Chapter 19

Hierarchical Rerouting Model for Fault Tolerance in Multi-Network Environment

Won-Kyu Hong, Dong-Il Kim, Seong-Sook Yoon, Seong-Ik Hong, Mun-Jo Jung
Telecommunications Network Lab., R&D Group, Korea Telecom
463-1, Junmin-dong, Yusung-gu, Taejeon, Korea
Phone : +82-42-870-8254 Fax : +82-42-870-8229
{wkhong,dikim,pseudo,yeolin,mjjung}@kt.co.kr

Key words: Hierarchical Network Management, Rerouting, Fault Tolerance, CORBA

Abstract: ATM virtual path has recently been paying attention to the effective deployment of IP over ATM. The effective IP service provisioning depends fully on the reliability and optimality of ATM VP layer network because the relationship between IP and ATM VP networks is client and server. In order to guarantee the network survivability of ATM VP layer network and to provide the reliable IP service provisioning, this paper proposes a hierarchical rerouting model in multi-network environment of ATM VP and IP networks. In addition, this paper proposes the alarm correlation and localization model in the hierarchical transport network. And this paper describes the COBRA-based implementation model and its experience.

1. INTRODUCTION

Due to the rapidly growing demand for multimedia information transfer across the communication networks, the need for reliable communication service become more important. The potential effects of communication network failures have been demonstrated by several publicized studies, showing the need for survivable networks that are robust to failures [2,3]. A variety of network failures typically result from a failure by accidental cable cuts, hardware malfunctions, software errors, natural disasters, and human errors. Typically, failures can be classified into physical and software

J. N. de Souza et al. (eds.), *Managing QoS in Multimedia Networks and Services*

failures. Considering the failure by a fiber cable cut in a self-healing ring in a metropolitan area telecommunication network, we can restore it within several milliseconds by changing the direction of flow with other available backup links. However, using a ring approach in a national or an international network is likely to be cost-prohibitive. Because the spare capacity of the backup link provided for such restoration is unused during normal network operation and so we can make no profit by using the resource while being idle. Therefore, it is not cost-effective to provide for transmission level restoration in many networks.

The goal of fault recovery is to restore a large fraction of connections in usually less than two seconds. The restoration is performed at the lower levels of the transport hierarchy, such as the SONET/SDH transmission path layer, and is based on self-healing rings, spare backup trunks, and careful dimensioning of the network [6]. In an ATM based network, most restoration is performed at the Virtual Path (VP) layer, and consequently it provides the same QoS to all connections of the VP. There are three important issues related with restoration. One is how to correlate the alarms that may be generated by different network elements due to a failure, another is a fault isolation and localization, and the other is the time required to restore a failure by taking appropriate actions and the transient network behaviour.

On the other hand, layering concept is recently applied for the effective deployment of IP network and ATM network in terms of IP over ATM. The survivability of ATM network as a backbone of IP data network effects the reliable IP service provisioning because the relationship between ATM VP and IP layer networks is server and client. In order to guarantee the network survivability of ATM VP layer network and to provide the reliable IP service provisioning, this paper proposes a multi-layer network model that can commonly be applicable for IP network based on ATM network. This paper also proposes a hierarchical rerouting model based on the multi-layer network model that is very cost-effective because it does not need any extra capacities such as self-healing ring, spare trunks, etc. In addition, this paper proposes the alarm correlation and localization model in the hierarchical transport network. And this paper describes the COBRA-based implementation model and its experience.

2. HIERARCHICAL MULTI-NETWORK MODEL

In order to take the advantages of the capability of QoS guarantee of ATM and the capacity of diverse multimedia traffic delivery of IP network, we construct IP network over ATM backbone using the ITU-T G.805

layering concept [7]. ITU-T G.805 defines the ATM transport network architecture with the layering and partitioning concepts. From the perspective of layering concept, ATM VP network takes the role of server layer network and IP network takes the role of client layer network. All the Routers in IP network are interconnected with ATM VPC provided by ATM VP layer network and all the ATM VC switches in VC layer network are interconnected with ATM VPC provided by ATM VP layer network. Each layer network is designed in line with the ITU-T G.805 partitioning concept [1], ATMForum element view [7] and network view [8] as shown in Figure 1. Layer network partitioning aims to provide the network scalability and manageability and to promote the fault isolation and localization within the partitioned domain. Network Partitioning is normally done as the TMN functional layering concepts: Network Management Layer, Element Management Layer and Network Element.

Layer network is a topological component that includes both transport entities and transport processing functions that describe the generation, transport and termination of the particular characteristic information. Subnetwork (SNW) is a topological component that is used to define routing and rerouting domains of the specific characteristic information.

