UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

CISCO SYSTEMS INC.,

Petitioner

_____

IPR2025-00188
U.S. Patent No. 8,982,691

_____

DECLARATION OF HENRY H. HOUH, PH.D., UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW

TABLE OF CONTENTS

I. INTRODUCTION

1. I, Henry H. Houh, have been retained by counsel for Cisco Systems Inc. ("Petitioner") as a technical expert in connection with the proceeding identified above. I submit this declaration in support of Cisco's Petition for *Inter Partes* Review ("IPR") of U.S. Patent No. 8,982,691 ("the '691 patent").

2. I am being compensated for my work in this matter at an hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this matter. My compensation is not contingent on the outcome of this matter or the specifics of my testimony. I have no personal or financial stake or interest in the outcome of this proceeding.

3. I have been asked to provide my opinions regarding whether the subject matter of claims 1 to 10 (the "Challenged Claims") of the '691 patent would have been obvious to a person having ordinary skill in the art ("POSITA") as of the earliest claimed priority date. It is my opinion that the Challenged Claims would have been obvious to a POSITA after reviewing the prior art, as discussed below.

4. In the preparation of this declaration, I have considered:

(1) the '691 patent, Ex.1001;
(2) the prosecution history of the '691 patent, Ex.1002;
(3) U.S. Patent Pub. No. 2004/0218525, ("EDC_525"), Ex.1005;
(4) U.S. Patent Pub. No. 2004/0246892, ("EDC_892"), Ex.1006;
(5) Provisional Application 60,328,087, Ex.1007;
(6) U.S. Patent No. 8,913,481, Ex.1008;

(7) "Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks," Park et al, IEEE 2008, Ex.1009;

(8) "Optimal and Guaranteed Alternative LSP for Multiple Failures," Hundessa et al., IEEE 2004, Ex.1010;

(9) U.S. Patent No. 7,835,267, Ex.1011;

(10) U.S. Patent No. 9,559,947, Ex.1012;

(11) U.S. Patent Pub. No. 2009/0292943, ("Hanif"), Ex.1013;

(12) Microsoft Computer Dictionary, (1999), Ex.1014;

(13) U.S. Patent No. 7,821,951, Ex.1015;

(14) C++ Inside and Out, Eckel (1993), Ex.1016;

(15) Programming Microcontrollers in C, Sickle (1994), Ex.1017;

(16) RFC3945, Ex.1018;

(17) RFC4090, Ex.1019;

(18) U.S. Patent No. 7,672,226, Ex.1020;

(19) U.S. Patent No. 7,626,925, Ex.1021;

(20) Traffic Engineering with MPLS, Osborne (2003), Ex.1022;

(21) Fault-Tolerant IP and MPLS Networks, Hussain (2004), Ex.1023;

(22) U.S. Patent Pub. No. 2009/0219806A1, Ex.1024;

(23) U.S. Patent Pub. No. 2006/0159009A1, Ex.1025;

(24) MPLS Traffic Engineering Path Link and Node Protection Configuration Guide, (2011), Ex.1026;

(25) Protection Performance Components in MPLS Networks, Calle (2004), Ex.1027;

(26) U.S. Patent No. 7,616,637, Ex.1028;

(27) RFC3031, Ex.1029;

(28) Certified English Translation of CN101645848A, Ex.1030;

(29) CN101645848A, Ex.1031;

(30) Websters new World Dictionary of Computer Terms (2000), Ex.1032;

(31) Computer Desktop Encyclopedia (2001), Ex.1033;

(32) The C language interface to the SQLite library Ex.1034;

(33) University of Hawaii, EE160 Book, Chapter 9, Two Dimensional Arrays Ex.1035;

(34) Functional C (1999) Ex.1036;

(35) UT Austin Lecture_2010 Ex.1037;

(36) A Complete Guide to C++, Ex.1038; and

(37) Introduction to Pro_C, Ex.1039.

5. In forming the opinions expressed below, I have considered: the documents listed above; the relevant legal standards, including the standard for obviousness; and my own knowledge and experience based upon my work in the field of wireless communications as described below, as well as any additional materials cited herein.

6. Unless otherwise noted, all emphasis in any quoted material has been added.

II. QUALIFICATIONS

7. The details of my background and education, and a listing of all publications that I have authored, are provided in my *Curriculum Vitae*, a copy of which is submitted as Ex.1004. The following is a brief summary of my relevant qualifications and professional experience.

8. I received a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology ("MIT") in 1998. I also received a Master of Science degree in Electrical Engineering and Computer Science in 1991, a Bachelor of Science Degree in Electrical Engineering and Computer Science in 1989, and a Bachelor of Science Degree in Physics in 1990, all from MIT.

9. During my college studies, I focused on communications and data networking. I took specialized courses including graduate courses in telecommunications networks, optical communications, and data networking. I, along with other graduate students in a networking research group, maintained both the computer workstations and the networking devices in the research group.

10. I have worked in data networking and distributed networking systems on several occasions. As part of my doctoral research at MIT from 1991-1998, I worked as a research assistant in the Telemedia Network Systems ("TNS") group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit ATM network and applications which ran over the network, such as remote video capture (including audio), processing and display on computer terminals. In addition to helping design the core network components (such as the ATM switch), designing and building the high-speed ATM links, and designing and writing the device drivers for the interface cards, I also set up the group's web server, which at the time was one of the first several hundred web servers in existence. Our high-

speed data network carried multimedia data including video and audio data within ATM cells.

11. The TNS group was the first group to initiate a remote video display over the World Wide Web. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it; the video was encoded by TNS-designed hardware, streamed over the TNS-designed network and displayed using TNS-designed software.

12. I authored or co-authored twelve papers and conference presentations on our group's research. I also co-edited the final report of the gigabit networking research effort with Professor David Tennenhouse and Senior Research Scientist David Clark. David Clark is generally considered to be one of the fathers of the Internet Protocol and served as Chief Protocol Architect for the Internet. With its focus on networking, the group, including myself, set up and maintained the network and computer systems. These systems included the networking on the workstations and desktops, the distributed file system, desktops and workstations, setting up and maintaining the distributed file system (Network File System) and the authentication system (Network Information Service, formerly known as Yellow Pages).

13. I defended and submitted my Ph.D. thesis, titled "Designing Networks for Tomorrow's Traffic," in January 1998. As part of my thesis research, I analyzed local-area and wide-area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time. My thesis involved analyzing flows of data in the network and the routing efficiencies gained by labeling the flows at the edge of the network, and routing the data based on the label instead of the IP destination address. My analysis included different methods of setting up the granularity of the flows for the most efficient use of routing resources. This type of label switching became popular with Multiprotocol Label Switching (MPLS) later implemented in various commercial routers. I gathered a large amount of network traffic, used publicly available network traces, and broke the traffic into different types of flows using various parameters for classifying the flows. My flow analysis is applicable to the flow classification at the ingress to an MPLS domain. My thesis also addressed real-time streamed audio and video. The network traffic that I analyzed was IP protocol traffic, including UDP and TCP.

14. From 1997 to 1999, I worked at NBX Corporation, which was acquired by 3Com Corporation in 1999. During this time, I was a Senior Scientist and Engineer working in IP Telephony. NBX delivered the world's first fully featured business telephone system to run over a data network, the NBX100. NBX was one of the first business phone systems to be configurable via a web interface.

Users and administrators had access to varying levels of configuration for the phone system.

15. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones which depacketized the voice data and reconstructed the audio. In addition, I designed the voice data packet transmission algorithms. I created a system to capture and analyze network packets sent by devices in the NBX system for aid in testing and debugging. I also designed and validated the core packet transport protocol used by the phone system. In addition, I designed and oversaw the development of the underlying transport protocol used by the NBX100 phone system for reliable packet transport, used in the system to communicate from the network-based telephones to the call control unit. I wrote NBX's first demonstration IP software stack, which added the capability for utilizing the NBX100 phone system on an IP network. I also specified and prototyped the phone system's support for Differentiated Services. NBX first demonstrated a phone in the NBX100 system working over the Internet in 1998 at a trade show in Las Vegas, for which I acquired, set up, and configured Virtual Private Network tunnels to carry the traffic. I was later the lead architect in designing NBX's next-generation highly scalable system. After NBX was acquired by 3Com, I did some work with 3Com's cable equipment division, including demonstrating a working NBX IP phone system over 3Com's cable equipment infrastructure using an early version of

DOCSIS at a trade show in 1999. The NBX100 was the market's leading business phone system to run on a data network for several years following its introduction. During that time, I became more familiar with the various standards relevant to Internet telephony as well as the problems which designers of commercial telephony operations were faced with in implementing VoIP.

16. I, along with two of NBX's founders, were awarded U.S. Patent No. 6,967,963 titled "Telecommunication Method for Ensuring On-Time Delivery of Packets Containing Time-Sensitive Data," for some of the work we did while at NBX.

17. After NBX, I worked at Teradyne, a test tool company primarily focused on semiconductors. Teradyne had recently acquired Hammer, a company that specialized in load and functional testing for telecommunications systems. The Hammer product is well known as a telecom test tool. Teradyne spun out Hammer and several other internal divisions into an independent company called Empirix. I became Chief Technologist of the Hammer division of Empirix. Empirix was a leader in VoIP network testing and monitoring.

18. At Empirix, I laid out a new multi-year product vision for data network testing, secured internal funding for the effort, and led a team to deliver a new technology platform to the market in February 2001. This new product, PacketSphere, initially emulated network behavior so that wide-area VoIP

connections could be tested in a lab. The PacketSphere allowed the packet loss, jitter, and reordered packet rates to be adjusted to emulate the behavior of a real-world network inside the test lab. A later release allowed PacketSphere to generate high volumes of VoIP calls, including media streams, and to monitor the quality of VoIP voice streams. PacketSphere was also used in the Storage Area Network area. Later, the core technology was added to other Empirix products such as Empirix's Hammer XMS to monitor thousands of VoIP media streams in real time to determine their quality. PacketSphere was Empirix's most successful new platform introduction at the time. Companies purchased the PacketSphere product to emulate an Internet Protocol network to see the effects of deploying their product on the Internet prior to launch. PacketSphere received several industry awards. I applied for several patents covering this work, U.S. Patent Application Publication Nos. 20020016708 and 20020016937, both titled "Method and Apparatus for Utilizing a Network Processor as Part of a Test System" and which pertain to MPLS.

19. During my time at Empirix, I presented lectures on VoIP and data network testing to companies including Lucent Labs (formerly AT&T Bell Labs). I was also invited to present several guest lectures in a software engineering course at MIT. Since then, I have also participated twice as a unit lecturer in an experimental course that was taught by an Institute Professor (the highest award that a MIT

Professor can achieve) and sponsored by the Chairman of the MIT Corporation (MIT's board of trustees).

20. From 2004 to 2008, I was employed by BBN Technologies Corp., a technology research and development company located in Cambridge, Massachusetts. BBN Technologies is a world-renowned company with expertise in acoustics, speech recognition, and communications technology. BBN Technologies staff have pioneered many internetworking technologies and Internet applications and have built some of the world's largest government and commercial data networks.

21. My duties and responsibilities at BBN Technologies generally included commercialization of the technologies developed by BBN Technologies, which included spinning off companies and growing commercial businesses in-house. More particularly, I was involved in utilizing the award-winning AVOKE STX speech recognition technology to create the public audio/video search engine EveryZing (formerly known as PodZinger) which was spun out into a stand-alone company now known as RAMP, Inc. PodZinger won the 2006 MITX Technology Award for best Web 2.0 Application and was also named the 2006 Forbes Favorite Video & Audio Search Engine, beating out Google, Yahoo, and other companies. After managing the creation of the initial prototype system, PodZinger built out a full streaming audio and video search solution when I was the Vice President of

Operations and Technology there. I was also involved in the Boomerang Mobile Shooter Detection project as the Vice President of Engineering for the program. The Boomerang system was deployed to Iraq and Afghanistan and was credited with saving many lives.

22. In 2012, I opened Einstein's Workshop, a 7,000 square foot facility for teaching science, technology, engineering, and math to children. I installed and configured the telephone system, designed and programmed the website, and designed and configured the network, which has grown to roughly 100 computers, multiple WiFi access points, firewalls, multiple wireless networks, and multiple facilities. We also created an educational 3D Computer-Aided Design program, which we spun-out into a separate company, BlocksCAD. BlocksCAD has received grants from DARPA DSO and the USDA and has participated in the LearnLaunch, MIT Play Labs, and MassChallenge accelerator programs. BlocksCAD currently has over 150,000 registered users and is used in schools throughout the US.

23. From 1989 to 1990, I worked at AT&T Bell Laboratories on optical computers. This work generated six peer-reviewed papers, and multiple U.S. and European patent applications in which I was named as a co-author or inventor. I also interned at AT&T Bell Laboratories in 1987 and 1988. Additional relevant experience in the field of computer networking is listed in my *Curriculum Vitae*.

24. I am a named inventor on several patents and published patent applications that are related to VoIP technology including: U.S. Patent No. 6,967,963, entitled "Telecommunication Method for Ensuring On-Time Delivery of Packets Containing Time-Sensitive Data"; U.S. Patent Application Publication No. 20020015387, entitled "Voice Traffic Packet Capture and Analysis Tool for a Data Network"; U.S. Patent Application Publication No. 20020016708, entitled "Method and Apparatus for Utilizing a Network Processor as Part of a Test System"; U.S. Patent Application Publication No. 20020016937, entitled "Method and Apparatus for Utilizing a Network Processor as Part of a Test System"; and U.S. Patent No. 7,590,542, entitled "Method of Generating Test Scripts Using a Voice-Capable Markup Language."

III. LEVEL OF ORDINARY SKILL IN THE ART

25. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

26. A POSITA in the field of the '691 patent, as of the earliest claimed priority date of September 28, 2012, would have been someone knowledgeable and familiar with network communications and multiprotocol label switching-transport

("MPLS") techniques available at the time. Such a POSITA would have a bachelor's degree in computer science, computer engineering, electrical engineering, or equivalent training, and approximately two years of experience working in the field of network communications and would be knowledgeable regarding MPLS techniques. Additional work experience can substitute for specific educational background, and vice versa.

27. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my own experience and what a POSITA would have understood or known generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the relevant field as of the priority date of the '691 patent.

IV. RELEVANT LEGAL STANDARDS

28. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '691 patent, I am relying on certain legal principles that counsel has explained to me.

29. I understand that prior art to the '691 patent includes patents and printed publications in the relevant art that predate the priority date of the '691 patent. For purposes of this Declaration, I am applying the earliest claimed priority date of September 28, 2012, as the priority date of the '691 patent.

30. I have been informed by Cisco's counsel that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the claimed invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a POSITA. I have also been informed by Cisco's counsel that the obviousness analysis considers factual inquiries, including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

31. I have been further informed by Cisco's counsel that there are several recognized rationales for combining references or modifying a reference to show obviousness. These rationales include: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led a POSITA to modify the prior art or to combine prior art teachings to arrive at the claimed invention.

32. Also, I have been informed and understand that obviousness does not require physical combination/bodily incorporation, but rather consideration of what

the combined teachings would have suggested to a POSITA at the time of the alleged invention.

V. BACKGROUND

33. I discuss in this section general background information regarding MPLS protection techniques. It is my opinion that the information I discuss in this "BACKGROUND" section would have been background knowledge to a POSITA.

34. MPLS was well known in the art and is described for IP networks in RFC 3031, which was published in 2001. *See e.g.,* Ex.1028, 3:26-33 ("Multiprotocol Label Switching (MPLS) for IP networks is described in RFC 3031."); Ex.1029, RFC 3031-Multiprotocol Label Switching Architecture. And, although MPLS was originally developed for IP networks, it was extended to optical networks as early as 2002. Ex.1028, 3:26-33 ("Although label switching was originally developed in TCP/IP networks to simplify access to routing table entries, the techniques of the present invention contemplate using label switching in fibre channel networks to enable features such has [sic] traffic engineering, tunneling, and in order delivery in addition to facilitating routing table access."). Such optical networks utilize Generalized MPLS, which extends MPLS to optical networks, among others. *See e.g.,* Ex.1011, 1:25-27 ("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."); Ex.1018, 1 ("GMPLS

extends MPLS to encompass time-division (e.g., SONET/SDH, PDH, G.709), wavelength (lambdas), and spatial switching (e.g., incoming port or fiber to outgoing port or fiber)"). Accordingly, a POSITA would have understood that both IP networks and optical networks utilize MPLS, and that operating principles related to these technologies are generally applicable to each other.

35. It was also well-known in the art, indeed by over 10 years before the '691 patent's filing, to use one or more backup paths to provide protection. *See* Ex.1005, [0009] ("…one or more backup paths between the ingress and egress nodes, wherein each of the backup paths is activatable upon a failure condition associated with at least one of the working path and the backup paths."); Ex.1006, Abstract ("…associating channels in each link of the node to one or more protection paths…"); Ex.1007, 1 ("[I]n an optical network is allocated a pair of link-disjoint paths, where one of the path[s] is the primary or working path and the other is [the] backup or protection path that is activated only in case of failure."); Ex.1022, 294 ("The backup LSP is built along paths that are as diverse as possible from the LSP they're protecting."); Ex.1023, 281 ("…one or more associated backup tunnels.").

36. Typically, a POSITA would have understood an LSP to be protected if it has one or more backup paths preestablished (via setup signaling) before a failure. Ex.1022, 293 ("[T]he term protection should be associated with the fact that backup resources are preestablished… The preestablishment of protection resources is

fundamental for any protection strategy. If protection resources weren't preestablished, they'd have to be set up after the failure was detected; by then, it's too late."); Ex.1011, 3:7-9 ("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."), 4:7-9 ("LSPs are established during GMPLS tunnel setup."); Ex.1018, 37 ("data paths, i.e., from initiator to terminator and terminator to initiator, are established using a single set of signaling messages.").

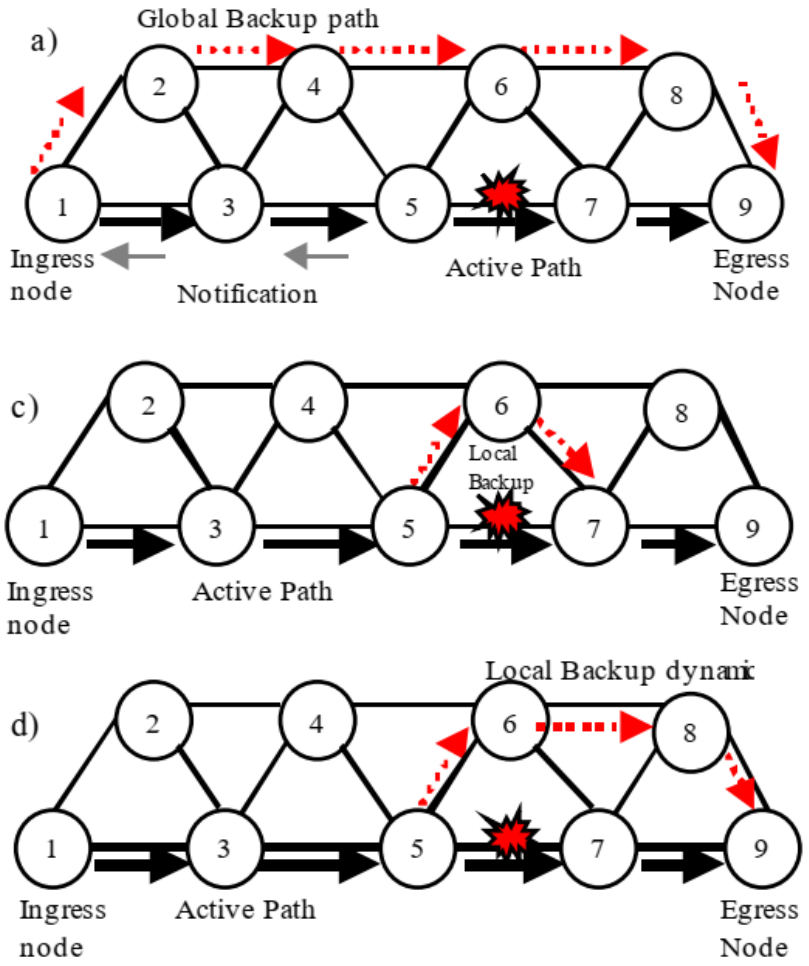
37. A POSITA would have understood that a "backup path" may be sometimes referred to by other terms, such as "protection path," "bypass path," "backup tunnel," "protection tunnel," and "bypass tunnel," all of which are substantially synonymous. *See* Ex.1022, 293 ("This chapter calls this preestablished LSP a backup tunnel or protection tunnel. They mean the same thing."), 296 ("In addition to the terms 'backup tunnel' and 'protection tunnel,' you might see the terms 'FRR tunnel' and 'bypass tunnel' being used to refer to this presignalled tunnel. They all mean the same thing."); Ex.1023, 281 ("…the backup LSPs (referred to as bypass tunnels) are established before the failure and provide local protection."); Ex.1005, [0034] ("…protection paths…backup paths…").

