Design of Resilient Ethernet Ring Protection (ERP) Mesh Networks With Improved Service Availability

Mohammad Nurujjaman, Samir Sebbah, and Chadi M. Assi

***Abstract*—Ethernet Ring Protection (ERP) has recently emerged to provide protection switching for Ethernet ring topologies with sub-50 ms failover capabilities. ERP's promise to provide protection in mesh packet transport networks positions Ethernet as a prominent competitor to conventional SONET/SDH and as the technology of choice for carrier networks. Higher service availability, however, in ERP has been challenged by the issue of network partitioning and contention for shared capacity caused by concurrent failures. In this paper, we show that in a network designed to withstand single-link failure, the service availability, in the presence of double link failures, depends on the designed ERP scheme, i.e., the RPL placement as well as the selection of ring hierarchy. Therefore, we present a study for characterizing service outages and propose a design method which strikes a balance between capacity requirement and service availability (i.e., the number of service outages resulting from concurrent failures). We observe that through effective design, remarkable reduction in service outages is obtained at a modest increase in capacity deployment.**

***Index Terms*—Dual failures, ethernet ring protection, restorability, service availability, survivable network design.**

I. Introduction

ETHERNET technology is expected to achieve carrier grade functionalities and it exhibits an enormous potential to be a cost-effective and less complex replacement of SONET/SDH, especially after the ratification of the IEEE 802.1Qay Provider Backbone Bridge-Traffic Engineering (PBB-TE) [1], [2]. The challenge of providing high service reliability with SONET/SDH-like fast restoration times (50 ms) is greatly reduced by the recent ITU-T Recommendation G.8032 [3], referred to as Ethernet Ring Protection (ERP), which certainly improves the candidacy of Ethernet to replace the legacy SONET/SDH networks in the near future.

ERP promises to provide high service reliability in Ethernet transport networks with a failure restoration mechanism that guarantees network recovery of less than 50-ms in a 1200-km ring with less than 16 nodes [3]. The advancement and prosperity of ERP, however, comes with new challenges in network design, due to its unique operational principles. The placement of Ring Protection Links (RPL) and the selection of logical ring hierarchies among interconnected rings play an important role in capacity allocation and design of cost effective ERP-based mesh networks. In addition, protection switching against double link failures have not been yet properly investigated and addressed by the ITU-T G.8032 recommendation, which specifies the operations of ERP. However, a dynamic recovery procedure is being discussed in the newer version of the recommendation G.8032v2 [3], but it has not yet been integrated into the recommendation. In a mesh network where multiple logical rings are interconnected, the protection switching may act unusually or unexpectedly in case of concurrent failures. The absence of a well-studied survivable plan in the recommendation to protect ERP against such failures is one of its major limitations.

There has been some recent effort related to the efficient design of ERP-based mesh networks with optimal capacity allocation to achieve 100% restorability against single-link failures [4], [5]. However designing a network to survive only single-link failures does not empower network providers to provide high service availability, which may be demanded by customers for mission-critical services, in case of multiple concurrent failures in the network. Dual failure survivability has been extensively studied during the last decade for different types of transport networks (e.g., WDM, MPLS, etc.) [6]–[10]. To the best of our knowledge, none of the previous work addressed the problem of provisioning a protection plan for the recently standardized Ethernet based transport networks to survive against dual failures.

Due to its unique operational principles, Ethernet's protection scheme (ERP) requires particular attention when the network design method is extended to address dual failure restorability. For example, investing adequate additional capacity in ERP to provide 100% dual failure restorability cannot guarantee uninterrupted services upon double link failures. Double failures in a single stand-alone ring will cause unavoidable network partitioning (*Physical segmentation*) and there will be obvious service interruption if the source and destination nodes of the requested service are in different segments of the network. Nevertheless, some service outages due to network partitioning (*Logical segmentations*) in ERP multi-ring mesh networks can be avoided by efficient logical design of interconnected ring hierarchies.

In this paper, we focus on minimizing the service outages caused by logical segmentations. We highlight a trade-off between the overall capacity investment and reducing service outages due to logical segmentations; this trade-off will be a subject for further investigation in this current paper. We develop a multi-objective Integer Linear Program (ILP) whose objective

Manuscript received May 03, 2012; revised September 09, 2012, October 20, 2012; accepted October 30, 2012. Date of publication November 15, 2012; date of current version December 28, 2012. This work was supported by an NSERC research discovery grant and by FQRNT.

The authors are with Concordia University, Montréal, QC, H3G 2W1, Canada (e-mail: m_nurujj@encs.concordia.ca, ssebbah@encs.concordia.ca, assi@encs.concordia.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2012.2227939

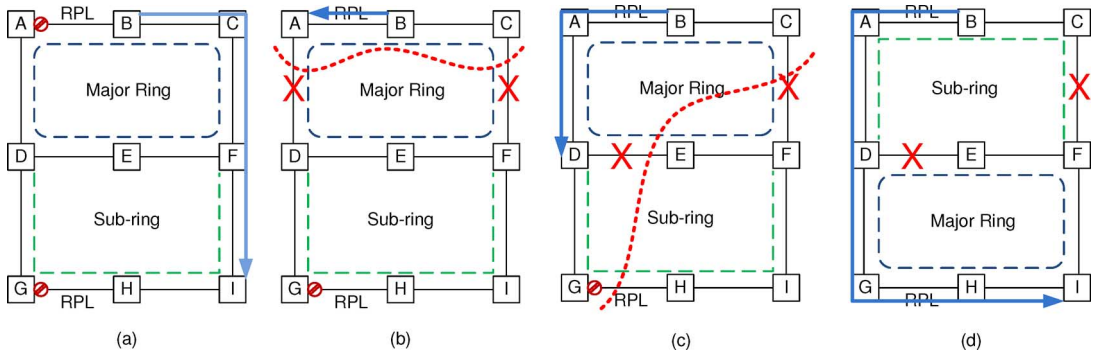


Fig. 1. Physical and logical segmentation.

is to minimize the overall number of service outages caused by network segmentations due to double link failures while minimizing the overall capacity investment in the network. Further, we consider those contending connections in our design which are restorable, but suffer from outages due to lack of capacity. We develop a routine to estimate the amount of additional capacity which needs to be deployed to eliminate contention for shared capacity. Finally, we present a comparative study about the impact of the design approaches on network-wide restorability.

The rest of the paper is organized as follows. Section II characterizes the service outages in ERP networks. We present the mathematical formulations of ILP model in Section III. The preliminary set of numerical results are presented and analyzed in Section IV. We analyze the further observations of preliminary results in Section V which includes the final set of numerical results. Section VI includes concluding remarks.

