UDC: 513.83:681.324
Original scientific paper

TOPOLOGICAL PLANNING OF COMMUNICATION NETWORKS

Mladen Kos, Matija Mikac, Domagoj Mikac
University of Zagreb
Faculty of Electrical Engineering and Computing, Zagreb, Croatia
{kos, matija, domagoj}@tel.fer.hr

Abstract: *In this paper, we concentrate on topological planning process of large-scale communication networks such as those used by telecom operators. Such networks are usually spread over large geographical area, and finding an optimal topology is very important part of the planning process. Network equipment used in such network is very expensive, and two connection points can be hundreds of kilometers apart. These networks, in most cases, form a backbone network of telecom operator, meaning that majority of traffic is carried through high-speed communication links of such network. Any cable cuts or equipment malfunctions could result in huge data losses. Therefore, such networks require high degree of availability and fault resistance, which must be considered during the planning process. Network topology providing fault resistance should offer at least two separate communication paths between any pair of network nodes. Most important issue in network topology planning is finding topology with lowest possible overall network price, while keeping all requirements (such as fault tolerance, availability, maximal number of hops, maximal blocking probability etc.) satisfied. Network design process can be divided into three stages. First step is making decisions about which network elements (nodes, existing edges) should be included in a backbone network (for instance, one of sub-problems appearing in this phase is facility location problem). Second step includes selection of network topology, so that all elements selected in first step will be interconnected satisfying given requirements. Last phase is used to determine node and link capacities needed for successful traffic transport as well as routings of traffic demands, including protection. Depending on technologies used in network, different routing and protection mechanisms, as well as specific topology models, can be used (e.g. SDH/WDM SHR, mesh, dual-homing etc.).*

Keywords: *topology, network, planning, backbone, algorithm.*

1. INTRODUCTION

In design process of today's high-capacity backbone networks, different network architectures are used. In order to minimize possible data losses and service unavailability in case of network failure, all the architectures must include reliable and fast protection and restoration mechanisms. Depending on the type of network, different approaches can be used. Other facts that has to be taken into account, during the network planning process, are, traffic demands, which represent the amount of traffic required between certain network nodes, maximal blocking probability, which determines the percentage of lost call due to network occupancy, relative price rations among different types of network equipments etc. The number of parameters taken into account determines the possible outcome of the planning process. The more input parameters lead to better solution. On the other hand, each parameter introduces another complexity dimension, and algorithms and calculation can become extremely complex even for the most powerful computers. For this reason different algorithms were developed, among which different input parameters can be used.

2. NETWORK DESIGN PROCESS

In our work, we concentrate on network that supports thousands of users on geographically large area. Quality of service is a key issue in such networks, and the following are just some of parameters that play an important role in network optimization. End-to-end delay and queuing delay should not be exceeded above some maximal value. This parameter is very important for networks serving a huge number of end users. Another parameter, which plays a major role in real time applications such as voice and video transmission, is a delay-variation. As mentioned before reliability and availability of services, and communication system must beat the high level, which can be achieved by redundant system and diverse communication paths. Decision on where to place network equipment is also an important issue. Usually network operator has many potential sites, and optimal facility placement can significantly reduce network cost. Type, and number of equipment required can also be optimized which can further reduce network cost. Price reduction of just few percent is significant reduction in the multi-million investments.

Network planning process can be divided into three stages. First step is to determine which of given network elements should be included in backbone network and make decisions about technologies and models that will be used. Next, based on input parameters, network topology should be selected, satisfying all the defined requirements. In order to satisfy survivability demands, topologies that are proposed should provide alternative protection routes and advanced automated recovery mechanisms. Finally, in third stage, node and link capacities have to be determined, so that all traffic demands can be transported through network. First stage will be called decision-making, second topology planning, and third stage network dimensioning. Each of these stages can further divided into many sub-problems that should be solved during the network planning process. This paper will discuss and briefly describe only few important network design and optimization problems.