38. MPLS protection techniques were generally grouped into two categories: (1) "global" or "path" protection, which uses a preestablished path to protect a primary path end-to-end from source to the destination, and (2) "local"

protection, which uses one or more preestablished backup paths to protect part of a primary path (e.g., using link protection or node protection). Ex.1022, 293-295; Ex.1023, 278; *see also* Ex.1022, 295 (In local protection "the backup LSP is routed around a failed link (in link protection) or node (in node protection), and primary LSPs that would have gone through that failed link or node are instead encapsulated in the backup LSP.").

39. A node would have been understood to correspond to a network device such as a router, and a link would have been understood to correspond to a physical connection such as a wire or optical fiber. Ex.1005, [0022]-[0023] ("…optical fiber…optical links"), [0026] ("…network node…router…"); Ex.1022, 291 ("…physical resources (link or nodes)…A link failure can be a fiber cut… A node failure can be anything from a power problem to a router crash…").

40. As an example, provided below is a prior art FIG. 1(a) illustrating global protection and FIGS. (c) and (d) illustrating local protection:



Ex.1027, FIG. 1(a), (c) and (d)

41. One typical difference between the two different protection techniques is that global (or path) protection is less scalable because it requires a dedicated 1:1 relationship between the primary and the backup. Ex.1022, 294 ("With path protection, the relationship between the backup LSP and the number of primary LSPs it is protecting is 1: 1. This makes the path protection scheme less scalable."). In contrast, local protection is more scalable because it supports sharing backup paths, e.g., 1:N where a single backup LSP protects N primary LSPs. Ex.1022, 295 ("Unlike path protection, for local protection, the relationship between the backup

LSP and the number of primary LSPs it is protecting is 1:N. In other words, a single backup LSP can protect N primary LSPs, making it more scalable than path protection. This scalability makes the local protection scheme extremely attractive.").

42. Although the two protection techniques are slightly different, a POSITA would have understood that in instances where there is a single domain with few internal nodes, applying global (or path) protection and local protection may result in setting up a same backup path, which begins at the same node as the primary path. *See e.g.,* Ex.1022, 297 ("The material presented so far might give you the impression that the primary tunnel headend and the PLR have to be two distinct things. This is not necessarily true in every case, even if it is the common situation. You might have configured link protection, protecting the link between the primary tunnel headend and its downstream neighbor. In this case, the primary tunnel headend is also the PLR. Basically, the PLR is where the backup tunnel begins.").

43. One common type of MPLS-based local protection is known as Fast ReRoute ("FRR"):

> MPLS-based local protection scheme that limits packet loss in the order of tens of milliseconds during network failure is known as Fast ReRoute (FRR).

Ex.1023, 281.

> Networks fail. More precisely, pieces of networks fail. Lots of things can cause something to fail in a network. They run the gamut from loosely connected cables to fiber cuts. Router crashes are another form of failure.
>
> From a router's perspective, there are two kinds of failures in a network—link failures and node failures. It doesn't matter what the underlying cause is. A link failure can be a fiber cut, an ADM problem, or any number of other things. A node failure can be anything from a power problem to a router crash to a router being taken down for scheduled maintenance. No matter what the cause, all failures are either a link failure or a node failure.
>
> It is highly desirable to reduce the negative effects of such failures, such as packet loss. As it turns out, MPLS TE and its ability to steer traffic away from the I-GP-derived shortest path helps mitigate packet loss associated with link or node failures in the network. MPLS TE's ability to do this is known as Fast Reroute (FRR) or simply MPLS TE Protection.

Ex.1022, 291; *see also* Ex.1001, 1:16-24 ("The most common way of LSP protection is Fast Re-Route (FRR)… MPLS Fast Reroute (also called MPLS local restoration or MPLS local protection) is a local restoration network resiliency mechanism. It is a feature of RSVP Traffic Engineering (RSVP-TE)."); Ex.1019, *generally* RFC 4090 - Fast Reroute Extensions to RSVP-TE for LSP Tunnels.

44. FRR (or local protection) was recognized as providing numerous benefits, including (1) quick rerouting on to one or more preestablished backup

LSPs in case of failure, (2) limiting packet loss, (3) reducing traffic disruption during failure, among others:

> MPLS FRR provides a mechanism to set up backup label-switched paths and quickly reroute traffic from protected TE LSPs onto the backup tunnels on detection of local link and node failures. Because the backup LSPs (referred to as bypass tunnels) are established before the failure and provide local protection, MPLS FRR can reroute traffic within tens of milliseconds (see Figure 10-15 for a summary of terminology).

Ex.1023, 281.

> [A] local recovery scheme provides a backup path closest to the point of failure and thereby avoids extra delay by propagating failure notification to the upstream nodes to reroute traffic onto the backup path. Avoiding delay is highly desirable to reduce traffic disruption during failure.

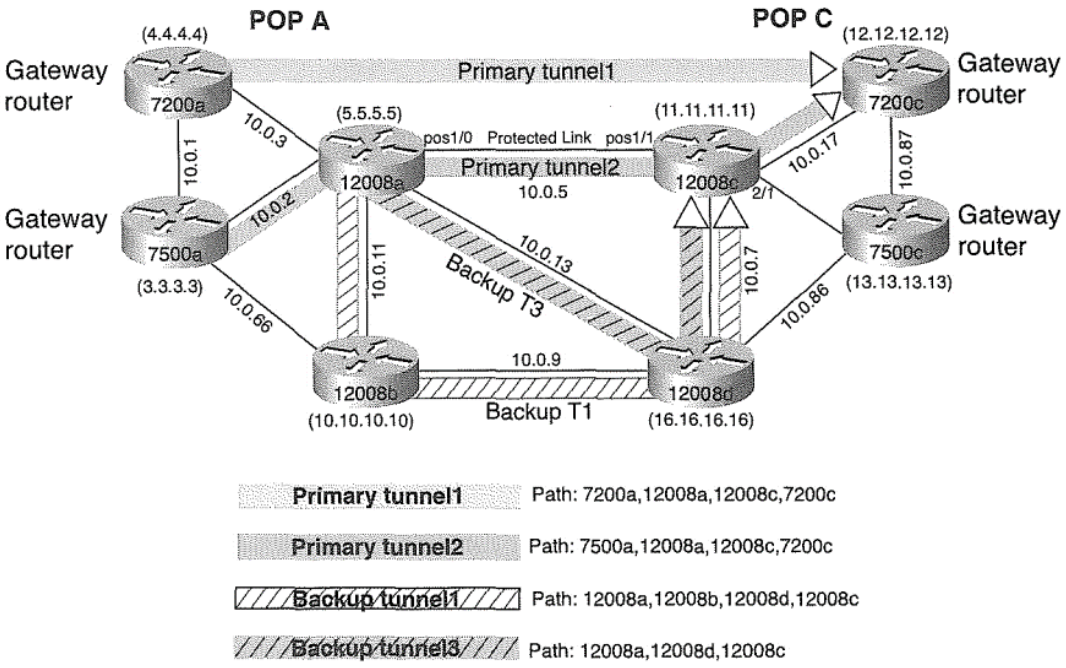
Ex.1023, 278.

> In local protection, the backup LSP is routed around a failed link (in link protection) or node (in node protection), and primary LSPs that would have gone through that failed link or node are instead encapsulated in the backup LSP. Local protection has several advantages over path protection—faster failure recovery, 1:N scalability, and the consumption of less network state, to name a few.

Ex.1022, 295; *see also id*. ("…for local protection…a single backup LSP can protect N primary LSPs, making it more scalable than path protection. This scalability makes the local protection scheme extremely attractive."); Ex.1011, 1:38-45 ("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… 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.").

45. In FFR (or local protection) the backup path begins at a node called Point of Local Repair ("PLR") and terminates at a node called Merge Point ("MP"), where the backup path rejoins the protected path. Ex.1001, 1:42-46 (a "node which redirects the traffic onto the preset Backup path is called the Point of Local Repair (PLR)…the node where a Backup LSP merges with the primary LSP is called Merge Point (MP)."); Ex.1022, 296 ("Point of Local Repair— The headend of the backup tunnel." "Merge Point—The merge point is where the backup tunnel terminates."), 297 ("Basically, the PLR is where the backup tunnel begins."). To

illustrate, below is a prior art example where two backup paths (Backup T1 and Backup T3) are provided between PLR (router 12008a) and MP (12008c):



Ex.1022, FIG. 7-17.

46. Consistent with the paragraph immediately above, it was known in the art to use multiple backup paths (which may be partially or fully disjoint) to protect from multiple failures. Ex.1005, [0008] ("…implementing a shared protection scheme under a scenario of multiple failures in a network… The backup paths may be based on link and/or node disjointedness, as well as resource-based cost constraints in an exemplary implementation."); Ex.1008, 2:6-13 ("…planning and provisioning fast, multiservice restoration from multiple failures in large-scale packet-over-optical mesh networks across multiple network layers. The method and system is based upon path protection…"); Ex.1009, 143 ("The salient feature of the

proposed approach is that it enables the paths to be dynamically selected under multiple failure occurrences in a general MPLS/GMPLS network, while satisfying the given resilience requirements."); Ex.1010, Abstract ("Fast rerouting mechanisms are being studied in order to provide fault tolerance for LSP in an MPLS network…This paper presents a mechanism that is able to handle multiple failures along an LSP…[using] at least one alternative LSP."); Ex.1012, 9:28-32 ("It is desirable that pre-planned recovery paths be fully disjoint from the working path, because they must be able to protect it from a failure occurring on any of its nodes or link[s].")

47. It was known for LSP paths to have an associated priority. Ex.1024, [0055] ("The Path message carries path feature information and an identifier indicating the LSP is a backup of the P2MP LSP; the Path message may also carry establishment priority, hold priority and protection mode (node protection or link protection, whether to allow local recovery, whether to include certain links, and whether to exclude certain links), and bandwidth requirement of the backup LSP."); Ex.1025, [0043]-[0044] ("FIG. 2 is a format of a FAST_REROUTE object used for setup of a backup LSP for fast rerouting…A Setup Priority field 200 contains a value representing priority of a backup LSP."); Ex.1026, 44 ("Each tunnel has a priority, and more-important tunnels take precedence over less-important tunnels."); Ex.1030, 6 ("A master LSP for carrying traffic and two backups LSP1, LSP2

playing a protective role exist between the LSRs of the ingress interface and the egress interface, wherein priorities are set for the master LSP, the backup LSP1, and the backup LSP2, respectively; and specifically, the master LSP is set to have the highest priority, which is set as master, and the priorities of the backup LSP1 and the backup LSP2 are set from high to low as backup 1 and backup 2.").

48. It was also known to use a backup path's priority to identify the sequence that a backup path would be used in case of failure. Ex.1026, 45 ("Enhanced path protection provides support of multiple backup path options per primary path option. You can configure up to eight backup path options for a given primary path option. Only one of the configured backup path options is actively signaled at any time. After you enter the **mpls traffic-eng path-option list** command, you can enter the backup path priority in the number argument of the **path-option** command… Priorities are configurable for each backup path option. Multiple backup path options and a single backup path option cannot coexist to protect a primary path option."); Ex.1030, 6-7 ("…the priority level of the backup LSP1 is higher than the priority level of the backup LSP2, such that the link carrying the traffic is switched from the master LSP to the backup LSP1… If an abnormality also occurs in the high-priority backup LSP1, the link carrying the traffic is switched from the master LSP to the backup LSP2, that is, according to the priorities of the backup LSP1 and the backup LSP2…").

49. Typically, computations to determine backup paths for MPLS were performed either at a central node or distributed over network nodes. Ex.1005, [0025]; Ex.1012, 12:37-13:10, FIGS. 9-10. The computations were typically performed by a processor executing program instructions implemented as functions. Ex.1008, 20:41-43 ("…computer readable medium containing a program which, when executed by a processor, performs method of provisioning a network allowing path protection…"); Ex.1011, 2:12-16 ("…a system for providing dynamic end-to-end protection in an optical network generally comprises a processor operable to create two or more paths…"); Ex.1012, 3:31-33 ("…a computer program having machine-readable instructions which when executed by a processor cause the processor to perform the method"); Ex.1013, [0060] ("The software components may include programs comprising code or instructions that are executed by processor."); Ex.1016, 95 ("Most modern languages have an ability to create named subroutines…called a function."); Ex.1014, 199 ("function…A general item for a subroutine."); Ex.1017, 37 ("The function is the heart of a [] program.").

50. The processor executing instructions typically generates a request, which was referred to in the art as a "function call," that has as input arguments or parameters needed by the function to perform the computations. *See, e.g.,* Ex.1012, 3:13-17 ("…control part being configured to request computation by sending a request to the local path computation element for computation of the new recovery

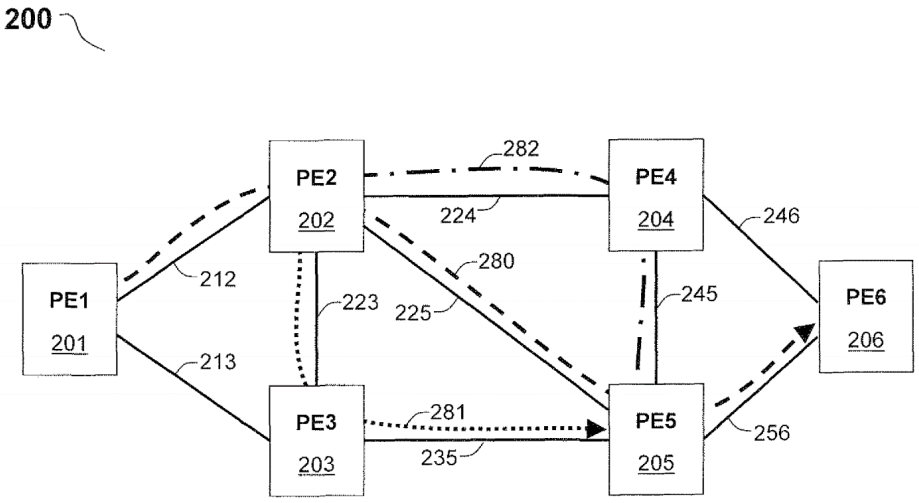
path.…"); Ex.1014, 200 ("function call…A program's request for the services of a particular function. A function call is coded as the name of the function along with any parameters needed for the function to perform its task."); Ex.1016, 96 ("[T]he argument list (which follows the name and is surrounded by parentheses) contains the types of arguments that must be passed to the function."); Ex.1017, 37 ("Function arguments are contained in parentheses following the function name. The values of the arguments are the parameters needed to execute the function."); Ex.1033, 380 ("function call A request by a program to use a subroutine…A function call written in a program states the name of the function followed by any values or parameters that have to be passed to it. When the function is called, the operation is performed, and the results are returned."). The called function typically returned a result. Ex.1016, 98 ("The return keyword exits the function block to the point right after the function call. If return has an argument, that becomes the return value of the function. You can have more than one return statement in a function."); Ex.1033, 380 ("function call A request by a program to use a subroutine…A function call written in a program states the name of the function followed by any values or parameters that have to be passed to it. When the function is called, the operation is performed, and the results are returned.").

VI. THE '691 PATENT

A. Summary of the '691 Patent

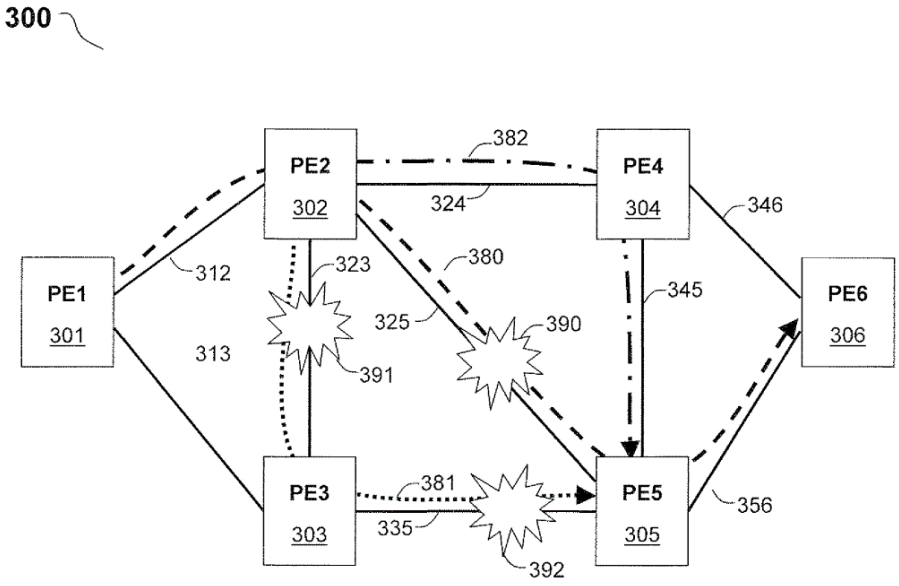
51. The '691 patent describes and claims nothing more than well-known techniques of using multiple backup paths to protect from multiple failures. The '691 patent is titled "System and Method Providing Standby Bypass for Double Failure Protection in MPLS Network." Ex.1001, Title. According to the '691 patent, although it was known in the prior art to use a backup path to protect against single faults, "[i]n the event of a scenario where an LSP is already [] protected by a Bypass LSP (FRR), and there is a second failure in the network which causes the FRR/Bypass LSP also to go down, the whole LSP would go down." Ex.1001, 1:63-67. The purported novelty of the '691 patent is that it utilizes multiple backup LSPs "to accommodate double-fault scenarios." Ex.1001, 2:1-27.

52. An example implementation is shown below at FIG. 2, where an MPLS network has three LSP paths; namely, primary LSP 280 (working path), a Bypass LSP 281 (first backup path), and additionally a Backup LSP 282 (second backup path) that provides protection in case the other paths fail. Ex.1001, 1:42-46, 5:38-46.