II. Characterizing Service Outages in ERP

A. ERP Background

Ethernet Ring Protection (ERP) is a recent recommendation from ITU-T which provides SONET/SDH-like reliability in Ethernet transport networks. ERP builds a logical ring topology to provide sub-50 ms restoration time while maintaining a loop-free forwarding mechanism by logically blocking a link port in the ring, referred to as Ring Protection Link (RPL). One or both adjacent nodes (RPL owner) of RPL are responsible to logically block/unblock the RPL port. Upon receiving control messages, that are sent by a failure detection mechanism, the RPL owner unblocks its designated RPL port. In such situation, filtering databases (FDB) in each node of the ring need to be flushed and repopulated by the Ethernet MAC source address learning process. A mesh network can be designed as a composition of multiple interconnected logical Ethernet rings (major/sub). A major ring constitutes a closed ring while a sub-ring constitutes an arc or a segmented arc (see Fig. 1(a)). Sub-rings are connected to a major ring or another sub-ring via interconnection nodes. Interconnected rings may share one or multiple links between them; however, only one ring will be responsible of managing the shared links. A logical hierarchy between interconnected rings can be established based on the ownership of the shared links. The major ring is always responsible for all of its links including the links that are shared with other sub-rings. A sub-ring is referred to as upper ring with respect to another sub-ring if it is responsible for the links that are shared between them and unblocks its RPL port in case of any failure in shared links.

B. Outages due to Partitioning and Suggested Remedies

As we mentioned earlier, any double link failure scenario in a single stand-alone ring will partition the network and will prevent some nodes in one segment to communicate with other nodes in the other segment. Such segmentations are referred to as physical segmentations, and there is no remedy for such a failure in a single ring topology. A physical segmentation will disrupt the service only when both the source and destination of a connection are in different segments of the network. Nonetheless, in ERP-based mesh networks, where multiple rings are interconnected with each other, service outages due to network partitioning resulting from some double link failures could be avoided by properly selecting the link RPLs as well as ring hierarchies, as will be illustrated in the sequel; such segmentations we refer to them as logical segmentations. A logical segmentation involves at least one failure on a link which is shared by interconnected rings. This work proposes a design strategy where the number of possible logical segmentations, in a network designed to withstand all single-link failures, can be reduced (hence the number of outages following double link failures) by efficiently selecting the owner of the shared links, i.e., by efficient design of logical hierarchy of interconnected rings and assignment of RPLs.

To illustrate, we consider a simple network with two interconnected rings as shown in Fig. 1. The major ring includes nodes A, B, C, F, E, and D while the sub-ring includes nodes D, G, H, I, and F. The RPLs of the major and the sub-ring are placed on links $A-B$ and $G-H$ respectively. A service is requested from node B to node I which is routed through $B-C-F-I$ in normal (Idle) state as presented in Fig. 1(a). Fig. 1(b) depicts a double link failure situation where links $C-F$ and $A-D$ fail causing physical segmentation, which are not restorable without topology change or additional resources. Another double link failure scenario is presented in Fig. 1(c) which includes double link failures on links $C-F$ and $D-E$. In this failure scenario, the network becomes logically segmented. This logical segmentation can be avoided by changing the logical hierarchy. Let us assume that the same network is designed as shown in Fig. 1(d) where the major ring includes

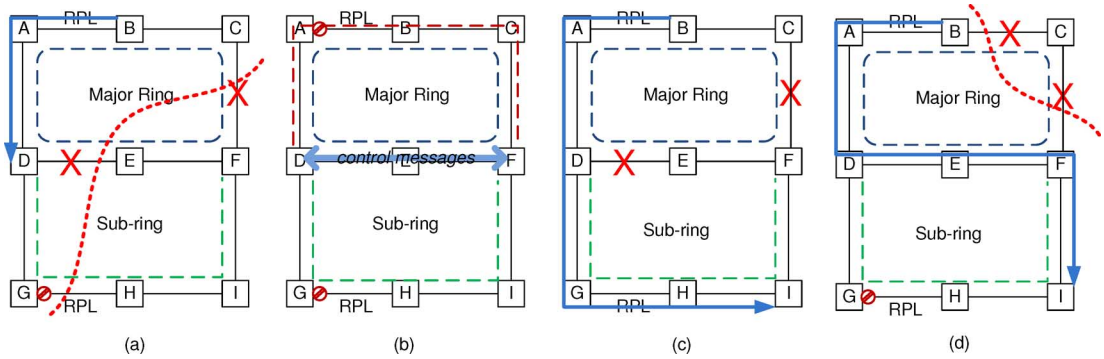


Fig. 2. Dynamic procedure.

nodes D, E, F, I, H, and G and the sub-ring includes nodes D, A, B, C, and F. In case of a failure on link $C-F$, the RPL port of the sub-ring will be unblocked and the subsequent failure on link $D-E$ will unblock the RPL port of the major ring. Hence, the network segmentation caused by this double link failures (Fig. 1(c)) will no longer cause any service outage.

The issue of network segmentation due to double link failures in interconnected ERP rings is somehow addressed by the ITU-T working group. A dynamic procedure has been suggested by the working group as a remedy against logical segmentations. In this procedure, interconnection nodes of two interconnected rings periodically exchange control messages to verify the connectivity between them by testing two tandem connections in the upper ring. Some additional management information is required to ensure proper functioning of the procedure. If any loss of connectivity is identified by the interconnection nodes, the block indication logic, based on the additional management information provided, performs the manual switch (MS) command to the sub-ring port which unblocks the RPL port of the sub-ring temporarily. Fig. 2(a) shows the identical double link failure situation of Fig. 1(c) where a logical segmentation has occurred. According to the suggested procedure, interconnection nodes D and F should periodically exchange control messages to verify the connectivity of two tandem connections $D-F$ and $D-A-B-C-F$ (Fig. 2(b)). Since the failure scenario of Fig. 2(a) yields a loss of connectivity between nodes D and F, the block indication logic that is implemented at nodes D and F performs the MS command to the sub-ring port and the sub-ring unblocks the RPL port on link $G-H$. Fig. 2(c) illustrates that the network is in MS mode and the particular logical segmentation is avoided.

The suggested procedure requires periodical exchange of control messages between all pairs of interconnected nodes to verify connectivity in order to overcome logical segmentation. In addition, the performance (e.g., restoration speed) of this procedure has not been studied and is not an integral part of the recommendation as of G.8032v2. The complex management associated with this procedure and the high overhead could result in poor network performance (e.g., slower restoration times), which makes it not appealing for service providers.

In contrast, here we present an effective network design (i.e., allocation of capacity and RPLs) which minimizes the number of logical segmentations (hence outages) in response to double link failures. Here, periodical exchange of additional control messages are not necessary; however, a service provider may still invoke the above reactive procedure to further improve the service availability. Given that the number of possible service outages is already minimized in the optimally designed ERP network through the design process, a significant reduction in the exchange of control messages is anticipated.

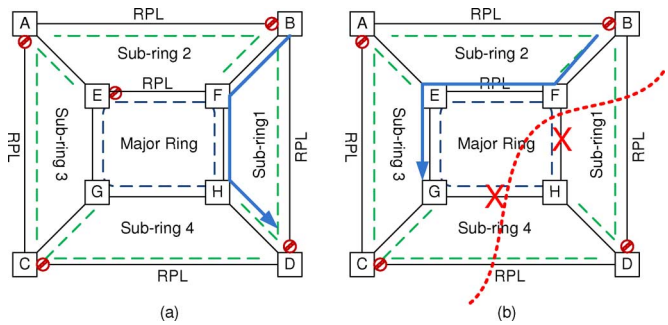


Fig. 3. Segmentation in a 3-connected network.

Note that there are situations where the service remains operational even though the network is segmented. Fig. 2(d) depicts this situation where the first failure $(C-F)$ affects the requested service of Fig. 1(a) which is restored through $B-A-D-E-F-I$. A second failure on link $B-C$ segments the network, but the requested service remains operational. These situations which do not cause service interruption are not among the concerns of our design approach.

