US 20060250948A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2006/0250948 A1

(43) Pub. Date: Nov. 9, 2006

Zamfir et al.

(54) DYNAMIC PATH PROTECTION IN AN OPTICAL NETWORK

(75) Inventors: **Anca Zamfir**, Kanata (CA); **Zafar Ali**, Windsor (CA); **David D. Ward**, Somerset, WI (US)

Correspondence Address:
Cindy S. Kaplan
P.O. BOX 2448
SARATOGA, CA 95070 (US)

(73) Assignee: **CISCO TECHNOLOGY, INC.**, San Jose, CA

(21) Appl. No.: **11/124,687**

(22) Filed: **May 9, 2005**

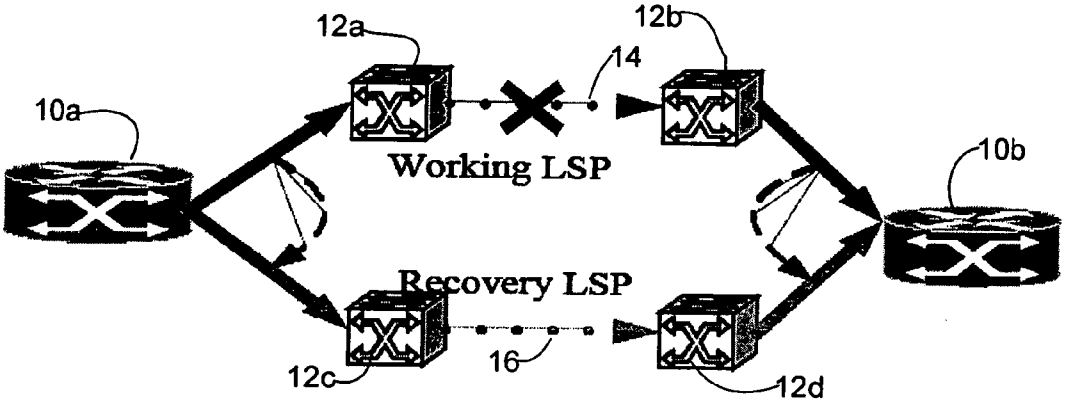
Publication Classification

(51) **Int. Cl.**
H04J 1/16 (2006.01)
H04L 12/56 (2006.01)

(52) **U.S. Cl.** **370/216**; 370/389

(57) **ABSTRACT**

A method and system for dynamic protection of virtual links for paths of an optical network in communication with an IP network are disclosed. The method includes establishing two or more paths within the optical network and grouping the paths in a dynamic bundle. The grouping is selected at a control plane level and the bundle of paths are recognized as a single routing adjacency in the IP network so that as long as one or more paths within the bundle is operating, the routing adjacency in the IP network is not affected by changes within the bundle.