Ex.1001, FIG. 2. **Fig. 2**

53. The presence multiple faults 390, 391, 392, is illustrated at FIG. 3:

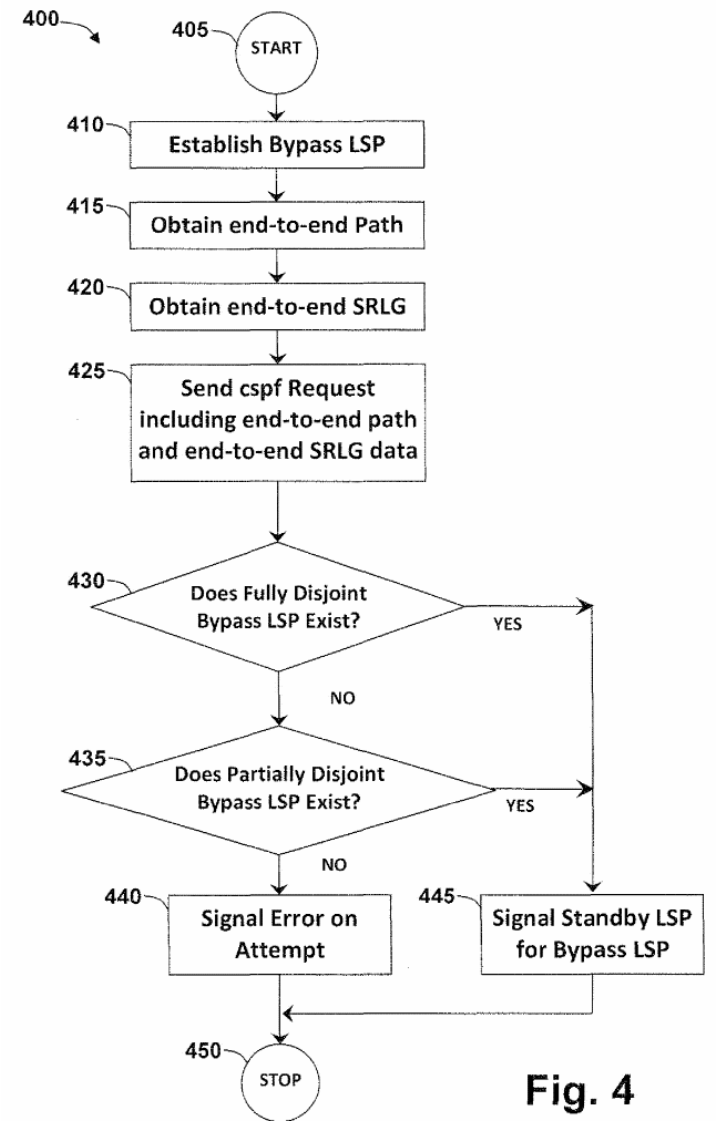


Ex.1001, FIG. 3. **Fig. 3**

54. According to the '691 patent, in the event that LSP 380 (primary path) has a fault (390) and the Bypass LSP 381 (first backup path) simultaneously also

has a fault (391, 392), the Backup LSP 382 (second backup path) provides protection. Ex.1001, 5:47-58.

55. The '691 patent's FIG. 4, reproduced below, illustrates a method for providing paths for multiple fault protection. Ex.1001, 6:4-50.



Ex.1001, FIG. 4.

56. In the above illustrated flowchart of the '691 patent, at step 410 the main Bypass LSP is established for a primary LSP. Ex.1001, 6:8-10. At step 415

and 20, an end-to-end path is obtained as well as Shared Risk Link Groups (SLRG) information. Ex.1001, 6:10-17. The obtained information is then used at step 425 to calculate a Backup LSP that is disjoint to the Bypass LSP, which also respects the associated SLRG if provided. Ex.1001, 6:17-22. If a fully disjoint path is available, at step 430, a signal is sent to the MPLS nodes along the path to setup the Backup LSP. Ex.1001, 6:23-28. If a fully disjoint path is not available, then a check is made for a partially disjoint path, at step 435, and if a partially disjoint is not available, an error signal is output at step 440.

57. Representative Claim 1 of the '691 patent is reproduced below:

> **1**. A method performed by a network processor of a Multiprotocol Label Switching (MPLS) label switch router for providing a Backup Label Switched Path (LSP) to a Bypass LSP already established for a Protected Primary LSP, the method comprising the steps of:
>
> protecting the Primary LSP against dual failures, comprising:
>
> establishing the Bypass LSP for the Protected Primary LSP having a Point of Local Repair node and a Merge Point node;
>
> obtaining the nodes traversed by an end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node;
>
> generating a request to a path calculator using the nodes traversed by said end-to-end path of said Bypass LSP for a disjoint path connecting said Point of Local Repair Node to said Merge Point node;
>
> receiving a response from said path calculator; and
>
> in response to determining that a fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP.

58. As I explain in detail below, however, there is nothing novel about the invention disclosed and claimed in the '691 patent. The arrangement in which two

LSP paths are used as backup to protect a primary LSP was already known at the time the '691 patent was filed.

B. Prosecution History

59. The '691 patent was filed September 28, 2012 and issued on March 17, 2015. In response to a rejection by the Examiner, Applicants and the Examiner amended the claims as follows:

> 1. (Currently Amended) A method performed by a network processor of a Multiprotocol Label Switching (MPLS) label switch router for providing a Backup Label Switched Path (LSP) to ~~an already established~~ a Bypass LSP already established for a Protected Primary LSP, the method comprising the steps of:
>
> protecting the Primary LSP against dual failures, comprising:
>
> establishing [[a]] the Bypass LSP for the Protected Primary LSP having a Point of Local Repair node and a Merge Point node;
>
> obtaining the nodes traversed by an end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node;
>
> generating a request to a path calculator using the nodes traversed by said end-to-end path of said Bypass LSP for a disjoint path connecting said Point of Local Repair Node to said Merge Point node;
>
> receiving a response from said path calculator; and
>
> ~~in the event that~~ in response to determining that a fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, ~~then~~ signaling, to at least one other MPLS label switch router, said fully disjoint path as [[a]] the Backup LSP to said Bypass LSP.

Ex.1002, 16-22. The Examiner appears to have allowed the claims to issue based on Applicant's argument that the amendments require that the Protected LSP,

Bypass LSP, and Backup LSP be in existence at the same time, and not calculated only upon a failure:

> The claims have been amended to clarify that the Bypass LSP is "already established for a Protected LSP," as described in the Specification at, for example, paragraphs [0001]-[0002], [0004]-[0005], [0034], and [0042], to further describe the subject matter of the invention, and emphasize that the Protected LSP and Bypass LSP are "established" at the same time as the Backup LSP. Thus it may be understood that the Bypass LSP is already established for a Protected LSP, and not calculated only upon failure of a first connection as in Canali.

Ex.1002, 41.

60. Notably, as I demonstrate below, there is nothing novel about claim 1 (or any of the other claims) of the '691 patent since the amended features, which appear to be the reason for allowance, were known in the art and it would have been obvious to combine the prior art as claimed.

VII. CLAIM CONSTRUCTION

61. It is my understanding that in order to properly evaluate the '691 patent, the terms of the claims must first be interpreted. It is my understanding that for purposes of *Inter Partes* Review, the claim terms must be construed according to their ordinary and customary meaning as would have been understood by one of ordinary skill in the art. I have also been informed that claim terms only need to be construed to the extent necessary to resolve the obviousness inquiry. It is my opinion that for purposes of applying the prior art presented herein to evaluate the patentability of the claims, no term requires express construction.

VIII. DETAILED UNPATENTABILITY ANALYSIS

62. I have been asked to provide my opinion as to whether the Challenged Claims of the ’691 patent would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references I reviewed teach the elements of the Challenged Claims of the ’691 patent.

63. As part of my analysis, I have considered the scope and content of the prior art and any potential differences between the claimed subject matter and the prior art. I conducted my analysis as of the earliest claimed priority date of the ’691 patent: September 28, 2012. I have also considered the level of ordinary skill in the pertinent art as of that date.

64. I describe in detail below the scope and content of the prior art, as well as any differences between the claimed subject matter and the prior art, on an element-by-element basis for claims 1 to 10 of the ’691 patent. This analysis supports my opinion that the differences between the Challenged Claims and the prior art discussed herein are such that the subject matter as a whole would have been obvious at the time of the filing of the ’691 patent to a person having ordinary skill in the art to which the subject matter pertains. I note that my analysis and proposed prior art combinations rely on the teachings of the references and not on physical incorporation of the elements.

65. Additionally, as part of my analysis, I have reviewed and appropriately cite to other prior art references as demonstrating knowledge in the art.

66. I will now describe, in the grounds below, on an element-by-element basis, how the prior art teaches all elements of claims 1 to 10. Unless otherwise noted, all emphasis in any quoted material has been added.

A. Ground 1: Claims 1-10 are obvious over EDC_525 in view of EDC_892 and Hanif

67. The combination of EDC_525, EDC_892, and Hanif renders obvious claims 1-10 as discussed below.

1. Summary of EDC_525

68. Like the '691 patent, U.S. Patent Publication No. 2004/021852 to Elie-Dit-Cosaque et al. ("EDC_525," Ex.1005) discloses techniques for providing multiple backup paths to protect from multiple failures in an MPLS network. Ex.1005, [0001]- [0009], Abstract, FIGS. 4, 6-9, Claims 1, 31.

69. In more detail, EDC_525 discloses a network 100 that corresponds to a "generalized multi-protocol label switched (GMPLS) optical transport network." Ex.1005, [0022], FIG. 1. A POSITA would have recognized that GMPLS is a version of MPLS designed for optical networks, among others. *See e.g.,* Ex.1011, 1:25-27 ("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."); Ex.1012, 15:43-47 ("Technologies such as Multi-

Protocol Label Switching (MPLS) and its extensions (i.e. GMPLS, T-MPLS), provide efficient TE solutions within a single domain thanks to their connection oriented nature, to minimize costs."); Ex.1018, 1 ("GMPLS extends MPLS to encompass time-division (e.g., SONET/SDH, PDH, G.709), wavelength (lambdas), and spatial switching (e.g., incoming port or fiber to outgoing port or fiber).")

70. EDC_525 discloses that a network administrator manager ("NAM") and a quality monitor ("QM") compute paths in its optical network 100 and provides that the NAM and QM "may be disposed centrally or distributed over one or more nodes." Ex.1005, [0025]; *see also* Ex.1005, [0042] ("…centralized or distributed entity…"). EDC_525 further explains that its network nodes perform routing and switching. Ex.1005, [0025]-[0026].

71. EDC_525 illustrates at FIG. 2, reproduced below, an exemplary node, responsible for control in the GMPLS network 100:

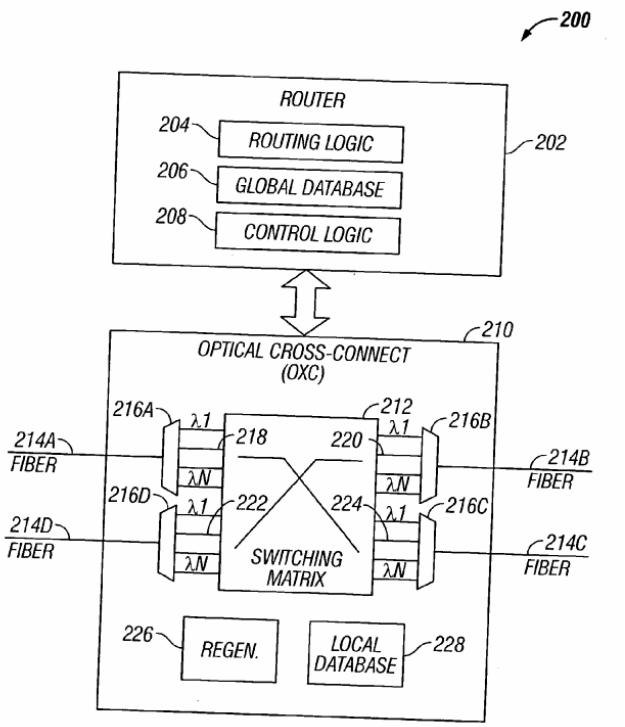


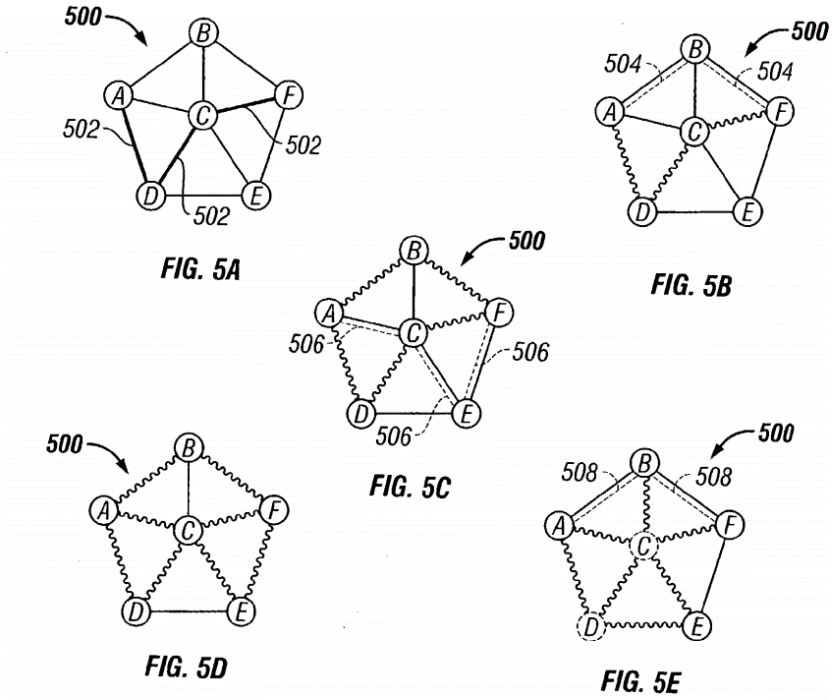
FIG. 2

Ex.1005, FIG. 2.

72. I note that almost 10 years before the '691 patents' filing date, EDC_525 recognized the problem that "protection path implementations do not address the issue of correlated multiple failures." Ex.1005, [0007]. To address this problem, EDC_525 discloses that its node (either centrally or distributed) performs path calculations and provides multiple backup paths for protection "under a scenario of multiple failures." Ex.1005, [0008]; *see also* [0025]-[0026], [0045], Abstract. EDC_525's node has "processor-accessible medium with instructions for carrying out the network operations," including "**instructions for computing a plurality of backup paths**" which are setup and can be used if there is "a failure condition associated with at least one of said working path and one of said backup

paths." Ex.1005, Claim 31; *see also* Ex.1005, [0008]-[0009], [0025]-[0026], [0031]-[0034].

73. In one example, illustrated at FIGS. 5A-5E, EDC_525 discloses computing and setting up a working path 502 and a plurality of disjoint backup paths 504 (first protection path) and 506 (second protection path) that provide protection in case of multiple failures:



Ex.1005, FIG. 5.

FIGS. 5A-5E illustrate different topological stages of an exemplary network 500 wherein multiple backup paths may be computed in accordance with the teachings of the present invention depending on link disjointedness and/or node disjointedness. Network 500 comprises five nodes, A through F, wherein an **exemplary working path** from Node A to Node F is identified as Path {A,D,C,F}, denoted by

> **reference numeral 502**… After removing the exemplary working path 502 from the network topology (i.e., links AD, DC and CF are shown in wavy lines), a **first protection path** is computed using any known algorithm. For purposes of illustration, a **protection path 504** is shown in a dashed line between the source node (Node A) and the destination node (Node F), using links AB and BF. Thereafter, if the requested connection session between nodes A and F warranted more than one backup, **another iteration of a protection path computation takes place**. As shown in FIG. 5C, links AB and BF are also removed from the network topology for this calculation (i.e., AB and BF links are shown in wavy lines). **A second protection path** between Node A and Node F is computed, again using any known or heretofore unknown algorithm, after removing all previously calculated links from the topological graph. Reference numeral **506 refers to the exemplary second protection path** comprising links AC and CF.

Ex.1005, [0032], FIGS. 5A, 5B. EDC_525 explains that FIGS. 5A-5E are merely "exemplary." Ex.1005, [0032]; *see also* Ex.1005, [0045] ("While the exemplary embodiments of the invention shown and described have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present invention."). EDC_525's instructions for computing uses "network topology" information from a global database to compute backup paths that are completely or partially disjoint. Ex.1005, [0026]-[0032]. After the working and at least one backup path is computed, "**appropriate setup and/or activation**

messages" are transmitted to the other nodes. Ex.1005, [0031]; *see also* Ex.1005, [0008], FIG. 4.

74. As a further improvement, EDC_525 discloses that during operation, one or more backup paths may be dynamically computed (using a previously disclosed suitable backup path technique) if a quality parameter is below a certain threshold or based on a defined Shared Risk Link Group (SRLG) that is predictive of correlated failures:

> **As a further improvement, the multiple backup path computation schemes set forth above may be provided with the capability so as to be dynamically invoked based on network quality**, which in turn may depend upon spatial and/or temporal correlation(s) of failures, e.g., a link or nodal degradation event. For instance, a centralized or distributed entity (e.g., QM 110 associated with administrator node 106 shown in FIG. 1) may continuously or periodically or otherwise monitor the quality of network components and upon occurrence of a particular condition, **a suitable multiple backup path technique may be activated to compute one or more backup paths**…For instance, a link could be given a rating with respect to an appropriate quality variable that is parameterized between 1 and 10. If the signal quality through that link is degraded or otherwise affected, or **if the quality parameter is below a certain threshold**, that condition exemplifies a "degradation event" in the network……In one embodiment, a timer may be started with a duration in the order of a minute and all the subsequent degradations occurring on other links during the same time

> window may be used for **defining a Shared Risk Link Group (SRLG)**. In other words, links that exhibit simultaneous degradation are more likely to fail at about the same time; which can help in early detection of multiple failures. **To reduce the possibility of multiple failures, however, two links belonging to the same SRLG are not used for the same lightpath connection (i.e., spatial diversification).** Once a degradation correlation profile is determined, an appropriate multiple backup path computation scheme (e.g., the complete link disjoint methodology) may be used to compute a predetermined number of backup paths based on failure prediction.

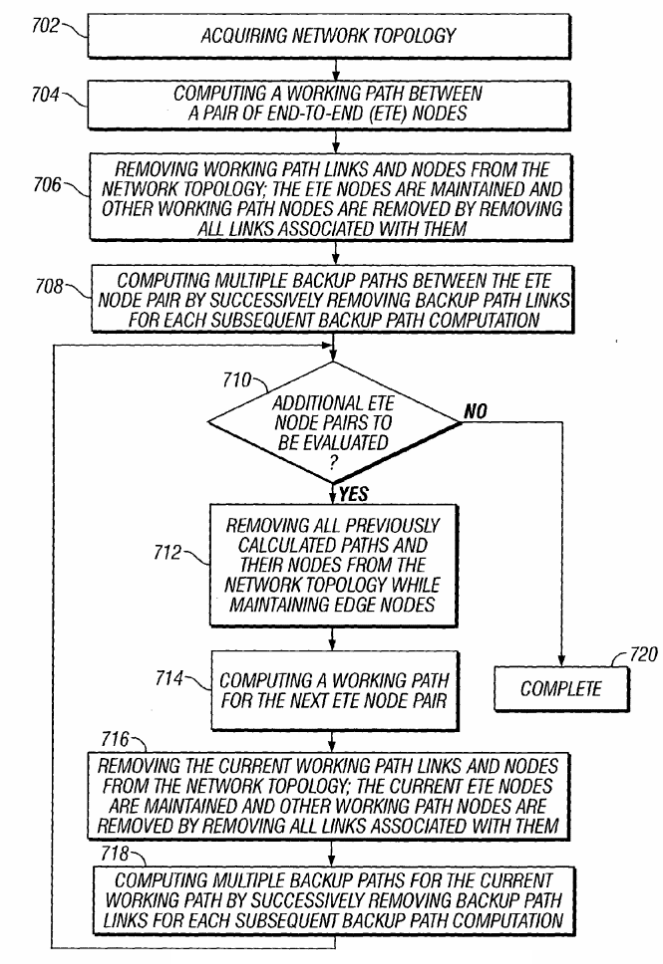
Ex.1005, [0042], Fig. 10; *see also* Ex.1005, [0008], [0025], [0026], Claim 27.

75. EDC_525 provides numerous path computation examples. *See* Ex.1005, FIGS. 4, 6-10 and corresponding text. As one example, EDC_525 at FIG. 7 discloses that the path calculator determines whether a completely (link and node) disjoint backup path is available from an ingress node to an egress node:

> In another embodiment, path computations may be predicated upon treating both links as well as nodes as completely disjoint. **FIG. 7 is a flow chart of an embodiment of a method of the present invention for computing multiple backup paths where the links and nodes are completely disjoint**. Similar to the process set forth above, a network topology is acquired first by an ingress node of an ETE pair (step 702). Again, all links in the network topology may be attributed the same cost using an appropriate metric. A working path is computed thereafter pursuant to a connection request between the ingress and egress nodes of the ETE pair (step 704). Both working path links and working path

> nodes are then logically removed from the network topology (Step 706) so as to ensure that they are not reused for subsequent paths. As explained before, a path node is removed by removing all the links connected to it. Clearly, the source and destination nodes are not removed from these computations. Subsequently, one or more backup paths between the ETE nodes may then be calculated in a similar fashion until the requisite number of paths are computed or the resultant topology does not sustain any more backups (step 708).