C. Service Outages Versus Network Connectivity

Given the unique characteristics and operational principle of ERP, increasing network connectivity in ERP-based networks may not completely eliminate the outages caused by logical segmentation. We present an illustrative example of a 3-connected mesh network composed of multiple interconnected ERP rings as shown in Fig. 3. The major ring includes the nodes E, F, H, and G and is surrounded by four sub-rings. The RPL links are marked in the figure. A service is requested from node B to node D, which is routed through $B-F-H-D$ in idle (normal) state as presented in Fig. 3(a). Upon the first failure on link $F-H$, the major ring unblocks its RPL and the connection is restored through $B-F-E-G-H-D$. A second link failure on link $G-H$ causes a logical segmentation and the connection is disrupted (Fig. 3(b)). Clearly, logical segmentations exist in highly

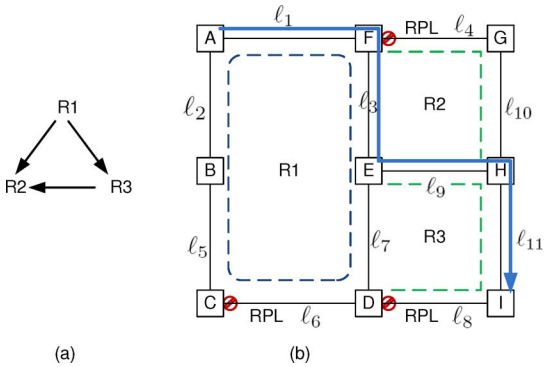


Fig. 4. Minimized capacity investment against single-link failure.

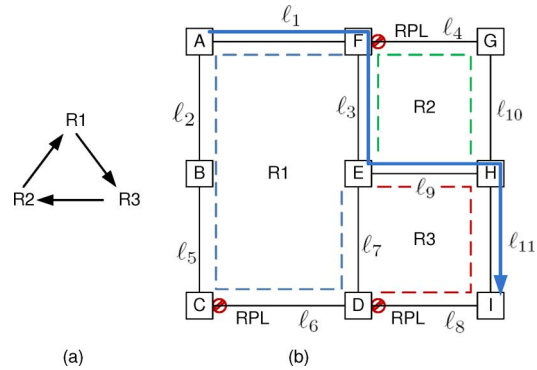


Fig. 5. Reduced segmentation.

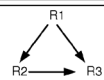
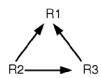
connected networks as well which, however, can be reduced by efficient design of the logical hierarchy.

D. Trade-Off Between Capacity and Outages

The authors of [4] presented a joint design approach for optimal capacity allocation in ERP-based mesh networks to withstand 100% restorability against single-link failures; they showed that the ring hierarchy selection and the RPL placement have significant impact on the capacity planning in ERP networks. Indeed as we will show here, the logical hierarchy of interconnected rings which is optimally designed to survive against all single-link failures may not be the same as the logical ring hierarchy that minimizes service outages caused by network segmentations (resulting from double link failures); these are two different design methods with different design objectives and hence design costs. To illustrate, we consider a small network with three interconnected rings R_1, R_2, and R_3 and one service request from node A to node I. Fig. 4(b) presents the outcome of the design approach presented in [4] which optimizes the capacity requirement with 100% restorability against single-link failures.

Fig. 4(a) shows the directed graph representation of the logical hierarchy of the rings which requires 9 unit of overall network capacity. In this figure, there are directed edges from R_1 to R_2 and R_3 which implies (in ERP terminology) that R_1 is a major ring and is responsible for the protection of the shared links with both R_2 and R_3 (see Fig. 4(b)). We then carefully examine all possible double link failures scenarios with the given ring hierarchy to identify the situations that cause service outages due to network segmentations. We observe 10 such instances of double link failures that involve the link pairs $\{\ell_1, \ell_2\}, \{\ell_1, \ell_5\}, \{\ell_1, \ell_6\}, \{\ell_1, \ell_7\}, \{\ell_3, \ell_2\}, \{\ell_3, \ell_5\}, \{\ell_3, \ell_6\}, \{\ell_3, \ell_7\}, \{\ell_9, \ell_8\}$, and $\{\ell_{11}, \ell_8\}$. However, the hierarchy of the given rings R_1, R_2, and R_3 can be designed in such a way that the number of service interruptions due to segmentation is reduced. Figs. 5(a) and (b) illustrate one of such ring hierarchies and logically designed rings respectively which observes 8 instances of service interruption due to failure of link pairs $\{\ell_1, \ell_2\}, \{\ell_1, \ell_5\}, \{\ell_1, \ell_6\}, \{\ell_1, \ell_7\}, \{\ell_3, \ell_4\}, \{\ell_3, \ell_{10}\}, \{\ell_9, \ell_8\}$, and $\{\ell_{11}, \ell_8\}$. Indeed, reduction of the number of potential service interruptions comes at the cost of increased capacity requirement. The latter design of the network requires 11 units of overall capacity to provide 100% restorability against single-link failures. Note that the example is illustrated with only one service request for simplicity.

TABLE I
COMPARISON OF ALTERNATIVE SOLUTIONS

	Hierarchy	RPLs	Capacity	Possible outages
Best solution		$\{\ell_1, \ell_{10}, \ell_{11}\}$	172	266
Alternate solution		$\{\ell_6, \ell_{10}, \ell_{11}\}$	184	188

Next, we continue our investigation with larger number of service requests to observe the trade-off between the capacity investment and the number of service interruptions. Table I presents the numerical results where unit demands between all pairs of nodes are considered. The best solution (includes hierarchy and RPL positions) requires 172 units of capacity which needs to be deployed to provide 100% restorability. However, 266 instances of possible service interruptions might be observed by this solution. In contrast, the alternative solution as presented in Table I could reduce the number of possible service interruptions to 188 (a 29.3% reduction) by changing the hierarchy and RPL positions of the preferred design at the cost of only 12 additional units (6.9%) of capacity. Hence, the obvious design question could be what will be the best design for the survivable ERP network? Clearly, the answer depends on the service requirements of the customers. Service providers may desire to reduce the number of potential segmentations for mission critical services and design the network with additional capacity investment. Next, we present our mathematical formulation that allows the service providers to explore trade-offs between higher service availability and optimal capacity investment.

III. PROBLEM FORMULATION

We denote a network topology by $G(\mathcal{V}, \mathcal{L})$ where $\mathcal{V}$ is the set of vertices or nodes, and $\mathcal{L}$ is the set links, indexed by v and ℓ, respectively. Unless specified differently, we assume bidirectional links in the network, and asymmetric traffic modeled by a set of unit-capacity connections $\mathcal{C}$ (indexed by c). We assume

that the set of all possible simple (without straddling-ring links) rings $\mathcal{R}$ (indexed by r) in the network are given. We define the following parameters, sets, and variables.

- Parameters and sets: α_r^ℓ equal to 1 if link ℓ belongs to ring r, 0 otherwise. $\mathcal{L}_r$ is the set of links spanned by ring $r \in \mathcal{R}$. S_c, D_c are the source and destination of connection c, respectively.
- Variables: We distinguish two classes of variables, including those used in ring hierarchy design and RPL placement and those used in capacity planning and optimization.