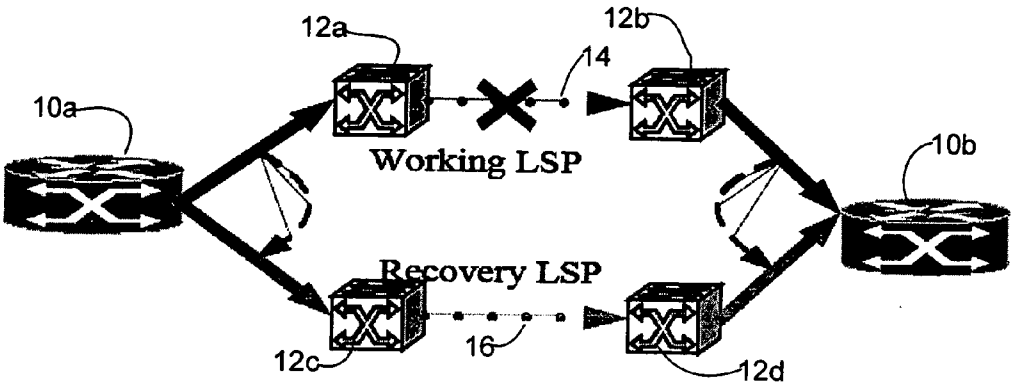

12a
12b
14
10a
Working LSP
10b
Recovery LSP
12c
16
12d

FIG. 1A

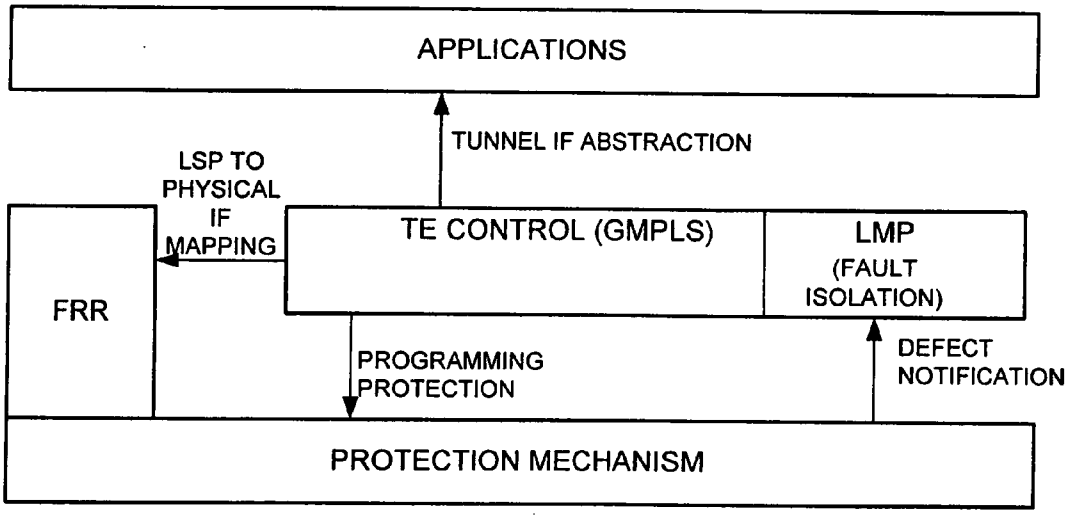

APPLICATIONS
TUNNEL IF ABSTRACTION
LSP TO PHYSICAL IF MAPPING
TE CONTROL (GMPLS)
LMP (FAULT ISOLATION)
FRR
PROGRAMMING PROTECTION
DEFECT NOTIFICATION
PROTECTION MECHANISM

FIG. 1B

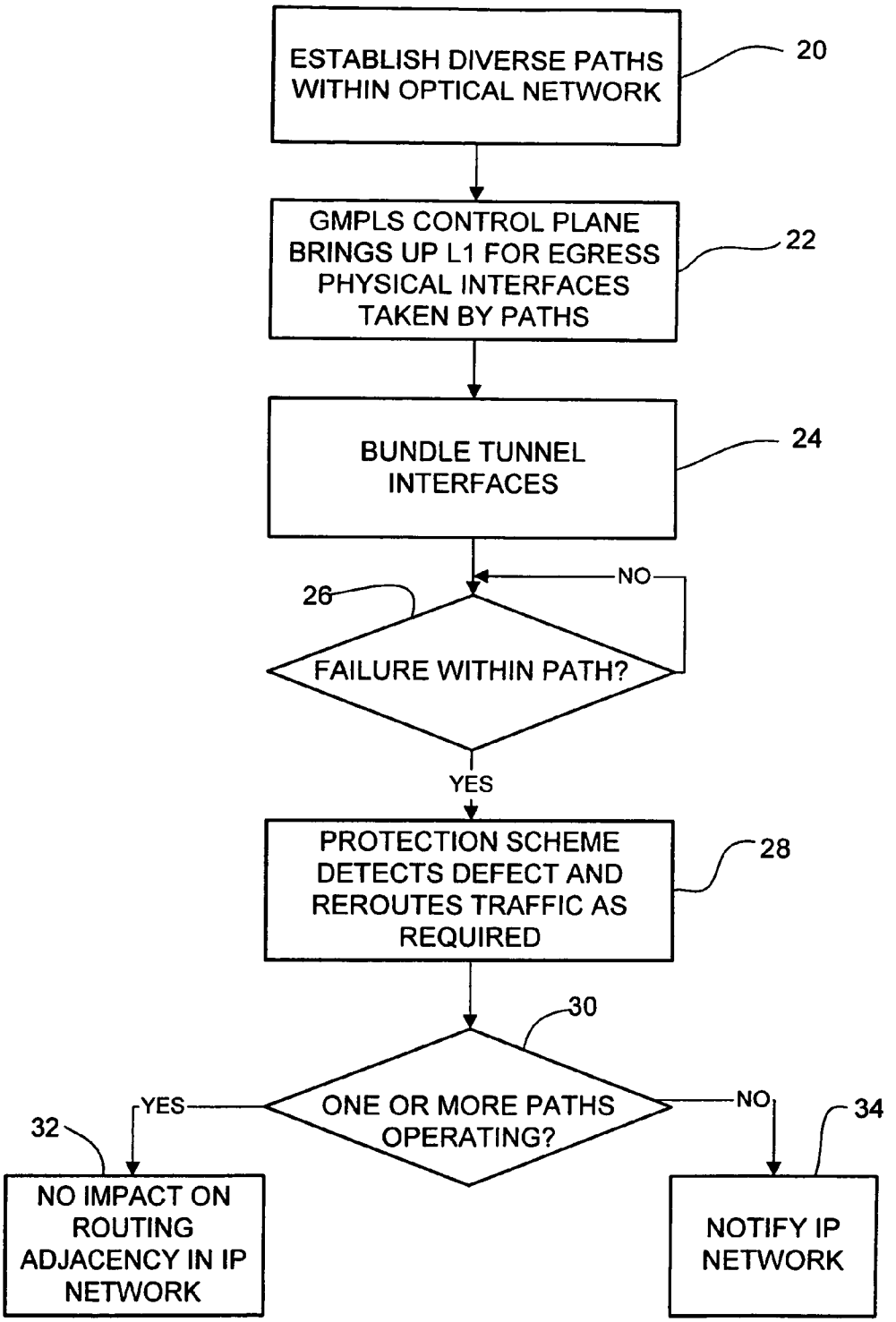

ESTABLISH DIVERSE PATHS WITHIN OPTICAL NETWORK
20
GMPLS CONTROL PLANE BRINGS UP L1 FOR EGRESS PHYSICAL INTERFACES TAKEN BY PATHS
22
BUNDLE TUNNEL INTERFACES
24
NO
26
FAILURE WITHIN PATH?
YES
PROTECTION SCHEME DETECTS DEFECT AND REROUTES TRAFFIC AS REQUIRED
28
30
ONE OR MORE PATHS OPERATING?
YES
NO
32
34
NO IMPACT ON ROUTING ADJACENCY IN IP NETWORK
NOTIFY IP NETWORK