It is necessary to define a simple and understandable network model, which can be used for mathematical definition of the problems. Network N can be defined as set of nodes V and set of edges E. Each node $v_i \in V$ can be described with arbitrary number of attributes, which depends on optimization problem that has to be solved. The simplest approach defines node using node location (geographical coordinates), node type and protection requirements. Node type is used to determine node installation cost and node classification – in planning process different node types are differently interpreted. Protection requirements define whether the node has to be protected (e.g. multiple connections with the rest of the network). Edges $e_i \in E$ are defined with two edge nodes, length and additional characteristics (cable type, regenerator spacing requirement etc.). Each subset of nodes

$SV \subset V$ and subset of edges $SE \subset E$ builds so-called sub-network. Sub-networking is often used in order to simplify network design – in that case, based on different principles, network is divided into few sub-networks. Each of these sub-networks is than processed separately, and finally all the sub-networks are interconnected building the main network. If existing network is to be improved, than initial set of edges includes existing edges, while in case of building a new network initial set of edges is empty. Traffic that has to be transported between nodes is defined in set of demands D. Each demand $d_i \in D$ is defined with source and destination nodes and required traffic amount. Using described model, where network N is defined with nodes V and edges E, and required traffic with traffic demands D, all the problems arising can be mathematically described. Additional requirements (such as fault tolerance, availability, maximal number of hops, maximal blocking probability etc.) represent constraints that have to be considered in planning process. In practice, it is not always the case that required input data is available, and optimization has to be performed using certain assumptions.

3. TOPOLOGY PLANNING

Topology planning process is used to suggest optimal topology for network being designed. Common models can be used for finding topologies on different network layers – physical layer and higher logical layers. Many different models were implemented in our designing tools *ATM Designer* and *Topology Designer*. Most of these models concentrate on finding topologies for survivable telecommunication networks. Failures in survivable networks can be restored using fast protection and restoration mechanisms, which will be described in following chapter. Protection mechanisms can work only if designed network provides at least two disjoint paths between every pair of network nodes. Higher degree of connectivity, meaning there are more than two disjoint paths between nodes, increases both network reliability and network costs. Therefore, it is necessary to find solution that would provide best reliability/cost ratio.

Topology planning methods implemented in our tools are divided into two basic classes — standard network topologies and hubbed network topologies. Both classes include methods for designing either single-connected, either two- or more- connected topologies, providing additional redundant edges that can be used for applying different protection mechanisms on different network layers. Standard network topologies include different mesh topology models, multiple tree models and single and multiple ring models. Hubbed network topologies include hierarchical relations between nodes, enabling simple node grouping and traffic concentration, with protection models like dual-homming.

As described in simple network model, each node $v_i \in V$ is defined with its coordinates, type and protection requirements. When finding topologies, coordinates are used to determine possible subnetwork groups and to calculate length of edges (edge price is proportional to its length). Node type is used for building hierarchy between nodes. Depending on protection requirements nodes are divided into two groups : special nodes and ordinary nodes. Special nodes are nodes that have to be protected, while ordinary nodes do not need protection. That means, special nodes must be at least two-connected, while ordinary nodes can be single connected to network using stars or trees.

Examples of standard network topologies are given in figures 1. and 2. In figure 1. resulting topology obtained using two trees combination is shown. All the special nodes in network are at least two-connected, providing satisfying protection possibilites. Ordinary nodes are single connected or multi-connected if that would not increase network costs. Figure 2. shows a result got using *RingHOP* method. This method builds huge single ring of all special nodes, includes ordinary nodes on ring using stars or trees, and finally adds additional edges in order to decrease overall number of hops in network.