Ex.1005, [0037]-[0038]; *see also* Ex.1005, Claim 21 ("[W]herein said backup paths comprise paths that are completely node disjointed with respect to one another.").



Ex.1005, FIG. 7.

76. A POSITA would have understood that the EDC_525's backup path computations, which are invoked dynamically and use a previously disclosed "suitable multiple backup path technique," may correspond to the path computations where the computed backup paths are completely link-disjoint as well as node-disjoint. *See* Ex.1005, [0042] ("To reduce the possibility of multiple failures, however, two links belonging to the same SRLG are not used for the same lightpath connection (i.e., spatial diversification).").

2. Summary of EDC_892

77. U.S. Patent Publication No. 2004/0246892 to Elie-Dit-Cosaque et al. ("EDC_892," Ex.1006) is titled "Informed Dynamic Path Protection For Optical Networks," and likewise generally pertains to setting up protection paths. Ex.1006, Abstract ("Protection paths are dynamically allocated….").

78. I note that EDC_525 cites to and incorporates by reference the disclosure of EDC_892:

> The working path may be calculated using a number of various well-known techniques. An exemplary embodiment is provided in the following co-pending commonly owned U.S. patent application entitled "Informed Dynamic Path Protection For Optical Networks," filed Nov. 29, 2001, application Ser. No. 09/998,362, cross-referenced herein above and incorporated by herein…Again, additional details concerning message transmission and wavelength assignment process

> may be found in the cross-referenced U.S. patent application identified above.

Ex.1005, [0031]. As such, a POSITA would have understood that EDC_892 provides additional disclosure that is relevant when implementing EDC_525.

79. EDC_525 discloses the use of a global database (also referred to as global allocation database) and the use of "protection messages" for updating the global allocation database of each node. Ex.1005, [0028]-[0031]. EDC_892 provides additional teachings, explaining that the "protection message" may be a setup message with a field that identifies the connection as used for protection and with a field that identifies the working path that needs the protection:

> Protection messages for updating the global allocation database 26 are received by the nodes 12 using LDP (Label Distribution Protocol) messages. The protection messages may be the same as those used for reservation of a working path, with the addition of two fields: (1) a Type field that indicates whether the connection is for a protection path (Type field set to "1") or a working path (Type field set to "0") and (2) a Working Path field that identifies the working path that needs the protection. The protection message may be either a SETUP or RELEASE message.

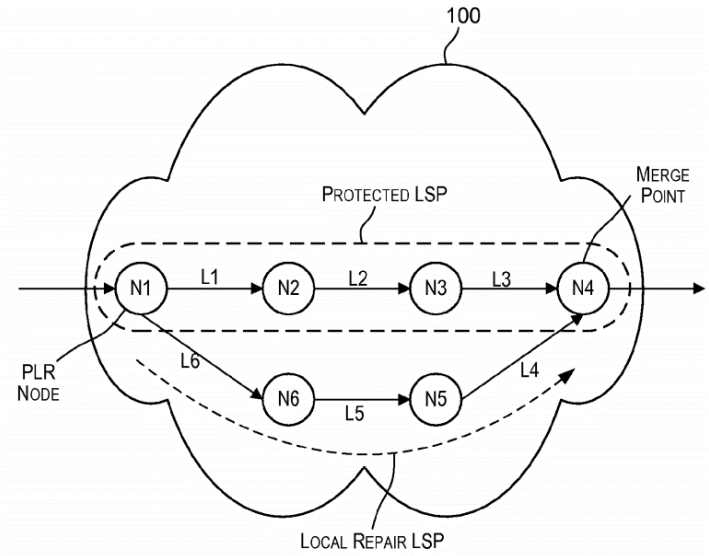
Ex.1006, [0033]; *see also* Ex.1006, [0036] ("The setup packet for said protection path includes the associated working path.")

80. Additionally, EDC_892 provides teachings relevant to computing of backup paths. *See e.g.,* Ex.1006, [0020]-[0040], FIGS. 2-4.

3. Summary of Hanif

81. U.S. Patent Publication No. 2009/0292943 to Hanif et al. ("Hanif," Ex.1013) is titled "Techniques for Determining Local Repair Connections." Ex.1013, Title. Like the '691 patent, generally pertains to "local repair connection for protected connections in a network environment." Ex.1013, [0002], Abstract.

82. Hanif's MPLS network is illustrated at FIG. 1, reproduced below:



Ex.1013, FIG. 1.

FIG.1 is a simplified diagram of a network 100 that may incorporate an embodiment of the present invention. Network 100 may use a connection-oriented protocol for data transmission. As previously described, in a network using a connection-oriented protocol, a connection is set up between two endpoints in the network prior to data transmission using that connection. Network devices at the end points of a connection use a preliminary protocol to establish an end-to-end connection before any data is sent. The connection has an associated

> path between the two end points comprising multiple nodes and links between the nodes. The preconfigured connection is then used to transport data between the end points. Examples of connection-oriented mechanisms include circuit switching protocols such as Asynchronous Transfer Mode (ATM) protocol, frame relay, Multi-Protocol Label Switching (MPLS), and others.

Ex.1013, [0028], FIG. 1.

83. Hanif's MPLS network includes an ingress point of local repair node N1 ("PLR NODE") and an egress node N4 ("MERGE POINT") where the protected LSP merges with the local repair LSP:

> In the example depicted in FIG.1, an LSP may be configured between nodes N1 and N4 having a path Nl-L1-N2-L2-N3-L3-N4. The path may be configured using an algorithm such as the CSPF algorithm and satisfy one or more constraints such as bandwidth, cost, and the like. The LSP comprises a list of node/link pairs from originating or ingress node N1 to the destination or egress node N4. The LSP carries data traffic from ingress node N1 to egress node N4 via link L1, LSRN2, link L2, LSRN3, and link L3. Once an LSP has been set up, the LSP is used to transmit data from the ingress node to the egress node (in FIG.1 from N1 to N4) along the preconfigured path. The egress node may then transmit the data to another device or network.

Ex.1013, [0032].

> Referring to FIG.1, the LSP from node N1to node N4 and having an OPATH N1-L1-N2-L2-N3-L3-N4 may be designated as a protected LSP and one or more local repair LSPs (which may be detour or backup

> LSPs) may be configured for the protected LSP. For example, a local repair LSP may be set up to protect node N2 in the OPATH. The LPATH for such a local repair LSP may start at node N1 and merge with the OPATH at node N3 or node N4. As depicted in FIG. 1, one such local repair LSP may be established having an associated LPATH N1-L6-N6-L5-N5-L4-N4, where node N1 is the PLR and node N4 is the merge point node where the local repair LSP rejoins the protected LSP. In one embodiment, processing to establish a local repair LSP may be performed or initiated by the PLR node.

Ex.1013, [0037].

84. Hanif further teaches that the network node may be a router that includes memory for storing network topology information and one or more processors that executes software to perform the various functions, including determining local repair LSPs based on the network topology information:

> FIG. 4 is a simplified block diagram of a network node 400 that may perform processing to set up and optimize local repair LSPs according to an embodiment of the present invention. Node 400 may be embodied as a network device such as a switch or router.

Ex.1013, [0066].

> Local repair LSP module 406 may comprise hardware components, software components, or combinations thereof. The hardware components may include ASICs, FPGAs, circuitry, and the like. The software components may include code or instructions that are

> executed by processor 408 or by processor within module 406. In one embodiment, module 406 may be part of module 404.

Ex.1013, [0072].

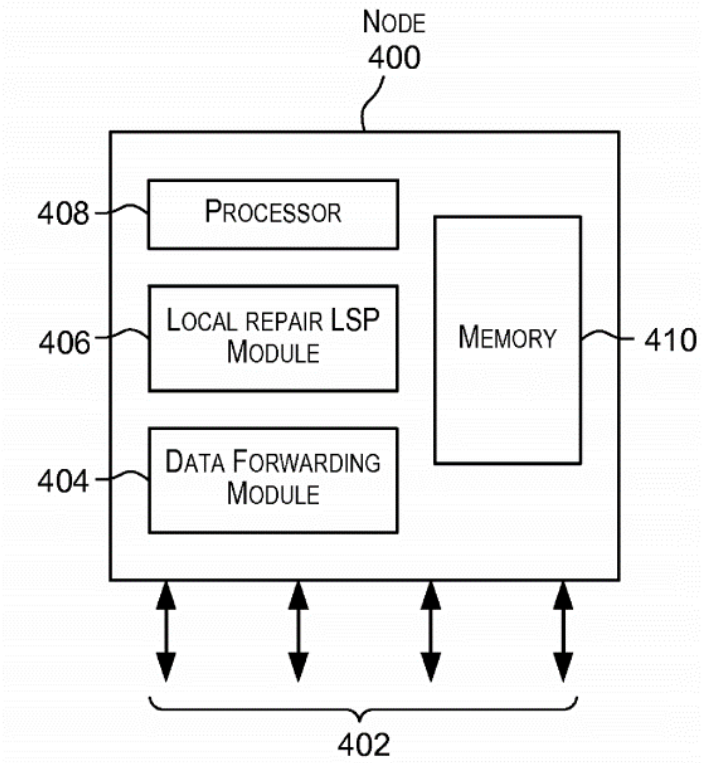
> Processor 408 is configured to perform processing for tasks performed by node 400. Processor 408 may execute software programs comprising code and instructions to perform the tasks. Processor 408 may also aid modules 406 and 404 in functions performed by those modules. In one embodiment, processor 408 may be configured to perform the functions performed by modules 404 and 406 such as data forwarding, creation of local repair LSPs, optimization of LPATHs, and the like.

Ex.1013, [0073]; *see also* Ex.1013, [0069] ("The software components may include programs comprising code or instructions that are executed by processor 408 or by a processor within data forwarding module 404.").

> Memory 410 acts as a repository for storing data that is used by node 400. For example, memory 410 may store information related to various LSPs. Memory 410 may also stored [sic] network topology information that is used for determining local paths associated with local repair LSPs. For example, information regarding various connections and associated OPATHs may be stored in memory 410. Information related to local repair LSPs may also be stored in memory 410. Memory 410 may also store programs comprising software code or instructions that are executed by processor 408 and/or by the other modules of node 400. For example, code or instructions which when executed by a processor cause the processor (or modules 404 and 406)

to determine local repair LSPs and optimize local paths, as described above, may be stored in memory 410.

Ex.1013, [0074].



Ex.1013, FIG. 4.

85. Hanif also teaches to output an error in instances where a local repair LSP cannot be established for a protected LSP:

A check is then made to see if node N is the egress node or endpoint node for the protected LSP (step 222). If it is determined in 222 that node N is the egress node for the protected LSP, then it implies that all the nodes in the OPATH downstream from the PLR have been considered for merge points for the local repair path and that a local repair path could not be found to any of the OPATH nodes downstream

> from the PLR. An error condition may then be output indicating that a local repair LSP could not be established for the protected LSP (step 224).

Ex.1013, [0050].

4. Reasons to Combine EDC_892 with EDC_525

a. ***EDC_525 and EDC_892 are Analogous Art***

86. EDC_525 and EDC_892 are both analogous art because they pertain to computer networks that use backup paths, like the '691 patent. Ex.1001, 1:6-10, Abstract; Ex.1005, [0001]- [0009], Abstract, FIGS. 4, 6-9, Claims 1, 31; Ex.1006, [0031], Abstract. Additionally, both EDC_525 and EDC_892, like the '691 patent, address the additional problems of using network topology information, SRLG information, or shortest path first information to calculate backup paths. Ex.1001, 2:10-13, 3:1-25; Ex.1005, [0022], [0026]-[0030], [0042], Claim 32; Ex.1006, [0012], [0025]-[0033], [0038], [0047].

b. ***Motivation to combine EDC_892 with EDC_525***

87. A POSITA would have considered and combined the teachings of EDC_892 with EDC_525 because EDC_525 suggests the combination by expressly citing to EDC_892 and incorporating it by reference. Ex.1005, [0031].

88. EDC_525 discloses that once backup path computations are completed, appropriate setup and/or activation messages are transmitted from the nodes along the path in the network. Ex.1005, [0031]. Consistent with EDC_525's

disclosure (see Ex.1005, [0030]), EDC_892 teaches that a "SETUP" message (1) indicates that the connection is for a protection path and (2) identifies the working path that needs the protection path. Ex.1006, [0033].

89. It would have been obvious to a POSITA to include in EDC_525's setup message an indication that the computed connection is used for protection and also identify the working path that needs the protection, per EDC_892, because such information would be useful for updating the receiving node's global database. *See* Ex.1005, [0028] ("…global database 206 includes information for determining the existence of links having channels currently used for protection paths…"), [0030] ("Information regarding other links in the global allocation database may be compiled from allocation information provided by other nodes in the network domain."); Ex.1006, [0033] ("…messages for updating the global allocation database 26 are received by the nodes…").

90. The proposed combination of EDC_892 with EDC_525 is nothing more than combining prior art elements (e.g., a setup message that specifically identifies the working path that is protected by a given backup path, per EDC_892, with EDC_525's setup messages) according to known methods to yield predictable results (e.g., providing information for updating a node's global database).

c. *Reasonable expectation of success*

91. The results would have been predictable and there would have been a reasonable expectation of success since EDC_525 incorporates the noted teachings of EDC_892 into its own specification and given the similarities of the two references. Additionally, a POSITA would have known how to use well-known software, hardware, and signaling techniques to implement the proposed combination.

5. Reasons to Combine Hanif with EDC_525

a. *Hanif is Analogous Art*

92. Hanif discloses providing a backup path (referred to as a local repair LSP) for a protected path in an MPLS network and is therefore analogous art to the '691 patent which likewise pertains to providing backup paths in an MPLS network. Ex.1001, 1:6-10, Abstract; Ex.1013, [0002], [0012], [0028], Abstract. Additionally, like the '691 patent, Hanif addresses the problem of using a processor to perform a method for providing the backup path in the MPLS network. Ex.1001, 2:14-28, 6:4-50, FIG. 4; Ex.1013, [0015], [0066]-[0067], [0069], [0072], [0074], FIG. 4.

b. *Motivation to combine Hanif with EDC_525*

93. A POSITA would have been motivated to combine the teachings of Hanif and EDC_525 (as modified in view of EDC '829) to produce numerous predictable and beneficial results.

i. a network processor of a Multiprotocol Label Switching (MPLS) label switch router

94. EDC_525 discloses that its network node has "processor-accessible medium having a plurality of instructions for carrying out network operations." Ex.1005, Claim 31. EDC_525, however, provides limited details regarding how the instructions on the processor-accessible medium are used to carry out the network operations. It was well-known in the art—indeed conventional—for the instructions to be executed by a processor. Ex.1008, 20:41-43 "…computer readable medium containing a program which, when executed by a processor, performs method of provisioning a network allowing path protection…"); Ex.1011, 2:12-15 ("…a system for providing dynamic end-to-end protection in an optical network generally comprises a processor operable to create two or more paths…"); Ex.1012, 3:31-33 ("…a computer program having machine-readable instructions which when executed by a processor cause the processor to perform the method").

95. Hanif discloses that instructions, like those disclosed by EDC_525, are "executed by [a] processor." Ex.1013, [0074]; *see also* Ex.1013, [0060],[0073]. It would have been obvious to a POSITA to consider and apply the teachings of Hanif, when implementing EDC_525's network node and execute the instructions stored on the processor-accessible medium to achieve the results that EDC_525 is already describing; namely, utilizing the instructions to carry out network operations.

96. The combination of Hanif with EDC_525 merely represents a simple combination of known elements (e.g., Hanif's processor that executes instructions with EDC_525's network node that includes instructions accessible by a processor) to yield predictable results (e.g., enabling EDC_525's network node to execute the instructions to carry out network operations).

ii. *a Point of Local Repair node and a Merge Point node*

97. EDC_525 discloses that its optical network has "a working path between an ingress node and an egress node." Ex.1005, [0008]. EDC_525 also contemplates that other devices may be connected before the ingress node and beyond the egress node, as illustrated at FIG. 1.

98. It was recognized in the art as important for repair to be localized within a network because local repair allows for addressing failures more quickly, efficiently, and avoiding or reducing effects of failures on other adjacent networks. Ex.1011, 1:38-45 ("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… 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.").

99. To that end, Hanif discloses local protection where an ingress node is implemented as a point of local repair and an egress node is implemented as a merge point where the protected path and the repair path merge. Ex.1013, [0007] ("Each local repair connection originates at a start node in the original connection and ends at a node in the original connection that is downstream from the start node. A local repair connection enables data traffic to be rerouted or diverted around a network failure point in the original connection."); *see also* Ex.1013, [0002]-[0009], [0012], [0035]-[0039], [0060]-[0062], Claim 2, Claim 20, FIGS. 1, 2, 3.

100. It would have been obvious to a POSITA to consider and apply Hanif's local repair teachings, when implementing EDC_525's teachings such that the ingress node is a point of local repair and the egress node is a merge point, to facilitate repairing a failed path quickly and efficiently and to avoid or reduce effects of failures to other adjacent networks. The above noted benefits, separately and together would have motivated a POSITA to make the proposed combination.

101. The proposed combination merely represents the application of a known technique (e.g., Hanif's technique of implementing the ingress node as point of local repair and an egress node as a merge point, to EDC_525's ingress and

egress nodes) to yield predictable and beneficial results (e.g., quickly and efficiently repair failures and avoid or reduce effects of failures on other adjacent networks, among other benefits).

c. *Reasonable expectation of success*

102. I note that the results would have been predictable and there would have been a reasonable expectation of success in the combination given the similarities in EDC_525 and Hanif, as analyzed above in prior art summary section. Also, the results would have been predictable and there would have been a reasonable expectation of success in the combination since processors were components well-known in the art and specifically designed to execute EDC_525's instructions. Moreover, there would have been a reasonable expectation of success in implementing EDC_525's ingress node and egress nodes as a local repair node and a merge node, respectively, as evidenced by Hanif itself and because local repair was well known. *See* Ex.0013, [0007]-[0008] (explaining that local repair connections were known and that RFC 4090 describes various techniques); Ex.1009, 2 ("The protection mechanism has generally been found to be effective in coping with local link failures at lower layers of the MPLS/GMPLS hierarchy."). Accordingly, a POSITA would have possessed the skills required to make the proposed combination with a reasonable expectation of success.

103. Additional analysis supporting the obviousness of the combination of EDC_525, EDC_892, and Hanif is provided in the detailed claim analysis below.

6. Claim 1

a. [1.0.1] *A method performed by a network processor of a Multiprotocol Label Switching (MPLS) label switch router*

104. To the extent limiting, EDC_525 alone and in combination with EDC_892 and Hanif renders obvious the preamble.

105. **First**, EDC_525 discloses a "*method*," by teaching a "**method** for implementing a shared protection scheme under a scenario of multiple failures in a network." Ex.1005, [0008]; *see also* Ex.1005, FIGS. 4, 6-9, Claims 1, 31. Additionally, EDC_525 expressly refers to the teachings of EDC_892 by its application number (09/998,362) and incorporates EDC_892's contents by reference. *See e.g.,* Ex.1005, [0031]. EDC_892 also discloses "**a method** and apparatus for providing shared path protection." Ex.1006, [0004]; *see also* [0009], Claim 1. It would have been obvious to a POSITA considering EDC_525 to also refer to and apply EDC_892's teachings because EDC_525 expressly directs and encourages this. *See also* Reasons to Combine EDC_892 with EDC_525.

106. EDC_525 renders obvious that its method is "*performed by a network processor of a Multiprotocol Label Switching (MPLS) label switch router*."