In determining the proper ring hierarchy and RPL placement, we use the following variables: x_r : equal to 1 if ring r is used, 0 otherwise. They are used to activate/deactivate rings. Only an active ring can carry traffic. η_r^ℓ : equal to 1 if link ℓ is the RPL of ring r, 0 otherwise. They are used to select the RPL of each active ring. y_r^ℓ : equal to 1 if ring r is the main w.r.t. ℓ, 0 otherwise. They are used to select the main ring of a link, i.e., the ring which is responsible to unblock the RPL in case of its failure. These variables are useful, especially, in the case of links that are shared or common to multiple rings. In capacity planning, we distinguish between two configurations of capacity: capacity in working state and in failure or protection state. We use the following variables to differentiate between the two states:

w_ℓ^c : equal to 1 if connection c in normal or working state is routed through ℓ, 0 otherwise.

$w_\ell^{\ell',c}$: equal to 1 if link ℓ' is traversed by connection c in case of failure on link ℓ, 0 otherwise.

Similarly, we define two sets of constraints: the first (1) to (5) contain constraints to set up the hierarchy of rings, and define the optimal set of RPLs; the second set contains constraints to optimize the required capacity. The first set is as follows:

$$\eta_r^\ell \le \alpha_r^\ell x_r \quad \ell \in \mathcal{L}, r \in \mathcal{R} \tag{1}$$

$$y_r^\ell \le \alpha_r^\ell x_r \quad \ell \in \mathcal{L}, r \in \mathcal{R} \tag{2}$$

$$\sum_{\ell \in \mathcal{L}} \alpha_r^\ell \eta_r^\ell = x_r \quad r \in \mathcal{R} \tag{3}$$

$$\sum_{r \in \mathcal{R}} y_r^\ell \le 1 \quad \ell \in \mathcal{L} \tag{4}$$

$$y_r^\ell = y_r^{\ell'} \quad \ell, \ell' \in \mathcal{L}_r \cap \mathcal{L}_{r'}, r, r' \in \mathcal{R} \tag{5}$$

$$\eta_r^\ell = 0 \quad \ell \in \mathcal{L}_r \cap \mathcal{L}_{r'}, r \ne r', r, r' \in \mathcal{R} \tag{6}$$

Constraint (1) states that link ℓ can be the RPL of ring r only if r is selected. Similarly, constraint (2) ensures that only a selected ring r can be the main ring w.r.t. ℓ. Constraint (3) states that a ring r, once it is selected, can have exactly one RPL. Constraint (4) limits a link to belong to at most one main ring and thus avoids unblocking of multiple RPLs in case of a failure on a shared link. This uniqueness is required to avoid forming a loop in ERP networks. Constraint (5) states that a set of links shared by any pair of rings r and r' must belong to the same main ring. For example, links DE and EF are shared between two interconnected rings in Fig. 1. DE and EF cannot be owned by two different rings and they must belong to exactly one of the two rings so that only one ring will unblock its RPL in case of a failure on DE or EF. Constraint (6) ensures that no RPL is placed on any link that is shared/spanned by multiple active rings. This is an additional constraint which is not part of the original standard ITU-T G.8032. The concept of RPL is introduced by G.8032 to ensure loop-free topology which is necessary for Ethernet forwarding. However, a loop can be formed when a RPL in unblocked in case of a link failure (i.e., in failure state) if the placement of RPL is not selected properly. We imposed this constraint to avoid forming loops especially in failure state. An alternate approach to constraint (6) can be ensuring a Directed Acyclic Graph (DAG) while determining logical hierarchy among interconnected rings. The capacity planning constraints are defined as follows:

- In working state :

$$\sum_{\ell \in v^+} w_\ell^c - \sum_{\ell \in v^-} w_\ell^c = \begin{cases} 1 & \text{if } v = S_c \\ -1 & \text{if } v = D_c \\ 0 & \text{Otherwise} \end{cases} \quad c \in \mathcal{C} \tag{7}$$

$$w_\ell^c \le 1 - \sum_{r \in R} \eta_r^\ell \quad \ell \in \mathcal{L}, c \in \mathcal{C} \tag{8}$$

$$w_\ell^c \le \sum_{r \in R} y_r^\ell \quad \ell \in \mathcal{L}, c \in \mathcal{C} \tag{9}$$

Constraint (7) is the flow conservation of each connection $c \in \mathcal{C}$ in working state. Constraint (8) states that a link ℓ can be used to carry traffic in working state only if it is not the RPL of any ring. Similarly, constraint (9) ensures that a connection c can use a link ℓ only if ℓ belongs to a main ring.

- In failure/protection state:

$$\sum_{\ell' \in v^+} w_\ell^{\ell',c} - \sum_{\ell' \in v^-} w_\ell^{\ell',c} = \begin{cases} 1 & \text{if} v = S_c \\ -1 & \text{if} v = D_c \\ 0 & \text{Otherwise} \end{cases} \quad c \in \mathcal{C} \tag{10}$$

$$w_\ell^{\ell',c} \le 2 - y_r^\ell - \sum_{r':r' \in \mathcal{R}-r} \eta_{r'}^{\ell'}$$
$$r \in \mathcal{R}, \ell \in \mathcal{L}_r, \ell' \in \mathcal{L} \tag{11}$$

$$w_\ell^{\ell',c} = 0 \quad \ell, \ell' (\ell' = \ell) \in \mathcal{L}, c \in \mathcal{C} \tag{12}$$

$$\psi_{\ell'} \ge \max\left(\sum_{c \in \mathcal{C}} w_{\ell'}^c, \max_\ell \sum_{c \in \mathcal{C}} w_\ell^{\ell',c} \right) \ \ell, \ell' \in \mathcal{L} \tag{13}$$

Constraint (10) is the capacity flow conservation in the protection state. The link ℓ' can be used to provide protection in case of a failure on link ℓ if and only if constraint (11) is satisfied; which states that ℓ has to be initially protected by a main ring r and link ℓ' is not the RPL of any ring r' that is different from r. Constraint (12) ensures that a link cannot protect itself. Constraint (13) assures that enough capacity is reserved on each link to restore the affected connections.