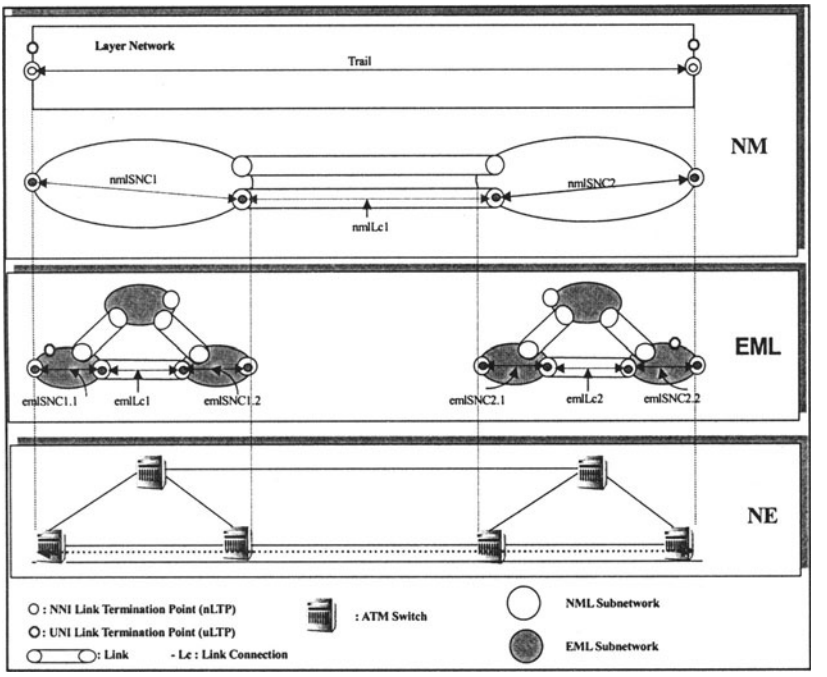

Figure 1. Hierarchical Network Model

Link is a topological component that describes a fixed relationship between one subnetwork and another subnetwork. Link connection (LinkConn) represents a transport entity that transfers information between nLtps across a link. UNI Link Termination Point (uLtp) is a reference point having the adaptation function between client and server layer network. NNI Link Termination Point (nLtp) is a reference point terminating link connection. Trail is a transport entity that is responsible for the transfer of specific characteristic information. Subnetwork connection is a transport entity that transfers information across a subnetwork and is formed by the association (or binding) of Ltps on boundary of the subnetwork. Connection Termination Point (ctp) is a reference point that is consisted of a pair of co-located bi-directional connections. Routeprofile is a transport entity that represents the route information of NML Subnetwork level. Subrouteprofile is a transport entity that represents the route information of EML Subnetwork level. Hierarchical transport network is described in terms of Rumbaugh's object modeling notation [9] as shown in Figure 2. It shows the object relationship between topological objects and connectivity objects.