EDC_525's method is implemented in the context of a "generalized multi-protocol label switched (GMPLS) optical transport network," illustrated below at FIG. 1:

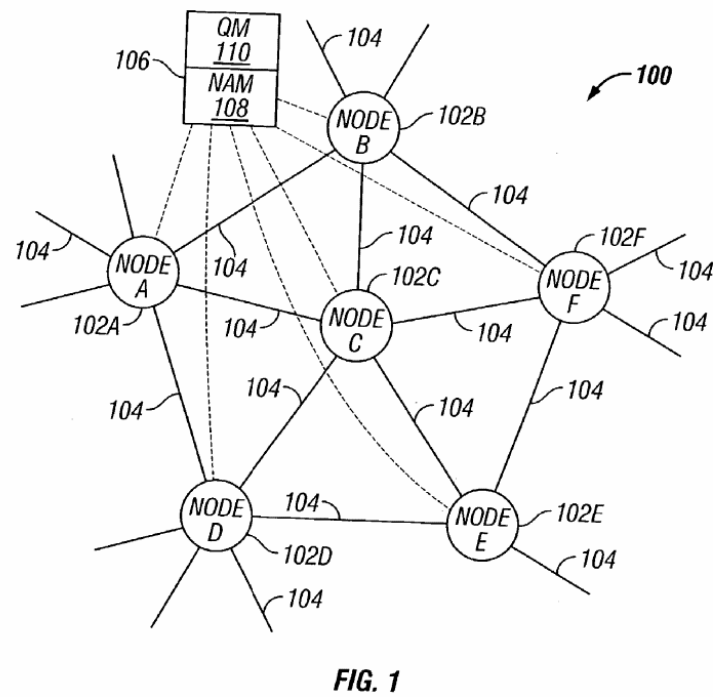


FIG. 1

Ex.1005, FIG. 1.

> The optical transport network 100, which may be implemented as a **generalized multi-protocol label switched (GMPLS)** optical transport network, includes a plurality of nodes or network elements 102A through 102F coupled by optical links 104. An optical link 104 is effectuated as a fiber carrying information between two nodes; for example, between Node A102A and Node D 102D.

Ex.1005, [0022], FIG. 1.

107. A POSITA would have recognized that GMPLS is a version of MPLS designed for optical networks, among others. *See e.g.,* Ex.1011, 1:25-27 ("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."); Ex.1018, 1 ("GMPLS extends MPLS to encompass time-division (e.g., SONET/SDH, PDH, G.709), wavelength (lambdas), and spatial switching (e.g., incoming port or fiber to outgoing port or fiber)").

108. Accordingly, EDC_525's GMPLS network renders obvious "*Multiprotocol Label Switching (MPLS)*" as recited in the preamble.

109. EDC_525 discloses a *"label switch router*" by teaching that the GMPLS network includes a network administrator manager ("NAM") and a quality monitor ("QM") that compute paths and that these elements "may be disposed centrally or distributed over one or more nodes." Ex.1005, [0025]; *see also* Ex.1005, [0042] ("…centralized or distributed entity…"). EDC_525's network node includes a "routing part…routing protocol logic…and control logic" that performs routing, switching with optical cross-connect ("OXC"), and also "controls signaling in the network.":

> **FIG. 2 depicts a block diagram of an embodiment of an exemplary optical network node 200. A routing part 202 including routing protocol logic 202, a global database 206 and control logic 208**, is coupled to an **optical cross connect (OXC) module 210 which includes a switching matrix 212** disposed between one or more input demultiplexers (DEMUXes) and one or more output DEMUXes. **In general operation, router 202 is responsible for control signaling in the network in which the node 200 is disposed**, e.g., the optical

> transport network 100 shown in FIG. 1, using appropriate routing logic 204.
>
> The OXC module 210 is responsible for passing information from a channel on an incoming fiber to a channel on an outgoing fiber using the switching matrix 212. By way of example, two incoming fibers 214A and 214D and two outgoing fibers 214B and 214C are shown. Reference numerals 216A and 216D refer to a pair of DEMUXes operable to separate the incoming channels 218 and 222 (w through WN) associated with the incoming fiber 214A and 214D, respectively, before being passed to the switching matrix 212. The switching matric [sic] 212 passes each incoming channel to an outgoing channel 220 as may be defined by a local database 228. A pair of MUXes 216B and 214C operate to multiplex the outgoing channels 220 and 224 for transmission onto fibers 214B and 214C respectively.

Ex.1005, [0026]-[0027], FIGS. 1, 2. An exemplary routing network node 200 is illustrated below at FIG. 2:

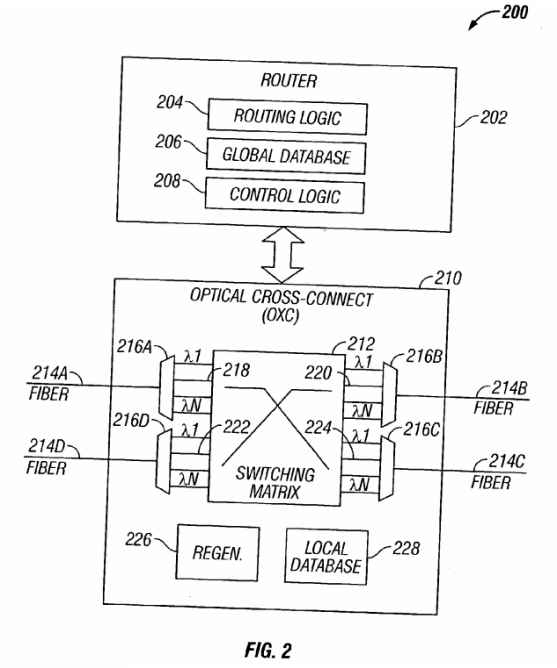


FIG. 2

Ex.1005, FIG. 2.

110. EDC_525's GMPLS network node, including its router and switching functionality, renders obvious a *"label switch router.*"

111. EDC_525 renders obvious a *"network processor*" by teaching that its network node has "processor" accessible medium and a "control structure" that may be embodied in hardware and software:

> A network element disposed as an ingress node in an optical network formed from a plurality of nodes that are inter-coupled via optical communication links, said ingress node including a **processor**-accessible medium having a plurality of instructions for carrying out network operations.

Ex.1005, Claim 31.

> In another aspect, the present invention is directed to a system for providing protection in a communications network including a plurality

> of nodes coupled by communication links. A structure is provided for computing a working path between a [sic] ingress node and an egress node responsive to a connection request received by the ingress node. Another structure is included for computing one or more backup paths between the ingress and egress nodes, wherein each of the backup paths is activatable upon a failure condition associated with at least one of the working path and the backup paths. A **control structure** is responsible for transmitting messages to nodes in the network for setting up the working path and backup paths. By way of implementation, these structures may be **embodied in software, hardware, or any combination thereof, and may be associated with a network node** or distributed in the network.

Ex.1005, [0009]; *see also* Ex.1005, [0025]-[0026], [0031], [0042].

112. A POSITA would have found it obvious to implement the control structure in hardware with a "*processor*" because EDC'525 describes a "processor-accessible medium" with executable "instructions for carrying out network operations." *See e.g.,* Ex.1005, claim 31. Such an implementation would have been consistent with well-known and commonly utilized techniques in the art. Ex.1008, 20:41-43 ("…computer readable medium containing a program which, when executed by a processor, performs method of provisioning a network allowing path protection…"); Ex.1011, 2:12-15 ("…a system for providing dynamic end-to-end protection in an optical network generally comprises a processor operable to create two or more paths…"); Ex.1012, 3:31-33 ("…a computer program having machine-

readable instructions which when executed by a processor cause the processor to perform the method").

113. Second, to the extent argued that "*a network processor of a Multiprotocol Label Switching (MPLS) label switch router*" is not expressly disclosed by EDC_892 and EDC_525, the further combination with Hanif renders it obvious.

114. Hanif discloses that a method to setup local repair paths is performed by a node "**embodied as a network device such as a switch or router" in a "Multi-Protocol Label Switching (MPLS)" network**. Ex.1013, [0028]-[0030], [0040], [0066]. The node utilizes a "**processor 408 or [] processor within module 406**" to perform network operations, such as determining paths and forwarding packets, among other network operations. Ex.1013, [0015], [0039]-[0061]-[0069], [0072], [0074], FIG. 4. Forwarding is performed by "switching fabric" using a "label switching protocol." Ex.1013, [0004], [0015], [0069], Claim 3. Hanif's processor 408 and the processor within module 406 of the node, separately and together, render obvious "*a network processor of a Multiprotocol Label Switching (MPLS) label switch router.*"

115. It would have been obvious to a POSITA to apply Hanif's teachings to EDC_525 and implement the control structure hardware of each network node with a processor, because a processor is specifically designed to access EDC_525's

"processor-accessible medium" and execute the stored "instructions for carrying out the network operations." Ex.1005, Claim 31 ("processor-accessible medium having a plurality of instructions for carrying out the network operations…"), [0009] ("… may be embodied in software…"); Ex.1013, [0069] ("The software components may include programs comprising code or instructions that are executed by processor."), [0072] ("The software components may include code or instructions that are executed by [a] processor."). A POSITA would have recognized that using a processor to execute the instructions to carry out the network operations would facilitate the computations of multiple backup paths and other network operations, thereby furthering EDC_525's objectives. *See e.g.,* Ex.1005, [0034]; *see also* Reasons to Combine Hanif with EDC_525.

116. Moreover, to the extent that Patent Owner argues that the optical networks that utilize GMPLS are outside the scope of the '691 patent, a POSITA would have recognized that the disclosure of EDC_525 and EDC_892 is relevant to other types of networks; they are not limited to optical networks. Ex.1005, [0003] ("The present invention generally relates to telecommunications and data communications networks."), [0045] ("various changes and modifications could be made therein without departing from the scope of the present invention as set forth in the following claims."), claim 1 (not reciting any optical limitation). That is, a POSITA would have recognized that the combined teachings are applicable when

implementing IP networks that utilize MPLS, as disclosed by Hanif. Accordingly, it would have been obvious to a POSITA to apply the combined teachings of EDC_525, EDC_892, and Hanif when implementing IP networks that utilize MPLS to obtain the predictable results of using local protection (per Hanif) while addressing multiple simultaneous network failures (per EDC_525 and EDC_892).

117. Thus, EDC_525 alone and in combination with EDC_892 and Hanif discloses a method performed by a network processor of a MPLS label switch node (e.g., implemented as a router), which renders obvious "*[a] method performed by a network processor of a Multiprotocol Label Switching (MPLS) label switch router,"* as recited.

b. [1.0.2] *for providing a Backup Label Switched Path (LSP) to a Bypass LSP already established for a Protected Primary LSP, the method comprising the steps of:*

118. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious the remaining elements recited in the preamble.

119. **First**, EDC_525 discloses "*a Bypass LSP already established for a Protected Primary LSP*." EDC_525 teaches that its "method commences by computing a working path between an ingress node and an egress node." Ex.1005, [0008]; *see also* Ex.1005, [0009], [0031]. EDC_525 further teaches that a "first

protection path[1] is computed using any known algorithm" and that the first protection path provides protection for the working path. Ex.1005, [0032]-[0034]; *see also* analysis at element [1.1], *infra*.

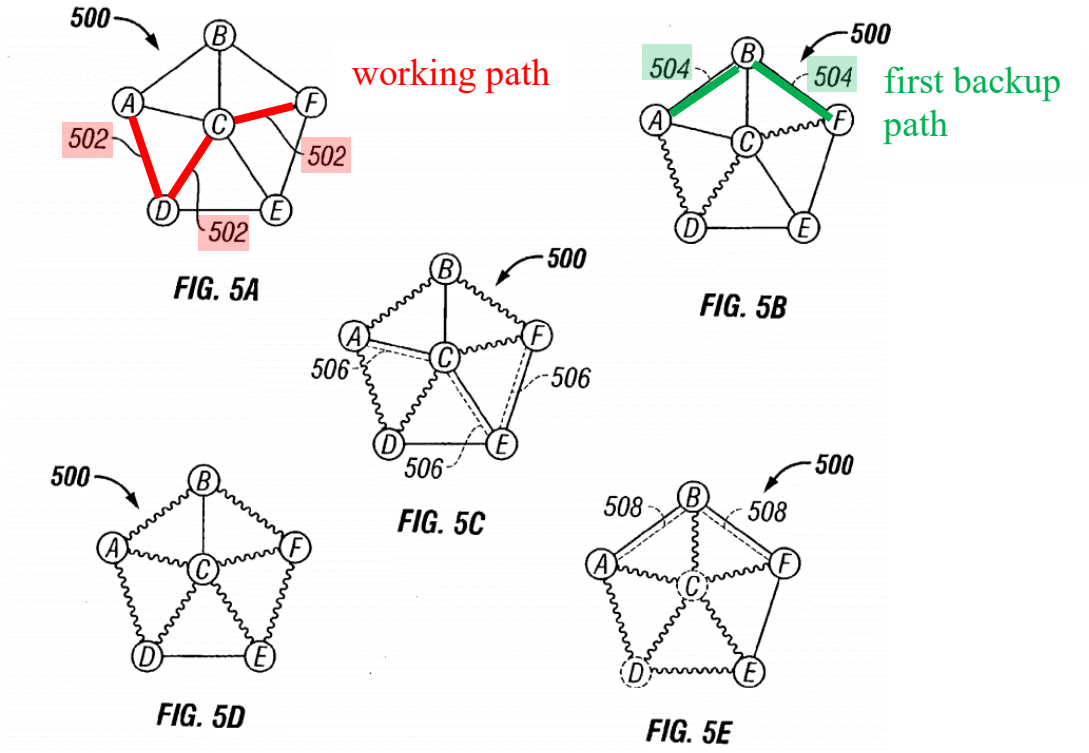
120. In one example, illustrated at FIGS. 5A and 5B, the working path corresponds to path 502 and the first protection or backup path corresponds to path 504:

> FIGS. 5A-5E illustrate different topological stages of an exemplary network 500 wherein multiple backup paths may be computed in accordance with the teachings of the present invention depending on link disjointedness and/or node disjointedness. Network 500 comprises five nodes, A through F, wherein an **exemplary working path** from Node A to Node F is identified as Path {A,D,C,F}, denoted by **reference numeral 502**. After removing the exemplary working path 502 from the network topology (i.e., links AD, DC and CF are shown in wavy lines), a **first protection path** is computed using any known algorithm. For purposes of illustration, a **protection path 504** is shown

[1] I note that EDC '525 uses the terms "protection path" and "backup path" interchangeably. *See, e.g.,* Ex.1005, [0030] ("…backup protection path."), [0034] ("…two backup paths… one of the protection paths…"). EDC '525's interchangeable use of these terms is consistent with the art. See Ex.1022, 296 ("…the terms 'backup tunnel'…'protection tunnel,'…'FRR tunnel'…'bypass tunnel'…all mean the same thing.").

in a dashed line between the source node (Node A) and the destination node (Node F), using links AB and BF.

Ex.1005, [0032], FIGS. 5A, 5B; *see also* Ex.1005, Abstract ("In one embodiment of the invention, a **working path** between an ingress node and an egress node is computed responsive to a connection request received in the network. **One or more backup paths** are computed between the ingress and egress nodes.").



Ex.1005, FIG. 5 (annotated).

121. The above figures are merely "exemplary" (Ex.1005, [0032]) and a POSITA would have understood that EDC_525's teachings apply generally to other network topologies that may comprise a lesser or greater number of nodes or links.

See also Ex.1005, [0045] ("While the exemplary embodiments of the invention shown and described have been characterized as being preferred, it should be readily understood that various changes and modifications could be made therein without departing from the scope of the present invention."), FIG. 1 (illustrating a broader network), FIG. 3 (disclosing additional path Q,R,S). In other network topologies, for example, a POSITA would have understood that the working path and the first backup path may be different. Also, a POSITA would have recognized that the path calculations may be performed in a different sequence in different network conditions (e.g., based on link availability and load) such that a different working path and a different first backup path are established. Additionally, EDC_525 teaches calculating "one or more backup paths" and "a predetermined number" of backup paths. Ex.1005, [0041]-[0042]. As such, a POSITA would have understood that EDC_525's disclosure is open ended and that one or a greater number of backup paths may be initially provided.

122. EDC_525 renders obvious that the working path and first backup path are "*established*" by teaching that "setup and/or activation messages" regarding the working path and backup path are transmitted to the nodes along the path:

> One or more backup paths are computed between the ingress and egress nodes, which are activatable upon a failure condition associated with the working path or the backup paths. The backup paths may be based on link and/or node disjointedness, as well as resource-based cost

> constraints in an exemplary implementation. **Setup messages regarding the working path and the backup paths are then transmitted to the nodes spanning the paths**.

Ex.1005, [0008].

> **Once the working path and multiple backup path computations are completed, appropriate setup and/or activation messages may be transmitted from the source node to the path nodes of the network (step 408).** Again, additional details concerning message transmission and wavelength assignment process may be found in the cross-referenced U.S. patent application identified above.

Ex.1005, [0031]; *see also* Ex.1006, [0036]-[0047], FIG. 4.

123. EDC_525's setup signaling is consistent with well-known techniques to establish paths at the time. Ex.1011, 3:7-9 ("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."), 4:7-9 ("**LSPs are established during GMPLS tunnel setup**."); Ex.1018, 37 ("data paths, i.e., from initiator to terminator and terminator to initiator, are established using a single set of signaling messages."). Moreover, it would have been obvious for the working and first backup paths to be "*established*" in view of EDC_525's disclosure of monitoring quality along paths during operation. *See, e.g.,* Ex.1005, [0008] ("…nodal and/or link quality degradation may be monitored..."); Ex.1021, 2:1-3 ("An LSP that has been established to carry traffic between a pair of nodes during normal operation.").

124. Moreover, it would have been obvious to a POSITA to "*establish[]*" the first protection path for the working path before operation begins, because it was recognized in the art that it was fundamental for a protection strategy to be preestablished before a failure was detected. *See* Ex.1022, 293 ("**The preestablishment of protection resources is fundamental for any protection strategy**. If protection resources weren't preestablished, they'd have to be set up after the failure was detected; by then, it's too late.").

125. Accordingly, EDC_525's disclosure of transmitting setup and/or activation messages for a first backup path and a working path renders obvious "*a Bypass LSP already established for a Protected Primary LSP.*"

126. Additionally, EDC_892 discloses that "**setup messages are sent to the working path and protection path nodes**," for "a new protection path to protect a defined working path." Ex.1006, [0010], [0036], Claim 1. In one example, "two setup packets are prepared and sent along the constrained working path and protection path respectively." Ex.1006, [0036]; *see also* Ex.1006, [0033], Claims 5, 15. That EDC_892's setup messages establish the backup path is confirmed by its cited provisional application. *See e.g.,* Ex.1007, 2 ("The protection path is established just after the calculation of the working path."). As analyzed above, it would have been obvious to combine the teachings of EDC_892 with EDC_525. *See* Reasons to Combine EDC_892 with EDC_525. Thus, EDC_525 in

combination with EDC_892 discloses that a first backup path is established for a working path, which renders obvious "*a Bypass LSP already established for a Protected Primary LSP.*"

127. Second, EDC_525 discloses "*providing a Backup Label Switched Path (LSP)*" by teaching that "another iteration of protection path computation" is performed to provide a second backup path:

> Thereafter, if the requested connection session between nodes A and F warranted more than one backup, **another iteration of a protection path computation takes place**. As shown in FIG. 5C, links AB and BF are also removed from the network topology for this calculation (i.e., AB and BF links are shown in wavy lines). A **second protection path** between Node A and Node F is computed, again using any known or heretofore unknown algorithm, after removing all previously calculated links from the topological graph. Reference numeral 506 refers to the exemplary second protection path comprising links AC and CF.

Ex.1005, [0032], FIGS. 5A, 5B, 5C; *see also* Ex.1005, Claim 31 ("A network element disposed as an ingress node in an optical network formed from a plurality of nodes that are inter-coupled via optical communication links, said ingress node including a processor-accessible medium having a plurality of instructions for carrying out network operations, comprising... computing a working path between said ingress node and an egress node...computing a **plurality of backup paths**

between said ingress and egress nodes, each of said backup paths being activatable upon a failure condition associated with at least one of said working path and one of said backup paths… setting up said working path and backup paths.")