FIG. 2

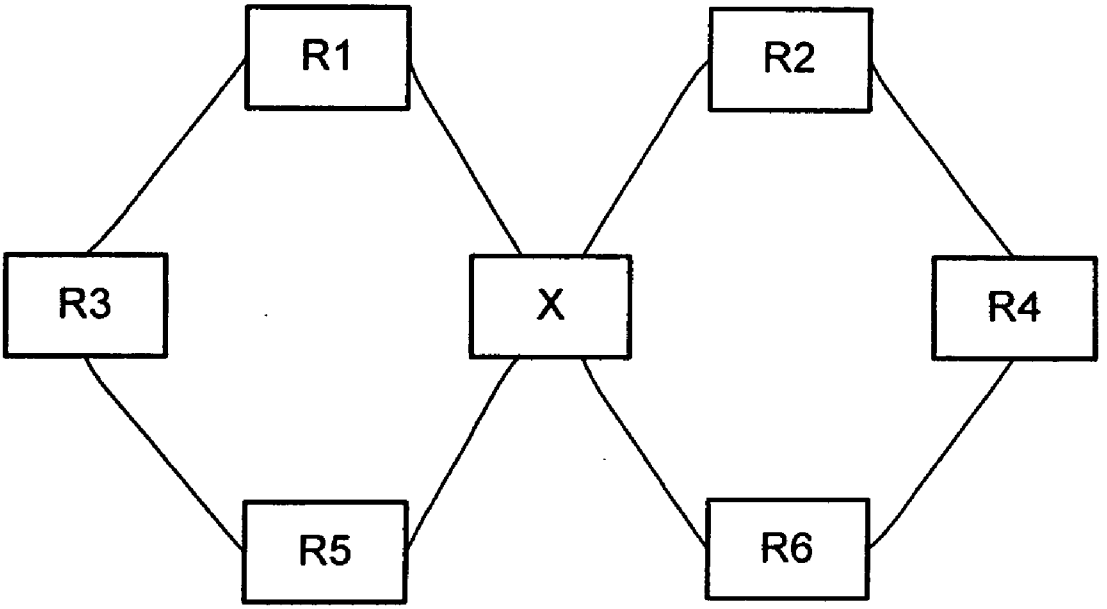


FIG. 3

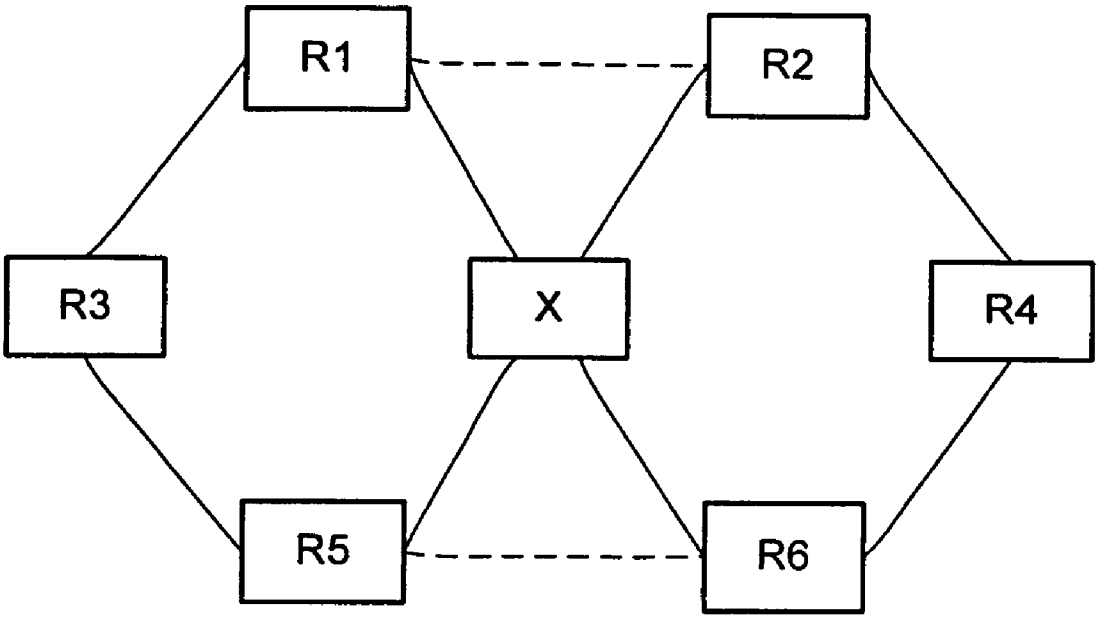


FIG. 4

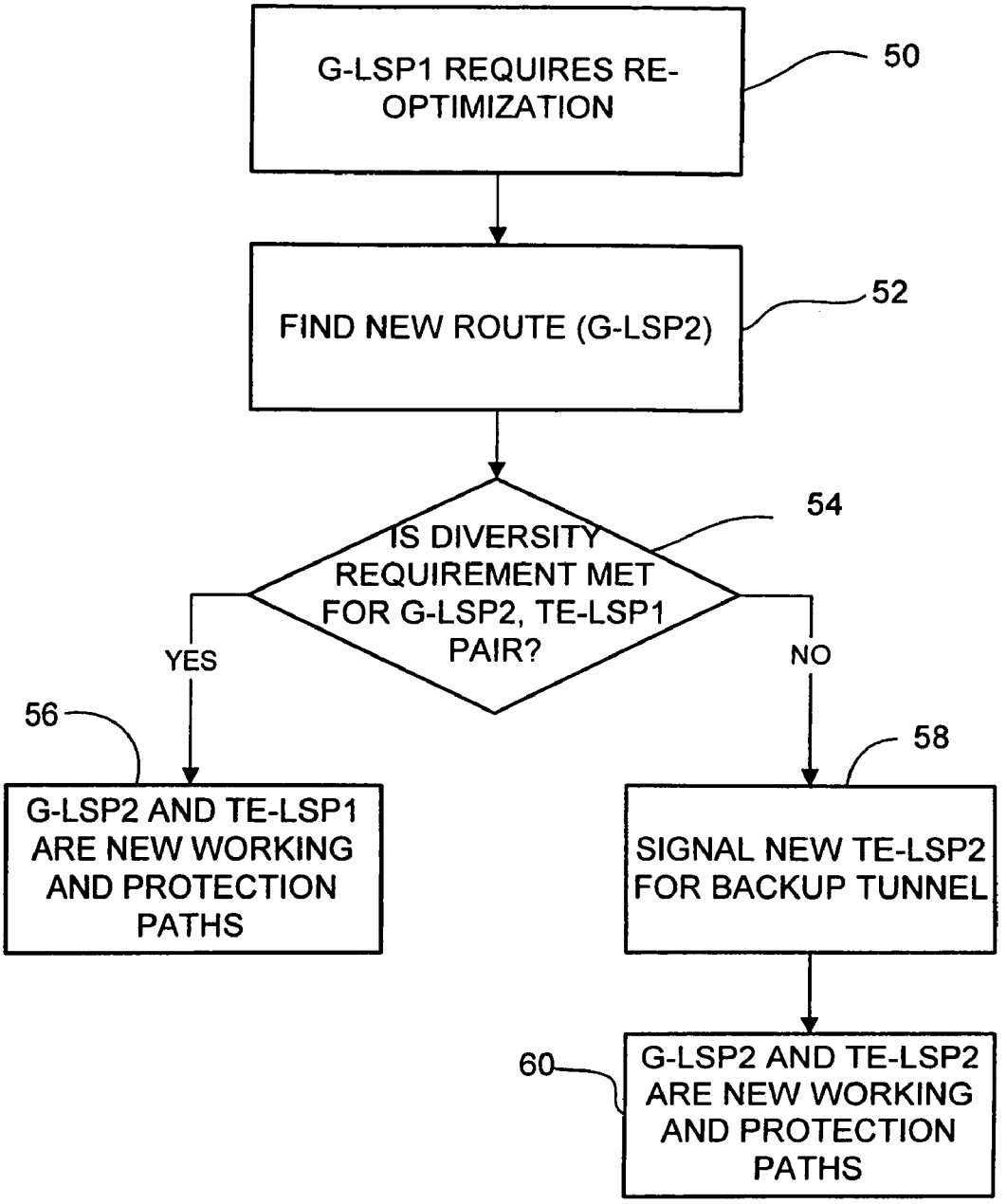

G-LSP1 REQUIRES RE-OPTIMIZATION
50
FIND NEW ROUTE (G-LSP2)
52
IS DIVERSITY REQUIREMENT MET FOR G-LSP2, TE-LSP1 PAIR?
54
YES
NO
56
G-LSP2 AND TE-LSP1 ARE NEW WORKING AND PROTECTION PATHS
58
SIGNAL NEW TE-LSP2 FOR BACKUP TUNNEL
60
G-LSP2 AND TE-LSP2 ARE NEW WORKING AND PROTECTION PATHS