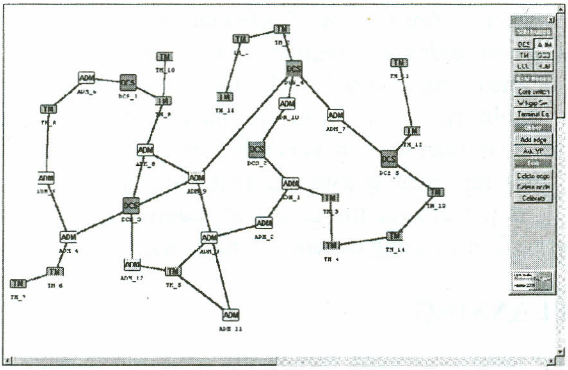

Figure 1 : Two trees combination

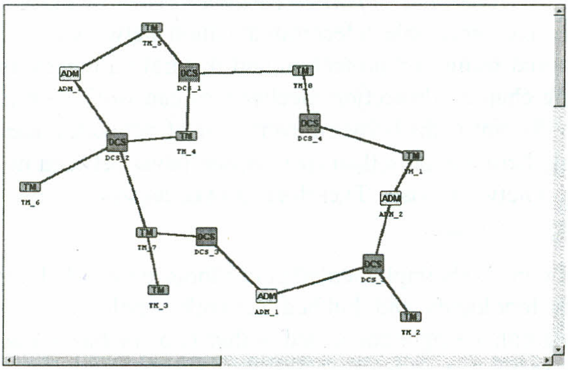

Figure 2 : *RingHOP* topology

Examples of hubbed network models are given on figures 3 and 4. Figure 3 shows standard hubbed network model. Different node types are interconnected hierarchicaly. Hubs are building small rings, and other nodes are connected using trees. In figure 4 advanced protection model is used for hub nodes. Each of those nodes is dual-hommed, meaning that it is connected with at least two, hierarchycally higher, nodes. On depicted example, dual-homming is achieved by multi-connecting groups (rings) of hub nodes.

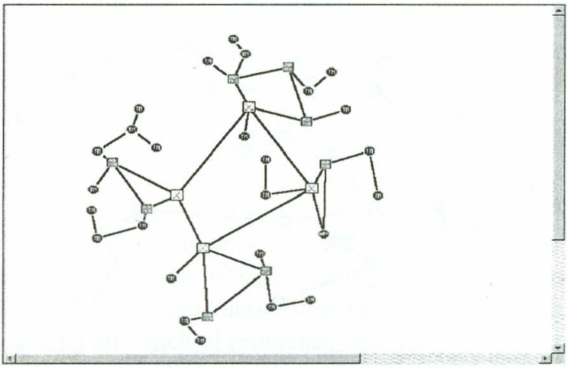

Figure 3 : Hubbed network

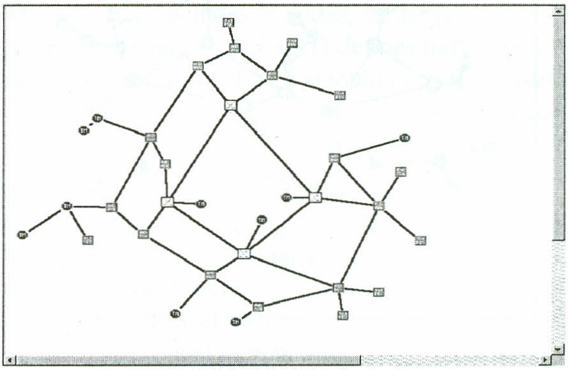

Figure 4 : Dual-homming model

During our research we came to conclusion that implemented methods do not always provide reasonable solutions, especially not for networks with iregular geographical characteristics. This is why, we developed additional methods for dividing network areas in subnetworks. Subnetworking approach was shown as a quite good solution for specific networks. Network topologies obtained using these methods consist of simple smaller rings, and stars or trees used for connecting ordinary nodes. Figure 5 shows two subnetworking approach examples. First example is obtained after dividing network in two parts, and second example is obtained using four subnetworks.