128. As a further improvement, EDC_525 provides another backup path based on monitored network quality. For example, network quality is monitored and if a quality parameter is below a certain threshold the previously disclosed backup path computations are dynamically invoked to provide "one or more backup paths":

> **As a further improvement, the multiple backup path computation schemes set forth above may be provided with the capability so as to be dynamically invoked based on network quality**, which in turn may depend upon spatial and/or temporal correlation(s) of failures, e.g., a link or nodal degradation event. For instance, a centralized or distributed entity (e.g., QM 110 associated with administrator node 106 shown in FIG. 1) may continuously or periodically or otherwise monitor the quality of network components and upon occurrence of a particular condition, **a suitable multiple backup path technique may be activated to compute one or more backup paths**…For instance, a link could be given a rating with respect to an appropriate quality variable that is parameterized between 1 and 10. If the signal quality through that link is degraded or otherwise affected, or if the quality parameter is below a certain threshold, that condition exemplifies a "degradation event" in the network.

Ex.1005, [0042], Fig. 10; *see also* Ex.1005, [0008], [0025], [0026].

129. A POSITA seeking to implement the teachings of EDC_525 would have found it obvious to monitor network quality, after establishing the working and first backup paths, and to dynamically provide an additional "one or more backup paths" in case the established working path and first backup path are observed to have diminished quality. I note that this disclosure in EDC_525 relates to establishing an additional (second) backup path while the working and first backup paths remain operational—before failure. Thus, this disclosure is unlike the prior art distinguished during prosecution, where an additional backup path was established only upon a failure of the working or first backup path. The dynamically provided "one or more backup paths" (a second backup path) would further EDC_525's goal providing "a diverse set of backup paths [that] can provide better protection against multiple failure." Ex.1005, [0034]; *see also* Ex.1005, [0031], Abstract.

130. Moreover, just like the '691 patent's disclosure of considering Shared Risk Link Group (Ex.1001, 2:44-50), EDC_525's further embodiment defines an SRLG that is used for early detection of potential failures and discloses providing a backup path that is not part of that group:

> In one embodiment, a timer may be started with a duration in the order of a minute and all the subsequent degradations occurring on other links during the same time window may be used for defining a **Shared Risk Link Group (SRLG).** In other words, links that exhibit simultaneous

> degradation are more likely to fail at about the same time; which can help in early detection of multiple failures. **To reduce the possibility of multiple failures, however, two links belonging to the same SRLG are not used for the same light path connection (i.e., spatial diversification). Once a degradation correlation profile is determined, an appropriate multiple backup path computation scheme (e.g., the complete link disjoint methodology) may be used to compute a predetermined number of backup paths based on failure prediction**.

Ex.1005, [0042].

131. A POSITA would have understood that defining a SRLG is predictive (e.g., identifies paths that may fail together) and that actual failure of a working path or its protection path has not occurred. That is, EDC_525 provides a means for predicting paths that have a risk of concurrent or correlated failures, without actual failure observed. *See e.g.,* Ex.1005, [0007] ("…address the issue of correlated multiple failures…"). In circumstances where there is a potential for correlated failures of the established working and protection path, an additional one or more backup paths would be computed and setup so as to not be part of the SRLG in case of correlated failure. *See e.g.,* Ex.1005, [0034] ("[B]enefits of multiple backup paths are clearly related to spatial and temporal distributions of the failures as well as the selected methodology for computing backup paths."), [0042] ("Once a degradation correlation profile is determined, an appropriate multiple backup path

computation scheme (e.g., the complete link disjoint methodology) may be used to compute a predetermined number of backup paths based on failure prediction."). Accordingly, it would have been obvious to a POSITA, after establishing the working and first backup paths (as discussed immediately above) to define a SRLG and setup a second backup path that is not part of the SRLG of the working and first backup paths, to thereby "reduce the possibility of multiple failures." Ex.1005, [0042].

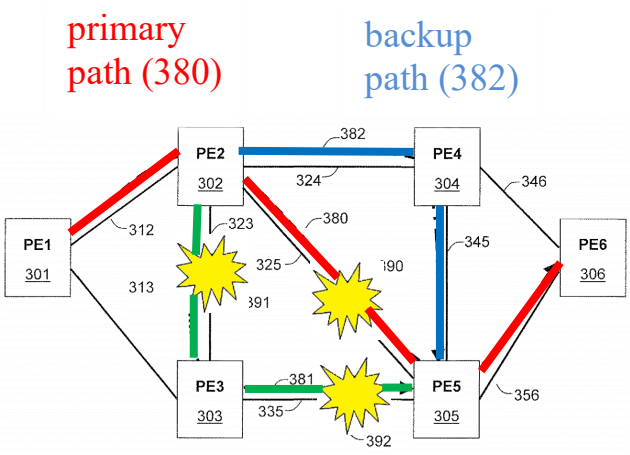
132. Additionally, Hanif teaches that "where the traffic needs to be redirected onto a backup or detour tunnel within a specified time limit (e.g., for voice over IP applications), the computing and signaling for the local repair connections is typically done in advance of the failure." Ex.1013, [0009]; *see also* Ex.1013, [0039] ("… the computing and signaling of local repair connections is done in advance such that the traffic can be redirected onto the local repair connection within a specified time limit without having to spend time in creating the local repair connection after the occurrence of a network failure."). Hanif also contemplates that there is "at least one local repair connection" set up. Ex.1013, [0010]. Accordingly, in view of Hanif, it would have been obvious to signal setup of EDC_525's second backup path before actual failure so that repair is performed quickly in case of correlated or simultaneous failures of both the established working and first backup paths (e.g., because they are part of the same SRLG).

Ex.1005, [0042] ("…defining a Shared Risk Link Group (SRLG)… links that exhibit simultaneous degradation are more likely to fail at about the same time…"), claim 15 ("…said failure condition is correlated with other failure conditions in said communications network. …"); Ex.1022, 293 ("If protection resources weren't preestablished, they'd have to be set up after the failure was detected; by then, it's too late.").

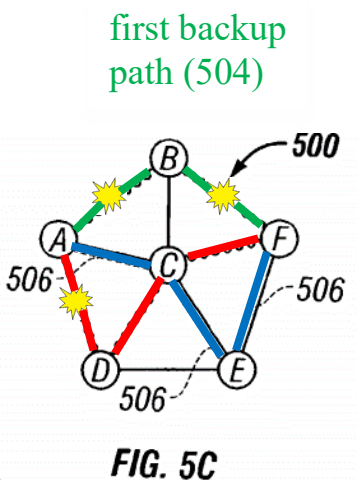
133. In summary, just like the '691 patent's embodiment of FIGS. 2-3, where two backup paths are provided, the prior art backup paths (e.g., a first backup path and a second backup path) provide protection against multiple failures:

'691 patent	**EDC_525**
A first fault 390 has disrupted facility 325, thus breaking Primary LSP 380. Bypass LSP 381 would normally compensate for the failure of facility 325 by providing an LSP connection from PE2 302 as a Point of Local Repair, to PE5 305 as its Merge Point. However, the presence of a second fault, namely fault 391 on facility 323 or fault 392 on facility 335 will break Bypass LSP 381. Backup LSP 382 connects to the same Point of Local Repair, namely PE2 302, and to the same Merge Point, namely PE5 305 as Bypass LSP 381. Thus, in the event of a fault on Bypass LSP 381, it may replace Bypass LSP 381 and provide protection for this LSP. Ex.1001, 5:48-58.	It should be appreciated that a diverse set of backup paths can provide better protection against multiple failure events in the network. For instance, in the example of a working path being protected by two backup paths, the probability of failure is intuitively low, as even after the failure of the working path and one of the protection paths it is still possible to restore the connection between the end nodes. A single backup path may also provide protection against multiple failures as long as the failures do not affect the working and protection paths simultaneously. Accordingly, having multiple backup paths advantageously decreases the probability of simultaneous interruption of all backups. Ex.1005, [0034].

134. For illustration purposes, I have provided a side-by-side comparison of the '691 patent's FIG. 3 and EDC_525's FIG. 5C, showing that the prior art second backup path provides protection in case the first backup path fails simultaneously with the working path:



Ex.1001, FIG. 3 (annotated).



Ex.1005, FIG. 5C (annotated and modified to show exemplary failure condition).

135. Accordingly, EDC_525's second backup path (which is dynamically provided after the working and first backup paths are established) corresponds to the claimed *"Backup Label Switched Path (LSP)."* *See also* Ex.1005, [0032]-[0042], FIGS. 5 to 10; analysis at element [1.6], *infra*.

136. Thus, to the extent the preamble is limiting, EDC_525 alone and in combination with EDC_892 and Hanif renders obvious "*providing a Backup Label*

Switched Path (LSP) to a Bypass LSP already established for a Protected Primary LSP," as recited.

c. [1.1] *protecting the Primary LSP against dual failures, comprising:*

137. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element.

138. First, as discussed at element [1.0.2], EDC_525 alone and in combination with EDC_892 and Hanif discloses that the method establishes a working path, which corresponds to "*the Primary LSP*," and further teaches a first and a second backup path.

"*protecting the Primary LSP against dual failures*"

139. Second, and consistent with the analysis at element [1.0.2], EDC_525 discloses "*protecting the Primary LSP against dual failures*," by teaching that the working path is "protect[ed] against multiple failures" using multiple backup paths:

> Accordingly, the present invention advantageously provides a system and method for implementing a shared **protection scheme under a scenario of multiple failures** in a network.

Ex.1005, [0008].

> [O]ne or more backup paths are computed using one of several methodologies set forth in detail below for purposes of **providing protection against multiple failures** (step 406). As will be seen, these methodologies vary depending upon link disjointedness, node

> disjointedness, and cost factors associated with spatial/temporal correlations among failures.

Ex.1005, [0031].

> It should be appreciated that a diverse set of backup paths can provide better protection against multiple failure events in the network. For instance, in the example of a **working path being protected by two backup paths**, the probability of failure is intuitively low, as even after the failure of the working path and one of the protection paths it is still possible to restore the connection between the end nodes. A single backup path may also provide protection against multiple failures as long as the failures do not affect the working and protection paths simultaneously. Accordingly, having **multiple backup paths advantageously decreases the probability of simultaneous interruption** of all backups.

Ex.1005, [0034]; *see also* Ex.1005, [0028]-[0042], [0045], FIGS. 6-9.

140. Thus, EDC_525 alone and in combination with EDC_892 and Hanif discloses protecting the working path against multiple failures, which renders obvious "*protecting the Primary LSP against dual failures, comprising*," as claimed.

d. [1.2] *establishing the Bypass LSP for the Protected Primary LSP having a Point of Local Repair node and a Merge Point node;*

141. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element.

142. First, as discussed at element [1.0.2], EDC_525 alone and in combination with EDC_892 and Hanif discloses that the method includes transmitting setup and/or activation messages to establish the first backup path for the working path, which renders obvious "*establishing the Bypass LSP for the Protected Primary LSP.*"

143. Second, EDC_525 discloses that the primary path "*ha[s] a Point of Local Repair node and a Merge Point node*" by teaching that the working path has an ingress node and an egress node within the optical network:

> In one aspect, the present invention is directed to a method for providing protection in a communications network including a plurality of nodes coupled by communication links. **The method commences by computing a working path between an ingress node and an egress node responsive to a connection request received in the network. One or more backup paths are computed between the ingress and egress nodes,** which are activatable upon a failure condition associated with the working path or the backup paths. The backup paths may be based on link and/or node disjointedness, as well as resource-based cost constraints in an exemplary implementation. Setup messages regarding the working path and the backup paths are then transmitted to the nodes spanning the paths.

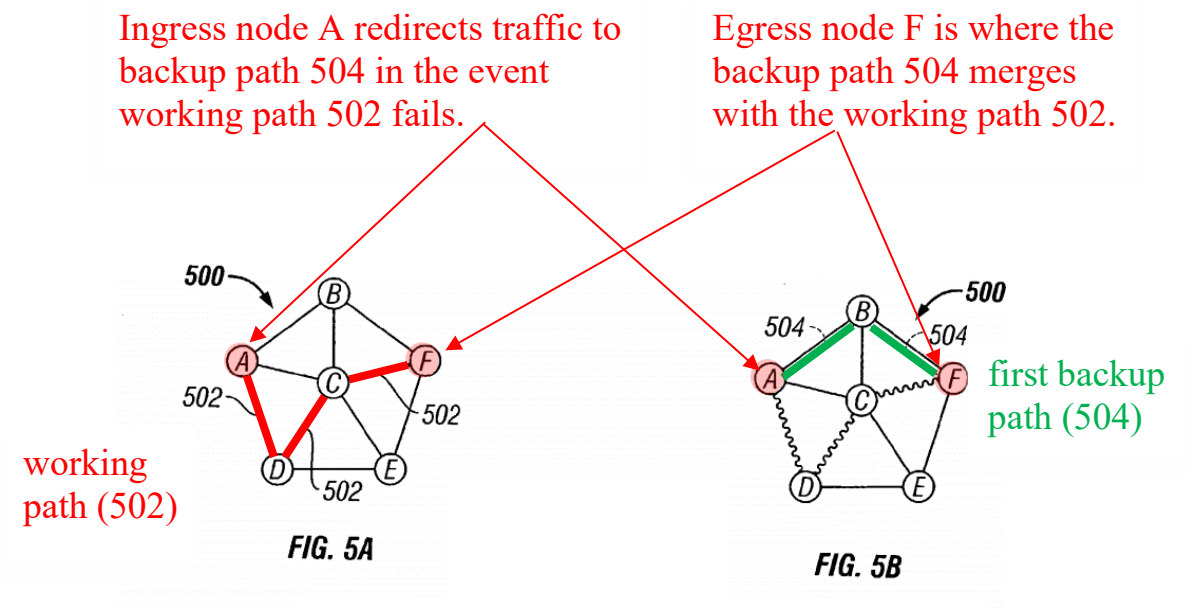
Ex.1005, [0008].

> In a presently preferred exemplary embodiment of the present invention, the protection path selection is performed at the source node

(i.e., ingress node), as is the working path selection. FIG. 4 is a flow chart of an embodiment of a method of the present invention for implementing a protection scheme capable of withstanding multiple failures. When a connection request is received at an ingress node (step 402), a working path is computed based on the network topology acquired from the co-located global database or from a centralized administrative node (Step 404). The working path may be calculated using a number of various well-known techniques. An exemplary embodiment is provided in the following co-pending commonly owned U.S. patent application entitled "Informed Dynamic Path Protection For Optical Networks," filed Nov. 29, 2001, application Ser. No. 09/998,362, cross-referenced herein above and incorporated by herein. Thereafter, one or more backup paths are computed using one of several methodologies set forth in detail below for purposes of providing protection against multiple failures (step 406). As will be seen, these methodologies vary depending upon link disjointedness, node disjointedness, and cost factors associated with spatial/temporal correlations among failures. Once the working path and multiple backup path computations are completed, appropriate **setup and/or activation messages may be transmitted from the source node to the path nodes of the network (step 408).** Again, additional details concerning message transmission and wavelength assignment process may be found in the cross-referenced U.S. patent application identified above.

Ex.1005, [0031]; *see also* Ex.1005, [0036]; Ex.1006, [0030], [0036]-[0037], FIG. 4.

144. In EDC_525's example of FIG. 5, network 500 "comprises five nodes, A through F, wherein an exemplary working path from Node A to Node F is identified as Path {A,D,C,F}, denoted by reference numeral 502." Ex.1005, [0032]. As shown below, it would have been obvious to a POSITA that in the event of working path failure, ingress Node A redirects traffic onto a first backup path {A,B,F}, denoted by reference numeral 504 that merges with the working path at egress Node F:



Ex.1005, FIGS. 5A and 5B (annotated).

145. A POSITA would have recognized, consistent with knowledge in the art, that the nodes in FIG. 5 are local to the optical network and that additional path connections may extend to other nodes of other domains. *See* Ex.1005, [0026] (discussing maintaining information regarding each link in the network domain). For example, EDC_525's FIG. 1 illustrates that additional paths extend from Nodes

A, B, D, E, F. Ex.1005, FIG. 1; *see also* Ex.1006, FIG. 1; Ex.1008, FIG. 1; Ex.1015, Abstract ("…a plurality of domains connected to one another at the border nodes of said domains…"), FIG. 1.

146. Additionally, a POSITA would have recognized that EDC_525's disclosure is in the context of local protection, at least because it supports sharing of backup paths for scalability. Ex.1005, [0008] ("[T]he present invention advantageously provides a system and method for implementing a shared protection scheme under a scenario of multiple failures in a network."); Ex.1022, 295 ("…for local protection, the relationship between the backup LSP and the number of primary LSPs it is protecting is 1:N. In other words, a single backup LSP can protect N primary LSPs, making it more scalable than path protection. This scalability makes the local protection scheme extremely attractive."). A global protection scheme, in contrast to local protection, typically requires a dedicated 1:1 relationship between the primary and the backup. Ex.1022, 294 ("With path protection, the relationship between the backup LSP and the number of primary LSPs it is protecting is 1:1. This makes the path protection scheme less scalable."). Accordingly, it would have been obvious to a POSITA for EDC_525's nodes to be implemented as "Local" nodes within the optical network, at least because EDC_525's optical network supports shared protection.

147. Thus, and consistent with the '691 patent, EDC_525's ingress node, which redirects traffic (e.g., along the first backup path 504), corresponds to the claimed "*Point of Local Repair node*." Ex.1001, 1:42-46 (a "node which redirects the traffic onto the preset Backup path is called the Point of Local Repair (PLR)."). Additionally, and consistent with the '691 patent, EDC_525's egress node, where the first backup path merges with the working path, corresponds to the claimed *"Merge Point node.*" Ex.1001, 1:42-46 ("[T]he node where a Backup LSP merges with the primary LSP is called Merge Point (MP).").

148. **Third**, to the extent argued that "*a Point of Local Repair node and a Merge Point node …*" is not sufficiently disclosed by EDC_525, the further combination with Hanif renders such obvious.

149. As discussed immediately above, EDC_525 discloses an ingress node where traffic is redirected and an egress node where traffic merges. Hanif further teaches performing "local repair" in an "MPLS network." Ex.1013, [0012]. In Hanif, both the protected LSP and the backup LSP share an ingress node that corresponds to a local repair node N1 ("PLR NODE") and an egress node that corresponds to a merge node N4 ("MERGE POINT"):

> **In the example depicted in FIG.1, an LSP may be configured between nodes N1 and N4** having a path N1-L1-N2-L2-N3-L3-N4. The path may be configured using an algorithm such as the CSPF algorithm and satisfy one or more constraints such as bandwidth, cost,

> and the like. **The LSP comprises a list of node/link pairs from originating or ingress node N1 to the destination or egress node N4**. The LSP carries data traffic from ingress node N1 to egress node N4 via link LI, LSRN2, link L2, LSRN3, and link L3. Once an LSP has been set up, the LSP is used to transmit data from the ingress node to the egress node (in FIG.1 from N1 to N4) along the preconfigured path. The egress node may then transmit the data to another device or network.

Ex.1013, [0032].

> Referring to FIG.1, the LSP from node N1to node N4 and having an OPATH N1-L1-N2-L2-N3-L3-N4 may be designated as a protected LSP and one or more local repair LSPs (which may be detour or backup LSPs) may be configured for the protected LSP. For example, a local repair LSP may be set up to protect node N2 in the OPATH. The LPATH for such a **local repair LSP may start at node N1 and merge with the OPATH at node N3 or node N4**. As depicted in FIG. 1, one such local repair LSP may be established having an associated LPATH N1-L6-N6-L5-N5-L4-N4, where node N1 is the PLR and node N4 is the merge point node where the local repair LSP rejoins the protected LSP. In one embodiment, processing to establish a local repair LSP may be performed or initiated by the PLR node.

Ex.1013, [0037]; Abstract ("**local repair connection starts at a node in the path associated with the protected connection and ends at a merge point node in the path associated with the protected connection that is downstream from the**

start node."); *see also* Ex.1013, [0007]-[0009], [0012], [0035]-[0039], [0060]-[0062], Claim 2, Claim 20, FIGS. 1, 2, 3.