FIG. 5

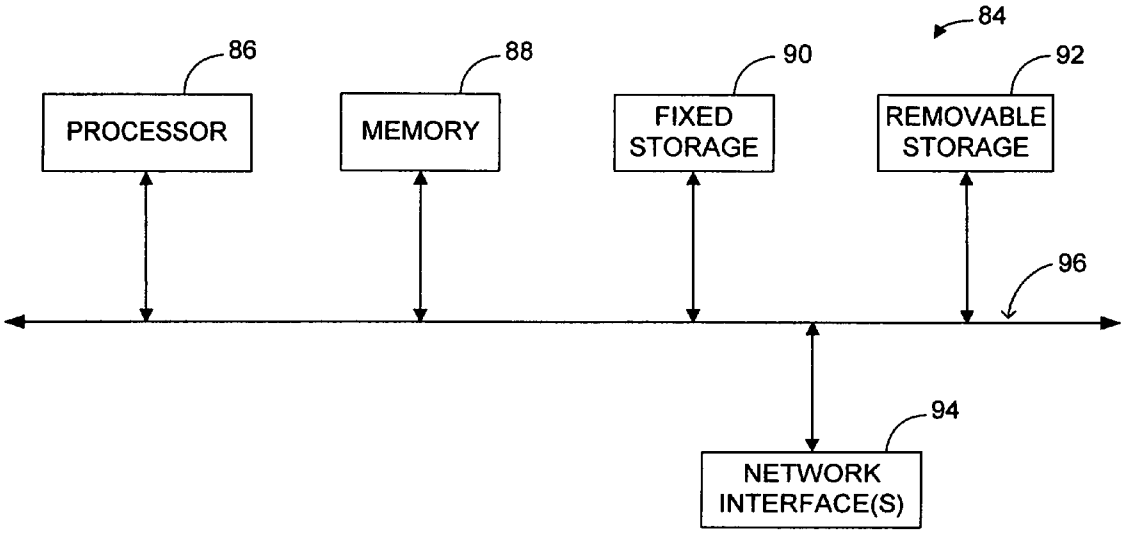

84
86
88
90
92
PROCESSOR
MEMORY
FIXED STORAGE
REMOVABLE STORAGE
96
94
NETWORK INTERFACE(S)

FIG. 6

DYNAMIC PATH PROTECTION IN AN OPTICAL NETWORK

BACKGROUND OF THE INVENTION

[0001] The present invention relates generally to communication networks, and more specifically, to dynamic path protection in an optical network and integration with link protection schemes in an IP network.