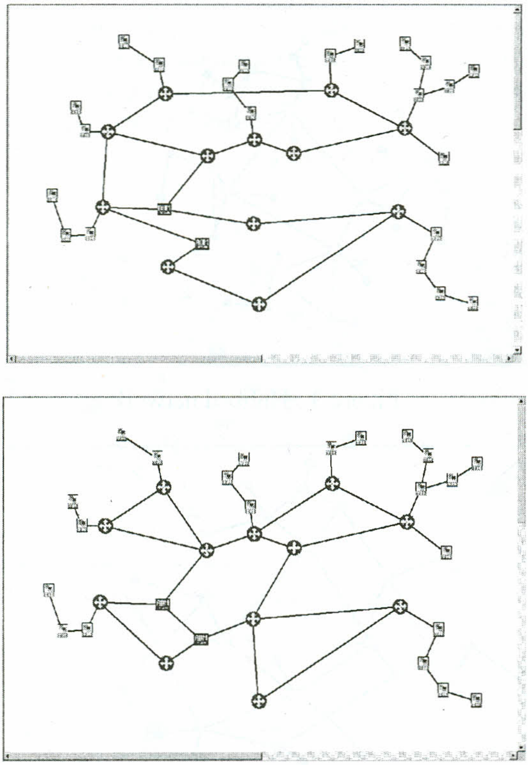

Figure 5 : Subnetworking approach

4. NETWORK DIMENSIONING

Final step in network planning process is network dimensioning. As a result of network dimensioning, each network element (node, edge) has to be fully defined/dimensioned. Node and link capacities needed for successful traffic transport have to be determined. Link and node capacity strongly depends, not only on traffic demands, but also on routing and protection mechanisms. By using optimal communication paths, network can be well balanced which guaranties than no links will be over-utilized or under-utilized.

Depending on network technology, different routing and protection mechanisms can be used. In ring networks (SDH, WDM) most widely used routing and protection models are those using self-healing ring (SHR) structures. Other approach is used in standard mesh networks (SDH, ATM, WDM), where routing and protection through network is made using more or less simple algorithms (e.g. shortest path + shortest disjoint path for protection).

4.1. RING NETWORK DIMENSIONING

Since introduction of SDH/SONET transport systems followed with development of WDM/DWDM transport systems, ring/cycle based networks became very popular and most common solution when building communication networks with advanced protection mechanisms. Using some simple principles, ring based networks provide execlent automatic protection solutions when facing possible failures in networks. Each network is built of certain number of interconnected rings. Traffic demands have to be routed through network, so that overall equipment costs (nodes, edge capacities, ring capacities) will be minimized. Problem of finding optimal solution, even for simplest ring networks, is very hard to solve. In single-ring networks, where whole network is built of one ring, only problem to be solved is optimal ring dimensioning – this problem is called ring dimensioning problem, sometimes also ring loading problem (RLP). RLP is main optimization problem in ring-based networks. When designing multi-ring networks, many other problems arise. It is important to find optimal node classification – nodes have to be classified and included on different rings, rings have to be interconnected optimaly, and finally, only after solving all bunch of problems, each ring has to be optimaly dimensioned solving RLP. Next, we will introduce ring dimensioning problem.

Based on our simple network model, let us define single ring network structure $R=(V,E,D)$. Set $V=\{v_1,v_2... v_N\}$, includes N nodes, set $E=\{e_{12},e_{23}... e_{N1}\}$, includes N edges eij between neighbor nodes vi and vj, and set D defines traffic demands dij between nodes vi and vj. Each demand is characterized with amount of traffic (positive integer value), and with its direction – if demand is routed from node v_i to node v_j passing node sequence (v_i, v_{i+1}, ... v_j) it is said to have a "clockwise direction", while if demand from node v_i to node v_j through node sequence (v_i, v_{i-1}... v_1, v_N,.. v_{j+1}, v_j) we say it has a "counter-clockwise direction".

Depending on possible direction of demands routing, rings are classified into two types – unidirectional and bidirectional rings. In unidirectional rings (USHR) all demands are routed in the same direction (either clockwise or counter-clockwise), while in bidirectional rings (BSHR) demands can be routed in both directions – clockwise and counter-clockwise. Additionally BSHR can be classified into two subclasses – rings without demand splitting and rings with allowed demand splitting. When demand splitting is allowed, one part of demand can be routed in clockwise, and another in counter-clockwise direction.

Link load is a sum of all demands passing through that link. The ring capacity is defined as maximum of all link loads. The ring cost is usually increasingly proportional with its capacity. Therefore, in order to minimize the ring cost we should try to find minimal ring capacity. In other words, optimal routing for given demands should be found, so that maximum link load will be minimized. Problem described previously is called Ring Dimensioning Problem or sometimes Ring Loading Problem (RLP).