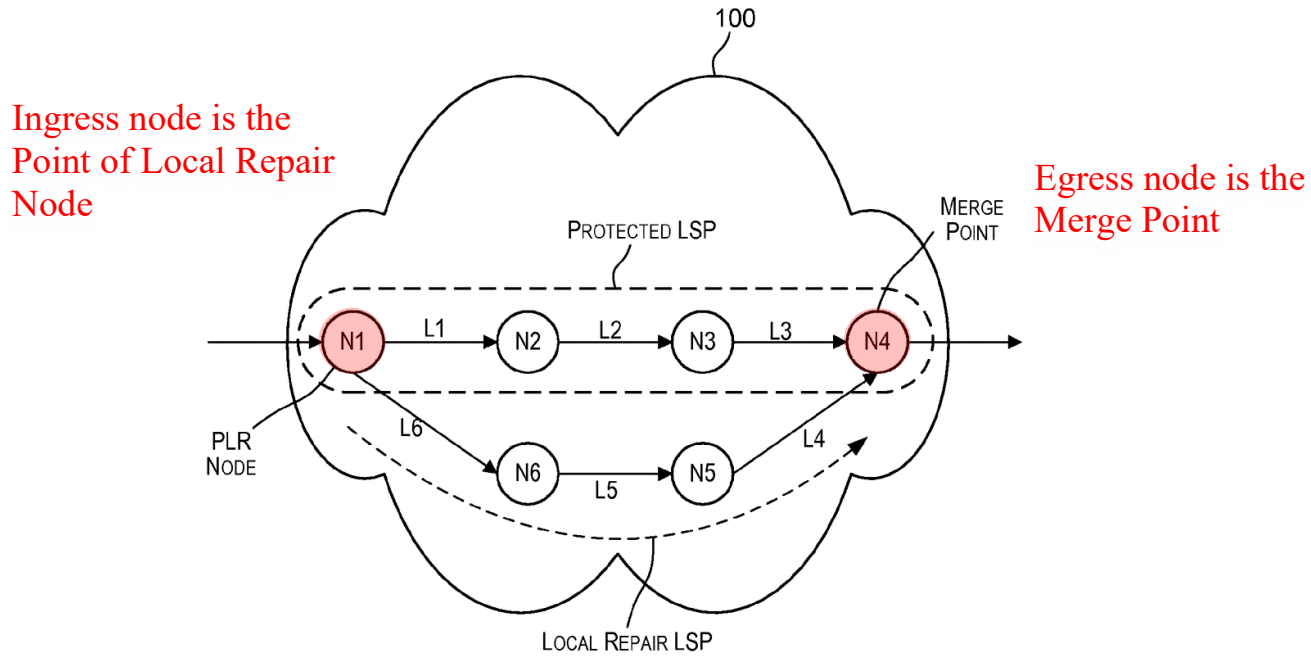


FIG. 1

Ex.1013, FIG. 1 (annotated).

150. It would have been obvious to a POSITA, in view of Hanif's local protection teachings, to implement EDC_525's ingress node as a PLR Node and the egress node as a Merge Point Node. Implementing EDC_525 with local protection, per Hanif, would have been recognized as beneficial because it would allow for repair to be performed (1) quickly and efficiently (2) avoid or reduce effects of failures in the optical network on adjacent networks (e.g., in the instance where the egress node connects to an IP network), (3) consume less network state, and (4) reduce traffic disruption during failure, among other benefits. Ex.1009, 144 ("The

protection mechanism has generally been found to be **effective in coping with local link failures** at lower layers of the MPLS/GMPLS hierarchy."); Ex.1013, [0032] ("The egress node…transmit[s] the data to another…network."); Ex.1011, 1:38-50 ("**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**… 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**."); Ex.1022, 295 ("**Local protection has several advantages** over path protection—**faster failure recovery**, 1:N scalability, and the **consumption of less network state**, to name a few."), 340 ("In the absence of local failure detection and repair, signalling propagation delay might result in packet loss that is unsuitable for real-time applications."); Ex.1023, 278 ("**Avoiding delay is highly desirable to reduce traffic disruption during failure**."); *see also* Reasons to Combine Hanif with EDC_525.

151. Thus EDC_525 in combination with EDC_892 and Hanif discloses establishing a first backup path for the working path having an ingress PLR node and an egress Merge Point node, which renders obvious "*establishing the Bypass*

LSP for the Protected Primary LSP having a Point of Local Repair node and a Merge Point node," as claimed.

e. [1.3] *obtaining the nodes traversed by an end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node;*

152. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element.

153. **First**, as discussed at element [1.2], a first backup path corresponds to the "*Bypass LSP*," an ingress node corresponds to the "*Point of Local Repair Node*," and an egress node corresponds to the "*Merge Point node*."

154. **Second**, EDC_525 teaches "*obtaining the nodes traversed by an end-to-end path*" by disclosing that each network node has a global database that comprises "current topology" information obtained for "each channel of each link in the entire network domain":

> FIG. 2 depicts a block diagram of an embodiment of an exemplary optical network node 200. A routing part 202 including routing protocol logic 202, a global database 206 and control logic 208, is coupled to an optical cross connect (OXC) module 210 which includes a switching matrix 212 disposed between one or more input demultiplexers (DEMUXes) and one or more output DEMUXes. In general operation, router 202 is responsible for control signaling in the network in which the node 200 is disposed, e.g., the optical transport network 100 shown in FIG. 1, using appropriate routing logic 204. **The global database 206 comprises one or more tables that provide a <u>current topology</u>**

> **of the network 100 for intelligent, dynamic creation of network paths under control of control logic 208. Preferably, in one implementation, the global database 206 provides information regarding each channel of each link in the entire network domain**.

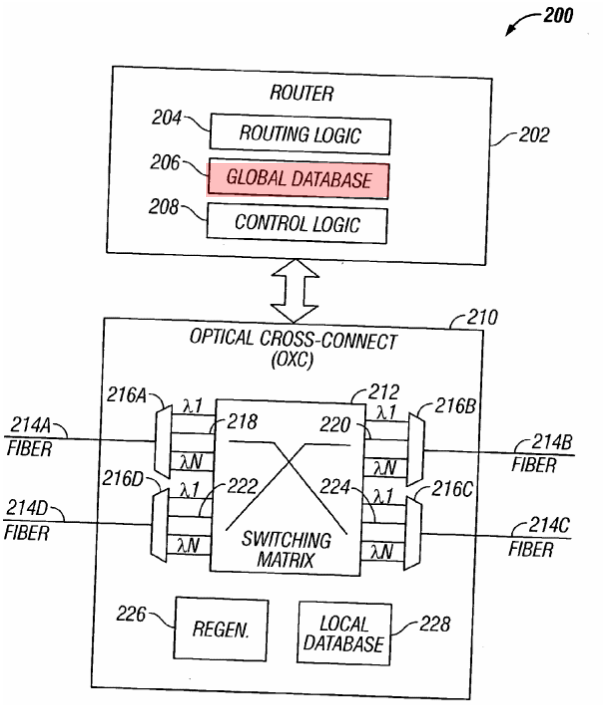
Ex.1005, [0026].

155. EDC_525's network topology information may be compiled from all nodes in the network:

> In operation, every exemplary network node 200 maintains the entries in the global allocation database for its own links. **Information regarding other links in the global allocation database may be compiled from allocation information provided by other nodes in the network domain. In one implementation, such information may be shared among all nodes in the network** using a variant of the Open Shortest Path First (OSPF) protocol upgraded for optical networks.

Ex.1005, [0030], FIGS. 3A, 3B.

156. As shown below at FIG. 2, the network node includes a global database 206:



Ex.1005, FIG. 2 (annotated).

157. In one example, EDC_525 discloses that network topology information is used to determine backup paths that are both link and node disjoint. Ex.1005, [0008], [0032]; *see also* Ex.1005, Abstract (calculating backup paths that are "based on link and/or node disjointedness"), [0033] ("…complete node disjoint scenario …"), claim 6 ("wherein said backup paths comprise paths that are completely node-disjointed with respect to one another."), FIG. 5A-5E. For example, path calculation logically removes from the topology information an already-used path node and then calculates "one or more backup paths between the ETE [end-to-end] nodes." Ex.1005, [0032]-[0033], [0038]. A POSITA would have understood that in order to calculate backup paths that are node disjoint, the topology information identifies the

nodes traversed from the ingress node to the egress node (i.e., end-to-end); these nodes are then avoided when calculating disjoint backup paths. Accordingly, it would have been obvious to a POSITA for the network topology information, which is obtained from "all nodes" for "each link in the entire network domain," to include information regarding nodes traversed by an end-to-end path of the first backup path ("*Bypass LSP*") from an ingress node ("*Point of Local Repair Node*") to an egress node ("*Merge Point node*").

158. Additionally, EDC_892 discloses a "global allocation database 26 [that] comprises one or more tables that provide **a current topology of the network 10 for intelligent, dynamic creation of network paths.**" where a path corresponds to "a sequence of nodes." Ex.1006, [0023], [0025]. EDC_892's database "provides information regarding each channel of each link in the network domain." Ex.1006, [0026]; *see also* Ex.1006, [0032] ("In operation, every node 12 maintains the entries in the global allocation database 26 for its own links. Information for other links in the global allocation database are compiled from information of the global allocation data bases from other nodes 12 in the domain. The information from the global allocation databases 26 of the various nodes is flooded to all nodes in the domain using a variant of the OSPF."). As analyzed above, it would have been obvious to combine the teachings of EDC_892 with EDC_525. *See* Reasons to Combine EDC_892 with EDC_525.

159. Third, to the extent argued that "*obtaining the nodes traversed by an end-to-end path*" is not sufficiently disclosed, the further combination with Hanif renders such obvious.

160. Hanif teaches that its node 400 includes "[p]rocessor 408 [] configured to perform processing for tasks performed by node 400" and a "processor within module 406" that may perform "creation of local repair LSPs, optimization of LPATHs, and the like." Ex.1013, [0072]-[0073]; *see also* Ex.1013, Claim 19. Hanif's processors may be implemented separately, together, or processor 408 "may…aid modules 406 and 404 in functions performed by those modules." Ex.1013, [0073]. In one example, processor 408 accesses memory 410 that includes "**network topology information that is used for determining local paths associated with local repair LSPs**." Ex.1013, [0074].

161. In view of Hanif, it would have been obvious to a POSITA when implementing the combination with EDC_525 (see analysis at element [1.0.1]) for the processor to obtain the network topology information stored in memory and provide the information to the instructions for computing paths to thereby determine local backup LSPs that are disjoint. Ex.1005, [0026] ("…a current topology of the network 100 for intelligent, dynamic creation of network paths under control of control logic…"), Claims 31 and 34 ("instructions for computing a plurality of backup paths between said ingress and egress nodes… in which said backup paths

are completely node-disjointed…"); *see also* Ex.1005, [0033]-[0041], Abstract, FIGS. 6-8; Ex.1013, [0073]-[0074] ("…modules 404 and 406…to determine local repair LSPs…"); analysis, *infra*, at elements [1.4]-[1.6]; Reasons to Combine Hanif with EDC_525.

162. Thus, EDC_525 alone and in combination with EDC_892 and Hanif discloses obtaining network topology information, including the nodes and links traversed by the end-to-end path of the first backup path from an ingress node to an egress node, which renders obvious "*obtaining the nodes traversed by an end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node*," as claimed.

f. [1.4] *generating a request to a path calculator using the nodes traversed by said end-to-end path of said Bypass LSP for a disjoint path connecting said Point of Local Repair Node to said Merge Point node;*

163. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element.

164. **First**, as discussed at element [1.2], a first backup path corresponds to the "*Bypass LSP*," an ingress node corresponds to the "*Point of Local Repair Node*," and an egress node corresponds to the "*Merge Point node*." Further, as discussed at element [1.3], the global database maintains obtained network topology information that includes the nodes traversed by the end-to-end path of the first

backup path (e.g., 504), which corresponds to *"the nodes traversed by said end-to-end path of said Bypass LSP*."

165. Second, EDC_525 teaches "*a path calculator*" by disclosing "processor-accessible medium having… instructions for computing a plurality of backup paths between said ingress and egress nodes":

> 31. A network element disposed as an ingress node in an optical network formed from a plurality of nodes that are inter-coupled via optical communication links, said ingress node including a **processor-accessible medium having a plurality of instructions** for carrying out network operations, comprising:
>
> ...
>
> **instructions for computing a plurality of backup paths** between said ingress and egress nodes....

Ex.1005, Claim 31. EDC_525's instructions to compute a plurality of backup paths, taken separately and together with the processor (see analysis at element [1.0.1]), corresponds to "*a path calculator*," as claimed.

166. Additionally, EDC_525 cites to EDC_892 for "well-known techniques" to calculate paths. Ex.1005, [0031]. In that regard, EDC_892 discloses that its node "calculat[es] a protection path" and provides various details regarding the calculation, which further renders obvious a "*path calculator*." Ex.1006, [0036]-[0047], [0052], FIGS. 4, 5. As analyzed above, it would have been obvious to

combine the teachings of EDC_892 with EDC_525. *See* Reasons to Combine EDC_892 with EDC_525.

"*generating a request…for a disjoint path connecting…*"

167. Third, EDC_525 renders obvious "*generating a request… for a disjoint path connecting said Point of Local Repair Node to said Merge Point node*." EDC_525's instructions compute a disjoint second backup path that connects the ingress node to the egress node:

> One or more backup paths are computed between the ingress and egress nodes, which are activatable upon a failure condition associated with the working path or the backup paths. **The backup paths may be based on link and/or node disjointedness**, as well as resource-based cost constraints.

Ex.1005, Abstract.

> Thereafter, **one or more backup paths are computed using one of several methodologies** set forth in detail below for purposes of providing protection against multiple failures (step 406). As will be seen, **these methodologies vary depending upon link disjointedness, node disjointedness**, and cost factors associated with spatial/temporal correlations among failures.

Ex.1005, [0031].

> FIGS. 5B through 5D depict three topologies that obtain with respect to the exemplary network 500 when **a complete link disjoint scheme is used for calculating multiple backup paths**…if the requested

> connection session between nodes A and F warranted more than one backup, another iteration of a protection path computation takes place.

Ex.1005, [0032]; *see also* Ex.1005, [0037] ("…path computations may be predicated upon treating both links as well as nodes as completely disjoint…"), Claim 33 ("…said backup paths are completely link-disjointed with respect to one another."); Ex.1005, Claim 34 ("…said backup paths are completely node-disjointed with respect to one another but for said ingress and egress nodes."); Ex.1005, Abstract ("[o]ne or more backup paths are computed…based on link and/or node disjointedness").

168. Furthermore, consistent with the analysis at element [1.0.2], EDC_525 discloses that during operation, "one or more backup path[]" computations are "dynamically invoked," e.g., if a quality parameter is below a certain threshold or if a potential concurrent failure is identified (e.g., because of SRLG):

> **As a further improvement, the multiple backup path computation schemes set forth above may be provided with the capability so as to be dynamically invoked based on network quality**, which in turn may depend upon spatial and/or temporal correlation(s) of failures, e.g., a link or nodal degradation event. For instance, a centralized or distributed entity (e.g., QM 110 associated with administrator node 106 shown in FIG. 1) may continuously or periodically or otherwise monitor the quality of network components and upon occurrence of a particular condition, **a suitable multiple backup path technique may be activated to compute one or more backup paths**…For instance, a

> link could be given a rating with respect to an appropriate quality variable that is parameterized between 1 and 10. If the signal quality through that link is degraded or otherwise affected, or if the quality parameter is below a certain threshold, that condition exemplifies a "degradation event" in the network……In one embodiment, a timer may be started with a duration in the order of a minute and all the subsequent degradations occurring on other links during the same time window may be used for defining a Shared Risk Link Group (SRLG). In other words, links that exhibit simultaneous degradation are more likely to fail at about the same time; which can help in early detection of multiple failures. To reduce the possibility of multiple failures, however, two links belonging to the same SRLG are not used for the same lightpath connection (i.e., spatial diversification). Once a degradation correlation profile is determined, an appropriate multiple backup path computation scheme (e.g., the complete link disjoint methodology) may be used to compute a predetermined number of backup paths based on failure prediction.

Ex.1005, [0042], Fig. 10; *see also* Ex.1005, [0008], [0025], [0026]. In situations where the working path and first backup path (established based on the connection request, see [1.0.2]) are impacted by the "degradation event" or are part of the SRLG, it would have been obvious to a POSITA to invoke the computing instructions dynamically to calculate an additional backup path with an appropriate computation scheme. *See e.g.* Ex.1005, FIG. 5 (steps 406 to 408), FIG. 6 (steps 608 to 620), FIG. 7 (steps 708 to 720), FIG. 8 (steps 808 to 810), FIG. 9 (steps 908 to

910), FIG. 10 (1008). Such an invocation of backup path computation would beneficially provide additional protection to the working path in case the degradation event gives rise to a failure or the SRLG fails.

169. Additionally, Hanif teaches that backup path (local repair LSP) calculations "may be initiated upon receiving a signal."

> As depicted in FIG. 2, **processing may be initiated upon receiving a signal to create or determine a local repair LSP** for a protected LSP (step 202). The signal in 202 may be received under various different circumstances. In one embodiment, the signal may be received when a particular LSP is tagged as a protected LSP and creation of a local repair LSP is requested for the protected LSP. The node or link of the protected LSP to be protected may also be identified. In another embodiment, the signal may be received whenever a new LSP is provisioned. In yet other embodiments, the signal may be received when a failure of a node and/or link is detected along an LSP.

Ex.1013, [0042]; FIG. 2. Hanif's backup path calculation considers nodes already used (downstream of the PLR) and does not recalculate the already established protected LSP. Ex.1013, [0042]-[0043], FIG. 2. Accordingly, consistent with the analysis immediately above, it would have been obvious to a POSITA to generate a signal requesting that EDC_525's computing instructions dynamically calculate an additional second backup path, without recalculating the already established working path and first backup path. In one example shown above, Hanif's backup

path calculation is initiated "**whenever a new LSP is provisioned**." Ex.1013, [0042], FIG. 2. Accordingly, in instances where EDC_525's "predetermined number of backup paths" is two or more (see Ex.1005, [0041]) and only one backup path is initially available, it would have been obvious to a POSITA to initiate backup path calculation whenever a new LSP is provisioned, as Hanif teaches, so that the predetermined number of backup paths is reached. Such an implementation would further EDC_525's goal. *See also* Reasons to Combine Hanif with EDC_525.

170. EDC_525 teaches that its "instructions for computing a plurality of backup paths" correspond to computer "**software**" and an "**algorithm**," and may be implemented "**using any technique**." *See, e.g.,* Ex.1005, [0009], [0032]-0033], Claims 2, 17, 32. It was known in the art to implement software algorithms in a modular fashion using a software subroutines known as functions that would be executed upon request. Ex.1014, 199 ("**function**…A general item for a subroutine."); Ex.1016, 95 ("Most modern [programming] languages have an ability to create named subroutines or subprograms…called a **function**."); Ex.1017, 37 ("The **function is the heart**…[of] programs."); Ex.1033, 380 (describing a "**function**" as "a self-contained **software** routine that performs a job for the program it is written in or for some other program. The function performs the operation and returns control of the instruction following the calling instruction or

to the calling program. Programming languages provide a set of standard functions and may allow programmers to define others.").