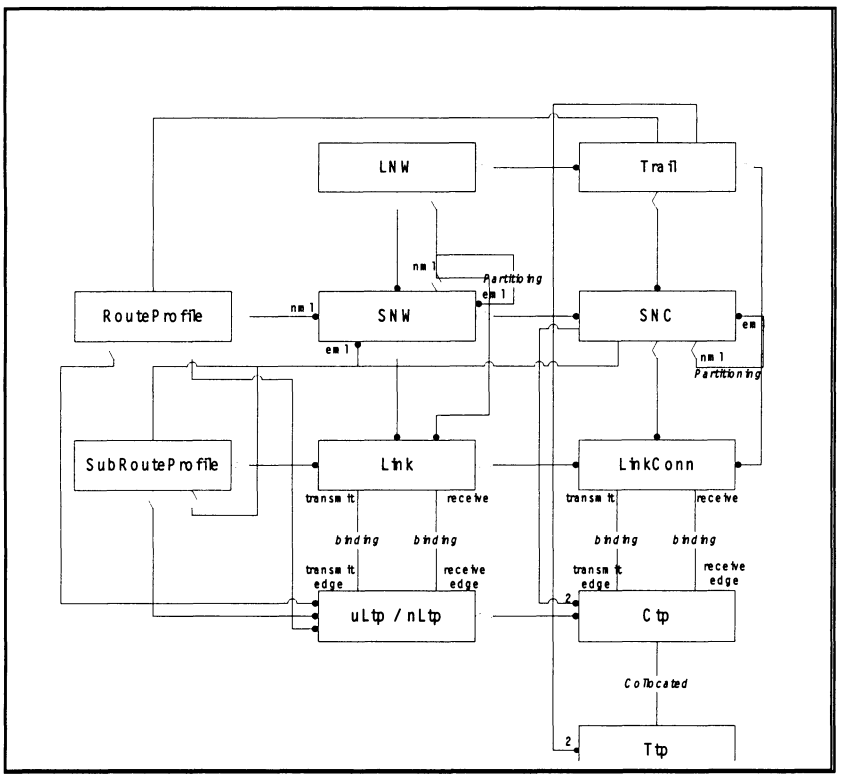

Figure 2. Hierarchical Transport Network Model

3. ALARM CORRELATION MODEL

Alarm correlation is generally made on the rule by which several alarms are narrowed from a mass of problems to a root cause and side effects. We define our own *Alarm Correlation Model (ACM)* taking into account the effective rerouting in the hierarchical transport network as our rules to identify the *Avoidance List (AL)* and to determine *Rerouting List (RL)* according to the fault location and types. The avoidance list represents the set of topological components that should be excluded in the rerouted path and the rerouting list represents the set of connectivity components that should be rerouted in the process of restoration.

We define only four kinds of alarm types for simplicity – UNI LTP (uLtp), NNI LTP (nLtp), SNW, and SNC. However we do not try to reroute in the case of uLtp alarm because there is no any alternative path. So we deal with only nLtp, SNW and SNC alarm as shown in Figure 3.

Our alarm correlation model is purely rule-based one as below:

In the case of *SNC fault* at Figure 3, the avoidance lists are the adjacent links (Link1 and Link2) connected with the nLtps (nLtp2 and nLtp3) that the fault SNC (SNC2) is terminated.

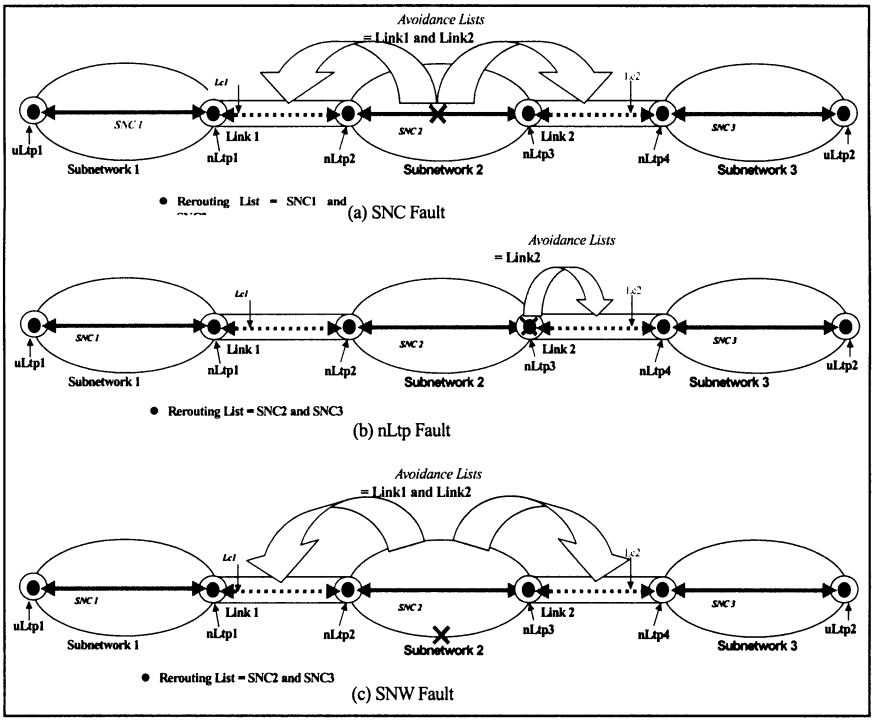

Figure 3. Alarm Correlation Model

The rerouting lists are the SNC1 terminated at the nLtp1 and the SNC3 terminated at the nLtp4 because the Link1 and Link2 are avoidance lists. When SNC alarm is generated, the SNC propagates alarm to its superior SNC and its terminating points of Ctps. The alarm is continuously propagated until the alarm is destined to IP Link of the client layer network like Figure 4.