It is obvious that when working with USHR, there is only one possible ring capacity (all the demands are routed clockwise or counter-clockwise, resulting the same maximum load through edges). Therefore, it is reasonable to define RLP only for BSHR rings. Example ring with non-optimal routing without demand splitting is given on figure 6. Demands for example ring are defined as shown in table 1. Ring capacity with demands routed as depicted on figure 6 is $C(R)$=29.

Table 1 : Example ring demands

Src.	Dest.	Demand
n_1	n_2	5
n_1	n_3	7
n_1	n_4	11
n_2	n_5	4
n_3	n_5	10
n_3	n_6	5
n_4	n_5	4

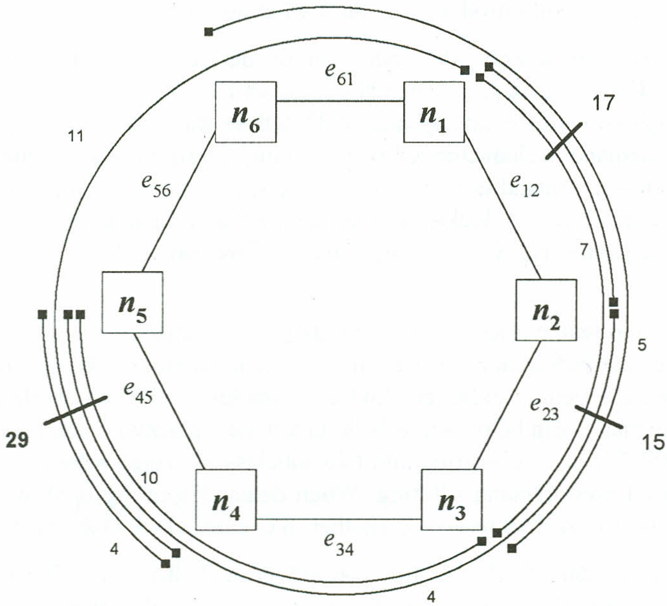

Figure 6 : Optimal demand routing for example ring

In order to find an optimal solution for ring dimensioning we should alternate all the possible routings for all demands, and pick the solution giving the best overall ring capacity. It is possible to do it for ring networks will small number of demands, but when we have to dimension larger rings such iteration process could take a lot of time even with fastest computers, which is often not acceptable. The number of iterations depends on number of traffic demands. Medium size networks can have couple hundred traffic demands, which makes impossible to find an optimal solution by simple iteration. In figure 7., number of iterations as a function of number of traffic demands is shown. In order to find an optimal or near-optimal solution, different fast algorithms for solving RLP were developed.

For obtaining optimal solutions linear programming approaches can be used – defined problem can be easily formulated as linear program, and solved using available software tools for mathematical programming. In our work we used AMPL [8] mathematical programming language and CPLEX solver.

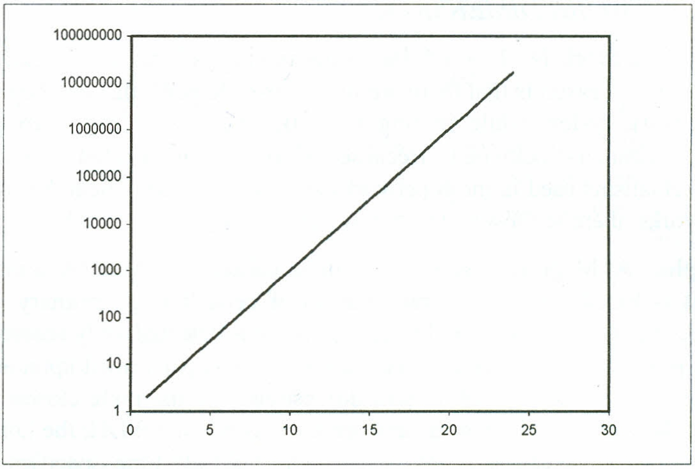

Figure 7: Number of iterations = f(number of traffic demands)

In our laboratory, we have developed software tool called *RingSolver* (figure 8) that efficiently solves RLP problems. RLP can be classified into two subclasses – without demand splitting and with demand splitting. When demand splitting is allowed, one part of demand can be routed in clockwise, and another in counter-clockwise direction. Link load is a sum of all demands passing through that link. The ring capacity is defined as maximum of all link loads. More reading material related to the ring loading problem can be found in [1][2][4][5][6][7].