The discussion, analysis, and examples in Section II has given us some insights about segmentations in ERP-based networks. The number of service outages that a given set of connections may experience due to segmentation depends on the routing of the connections in the working state; more precisely, the number of links that are used by the connection in working state. Denoteed by $\mathcal{L}_c^r$ is the set of links of ring r that are used by connection c in working state and $\bar{\mathcal{L}}_c^r$ the set of the rest of the links of ring r. Hence, the number of service outages due to segmentation for connection c in ring r (S_c^r) can be defined as $S_c^r = |\mathcal{L}_c^r| \times |\bar{\mathcal{L}}_c^r|$. Then, the total number of service outages due to segmentation

for connection c can be found by accumulating over all rings: $\sum_{r\in R} S_c^r$ or $\sum_{r\in R} |\mathcal{L}_c^r| \times |\bar{\mathcal{L}}_c^r|$. The objective of the optimization problem, which is composed of two components, can be expressed as:

$$\min \left\{ \rho \times \sum_{\ell' \in L} \psi_{\ell'} + (1-\rho) \times \underline{\sum_{c\in\mathcal{C}} \sum_{r\in R} |\mathcal{L}_c^r| \times |\bar{\mathcal{L}}_c^r|} \right\}$$

where ρ is a weighing parameter that helps to strike good balance between two components. $|\mathcal{L}_c^r|$ can be expressed in terms of w_ℓ^c and y_r^ℓ as $|\mathcal{L}_c^r| = \sum_{\ell\in r} w_\ell^c \times y_r^\ell$. However, this introduces nonlinearity to the model. We introduce an additional variable $o_{c,\ell}^r$ in order to maintain the linearity of the model, where $o_{c,\ell}^r$: equal to 1 if link ℓ of ring r is used by connection c in working state, 0 otherwise. Constraints (14)–(16) presents the linearized definition of $|\mathcal{L}_c^r|$.

$$o_{c,\ell}^r \le w_\ell^c \quad \ell \in \mathcal{L}_r, r \in \mathcal{R}, c \in \mathcal{C} \tag{14}$$

$$o_{c,\ell}^r \le y_r^\ell \quad \ell \in \mathcal{L}_r, r \in \mathcal{R}, c \in \mathcal{C} \tag{15}$$

$$o_{c,\ell}^r \ge w_\ell^c + y_r^\ell - 1 \quad \ell \in \mathcal{L}_r, r \in \mathcal{R}, c \in \mathcal{C} \tag{16}$$

Then $|\mathcal{L}_c^r|$ can be found by $|\mathcal{L}_c^r| = \sum_{\ell\in\mathcal{L}_r} o_{c,\ell}^r$ and constraint (17) defines $|\bar{\mathcal{L}}_c^r|$.

$$|\bar{\mathcal{L}}_c^r| = \sum_{\ell\in\mathcal{L}_r} y_r^\ell - \sum_{\ell\in\mathcal{L}_r} o_{c,\ell}^r \quad r \in \mathcal{R}, c \in \mathcal{C} \tag{17}$$

Nevertheless, the underlined term in the objective $|\mathcal{L}_c^r| \times |\bar{\mathcal{L}}_c^r|$ which represents the number of outages that connection c may experience in ring r remains nonlinear. We apply an alternative approach which requires an additional variable $\gamma_{c,\ell}^r$ to avoid the nonlinearity, where $\gamma_{c,\ell}^r$ is an integer variable that represents the number of possible service outages for connection c given that link ℓ of ring r is used by c in working state. $\gamma_{c,\ell}^r$ is defined by $\gamma_{c,\ell}^r = o_{c,\ell}^r \times |\bar{\mathcal{L}}_c^r|$ and constraints (18) and (19) are used to linearize it.

$$\gamma_{c,\ell}^r \le |\bar{\mathcal{L}}_c^r| + M(1 - o_{c,\ell}^r) \quad \ell \in \mathcal{L}_r, r \in \mathcal{R}, c \in \mathcal{C} \tag{18}$$

$$\gamma_{c,\ell}^r \ge |\bar{\mathcal{L}}_c^r| - M(1 - o_{c,\ell}^r) \quad \ell \in \mathcal{L}_r, r \in \mathcal{R}, c \in \mathcal{C} \tag{19}$$

where M is a large integer number.

Then, the revised **optimization objective** will be:

$$\min \left\{ \overbrace{\rho \times \sum_{\ell' \in \mathcal{L}} \psi_{\ell'}}^{\text{capacity}} + \overbrace{(1-\rho) \times \sum_{c\in\mathcal{C}} \sum_{r\in\mathcal{R}} \sum_{\ell\in\mathcal{L}_r} \gamma_{c,\ell}^r}^{\text{service outages}} \right\}$$

IV. Numerical Results I

In this section, we evaluate numerically our proposed design approach whose objective is presented in the previous section. We present a comparison between numerous variants of the model by varying the value of ρ. For example, selecting $\rho = 1$ allows us to focus only on minimizing the overall network capacity provisioning where the network is designed to withstand against single link failures only as presented in [4]. Alternatively, when $\rho = 0.5$, the model assigns balanced weights to the capacity as well as to minimizing the number of service outages that may result from double link failures. We consider three network topologies, namely, the COST239, NSFNET, and ARPA2 [11] in following study and assume three different traffic distributions (High load, medium load, and light load). In high traffic distribution, we consider unit demands between all possible source-destination pairs in the network whereas the medium and light traffic distributions are realized by randomly selecting 50% and 10% of the total demands that are considered in high traffic distribution respectively. Light, medium, and high traffic distributions are denoted by Instance 1, Instance 2, and Instance 3 respectively in the following figures which present the numerical results.

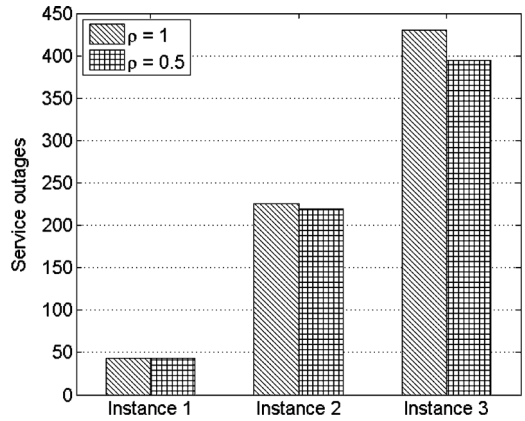


Fig. 6. COST239 service outages.

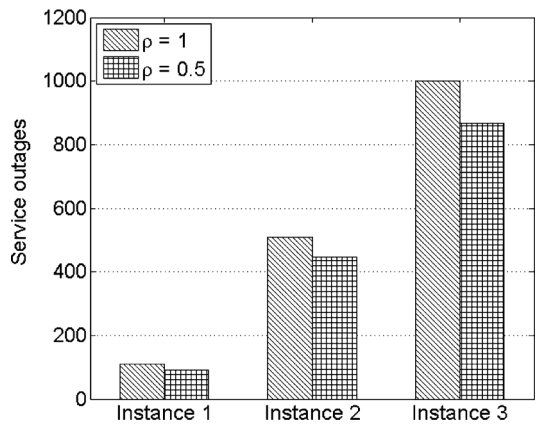


Fig. 7. NSFNET service outages.

Figs. 6, 7, and 8 compare the numerical results in terms of the number of service outages caused by double link failures segmentations that are obtained by the proposed design approach for the COST239, NSFNET, and ARPA2 networks respectively. Each comparison consists of three traffic distributions: Instance 1 for light, Instance 2 for medium, and Instance 3 for high traffic scenarios.

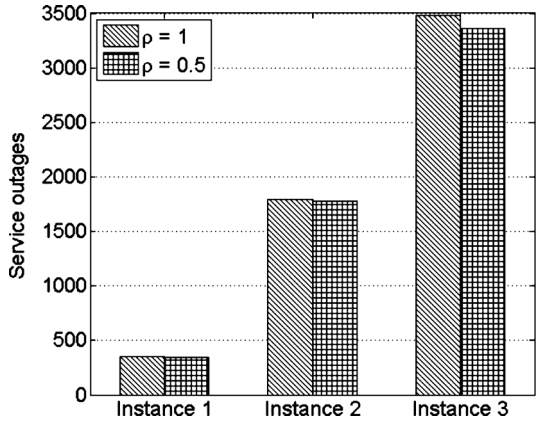


Fig. 8. ARPA2 service outages.