[0002] The rapid growth of the Internet and the widespread deployment of networks built around the Internet Protocol suite are creating a demand for new capabilities in IP (Internet Protocol) networks. MultiProtocol Label Switching (MPLS) provides a number of powerful capabilities such as traffic engineering, etc. As with IP routers, MPLS nodes use a routing protocol such as OSPF or IS-IS to calculate network paths and establish reachability. MPLS is an IETF (Internet Engineering Task Force) initiative that integrates Layer **2** information about network links (bandwidth, latency, utilization) into Layer **3** (IP) within a particular autonomous system in order to simplify and improve IP packet exchange. MPLS-TE provides network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

[0003] Generalized MPLS (GMPLS) extends MPLS-TE to provide a control plane (signaling and routing) for devices that switch in domains such as packet, time, wavelength, and fiber. This common control plane simplifies network operation and management by automating end-to-end provisioning of connections, managing network resources, and providing a level of QoS that is expected in new applications. GMPLS extends the suite of IP-based protocols that manage and control the establishment and release of label switched paths (LSPs) that traverse any combination of packet, TDM, and optical networks.

[0004] Protection of switched LSPs is important, and more particularly, with respect to GMPLS nodes connected in a general topology and under tight time constraints. One requirement for protection in IP and optical networks is to avoid or reduce the effects of failures in optical network in the IP topology/traffic. More specifically, if a link that is part of an end-to-end GMPLS connection fails, it is preferred that this failure not result in a failure of routing adjacency (e.g., IGP adjacency). This is because local failures can be addressed much more quickly and efficiently inside the optical network. Also, IP convergence is slower than any technique that optical networks can provide and there is a need for service isolation. Thus, service providers in general would like the GMPLS network to handle failures in the optical networks such that they do not affect routing adjacencies.

[0005] Conventional approaches for protection against failures in optical networks in the IP topology/traffic have the drawback that a failure in doing local restoration results in failure of routing adjacencies.

[0006] There is, therefore, a need for a system and method for handling failures in an optical network such that the failure does not affect routing adjacencies.

SUMMARY OF THE INVENTION

[0007] A method and system for dynamic path protection in an optical network and integration with link protection schemes in an IP network are disclosed. The method includes establishing two or more paths within the optical network and grouping the paths in a dynamic bundle. The grouping is selected at a control plane level and the bundle of paths are recognized as a single routing adjacency in the IP network so that as long as one or more paths within the bundle is operating, the routing adjacency in the IP network is not affected by changes within the bundle.

[0008] In another aspect of the invention, a method for dynamic end-to-end path protection in an optical network generally comprises the establishment of a number of working and protecting paths and selecting new paths for a subset of these paths when an event causing network topology changes occurs. The new paths are selected such that the overall diversity and optimality degree are maintained to a level allowed by the new topology.

[0009] In yet another aspect of the invention, a system for providing dynamic end-to-end protection in an optical network generally comprises a processor operable to create two or more paths within the optical network and group two or more of the paths in a bundle. The system further comprises a protection module configured to dynamically identify the physical interfaces spanned by optical LSPs, manage the component interfaces of the bundle, and maintain synchronization with the data plane protection scheme activated for the bundle.

[0010] Further understanding of the nature and advantages of the inventions herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] **FIG. 1A** is an example of a network in which the present invention may be implemented.

[0012] **FIG. 1B** illustrates interaction between GMPLS control plane and a protection mechanism of the present invention.

[0013] **FIG. 2** is a flowchart illustrating a process for maintaining dynamic bundles for protection in an IP +optical network.

[0014] **FIG. 3** illustrates a plurality of nodes having two dynamic bundles with two component LSPs.

[0015] **FIG. 4** illustrates the plurality of nodes shown in **FIG. 3** with two new links added.

[0016] **FIG. 5** is a flowchart illustrating a process for dynamic FRR.

[0017] **FIG. 6** is a system block diagram of a computer system that can be utilized to execute software of an embodiment of the present invention.

[0018] Corresponding reference characters indicate corresponding parts throughout the several views of the drawings.

DESCRIPTION OF SPECIFIC EMBODIMENTS

[0019] The following description is presented to enable one of ordinary skill in the art to make and use the invention. Descriptions of specific embodiments and applications are provided only as examples and various modifications will be readily apparent to those skilled in the art. The general

principles described herein may be applied to other embodiments and applications without departing from the scope of the invention. Thus, the present invention is not to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features described herein. For purpose of clarity, details relating to technical material that is known in the technical fields related to the invention have not been described in detail.

[0020] The present invention operates in the context of a data communication network including multiple network elements. A network element may be, for example, a terminal multiplexer, an add-drop multiplexer (ADM), photonic switch (PXC), optical crossconnect (OXC) with optical-electrical-optical (OEO) conversion, SONET crossconnect, signal regenerator, router, switch, or other optical or IP node interface. The network may include an IP based packet switching network connected to an optical transport network (OTN). A router is connected to the OTN nodes using standard interfaces (e.g., 4×OC192 POS, 16×OC48 POS, N×10GE, etc.), as is well known by those skilled in the art.

