has been minimized to the possible extent. On line modification of the VPC bandwidth is not possible, and as such the VPC connection endpoints and connecting points of the protection VPC needed to be explicitly deleted and (re-) created in the switching equipment. In the case of the FORE switch, these actions take place atomically for both directions of the VPC leads to degraded restoration responsiveness.

A problem specific to the CISCO and OLICOM switches is that when a link is removed, the SNMP software cannot function (and therefore cannot switch-over) because the Administration status of the port is going to "DOWN" resulting the banning of any SNMP actions that involve this port. Therefore, connection endpoints have been implemented on the FORE switch. Besides of the unidirectional logic involved with the FORE switch, it is the only switch to adhere the notion of termination point, that is to say, before a VC connecting point can be instantiated, the VP termination point has to be in place.
The following provides the reader with the analysis of the measurements, which broadly quantify our expectations of performance of the self-healing function in a field trial. Wherever necessary, the implementation related influences are discussed.

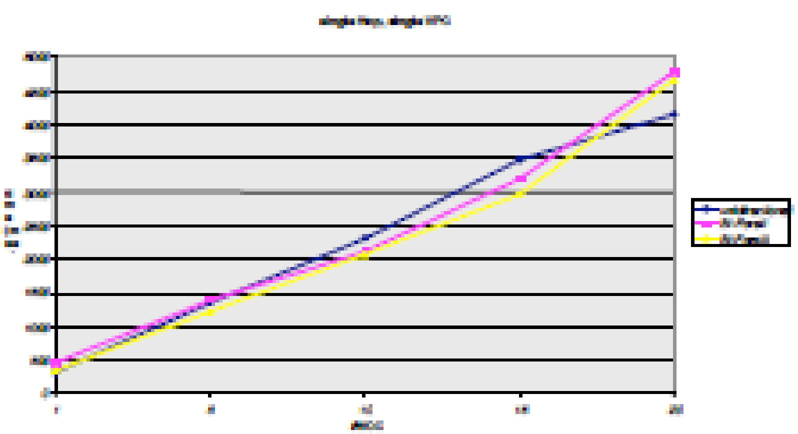

Fig. 7: 1 Hop, 1 VPC, unidirectional failure

Fig.7 shows the influence of the number of VCCs active in a VPC, for the single hop case. Both unidirectional and bi-directional failures have been depicted. In this picture we see the relative large influence of the single VCC reconfiguration time on the restoration results. Theoretically, the time needed for unidirectional failure restoration should be larger than the restoration time for bi-directional failure, since in the former situation, the remote side needs to be invoked by means of the reroute_req message, rather then by the invocation of its own FD functionality. This is a result that we do not explicitly find here in the results and the reason for this is because in both cases only unidirectional fault occurred. This can be explained as follows. The two FDs at the edges of the VPC are not synchronized. This means, that when a bi-directional fault occures, the

FDs don't report it at exactly the same time. Now, if a reroute request message arrives at one edge from the peer SH before the local FD reports any fault, the protocol thinks that this is a case of a unidirectional fault, as it has no indication that a fault occurred to both directions. So, all the actions that are taken are the same of a unidirectional fault. This of course happens only if the time for the reroute request packet to travel along the protection VP path is less than the " lag" that the FD has to its peer one. Such a case is the configuration of one hop, as the path of the protection VP through which the reroute request message travels, is short.

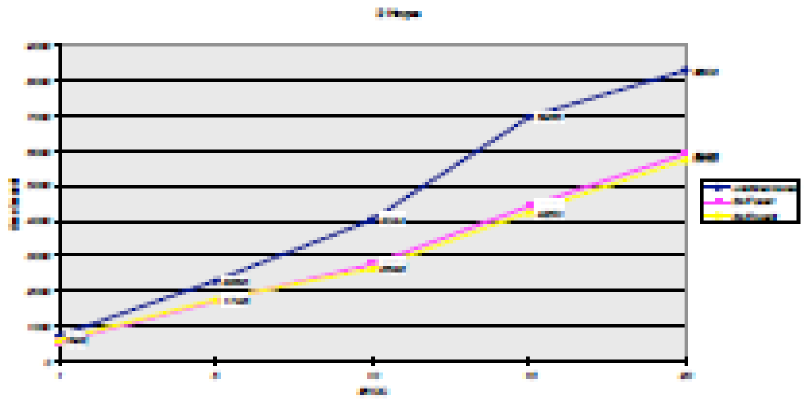

Fig. 8: 2 hops, 1 VPC

Fig. 8 shows the relative influence of the number of VCCs on the restoration time in case of 2 hops. In this case, since the processing time in the intermediate nodes is augmented, indeed, 2 hops need to be passed, the relative time difference between unidirectional and bidirectional failure is more pronounced. Note here that the restoration times for 20 active VCCs has risen from 4.5 seconds for the single hop case to 5.5 seconds for the double hop case.