TABLE II
CAPACITY TRADE-OFF BETWEEN TWO APPROACHES

	COST239		NSFNET		ARPA2	
	$\rho = 1$	$\rho = 0.5$	$\rho = 1$	$\rho = 0.5$	$\rho = 1$	$\rho = 0.5$
	(unit capacity)		(unit capacity)		(unit capacity)	
Instance 1	34	36	68	76	179	188
Instance 2	172	183	299	314	952	981
Instance 3	310	332	589	630	1856	1908

The figures show that when $\rho = 0.5$, the number of outages resulting from double link failures is reduced and the reduction becomes substantial for traffic instance 3 (i.e., at high loads). For example, when $\rho = 0.5$, the design model achieves a reduction of 13.3% in the number of service outages for NSFNET network at the cost of only 6.9% increase in capacity deployment (Table II) by comparison to the values when $\rho = 1$. Clearly, a higher value of ρ yields a more effective capacity allocation, which is obtained at the cost of having a network that is more vulnurable to service outages in the presence of double link failures and results lower service availability. Similar results are observed for COST239 and ARPA2 (Figs. 7 and 8) where the number of service outages is reduced by 8.1% and 3.3% respectively at the cost of 7.0% and 2.8% (Table II) increase in capacity deployment for NSFNET and ARPA2 networks respectively.

V. FURTHER OBSERVATIONS

By further dissecting the above numerical results, we observe that the reason some of the connections are vulnerable to a second failure is due to the lack of provisioned capacity. For example in traffic instance 3 of previous section, we identified that 22%–32% of the total outages that may be caused by double link failures are due to insufficient capacity in the network, after restoring all connections affected by the first failure. In light of this observation, the service outages in ERP can further be characterized into three categories: (i) outages due to physical segmentations, (ii) outages due to logical segmentations, and (iii) outages due to lack of capacity. The first two categories have been addressed by the proposed ILP model on Section III which minimizes the number of outages caused by the logical segmentations while the physical segmentations are referred as unavoidable. Now, we address the third category of service outages and its possible remedy.

In an efficiently designed ERP mesh network, the spare capacity that is reserved for protection switching is shared as much as possible between existing connections. When a link fails, all of the connections that are traversing the link are disrupted. The network enters into a failure state and all of the affected connections are restored via alternate available paths. At this point, all of the connections in the network are operational; however some of these connections, more precisely the connections that share spare capacity with the affected connections of the first failure, are vulnerable to subsequent failure. Thus, one needs to identify these connections which are vulnerable in the presence of multiple concurrent failures and provision capacity in the network in a way to reduce the number of possible service outages caused by multiple failures.

We represent the network state (working/failure) by a binary link-state vector S_k [12], [5], such that $S_k = \{S_{k,\ell} = 0 \text{ for blocked links; } 1 \text{ otherwise. } \forall \ell \in \mathcal{L}\}$. A link ℓ can be referred to as blocked if either it is selected as an RPL in working state or it is affected by a failure. Then, the set of K different link state vectors corresponds to all possible single-link failure scenarios. Each S_k represents a tree of the network which uniquely determines the forwarding paths and corresponding link loads. The load of link ℓ is the number of connections passing through it and is denoted by $\lambda_\ell(S_k)$ which is interchangeably referred to as the required capacity of link ℓ. Let us denote the link capacity vector by $C_\ell^{\ell'}$ which is an integer set and specifies the number of connections that are traversing link ℓ' in working state and are provisioned to traverse link ℓ in case of failure on link ℓ'. Then $C_\ell^{\ell'} \geq \lambda_{\ell'}(S_k), \forall \ell' \in \mathcal{L}$. Thus, the amount of capacity which needs to be reserved for protection switching on link ℓ is $C_\ell^* = \max_{\forall \ell'} C_\ell^{\ell'}$. However, when a failure occurs and the protection switching is activated, some of the spare capacity on link ℓ may be used. In such event, C_ℓ^* should be updated according to the current network state. One may find that $\bar{C}_\ell \leq C_\ell^*$, where $\bar{C}_\ell$ is the amount of spare capacity still available on link ℓ after first failure occurred. $\bar{C}_\ell < C_\ell^*$ also represents that some connections may contend for the spare capacity on link ℓ upon next failure and may become vulnerable. Such connections are referred to as *Vulnerable Connections* while the rest of the connections which have $\bar{C}_\ell \geq C_\ell^*$ on all of the links of their working and restoration path are referred to as *Protected Connections*. To illustrate better the service outages due to lack of capacity, we present an example as follows.

Fig. 9(a) presents an ERP network with the logical hierarchy of two interconnected rings and the corresponding RPL positions. Two services (one unit each) are requested from node B to node F (c_1) and from node H to node F (c_2) which are routed through $B-C-F$ and $H-I-F$ respectively in working (Idle) state. Fig. 9(b) shows the capacity allocations (C_ℓ^*) on each link (presented besides each link). Let us assume that the first failure occurred on link $C-F$ and the affected connection c_1 is restored through alternate path $B-A-D-E-F$ (Fig. 9(c)). Now, we update the value of C_ℓ^* according to the current network state and find that $C_{\ell_{\rm DE}}^* = 1$ and $C_{\ell_{\rm EF}}^* = 1$, however $\bar{C}_{\ell_{\rm DE}} = 0$ and $\bar{C}_{\ell_{\rm EF}} = 0$, i.e., no spare capacity is available on links $D-E$ and

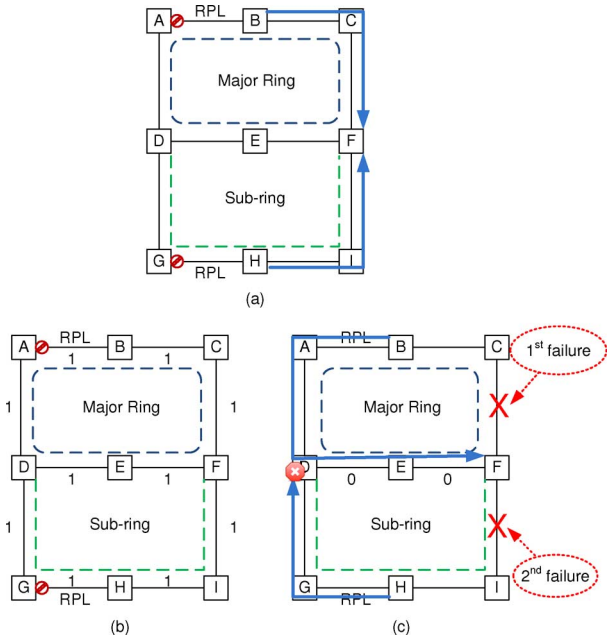


Fig. 9. Service outages due to inadequate capacity.

$E-F$ after link $C-F$ fails and the connection c_2 becomes vulnerable to next failure. Let us now assume that another failure occurs on link $F-I$ before the repair of link $C-F$. Then c_2 cannot be restored and it experiences service outage due to lack of capacity on links $D-E$ and $E-F$.