[0021] **FIG. 1A** illustrates an example of a network in which data transmission occurs on generalized label-switched paths (G-LSPs). The G-LSPs are automatically setup and torn down by means of a signaling protocol, as is well known by those skilled in the art. (In the following description, the term LSP is also used to refer to generalized LSPs.) **FIG. 1A** illustrates end-to-end protection with one working path **14** (between nodes **12***a* and **12***b*) and one protecting (recovery) path **16** (between nodes **12***c* and **12***d*). The working and protecting paths **14**, **16** are preferably signaled as two LSPs that belong to the same tunnel. The working LSP **14** transports traffic between routers **10***a* and **10***b* and the protecting LSP **16** is used to transport traffic when the working LSP fails. End-to-end recovery provides recovery of the entire LSP from its source (ingress router end-point **10***a*) to its destination (egress router end-point **10***b*).

[0022] It is to be understood that the arrangement shown in **FIG. 1A** is only one example and the invention described herein may be applied to a network having any number of working or recovery LSPs.

[0023] A method and system disclosed herein provide integration of GMPLS control plane and available data plane protection techniques. Dynamic protection is provided for virtual links associated with the GMPLS LSPs that are used in communication with the IP network. More specifically, the method and system provide dynamic end-to-end path protection in an optical network and integration of the optical network with link protection schemes in the IP network. The data plane protection techniques include: link bundling of GMPLS tunnel interfaces; SONET APS protection for GMPLS tunnel interfaces; and FRR over GMPLS tunnel interfaces. The first two techniques are described together under Dynamic Bundles in the following detailed description and the third technique is described separately under Dynamic FRR.

[0024] **FIG. 1B** illustrates interaction between the GMPLS control plane and a protection mechanism (e.g., link bundling of the GMPLS tunnel interfaces, SONET APS protection for GMPLS tunnel interfaces, FRR over GMPLS tunnel interfaces, described below). TE control is used to program the protection mechanism. The GMPLS control plane uses APIs provided by the protection layer to associate the physical interfaces traversed by the working and protecting optical LSPs **14**, **16** (**FIG. 1A**). This is referred to as "programming protection" in **FIG. 1B**. GMPLS has support from the protection layer so that the set of working/protecting interfaces can be changed on-the-fly without traffic loss. TE control abstracts tunnel/LSP interfaces from the protection layer (i.e., protection mechanism), which is not aware how protection is configured by GMPLS. One exception to this abstraction is the FRR (MPLS layer), which has knowledge of the optical LSP interfaces. GMPLS layer provides LSP interface to physical interface mapping such that FRR can take appropriate actions upon defect notification for the physical interfaces in question. Defect notification is not needed by the TE control, which receives alarm notifications or responds to failure based RSVP (Resource ReSerVation protocol) notification (e.g., on Path Error notification).

[0025] TE control abstracts the underlying physical interfaces of an optical LSP from the applications. Failure of the working or protecting component LSP is not visible to the applications using the tunnel interfaces as long as there are other means (via protection) for forwarding the traffic over the tunnel interface.

[0026] The following describes the present invention from a router-to-router GMPLS circuit perspective, however, it is to be understood that the invention is also applicable to other optical/routing devices which establish forwarding adjacency using GMPLS or any other optical technology.

Dynamic Bundles

[0027] A number of LSPs are established during GMPLS tunnel setup. The traffic may be arranged or duplicated any number of ways, as is well known by those skilled in the art. The paths are grouped into one or more bundles. With link bundling of the GMPLS interface, the component membership to the bundle is decided upon by the GMPLS control plane, which brings in the data plane aspect of dynamic membership. The LSPs in a bundle are established between the same source and destination nodes and, based on configuration or enforced SLA, they have a certain degree of diversity and optimality. These LSPs may be re-optimized or re-routed due to topology changes or failures in the network. As different network events change the egress physical interfaces of the LSPs, the membership in the dynamic bundle changes on-the-fly. The data plane protection mechanism (e.g., link bundling of GMPLS tunnel interfaces or SONET APS protection for GMPLS tunnel interfaces) is also selected based on the configuration or SLA. The selected data plane protection mechanism also may change due to configuration or policy changes. These changes are handled with minimum impact by the GMPLS control plane when handled through dynamic bundles.

[0028] Another aspect of dynamic bundles is the handling of LSP bundles in the control plane. When an LSP set is created, if the routes are dynamically computed, a certain degree of diversity/optimality may be requested and realized. When a re-optimization operation is triggered (for example in the case where there is a change in topology or when an LSP needs to be re-routed due to a failure), an attempt is preferably made to maintain the degree of diversity/optimality at the set level. To realize this, path computation is used to determine a new LSP set. The LSPs in the new set can share resources with any subset of the old paths.

This procedure is referred to as "make-a-set-before-break-a-set" and is described below.