It can be shown, and calculated using our tools, that optimal routing without demand splitting decreases ring capacity for example ring (table 1., figure 6.) to $C(R)$=25. If demand splitting is allowed, ring capacity is even smaller, $C(R)$=24.

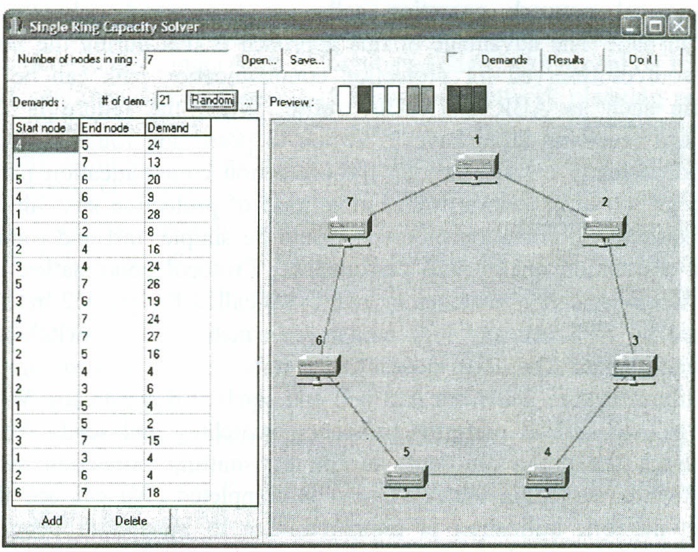

Figure 8 : RingSolver software tool

4.2. MESH NETWORK DIMENSIONING

When mesh network is observed, the dimensioning is more complicated than in ring networks. The main reason is that there are many possible paths that can be used to connect a pair of network nodes; while in ring networks there were only two possible paths (clockwise or counter-clockwise). Because of more complicated topology structure, protection mechanisms used in mesh networks are also more complicated and much slower. In ATM networks, there are few restoration techniques that can be used.

The simplest ATM protection mechanism is called 1+1 APS (Automatic protection switching). It is based on parallel transmission of cells through primary and secondary virtual connection. When failure on the primary route is detected, only receiving side has to switch to the protection route. The protection switching is performed upon arrival of alarm indication signal (AIS) cell which is sent downstream by the node closest to the failure. Optionally, if there exists lower layer network such as SONET/SDH, the hold-off time can be set for receiving protection ATM switch. The hold-off time specifies how long the protection switch has to wait after AIS-cell has arrived before it performs protection switching. The reason is that the lower layer network may have some kind of restoration mechanism and in that case it has advantage over the higher layer protection.

During the normal network operation, i.e. without failure in the network, the capacities reserved on protection route cannot be used for any other purposes, such as low priority UBR and ABR traffic. The reason for this is that working and protection virtual connection are permanently bridged at the transmitting protection switch. This method is very fast and simple, but on the other hand it gives very poor network utilization. This method can be used when extremely fast restoration is required.

Improvement of the 1+1 concept can be achieved if we try not to use parallel transmission. In this concept, which is called 1:1 APS, primary and secondary communication path are established the same way as in 1+1 APS with only difference that during the normal network operation cells are transmitted only through primary communication path. The advantage of this approach is that during the normal network operation, resources reserved for protection communication path can be used for low priority traffic such as ABR and UBR traffic. When the failure is detected, both transmitting and receiving sides have to switch to protection route, discarding the low priority traffic currently carried through the protection communication path. Since both sides have to switch to protection route, some kind of protection switching coordination protocol is required. Coordination protocol should be simple, fast and robust in order to give the best restoration quality and performance. Protocol coordination information is conveyed between protection switches by two bytes called K1 and K2 bytes. These bytes are transported by APS cell and they contain information about switching request and protection switch status. The node closest to the failure in the downstream direction first detects the failure. It than generates AIS cell and sends it downstream. When protection switch receives AIS cell, it performs protection switching and sends APS-request cell upstream through the protection route to the transmitting protection switch. After it performs protection switching the restoration is completed. We can see that using this approach, the network utilization is improved, due to bandwidth being reserved for protection communication path can be used for low priority UBR and ARB traffic.