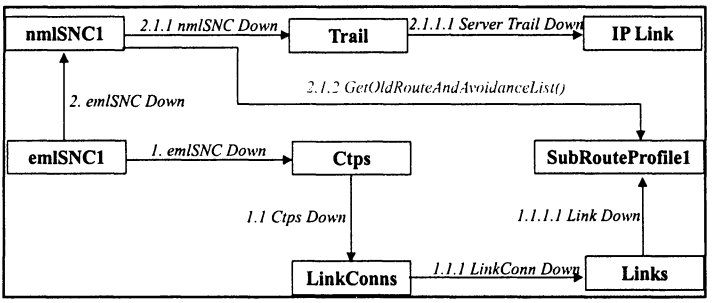

Figure 4. Alarm Propagation Model for SNC Alarm

In the case of *nLtp fault* at Figure 3, the avoidance list is the link (Link2) connected with the failed nLtp (nLtp3). Because Link2 is avoidance list, the SNC3 terminated at the nLtp4 and the SNC2 terminated at nLtp3 are rerouting lists. When nLtp alarm is generated, the nLtp propagates alarm to its bound Link and its contained Ctp. The alarm propagation is continued until the alarm is destined to IP Link of the client layer network like Figure 5.

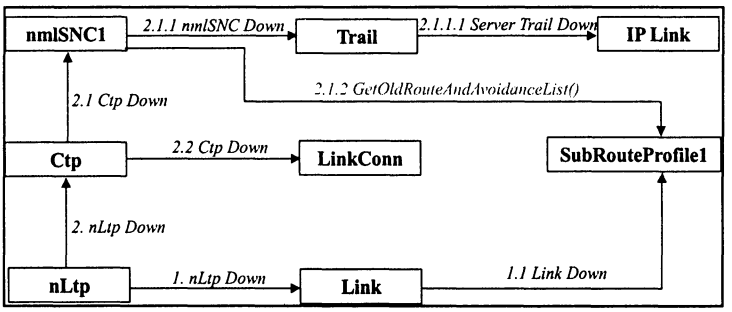

Figure 5. Alarm Propagation Model for nLtp Alarm

In the case of *SNW fault* at Figure 3, the avoidance lists are the adjacent links (link1 and link3) that belong to the failed SNW (SNW2) and the failed SNW itself. Because Link1 and Link2 are avoidance lists, the SNC1 terminated at the nLtp1 and the SNC3 terminated at the nLtp4 are rerouting lists. When SNW alarm is generated, the SNW propagates alarm to the Ltps

and the SNCs within the fault SNW. The alarm propagation is continued until the alarm is destined to IP Link of the client layer network like Figure 6.

In addition to identify the avoidance list and rerouting list, there is another difficult problem that is how we can determine and minimize the portion of restoration affected by a certain of alarm. It means the identification of rerouting scope. Fortunately, there is a useful concept of ITU-T G.805 partitioning [1] to determine the rerouting scope. A layer network can be partitioned into subnetworks according to the administrative domain or management boundary. Also, the partitioned subnetworks are recursively partitioned until the lastly partitioned subnetwork is corresponding to a switching fabric as shown in Figure 1.

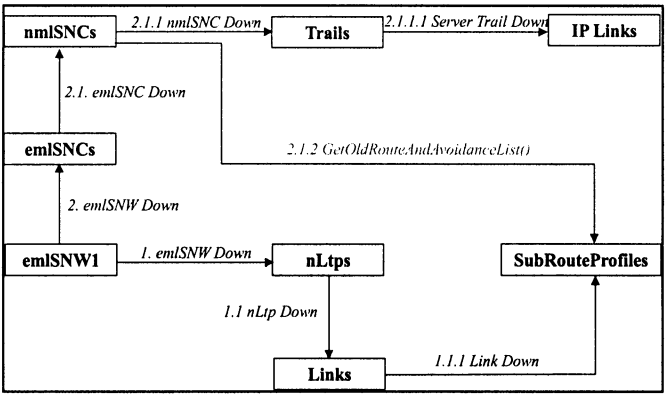

Figure 6. Alarm Propagation Model for SNW Alarm

Therefore the partitioned subnetwork itself can be the rerouting scope. The identification of avoidance list and routing list for rerouting is the role of NML function. There is another important concept for localizing rerouting scope. Rerouting scope in hierarchical transport network is determined by the location of alarm in hierarchical transport network like Figure 7. There are two kinds of rerouting scopes – subnetwork and layer network level. If an alarm is occurred at any object within a NML subnetwork (nmlSNW), its rerouting scope is the NML subnetwork. If an alarm is occurred at nLtps at the boundary of NML subnetwork, its rerouting scope is the layer network.