[0029] **FIG. 2** is a flowchart illustrating one example of a process of the present invention for maintaining and using dynamic bundles for network protection. At step **20**, "N" link/node/SRLG (Shared Risk Link Group) diverse paths are established inside the optical network. The value "N" is a configurable parameter. After path computation and signaling is completed, TE control has the knowledge of physical interfaces that need to be protected (i.e., egress interfaces on GMPLS paths). At step **22**, the GMPLS control plane brings up the L**1** (via optical cross connect devices) for the egress physical interfaces taken by the GMPLS path. TE control uses APIs provided by the L**2** bundling to bundle the tunnel interfaces using the physical interfaces previously computed (step **24**) (see "programming protection" described above). After step **24**, there are a bundle of "N" optical connections at the two ends of the routers using a L**2** bundling technique that is supported, for example, by routers such as GSR (Gigabit Switch Router) and CRS (Carrier Routing System). The "N" GMPLS paths appear as a single routing adjacency in the IP network. When a failure occurs on any node/link on the path of the GMPLS LSPs, the protection scheme detects the defect (e.g., LOS, RDI, etc.) without involvement of the GMPLS control plane (steps **26** and **28**). As long as 1-out-of-N GMPLS paths is up, routing adjacency at the IP network is not effected by the failure in the optical network (steps **30**, **32**, **34**). The protection scheme is also able to make protection decisions without involving GMPLS control plane. In particular, there is no need to wait for LMP fault isolation or RSVP perr message. Similarly, defect notification is not needed by the TE Control. TE Control responds to failures based on RSVP notification (e.g., on Path Error notification).

[0030] When a new optical tunnel is created and added to the bundle, the physical interfaces associated with the optical tunnel interface is identified by a protection module and added to the bundle. If a failure occurs on an optical LSP which is also a component in the L**2** bundle, the GMPLS control plane restores the LSP using, for example, a new physical interface and the protection module performs the translation to the new interface that will replace the old one. In other words, as GMPLS LSPs can change paths on-the-fly (e.g., due to rerouting in the event of a failure, re-optimization, etc.), TE control can change membership of the bundled interface in the event of a re-route of the GMPLS LSP.

[0031] In order to better illustrate the make-a-set-before-break-a-set process, the following example is provided. In this example, a dynamic bundle with two components LSP**1** and LSP**2** is created, with the two LSPs being setup with link and node diversity (**FIG. 3**):

*LSP*1–*R*3, *R*1, *R*6, *R*∝(cost=30)

*LSP*2–*R*3, *R*5, *R*2, *R*4 (cost=30)

In this example, all links are assumed to have cost equal to 10, therefore LSP**1** and LSP**2** each have a cost equal to 30.

[0032] As shown in **FIG. 4**, two new links (shown with dashed lines) with cost equal to 5 are added to connect R**1** with R**2** and R**5** with R**6**. If re-optimized as a set the new LSPs will be:

LSP1–R3, R1, R2, R4 (cost 25)

LSP2–R3, R5, R6, R4 (cost 25)

Without an optimization that treats the two LSPs as a set, where LSPs are individually re-optimized, the new paths would not be found if the diversity requirement is kept.

[0033] It is to be understood that changes may be made to the process described above without departing from the scope of the present invention. For example, the process may be extended to a generic set of LSPs (e.g., all LSPs between two nodes or all LSPs with certain affinity requirements).

Dynamic FRR

[0034] Dynamic FRR extends link protection schemes, such as FRR (Fast Reroute), to handle GMPLS LSPs. A GMPLS LSP (G-LSP) is protected using a backup tunnel (TE-LSP) in a similar way as to how FRR is realized for physical links.

[0035] The association between the outgoing interface of G-LSP (the FRR protected interface) and the backup tunnel interface of TE-LSP is dynamic in nature and is handled by the GMPLS control plane for seamless integration. There is a new diversity aspect that is introduced by the fact that the 'protected link' is an LSP with the dynamic aspect attached to it. G-LSP and TE-LSP are preferably initially setup with a maximum diversity degree. Different network events may change the route of the G-LSP that may end up sharing resources (or SRLGs) with the TE-LSP. However, this is not desirable, and a new procedure is required. The procedure described herein coordinates between a number (two for the FRR case) of make-before-break operations. The procedure is referred to herein as set-of-make-before-breaks and is described below.

[0036] In general, set-of-make-before-break refers to the synchronization of a number of make-before-break procedures for related LSPs. In the case of FRR, the G-LSP re-route or re-optimization procedure is performed in parallel with the path re-computation for the backup TE-LSP, with the diversity requirement defining the relation between the two.

[0037] **FIG. 5** is a flowchart illustrating one example of a process of the present invention for dynamic FRR. At step **50**, G-LSP**1** needs to be re-optimized. A new (better) route is determined and G-LSP**2** is ready to be signaled using a make-before-break procedure (step **52**). Since G-LSP**1** is protected by TE-LSP**1**, a determination is made if the (G-LSP**2**, TE-LSP**1**) pair still satisfies the diversity requirement (step **54**). If this requirement is met, G-LSP**2** and TE-LSP**1** are the new working and protecting paths, respectively (step **56**). If this requirement is not met, a new TE-LSP**2** is signaled for the backup tunnel using a make-before-break procedure (steps **58** and **60**). In order to minimize the window where a failure will have an impact on the data traffic, these two procedures are synchronized. The diversity requirement may be specified, for example, with respect to link diversity, node diversity, SLRG diversity, or any combination thereof.

[0038] The invention described herein may be implemented in dedicated hardware, microcode, software, or photonic (optical) logic. **FIG. 6** shows a system block diagram of computer system **84** that may be used as a router or host or used to execute software of an embodiment of the

invention. The computer system **84** includes memory **88** which can be utilized to store and retrieve software programs incorporating computer code that implements aspects of the invention, data for use with the invention, and the like. Exemplary computer readable storage media include CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive. Additionally, a data signal embodied in a carrier wave (e.g., in a network including the Internet) may be the computer readable storage medium. Computer system **84** further includes subsystems such as a central processor **86**, fixed storage **90** (e.g., hard drive), removable storage **92** (e.g., CD-ROM drive), and one or more network interfaces **94**. Other computer systems suitable for use with the invention may include additional or fewer subsystems. For example, computer system **84** may include more than one processor **86** (i.e., a multi-processor system) or a cache memory.