Note here that the bi-directional fault could be restored even faster. The bottleneck in our experiments is the use of the same switch (FORE) as the endpoint-nodes (as discussed before). Although the FORE switch was logically divided into three switches, there was only one SNMP agent to support the SNMP requests for switchover. This resulted in the fact that although the switch overs at the edges were performing in parallel, the total time was more than the time that would be needed if the switchovers occurred sequentially. This overhead can be better depicted as following.

In order to perform the switch over we have to delete all the VCCs that passed through the effected VP and create new ones at the new VP. Also, we have to do this twice, once for the termination side and once for the originating. (The FORE switch has unidirectional logic, so we have to create / delete both sides). So, in order to perform one VC switch over, 24 SNMP actions are needed. If we multiply this with the number of connections thar are passing through the affected VP, we have the total of the SNMP actions that are needed for the switch-over. Although these actions seem to happen in parallel, the agent cannot support all of them, leading to a time larger than the one we expected. Although we have measured the average time that is needed for a VC to be switched over, and the average time that is needed for a VC to be switched over in parallel with another one (which is twice the previous time), we are not able to calculate how much is the overhead time that is the result of this non parallel operation. The reason for this is that there is again some time differences between the actions that happen at the two edges of the VPC. So, athough it seems that the two swichovers happen in parallel, there is some time where only one edge performs switch over. After a while, the other side performs also switch-over, overloads of the SNMP agent, and increases the avarage switch over time.

The effect of the introduction of new hops is more pronounced when looking at Fig. 9. When 3 hops are introduced, the restoration time for bidirectional failure further increases to 6 seconds.

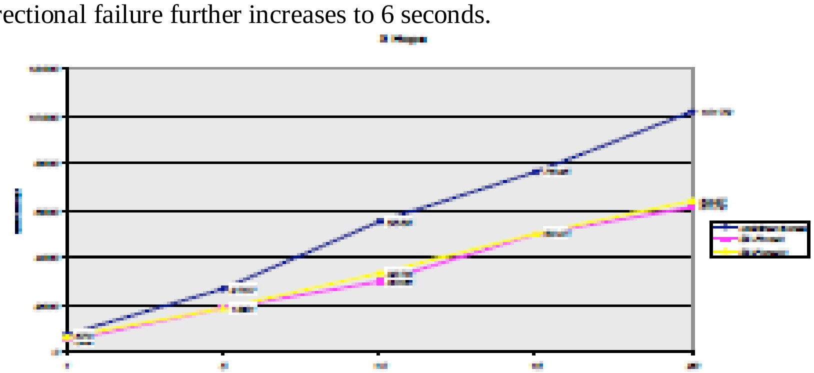

Fig. 9: 3 hops, 1 VPC

Fig. 10 depicts the relative influence of the number of hops on the restoration time. One can see that the relative influence of the number of active connections is larger than the influence of the number of hops. This is a result that one also can expect from an implementation viewpoint, since the processing effort needed to reconFig. both VP end points and all included VCC connections can be expected to be much larger than the time needed to reconFig. a single VP connecting point without the need to reconFig. the VC level.

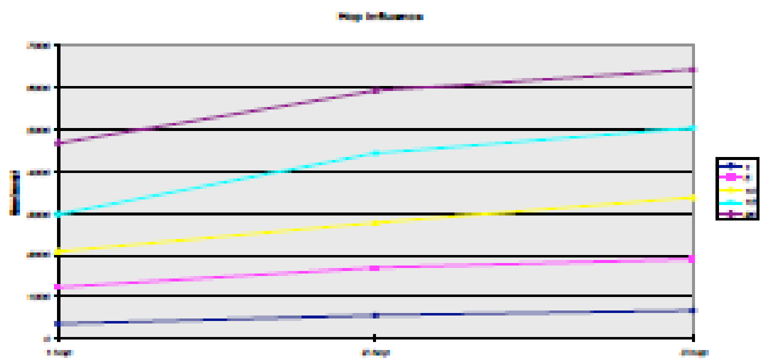

Fig.10: Hop influence on restoration speed

The times measured above, are the total times that passed from the moment that SH received the alarm from the FD until the time that SH has finished all the actions needed and notifies RA about the successful restoration. In the case of bidirectional fault, the actual time could be less. The reason for this is the way the switchover is performed. As there isn't any API to change the switching table inside the switch, SNMP is used to delete and create each VCC that crosses the VP that are to be switched over. So, the connections that are at the top of the list that holds the active connections of the VP are switched over much faster than the ones that are at the end of the list. This means that we can use this in order to achieve better restoration results for connections that are of higher restoration class by putting these VCCs at the top of the list.