For example, in the first case of fault at Figure 7, its rerouting scope is nmlSNW1 and routed connection is nmlSNC1. If the restoration of nmlSNC1 fails within the nmlSNW1, its rerouting scope is expanded to layer network of Trail. In the second case of fault at Figure 7, the alarm is occurred at the nLtp of the boundary nmlSNW2 and its avoidance list is the Link between nmlSNW2 and nmlSNW3. The avoidance list of Link is managed by layer network and its rerouting scope is layer network of Trail.

There is another kind of alarm that cannot be restored in this model and any other models. It is the alarm of uLtp or nLtp that is the termination point of Trail like the third case of fault at Figure 7. Because we confine the end-to-end connection management scope in the UNI-to-UNI or NNI-to-NNI excepting the UNI Link, there are no more alternatives to restore such kinds of faults as the uLtp and nLtp containing the terminating trail termination point.

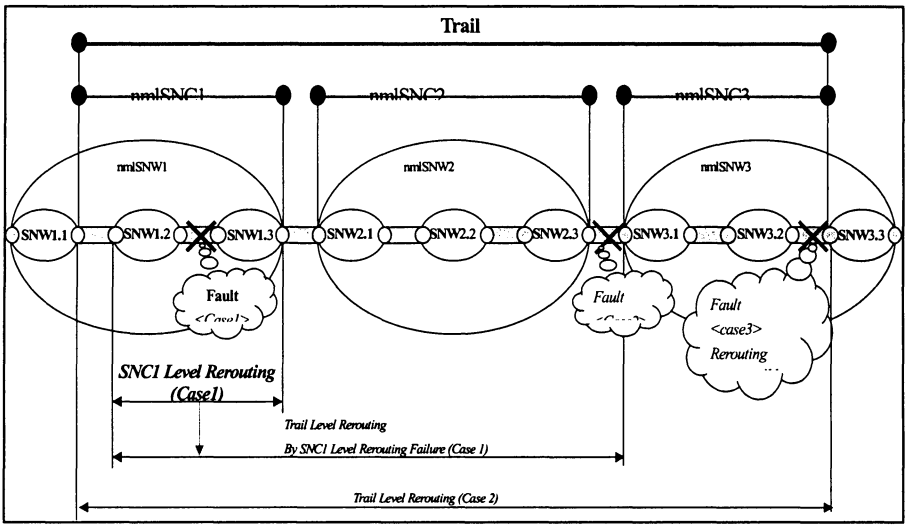

Figure 7. Rerouting Scope Model

4. HIERARCHICAL REROUTING MODEL

Our rerouting procedure is composed of five steps: (1) alarm propagation, (2) determination of avoidance list, (3) identification of rerouting list, (4) finding alternative route avoiding the avoidance list, and (5) restoration by SNC manipulation. Rerouting function is the role of the Network Management Layer (NML) function of TMN functional architecture. Therefore, there is not any rerouting function in the Element Management Layer (EML) but notification function of alarm occurrence to Network Management Layer (NML). Figure 8 shows the hierarchical rerouting model, which an end-to-end connection of Trail is composed of two nmlSNCs of nmlSNC1 and nmlSNC2. And each nmlSNCs are composed of two emlSNCs. This paper describes the rerouting procedure when the nLtp is down as shown in Figure 8 in line with the hierarchical rerouting procedure as shown in Figure 9.

Alarm Generation – A NNI Ltp (nLtp) down is notified to network management system.

Alarm Propagation - Alarm is propagated according to our alarm propagation rule. In the case of nLtp down, nLtp down alarm is propagated with the alarm propagation model of nLtp alarm of Figure 5.

Determination of Avoidance List – The first rerouting scope is nmlSNC1. The nmlSNC1 determines the avoidance list with the routing information stored in the SubRouteProfile. The avoidance list is Link1.1.

Find Alternative Route – The nmlSNC1 finds the alternative route that detours the avoidance list of Link1.1. There is one alternative route traversing the Link1.2 and Link1.3.