A. Suggested Remedy

Contention for capacity among vulnerable connections can be resolved by reserving more spare capacity on the links that are shared by these contending connections. We develop a procedure to estimate the amount of additional capacity requirement on contention links. The overall requirement of spare capacity in the network is recomputed in the subroutine such that all of the service outages due to lack of capacity are eliminated while the amount of spare capacity is minimized.

The developed routine operates on the optimal configuration found by the ILP model of Section III, i.e., we assume the logical hierarchy of the interconnected rings and their corresponding RPLs are given to the routine. The function iterates over all single-link failure situations as described in the procedure *ESTIMATE-SPARE-CAPACITY*. The average running time of the routine is in the order of $O(\mathcal{LC}+\mathcal{L}^2)$ where $\mathcal{L}$ and $\mathcal{C}$ are the number of bidirectional links and the number of connections respectively. We denote the affected link by ℓ'. We identify the set of affected connections, restore them and update C^*_ℓ for each link $\ell \in \mathcal{L}$. Then we build the set of link state vectors S of K different link states. Each item S_k in the set S represents a double link failure scenario by blocking the first link ℓ' and any other link $\ell'' : \ell'' \in \mathcal{L}\text{and}\ell'' \neq \ell'$. We identify the set of vulnerable connections for each element S_k and compute the required additional capacity $C^{\ell',\ell''}_{\ell,k}$ on each contending link such that $C^{\ell',\ell''}_{\ell,k} = C^*_\ell - \bar{C}_\ell$. Then we evaluate the additional spare capacity which needs to be provisioned on link ℓ by $C^{\ell',\ell''}_{\ell} = \max_{\forall k} C^{\ell',\ell''}_{\ell,k}$ and update the value of C^*_ℓ by $C^*_\ell + C^{\ell',\ell''}_{\ell}$.

ESTIMATE-SPARE-CAPACITY 1 Capacity estimation

Input: Network topology, traffic matrix, logical design;
Output: Additional capacity per link to be provisioned;
for all failure on link $\ell' \in \mathcal{L}$ **do**
  Identify the set of affected connections C_a;
  Make necessary changes to the network topology (i.e., blocking failed link port, unblocking corresponding RPL);
  for all $c \in C_a$ **do**
    Restore the affected connection c;
  end for
  for all $\ell \in \mathcal{L}$ **do**
    Update C^*_ℓ and $\bar{C}_\ell$;
  end for
  Build the link state vector S of K items: each S_k represents double (ℓ', ℓ'') failures;
  Compute $C^{\ell',\ell''}_{\ell,k}$ such as $C^{\ell',\ell''}_{\ell,k} = C^*_\ell - \bar{C}_\ell$;
  for all $\ell \in \mathcal{L}$ **do**
    Compute $C^{\ell',\ell''}_{\ell} = \max_{\forall k} C^{\ell',\ell''}_{\ell,k}$;
  end for
  return $C^{\ell',\ell''}_{\ell}$;
end for

Note that some of the elements S_k in S may represent physical or logical segmentations and hence, some of the connections may suffer service outages due to this. We ignore to restore such connections in the subroutine.

B. Dual-Failure Restorability

Finally we extend our study to analyze the impact of our network design approaches on the level of network restorability. The double link failures restorability $R_2^{\ell',\ell''}$ of a given pair of links (ℓ', ℓ''), as defined in [12], is the fraction of the total failed connections traversing through links ℓ' and ℓ'' in working state that can be restored in the case of concurrent dual failures on links ℓ' and ℓ''. Let us denote the number of non restorable connections in the case of failure on links ℓ' and ℓ'' by $F_{\ell',\ell''}$ and the connections that traverse link ℓ' and ℓ'' in working state by $W^c_{\ell'}$ and $W^c_{\ell''}$ respectively. Then, the restorability $R_2^{\ell',\ell''}$ can be defined as: $R_2^{\ell',\ell''} = 1-(F_{\ell',\ell''})/(W^c_{\ell'}+W^c_{\ell''})$. The network-wide restorability is denoted by R_2 which is defined as the average of over all ordered (ℓ', ℓ'') double link failures combinations [12]. Then $R_2 = 1 - (\sum_{\forall(\ell',\ell''):\ell'\neq\ell''} F_{\ell',\ell''})/(\sum_{\forall(\ell',\ell''):\ell'\neq\ell''}(W^c_{\ell'}+W^c_{\ell''}))$. The above presented subroutine is used to compute the network-wide restorability as well and the numerical results are presented as follows.

C. Numerical Results II

In this section, we analyze the additional capacity requirement estimated by the suggested remedy to eliminate the service outages due to the lack of capacity and the impact on the service outages. We compare the capacity-outages trade-off with the results that are presented in Section IV. The numerical results compare three design approaches: the first two approaches are different variants of the ILP model ($\rho = 1$ and $\rho = 0.5$ without

TABLE III
CAPACITY TRADE-OFF BETWEEN THREE APPROACHES

	COST239			NSFNET			ARPA2		
	Instance 1	Instance 2	Instance 3	Instance 1	Instance 2	Instance 3	Instance 1	Instance 2	Instance 3
	(unit capacity)			(unit capacity)			(unit capacity)		
$\rho = 1$	34	172	310	68	299	589	179	952	1856
$\rho = 0.5$	36	183	332	76	314	630	188	981	1908
$\rho = 0.5$ *with modification of sec. V*	45	218	384	94	393	743	246	1181	2224

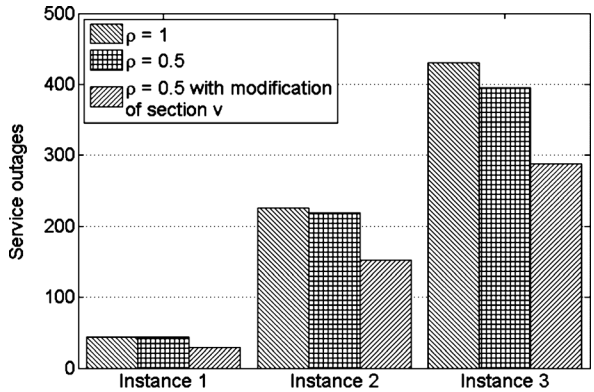


Fig. 10. COST239 service outages.

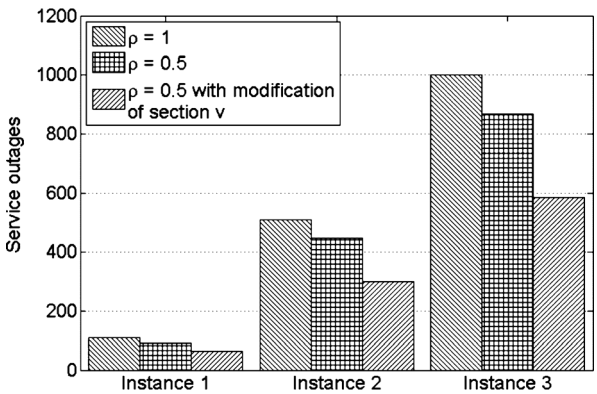


Fig. 11. NSFNET service outages.