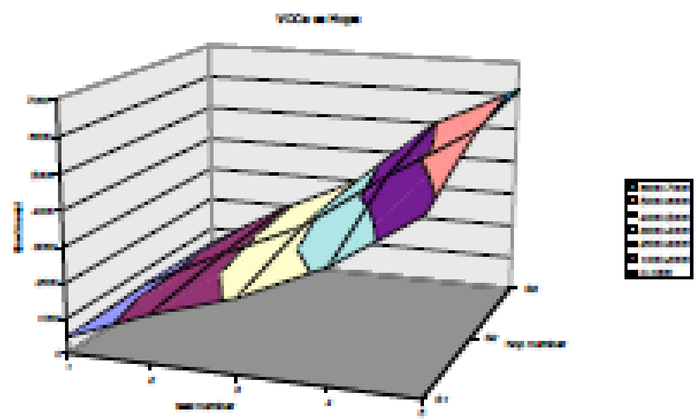

Fig. 11 : 1 VPC, relative influence of number of hops and VCCs (test number : 1=1VCC, 2=5VCC, 3=10VCC, 4=15VCC, 5=20VCC

Finally Fig.11 depicts the overall results of the performed tests, and so the relative influence of hop number and number of VCC active connections on the restoration time within the REFORM system.

6. Conclusion

In this paper, we presented the Self-Healing implementation of the REFORM system. The implementation approach as well as the evaluation of the component was presented based on real experiments performed in the REFORM/EXPERT testbed in Basle, Swiss. The following conclusion has been drawn:

The tests above have proven that the restoration times that are envisioned for the prototyping of an integrated solutions towards survivability and availability are within the reach of the project, furthermore has the project a good indication of how much time is involved in reconfiguration through means of SNMP actions, which indicates us that although ATM layer protection switching may involve more actions than SDH protection switching, a reconfiguration of the ATM layer may succeed well within the 2 seconds limit.

References

[1] ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures", Geneva, 1995.
[2] Draft baseline document on ATM Network Survivability Architectures and Mechanisms, version 3, February 1997, Seoul, Korea.
[3] ITU-T Recommendation I.ps, "ATM protection switching", Seoul, 1997.
[4] Veitch P., Hawker I., Smith G., "Administration of Restorable Vitrual Path Mesh Networks", IEEE Communications Magazine, December 1996.
[5] Kawamura R., Sato K-I, Tokizawa I., "Self-Healing ATM Network Techniques utilizing Virtual Paths", Networks 92", Kobe , Japan.
[6] Kawamura R., Sato K-I., Tokizawa I., "Self-Healing ATM Networks Based on Virtual Path Concepts" , IEEE JSAC, vol. 12, no. 1, January 1994
[7] Kawamura R., Hadama H., Tokizawa I., "Implementation of Self-healing Function in ATM Networks Based on Virtual Path Concept", Proceedings Infocom 95, 3b.1 , p303-311
[8] Kawamura R., Tokizawa I., "Self-Healing Virtual Path Architecture in ATM Networks "I,EEE Communications Magazine, September 1995.
[9] AC208-REFORM, Deliverable 1, January 1997
[10] Imai K., Honda T., Kasahara H., Ito T., "ATMR: Ring Architecture for Broadband Networks", Proceedings of IEEE GLOBECOM"90, December 1990.
[11] Anderson J. , Doshi B.T. , Dravida S., Harshavardhana P., "Fast Restoration of ATM Networks", IEEE JSAC, vol. 12, no.1, January 1994
[12] ATM Forum, ATM User-Network Interface Specification Version 3.1, September 1994
[13] Nederlof L., Struyve K., O'Shea C., Misser H., Du Y., Tamayo B., "End-to-End Survivable Broadband Networks", IEEE Communications Magazine, September 1995
[14] Robin Gareis, Peter Heywood, "Tomorrow's Networks Today's Data Communications, September 1995, pp. 55-65
[15] ITU-T Recommendation G.841, "Types and characteristics of SDH network protection architectures," Geneva, 1995. IFIP '97 conference Brandford.

Author's Profile

Dr.M.Usha Rani is an Associate Professor in the Department of Computer Science and HOD for MCA, Sri Padmavati Mahila Visvavidyalayam (SPMVV Womens' University), Tirupati. She did her Ph.D. in Computer Science in the area of Artificial Intelligence and Expert Systems. She is in teaching since 1992. She presented many papers at National and Internal Conferences and published articles in national & international journals. She also written 4 books like Data Mining - Applications: Opportunities and Challenges, Superficial Overview of Data Mining Tools, Data Warehousing & Data Mining and Intelligent Systems & Communications. She is guiding M.Phil. and Ph.D. in the areas like Artificial Intelligence, DataWarehousing and Data Mining, Computer Networks and Network Security etc.

K.Sailaja is a Research scholar in the Department of Computer Science (SPMVV) and working as assistant Professor in the Department of MCA, Chadalawada Ramanamma Engineering College, Tirupati. She is in teaching since 1999. She did her M.Phil in computer science in the area of WDM networks. She presented papers at National and Internal Conferences and published articles in national & international journals.