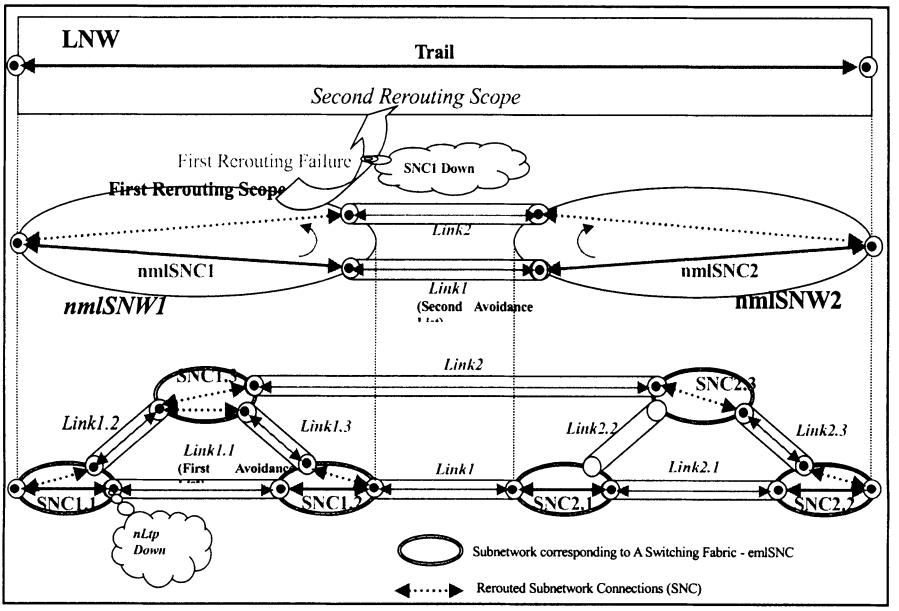

Figure 8. Hierarchical Rerouting Model

Identification of Rerouting List – As the comparison of old with alternative routes, it determines the rerouting list. Because rerouting list is the SNC that one of source or destination Ctp is changed comparing old with alternative route, the identified rerouting lists are SNC1.1 and SNC1.2.

Restoration by SNC Manipulation – There are three types of SNC manipulation for restoration: rerouting, creation, and deletion. The SNC that is not pertained in the old route but new route is newly created. The SNC that is not pertained in the alternative route but old route is deleted. With these rules, the SNC1.1 and SNC1.2 are rerouted and SNC1.3 is newly created. Whereas there is no deleted SNC because there is no SNC that is not pertained in alternative route but old route.

The restoration is done within the nmlSNC level. If the restoration of nmlSNC level failed, its rerouting scope should be expanded to the Trail level. And the avoidance list will be the Link1 and the rerouting lists will be nmlSNC1 and nmlSNC2.

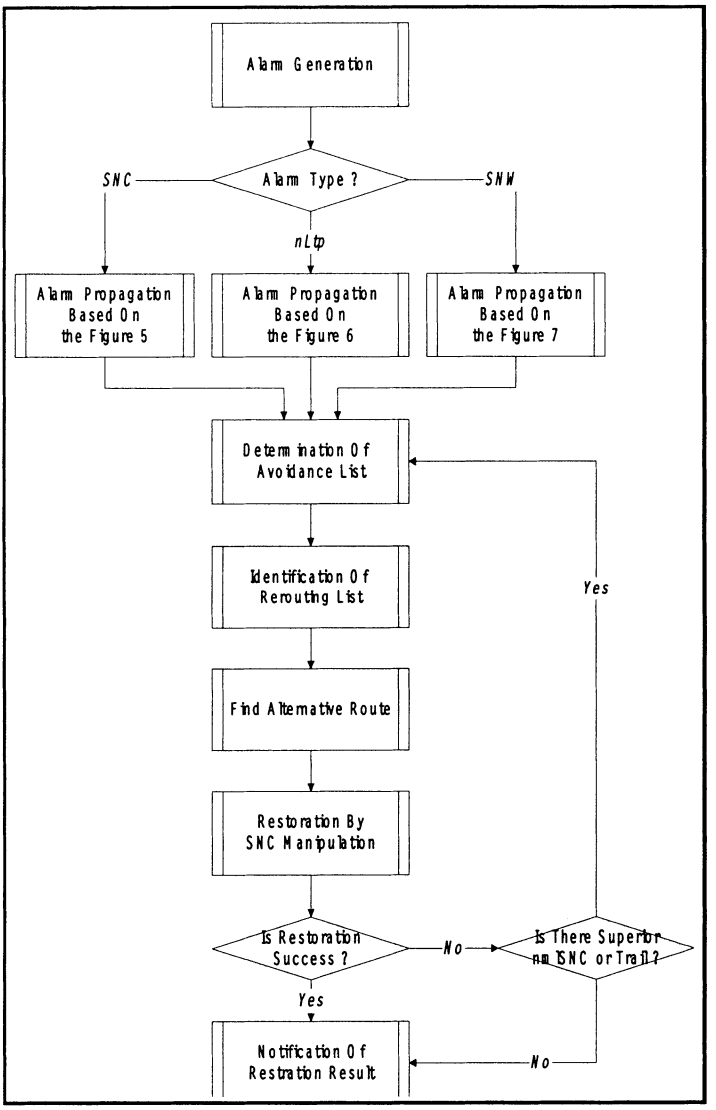

Figure 9. Hierarchical Rerouting Procedure

5. IMPLEMENTATION AND ITS EXPERIENCES

We implement the proposed hierarchical rerouting model with the CORBA platform to support distributed network management. We use the CORBA Event Service (ES) for alarm propagation. Our implementation model is shown in Figure 10.