Previous two APS schemes are already specified by ITU-T organization [10], but the open question is how to reduce the amount of extra network resources needed for protection communication path. The answer to this question can be found if we try to share protection communication path among two or more working paths. To make this possible, we have to make an assumption that never more then one failure occurs at the same time. This assumption is quite realistic, since probability that two failures will occur at the same time is negligible. Taking this into account, it is possible to design a network in which two or more primary virtual connections share a common protection resource. This model is called m:n APS model, because n primary virtual connections share m secondary virtual connections, where m is less or equal to n. Protection resources can protect only those primary connections that use independent routes. Therefore, when single failure occurs only one primary connection has to be switched to its protection route. The other primary connections that share the same protection resource do not have to be rerouted because they are on different routes, which are not affected by the failure. If route independency would not be taken into account, then the single failure could cause the situation where two or more primary connections are rerouted to the shared protection resource, which is not possible. Coordination protocol for m:n APS can be the same as in 1:1 approach. It is understandable because for the end user, m:n APS acts as 1:1 protection. The only difference is that network designer assumes that never more than one failure occurs at the same time, and assigns the same protection resource to more than one carefully chosen working connection. Restoration time is the same as in 1:1 APS approach. As we can see, m:n APS requires minimal amount of extra network resources, and gives the best network utilization. The amount of extra resources is directly proportional to the network cost. Therefore, reducing the amount of extra recourses is very important for telecom operators, especially if they have to lease bandwidth from SDH operator. More reading material on protection mechanisms can be found in [1][11][9].

5. CONCLUSION

In this paper, we have conceptually described a network topology planning process. Our approach defined three main steps in topology design, with accent on few optimization problems that can arise during planning process. But, network planning process is much more complex than described. Real-world networks cannot be planned with such ease, because of many additional problems that can arise. Even when trying to define real-world networks using simple network model, many problems due model limitations can arise. There are no universal tools for designing networks available. Each tool developed, commercial or non-commercial, is focused on solving group of specific problems. Even when producing feasible solutions, additional steps in designing process have to be used to verify given solutions.

REFERENCES

[1] Wu, T.H, (1992): *Fiber Network Service Survivability*, Artech House, Massachusetts

[2] A. Schrijver, P. Seymour, P. Winkler (1998): *The Ring Loading Problem*, SIAM J. Descrete Math., Vol. 11, No. 1, pp. 1-14,

[3] Gavish B. (1992): *Topological design of computer communication networks – The overall design problem*, EJOR Vol. 58, pp. 149-179

[4] S.Cosares, I. Saniee, "An optimization problem related to balancing loads on SONET rings", Telecommunication Systems, 3 (1994), pp. 165-181.

[5] C.Y.Lee, S.G.Chang, "Balancing loads on SONET rings with integer demand splitting", Computers Ops. Res., Vol. 24, No. 3. pp. 221-229, 1997.

[6] Y-S.Myung, H-G.Kim, D-W.Tcha, "Optimal load balancing on SONET bidirectional rings", Operations Research, Vol. 45, No.1, January-February 1997.

[7] A. Schrijver, P. Seymour, P. Winkler, "The Ring Loading Problem", SIAM J. Descrete Math., Vol. 11, No. 1, pp. 1-14, February 1998.

[8] AMPL: A Modeling Language for Mathematical Programming, www.ampl.com

[9] C. Wu, S. Lee, "Modeling, Algorithms and Analysis of Survivable VP Planning in ATM Networks", IEICE Trans. Commun., Vol. E82-B, No. 4, pp. 591-599, April 1999.

[10] ITU-T Recommendation I.630, "ATM protection switching", February 1999.

[11] CCITT Recommendation M.495, "Transmission restoration and transmission route diversity: terminology and general principles", November 1988.

Received: 9 January 2003
Accepted: 9 October 2003