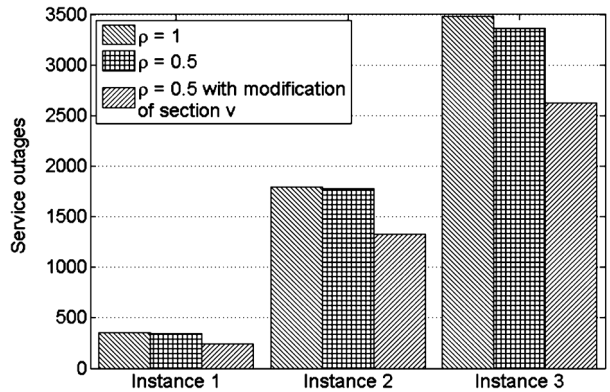


Fig. 12. ARPA2 service outages.

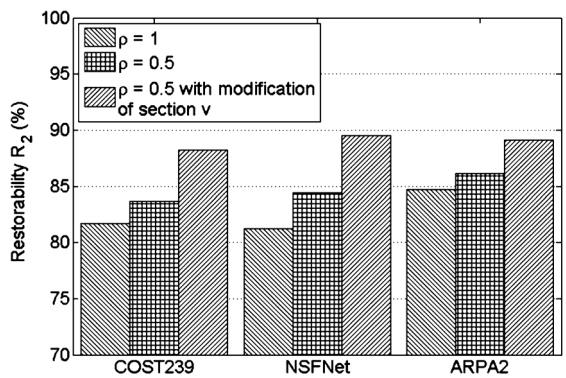


Fig. 13. Comparison of network-wide restorability.

modifications of Section V) and the third approach ($\rho = 0.5$ with modifications of Section V) estimates the additional capacity required to completely protect all restorable connections. We adopt the same traffic distributions as of numerical results presented in Section IV.

Figs. 10, 11, and 12 present the number of service outages in three different network instances COST239, NSFNet, and ARPA2 respectively with different traffic distributions and Table III shows the corresponding capacity requirements. The figures show that our suggested remedy in the procedure *ESTIMATE-SPARE-CAPACITY* can further reduce the number of service outages in the networks. For example, in COST239 with high traffic load (Instance 3), 15.6% of additional capacity (Table III) yields a 27.1% reduction in service outages over the previous design method ($\rho = 0.5$). Similar results are observed for NSFNet and ARPA2 networks where the number of service outages are shown to be reduced by 32.7% and 21.9% in traffic instance 3 with additional 17.9% and 16.5% capacity investment respectively.

Fig. 13 presents the network-wide double link failures restorability (R_2) that can be achieved by the three design approaches in three network instances with high load (Instance 3). The figure shows that the network-wide restorability is improved by the third approach for all three network instances at the cost of additional capacity deployment. The first design approach ($\rho = 1$) which was intended to achieve 100% restorability against any single-link failure can achieve 81% restorability against double link failures (R_2) in NSFNet network with high traffic load (Instance 3) and R_2 can be increased by 10% with additional capacity investment as estimated by the third approach. Similar trends are observed for COST239 and ARPA2 networks as well. A service provider may be interested to estimate the amount of capacity need to be deployed to achieve a targeted level of restorability.

VI. Conclusion

We proposed an effective design approach for ERP mesh networks which addresses the issue of service outages due to double link failures. We developed a mathematical model to effectively design ERP networks with the balance in design objective between minimizing capacity requirement and improving service availability. We also addressed the issue of service outages suffered by contending connections due to lack of capacity on some shared links. Numerical results show that the number of service outages can be significantly reduced and the network-wide restorability can be substantially improved with reasonable additional investment in capacity deployment. This could be a practicable solution for service providers to offer and accommodate more clients with higher service availability for their mission critical applications.

References

[1] J. Ryoo, H. Long, Y. Yang, M. Holness, Z. Ahmad, and J. Rhee, "Ethernet ring protection for carrier Ethernet networks," *IEEE Commun. Mag.*, vol. 46, no. 9, pp. 136–143, Sep. 2008.

[2] *IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks Amendment 10: PBB-TE*, IEEE Std 802.1Qay-2009, May 2009, pp. c1-131.

[3] Ethernet Ring Protection Switching ITU-T Rec. G.8032/Y.1344, 2010.

[4] M. Nurujjaman, S. Sebbah, C. Assi, and M. Maier, "Optimal capacity planning and RPL placement in carrier ethernet mesh network design," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2012.

[5] D. Lee, K. Lee, S. Yoo, and J.-K. K. Rhee, "Efficient Ethernet ring mesh network design," *IEEE J. Lightw. Technol.*, vol. 29, no. 18, pp. 2677–2683, Sep. 2011.

[6] J. Zhang, K. Zhu, and B. Mukherjee, "Backup reprovisioning to remedy the effect of multiple link failures in WDM mesh networks," *IEEE J. SAC*, vol. 24, no. 8, pp. 57–67, 2006.

[7] S. Ramasubramanian and A. Chandak, "Dual-link failure resiliency through backup link mutual exclusion," *IEEE/ACM Trans. Networking*, vol. 16, no. 1, pp. 157–169, 2008.

[8] A. Grue and W. Grover, "Upsr-like p-cycles: A new approach to dual failure protection," in *Proc. Int. Conf. Ultra Modern Telecommunications Workshops*, 2009, pp. 1–6.

[9] D. Schupke, W. Grover, and M. Clouqueur, "Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks," in *Proc. IEEE ICC*, June 2004, vol. 3, pp. 1628–1633.

[10] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. Hansen, "Fast recovery from dual-link or single-node failures in IP networks using tunneling," *IEEE/ACM Trans. Networking*, vol. 18, no. 6, pp. 1988–1999, 2010.

[11] R. Ramaswami, K. Sivarajan, and G. Sasaki, *Optical Networks: A Practical Perspective*. Burlington: Morgan Kaufmann, 2009.

[12] M. Clouqueur and W. Grover, "Availability analysis of span-restorable mesh networks," *IEEE JSAC*, vol. 20, no. 4, pp. 810–821, May 2002.

Mohammad Nurujjaman received the B.Sc. degree from Jahangirnagar University, Dhaka, Bangladesh in 2003, and the M.Sc. degree from Concordia University, Montreal, QC, Canada, in 2003 and 2009, respectively. His master thesis focused on finding the empirical upper bound on the performance of OBS networks. He is currently pursuing the Ph.D. degree in computer science at Concordia University.

His current research interests are in the area of energy efficient packet transport networks, carrier Ethernet networks' performance and survivability. Before beginning his master studies in 2007, he worked as a Software Engineer at Jaxara IT Ltd from 2003 through 2006.

Samir Sebbah received the Ph.D. degree in electrical and computer engineering from the University of Concordia, Montreal, Canada, and a master's degree in computer science and operational research from the University of Paris 8.

He is a Research Visiting Fellow at the Centre for Operational Research and Analysis at Defence R&D Canada, Ottawa, Canada and a Research Associate at Concordia University, His research interests are in design and optimization of telecommunications networks, large scale optimization, design and planning of logistics networks.

Chadi M. Assi received the Ph.D. degree from the Graduate Center, City University of New York (CUNY), in 2003.

He is currently an Associate Professor with Concordia University, Montreal, Canada. His current research interests are in the areas of network design and optimization, and network modeling.

Dr. Assi received the prestigious Mina Rees Dissertation Award from CUNY for his research on WDM optical networks. He is on the Editorial Board of the *IEEE Communications Surveys and Tutorials* and the IEEE Communications Letters.