Configuration Manger (ConfManger) takes the roles of provisioning and status monitoring of topological entities: layer network, subnetwork, uLtp, nLtp and link. Connection Manger (ConManager) takes the roles of creation, deletion and modification of connectivity entities of Trail, Subnetwork Connection, Link Connection, Trail Termination Point and Connection Termination Point. It also takes the major role of restoration by rerouting, creation and deletion of SNC in the procedure of *Restoration by SNC Manipulation*. Alarm Handler (AlarmHandler) takes the roles of alarm propagation and logging. Route Manager (RouteManager) maintains the routing tables and provides an optimal route in the case of connection setup and an alternative route in the case of rerouting. The routing and rerouting functions are solely defined in the NMS.

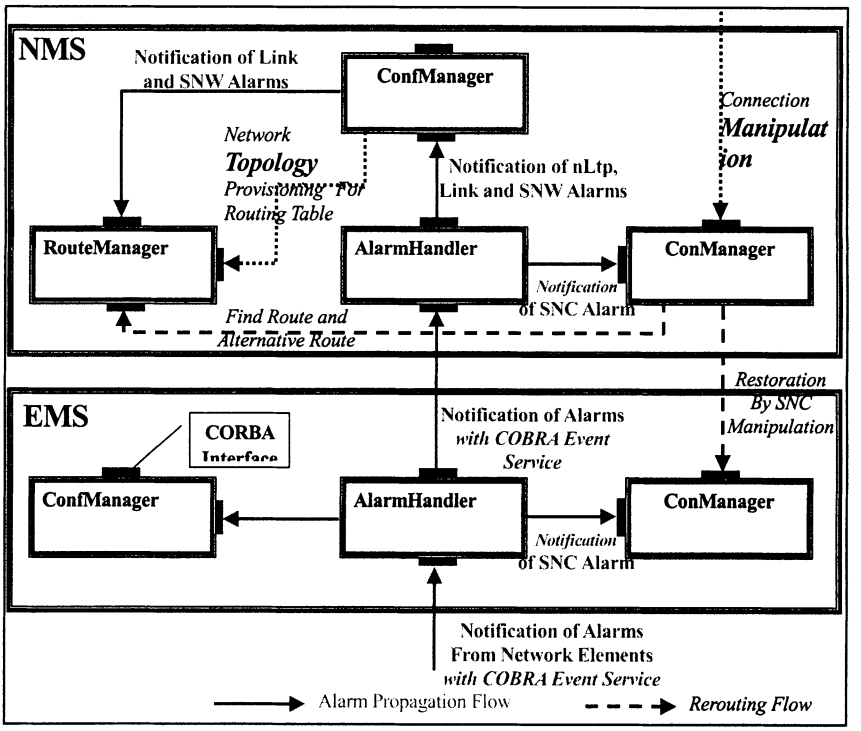

Figure 10. Implementation Model

We measure the empirical performance to validate the proposed rerouting model with the network topology like Figure 11. There are four nmlSNWs and each nmlSNW maintains the five emlSNWs. We measure the average restoration time in the two cases of the link down – one is contained within the nmlSNW, the other is contained within the layer network.

By our empirical performance analysis, we learn that the proposed hierarchical rerouting model can be applied to the large-scale ATM backbone network where each node is connected with STM-1. Figure 12 also shows the empirical VP restoration time in the case of nmlSNC and Trail level restoration with the test topology. The restoration time is measured in the case of failure of the STM-1 link that contains up to 10 VP connections. The average connection restoration time of nmlSNC level takes 1.1 seconds and that of Trail level takes 2.8 seconds including alarm propagation because of the restoration failure of nmlSNC level. The proposed rerouting model can be applicable for VP network taking the role of server layer of IP network. In the case of data network, average 2.8 seconds restoration time is reasonable.