[**0039**] The system bus architecture of computer system **84** is represented by arrows **96** in **FIG. 6**. However, these arrows are only illustrative of one possible interconnection scheme serving to link the subsystems. For example, a local bus may be utilized to connect the central processor **86** to the system memory **88**. Computer system **84** shown in **FIG. 6** is only one example of a computer system suitable for use with the invention. Other computer architectures having different configurations of subsystems may also be utilized. Communication between computers within the network is made possible with the use of communication protocols, which govern how computers exchange information over a network.

[**0040**] As can be observed from the foregoing, the system and method described herein have many advantages. The present invention provides load balancing in IP+optical networks, transparency to network applications, flexible incremental bandwidth, and resiliency and fast convergence. The method and system described herein also make use of existing protection schemes (including SONET APS functions and hardware) by introducing a layer for mapping tunnel interface to physical interface and programming the protection scheme that is supported. The present invention also provides a more optimum way to reoptimize resources by extending the shared resources to a bigger set of LSPs. The method and system also provide a solution for reoptimization for a tunnel protected end-to-end system and makes use of local protection if local protection is supported by the optical network. Furthermore, a solution for use of FRR in the context of GMPLS is provided.

[**0041**] Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations made to the embodiments without departing from the scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

What is claimed is:

1. A method for dynamic protection of virtual links for paths of an optical network in communication with an IP network, the method comprising:

establishing two or more paths within the optical network; and

grouping two or more of said paths in a dynamic bundle, the grouping selected at a control plane level;

wherein said bundle of paths are recognized as a single routing adjacency in the IP network such that as long as one or more paths within the bundle is operating the routing adjacency in the IP network is not affected by changes within said bundle.

2. The method of claim 1 wherein the virtual links are implemented as generalized label switched paths.

3. The method of claim 1 further comprising detecting a failure in one of said paths at a data plane level.

4. The method of claim 3 further comprising rerouting traffic to a backup path within said bundle.

5. The method of claim 3 further comprising recovery of an entire generalized label switched path from its source to its destination.

6. The method of claim 1 further comprising creating a new path and adding said new path to said bundle.

7. The method of claim 6 wherein adding said new path to said bundle comprises adding a physical interface associated with said new path to said bundle.

8. The method of claim 1 wherein the optical network is a GMPLS network.

9. The method of claim 1 further comprising re-optimizing said paths within said bundle.

10. The method of claim 9 further comprising maintaining optimality or diversity during optimization.

11. The method of claim 1 further comprising protecting said paths using a data plane protection mechanism.

12. The method of claim 11 wherein said data plane protection mechanism is SONET APS protection.

13. The method of claim 1 wherein grouping two or more paths comprises bundling GMPLS tunnel interfaces.

14. A computer program product for dynamic protection of virtual links for paths of an optical network in communication with an IP network; the product comprising:

providing dynamic link protection in an optical network in communication with an IP network, comprising:

code that establishes two or more paths within the optical network;

code that groups two or more of said paths in a dynamic bundle, the groups selected at a control plane level; and

a computer-readable storage medium for storing said codes;

wherein said bundle of paths are recognized as a single routing adjacency in the IP network such that as long as one or more paths within the bundle is operating the routing adjacency in the IP network is not affected by changes within said bundle.

15. The computer program product of claim 14 further comprising code that detects a failure in one of said paths at a data plane level.

16. The computer program product of claim 14 wherein the optical network is a GMPLS network.

17. A system for dynamic protection of virtual links for paths of an optical network in communication with an IP network, the system comprising:

means for establishing two or more paths within the optical network; and

means for grouping two or more of said paths in a dynamic bundle, the grouping selected at a control plane level;

wherein said bundle of paths are recognized as a single routing adjacency in the IP network such that as long as one or more paths within the bundle is operating the routing adjacency in the IP network is not affected by changes within said bundle.

18. The system of claim 17 further comprising means for maintaining optimality or diversity during optimization.

19. A system for dynamic protection end-to-end path protection in an optical network in communication with an IP network, the system comprising:

a processor operable to create two or more paths within the optical network and group two or more of said paths in a bundle, said bundle comprising at least one working path and at least one protecting path each extending from an ingress router to an egress router; and

a protection module configured to dynamically identify a physical interface associated with an optical tunnel interface for a new path and replace one of said paths in said bundle with said new path.

20. The system of claim 19 wherein the paths are generalized label switched paths.

21. The system of claim 20 wherein the processor is configured to restore a failed generalized label switched path using the GMPLS control plane.

22. The system of claim 21 wherein the protection module is further configured to manage component interfaces of the bundle and maintain synchronization with a data plane protection mechanism.

23. A method for providing dynamic path protection in an optical network in communication with an IP network, the method comprising:

establishing a set of working and protecting paths, each of said working paths having at least one of said protecting path designated as its backup path;

following a failure or during optimization, selecting and establishing at least one new working path to replace one of said working paths;

determining if said new working path and said designated backup path provide a predefined degree of diversity; and

selecting a new protecting path if said predefined degree of diversity is not met.

24. The method of claim 23 wherein selecting a new working path comprises utilizing fast reroute.

25. The method of claim 23 wherein said path interfaces are defined by a GMPLS control plane.

* * * * *