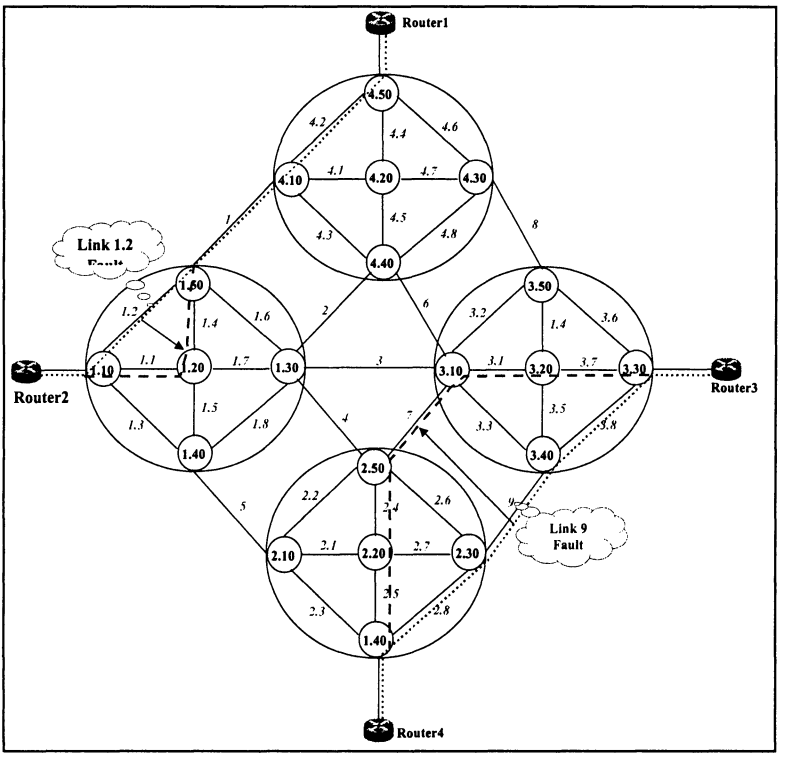

Figure 11. Network Topology for Empirical Performance Analysis

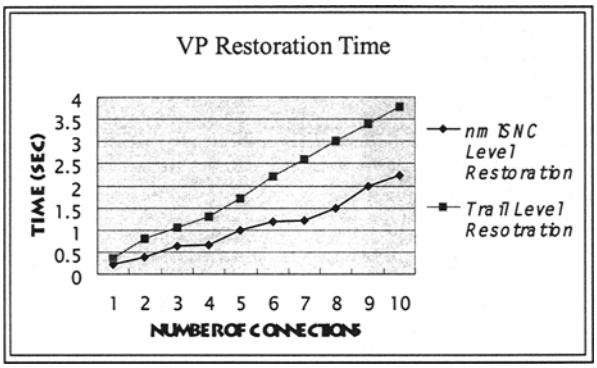

Figure 12. VP Restoration Time

6. CONCLUDING REMARKS

This paper proposes the hierarchical transport network model that can be applicable for multi-network environments. In the multi-network environment of IP and ATM VP layer networks, the reliability of VP layer network is essential for robust and efficient IP service provisioning. For reliable VP network management, this paper proposes a rule-based alarm correlation model fitted with the proposed hierarchical transport network and a hierarchical rerouting model applicable for VP layer network without any extra network facilities for restoration. With the proposed two levels of restoration – nmlSNC and Trail, we makes the restoration performance better by isolating the restoration scope within nmlSNC and increases the restoration probability by expanding the restoration scope to Trail in the case of restoration failure of nmlSNC level. Our empirical performance analysis shows that the proposed hierarchical rerouting model can be applicable for the large-scale ATM VP network with average 2.8 seconds restoration time.

REFERENCES

[1] ITU-T G.805, "Generic Functional Architecture of Transport Networks," November 19995.

[2] W. E. Falconer, "Service Assurance in Modern Telecommunications Network," IEEE Communications Magazine, Vol. 28(6), pp. 32-39, June 1990.

[3] T. H. Wu, Fiber Network Service Survivability, Artech House, Boston, Mass., 1992.

[4] Branerjea, "Simulation study of the capacity effects of dispersity routing for fault tolerant realtime channels," in Proceedings SIGCOM Symposium, pp. 194-205, August 1996.

[5] Banerjea, C. J. Parris, and D. Ferrari, "Recovery guaranteed performance service connection from single and multiple faults," in Proceedings IEEE Globecom, pp. 162-168, November 1994.
[6] J. C. McDonald, "Public network integrity – avoiding a crisis in trust," IEEE Journal on Selected Areas in Communications, vol. 12, no. 1, pp. 5-12, January 1994.
[7] ATMFroum, af-nm-0095.0001, "SNMP M4 Network Element View MIB," July 1998.
[8] ATMFroum, af-nm-0073.000, "M4 Network View CMIP MIB Specification Version 1.0," January 1997.
[9] James Rumbaugh, "Object-Oriented Modeling and Design," Prentice Hall, 1991.