171. A POSITA would have found it obvious to utilize a processor (see [1.0.1]-[1.0.2]) to execute the instructions for computing a plurality of backup paths dynamically, e.g., based on network quality or a defined SRLG. Ex.1005, [0042]. In doing so, it would have been obvious to a POSITA for the processor executing the instructions to generate a request (known in the art as a "function call") to perform path computation and to provide the obtained network topology information to be used in the path computation (for example, as parameters or arguments). Ex.1012, 3:13-17 ("…control part being configured to **request computation by sending a request to the local path computation element** for computation of the new recovery path.…"); Ex.1014, 200 ("**function call…A program's request** for the services of a particular function. A function call is coded as the name of the function along with any **parameters needed for the function** to perform its task."); Ex.1016, 96 ("[T]he argument list (which follows the name and is surrounded by parentheses) contains the types of **arguments that must be passed to the function**."); Ex.1017, 37 ("Function arguments are contained in parentheses following the function name. The **values of the arguments are the parameters needed to execute the function**."); Ex.1033, 380 ("**function call A request by a program** to use a subroutine…A function call

written in a program states the name of the function followed by any **values or parameters that have to be passed to it**. When the function is called, the operation is performed, and the results are returned.").

172. A POSITA would have known how to implement EDC_525's network topology information in the global database in numerous ways, including as an array of arrays; in such an implementation, the network topology information would be passed to the function call, for example, as a pointer to the array of arrays. Ex.1035, 341, ("…we can **access the data in such a structure using indices and pointers**…"), 394 ("…this index will allow us to retrieve the entire record in the case where our **array is part of a database**."); Ex.1036, 125, ("In C, the call-by-reference mechanism is based on manipulating, not the data itself, but pointers to the data. A **pointer is a reference to a place where data is stored**, it is pointing to some data location."), 133 ("An array gathers an arbitrary number of elements into a single entity… Sample **applications of arrays are vectors of numbers and databases** of records."); Ex.1037, 11 ("We can declare and create a pointer to a struct"), 12 ("Most of the time, you'll want to **pass a pointer** to a struct."), 20 (using C programming to "**[c]reate an inventory database** for a used car lot"); Ex.1038, 321-379 (disclosing C programming with arrays and pointers). The function would use the pointer to access the network topology information from the arrays and would perform path calculations, including, depending on the desired

computation, logically removing used links or nodes. Additionally, as another example, a POSITA would have known that the network topology information in the global database may be implemented as a file, and the path-computation function would receive as a parameter the file name (or a pointer to the file). Ex.1034 (disclosing that C programing works with SQLite database); Ex.1036, 221, 403-404 (disclosing C programming file input and output); Ex.1038, 379-392 (disclosing C programming file input and output), 651-672 (disclosing C programming with database files); Ex.1039, 1 ("Embedded SQL is a method of combining the computing power of a high-level language like C/C++ and the database manipulation capabilities of SQL. It allows you to execute any SQL statement from an application program."). 10 ("…use these techniques to code your own database application program."). In such a circumstance, the function would retrieve the network topology information from the named file and perform path calculations, including logically removing nodes to compute a completely disjoint second backup path. I note that these are merely examples, and potentially tens if not hundreds of different implementations would have been known to a POSITA, based on the programming language utilized.

173. Accordingly, it would have been obvious to a POSITA for EDC_525's instructions for computing a plurality of backup paths to be invoked by a request (e.g., function call) that uses the obtained network topology information (e.g., a

parameter pointer to an array or file of the information). *See* element [1.3]; Ex.1005, [0026], [0030]. For instance, in EDC_525's example of dynamically invoking path computations based on network quality (see Ex.1005, [0042]), it would have been obvious to a POSITA for a processor to generate a request for a second backup path using a parameter (e.g., a pointer or a file name) corresponding to the network topology information (which includes nodes traversed by the end-to-end path of the first backup path (see [1.0.2])) because such a request would inform the instructions for computing which nodes should be logically removed from the computations so that the computed backup path is completely disjoint. *See e.g.,* Ex.1005, [0008], Abstract; *see also* Ex.1005, [0031]-[0032], [0041]-[0044], claims 6, 7, 33-36. Thus, EDC_525 alone and in combination with EDC_892 and Hanif discloses generating a request to a path calculator (e.g., software instructions for computing backup paths) using the nodes traversed by the end-to-end path of the first backup path for a disjoint second backup path that connects the ingress node to the egress node, which renders obvious "*generating a request to a path calculator using the nodes traversed by said end-to-end path of said Bypass LSP for a disjoint path connecting said Point of Local Repair Node to said Merge Point node*," as claimed.

g. [1.5] *receiving a response from said path calculator; and*

174. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element. **First**, as discussed at element [1.4], the prior art instructions

to compute backup paths, taken separately and together with the processor, corresponds to a "*path calculator*," as claimed.

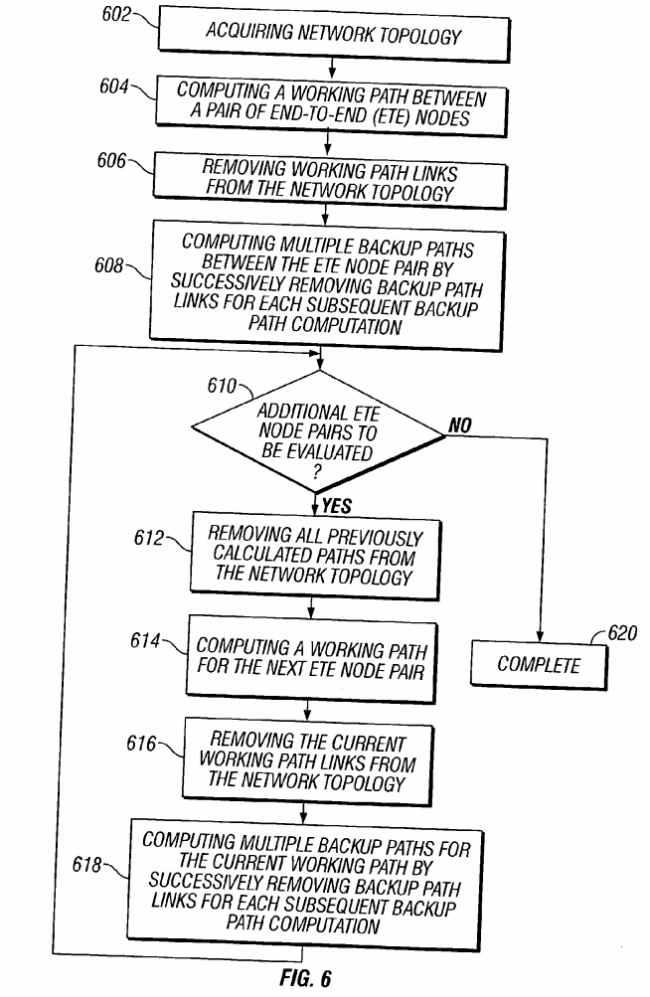
175. Second, EDC_525 renders obvious "*receiving a response*." EDC_525's instructions for computing determine whether a backup path is available and the level of disjointness, in three different ways.

Completely link disjoint example

176. In one example, EDC_525 determines the availability of a backup path that is "completely link disjoint" with respect to the other paths from the ingress node to the egress node:

> **FIG. 6 is a flow chart of an embodiment of a method of the present invention for computing multiple backup paths where the links are completely disjoint**. First, a network topology is acquired (step 602), wherein all links in the network topology may be attributed the same cost. Thereafter, a working path is computed pursuant to a connection request between a pair of end-to-end (ETE) nodes, i.e., the source and destination nodes (step 604). As noted in the foregoing discussion, any known or heretofore unknown routing technique may be employed that optimizes a suitable metric (e.g., hop count, path distance, etcetera). Working path links are then logically removed from the network topology (step 606) so as to ensure that they are not reused for subsequent paths. One or more backup paths between the ETE nodes may then be calculated in a similar fashion until the requisite number of paths are computed or the resultant topology does not sustain any more backups (step 608).

Ex.1005, [0035], FIG. 6; Ex.1005, Claim 33 ("The network element as set forth in claim 31, wherein said instructions for computing said backup paths include instructions operable to determine multiple backup paths using a methodology in which said backup paths are **completely link-disjointed** with respect to one another."); *see also* Ex.1005, [0037]-[0039].



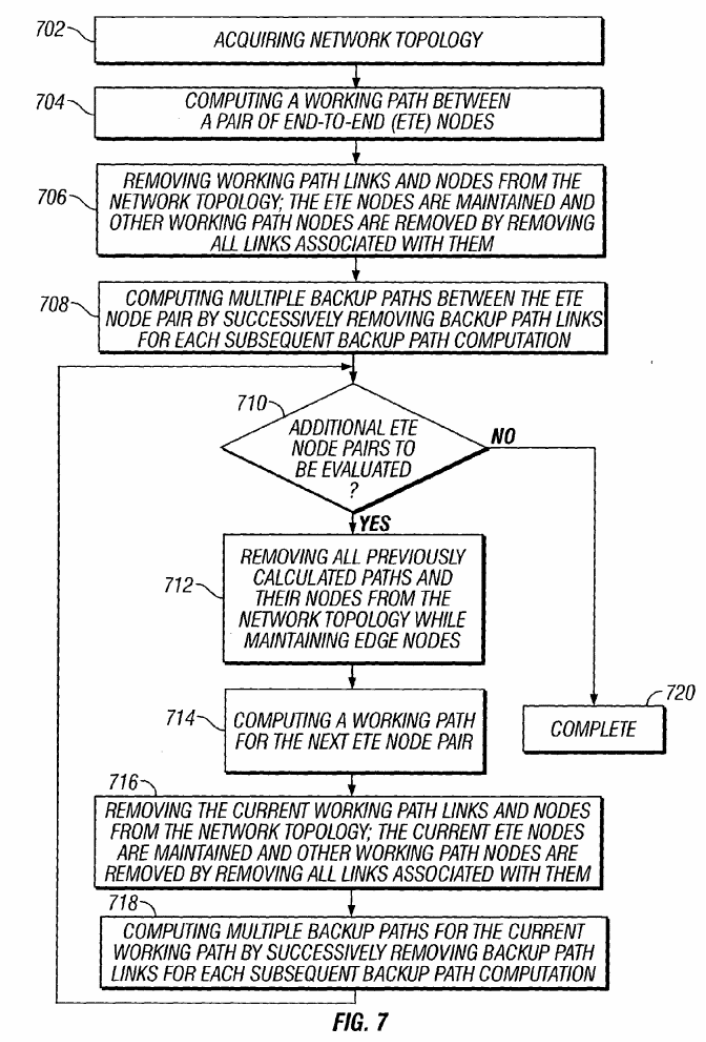
Ex.1005, FIG. 6.

Completely node and link disjoint example

177. In another example at FIG. 7, EDC_525's path calculator determines that a backup path, with both links and nodes completely disjoint, is available from the ingress node to the egress node:

> In another embodiment, path computations may be predicated upon treating both links as well as nodes as completely disjoint. **FIG. 7 is a flow chart of an embodiment of a method of the present invention for computing multiple backup paths where the links and nodes are completely disjoint**. Similar to the process set forth above, a network topology is acquired first by an ingress node of an ETE pair (step 702). Again, all links in the network topology may be attributed the same cost using an appropriate metric. A working path is computed thereafter pursuant to a connection request between the ingress and egress nodes of the ETE pair (step 704). Both working path links and working path nodes are then logically removed from the network topology (Step 706) so as to ensure that they are not reused for subsequent paths. As explained before, a path node is removed by removing all the links connected to it. Clearly, the source and destination nodes are not removed from these computations. Subsequently, one or more backup paths between the ETE nodes may then be calculated in a similar fashion until the requisite number of paths are computed or the resultant topology does not sustain any more backups (step 708).

Ex.1005, [0037]-[0038]; *see also* Ex.1005, Claim 21 ("wherein said backup paths comprise paths that are completely node-disjointed with respect to one another.").



Ex.1005, FIG. 7.

Partially disjoint example

178. In yet another example at FIG. 8, EDC_525's path calculator determines that a partially disjoint path from the ingress node to the egress node is available:

> Because of resource constraints and connectivity blocking in a network, it may not be feasible to treat the links, nodes, or both, in a completely disjointed fashion for calculating the backup paths. A variable cost

> factor may be employed to penalize the links and/or nodes already used for a connection. **FIG. 8 is a flow chart of an embodiment of a method of the present invention for computing multiple backup paths where the links are <u>partially disjoint</u>**. Upon obtaining the network topology (step 802), prior-use penalty costs (C_1) associated with the network links may be initialized (step 804). A working path is then computed for the ingress and egress node pair associated with the connection request (step 806). Subsequent multiple backup paths are computed thereafter by successively updating the link penalty costs after each backup path calculation (step 808). As a result, the methodology attempts to avoid the links that have already been used in a working path connection or a backup connection. The backup paths, therefore, are the destination paths calculated with the new metric that is cost-aware for each iterative step. These steps may be repeated until the number of backup paths requested is reached or when the network topology no longer sustains any additional backup paths between the ETE node pair (decision block 810). If additional ETE node pairs are available that require path computations, the working path and backup paths may be computed by utilizing the process flow set forth above, wherein link penalty costs are properly taken into account for each pair and each path computation (step 812).

Ex.1005, [0040]; Ex.1005, Claim 36 ("The network element as set forth in claim 31, wherein said instructions for computing said backup paths include instructions operable to determine multiple backup paths using a methodology in which said **backup paths are partially link-disjointed with respect to one another**."); *see*

also Ex.1005, [0041], FIG. 9 (disclosing that the computing instructions considers disjointness and path costs).

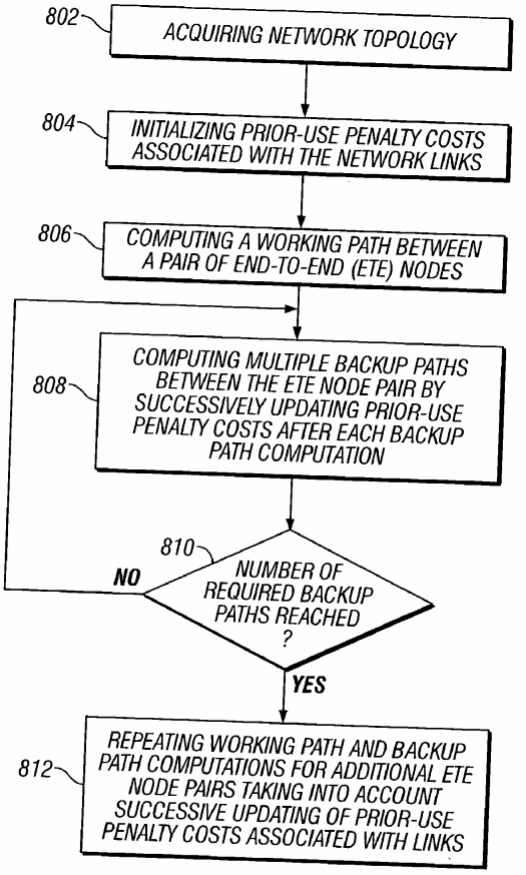


FIG. 8

Ex.1005, FIG. 8.

179. Consistent with the analysis at element [1.4] and knowledge in the art, it would have been obvious to a POSITA for EDC_525's "instructions for computing a plurality of backup paths" (e.g., implemented as a function) to return the result of the path computations (e.g., a determination that a backup path was

successful and its level of disjointness). Ex.1016, 98 ("The **return** keyword exits the function block to the point right after the function call. If return has an argument, that becomes the return value of the function. **You can have more than one return statement in a function**."); Ex.1033, 380 ("function call A request by a program to use a subroutine…A function call written in a program states the name of the function followed by any values or parameters that have to be passed to it. **When the function is called, the operation is performed, and the results are returned**.").

180. It would have been obvious to a POSITA to receive a response from EDC_525's instructions for computing backup paths that indicates whether the computations were successful and the level of disjointness of the computed backup path (e.g., completely link-disjointed, partially link-disjointed, or both link- and node-disjoint with respect to the first backup path). Receiving an indication that the path computation was successful would beneficially facilitate further action to be taken, including, transmitting appropriate setup/activation messages to the nodes along the path. *See* Ex.1005, [0008] ("Setup messages…are then transmitted to the nodes spanning the paths…"), [0031] ("Once…multiple backup path computations are completed, appropriate setup and/or activation messages may be transmitted from the source node to the path nodes of the network…"); Ex.1006, [0036] ("If…

path calculations are successful, setup messages are sent…"); *see also, infra*, element [1.6].

181. Thus, EDC_525 alone and in combination with EDC_892 and Hanif renders obvious *"receiving a response from said path calculator*," as claimed.

h. [1.6] *in response to determining that a fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP.*

182. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious this element.

183. **First**, as discussed at element [1.5], it would have been obvious to receive a response that indicated whether the computed backup path is completely link-disjointed, partially link-disjointed, or both link and node disjoint with respect to the established first backup path. Instances where EDC_525's computed second backup path is determined to be available with "**links and nodes [that] are completely disjoint**" (see Ex.1005, [0037]-[0038]) render obvious "*determining that a fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is available*."

184. **Second**, EDC_525 teaches "*signaling, to at least one other MPLS label switch router*," by disclosing that the network node transmits "setup and/or activation messages… to the path nodes of the network":

> Once…backup path computations are completed, **appropriate setup and/or activation messages may be transmitted from the source node to the path nodes of the network** (step 408).

Ex.1005, [0031]; *see also* Ex.1005, [0008] ("The backup paths may be based on link and/or node disjointedness…Setup messages…are then transmitted to the nodes spanning the paths."). As already analyzed above, EDC_525's GMPLS network nodes correspond to label switch routers. Ex.1005, [0026]-[0027], FIGS. 1, 2. Accordingly, EDC_525's transmission of setup and/or activation messages to the path router nodes renders obvious "*signaling, to at least one other MPLS label switch router*," as claimed.

185. Furthermore, EDC_525's transmission is "*in response to determining*…" because the setup and/or activation messages are transmitted, at least in some instances, "**[o]nce…backup path computations are completed**" and it is determined that a second backup path with "links and nodes [which] are completely disjoint" is available. Ex.1005, [0031], [0037]; *see also* Ex.1005, Claim 21 ("…said backup paths comprise paths that are completely node-disjointed with respect to one another.")

186. **Third**, EDC_525 teaches signaling the "*fully disjoint path as the Backup LSP to said Bypass LSP."* EDC_525 provides example information that may be included in transmitted messages and further cites to EDC_892's "additional details concerning message transmission and wavelength assignment

process." Ex.1005, [0030]-[0031]. In that regard, EDC_892 discloses that the transmitted setup message (also called a "protection message[]") identifies that the path is used for protection and also identifies the working path that needs the protection:

> Protection messages for updating the global allocation database 26 are received by the nodes 12 using LDP (Label Distribution Protocol) messages. **The protection messages may be the same as those used for reservation of a working path, with the addition of two fields: (1) a Type field that indicates whether the connection is for a protection path (Type field set to "1") or a working path (Type field set to "0") and (2) a Working Path field that identifies the working path that needs the protection. The protection message may be either a SETUP or RELEASE message**.

Ex.1006, [0033]; *see also* Ex.1006, [0036] ("The setup packet for said protection path includes the associated working path.")

187. Consistent with the analysis immediately above and at elements [1.1], [1.4]-[1.5], EDC_525's second protection path (which may be completely link and node disjoint) provides backup protection in the event that both the working path and the first backup path fail. *See e.g.,* Ex.1005, [0034] ("It should be appreciated that a diverse set of backup paths can provide better protection against multiple failure events in the network. For instance, in the example of a working path being protected by two backup paths, the probability of failure is intuitively low, as even

after the failure of the working path and one of the protection paths it is still possible to restore the connection between the end nodes."), Claim 31 ("…each of said backup paths being activatable upon a failure condition associated with at least one of said working path and one of said backup paths…").

188. In view of EDC_892's setup message teachings, it would have been obvious for a POSITA to implement EDC_525's setup messages to identify that the completely disjoint second backup path is used to protect the working path that is also protected by the first backup path. Because the second backup path (which is completely disjoint to the first backup path) protects the same working path, the second backup path is the backup to the first backup path when the first backup path fails (and vice versa). Thus, EDC_525 in combination with EDC_892 renders obvious signaling the fully disjoint path "*as the Backup LSP to said Bypass LSP."* [2]

189. As analyzed above, it would have been obvious to combine the teachings of EDC_892 with EDC_525 because EDC_525 expressly suggests the combination. Ex.1005, [0031]. Additionally, it would have been obvious to a POSITA to include in EDC_525's setup message the noted information, per

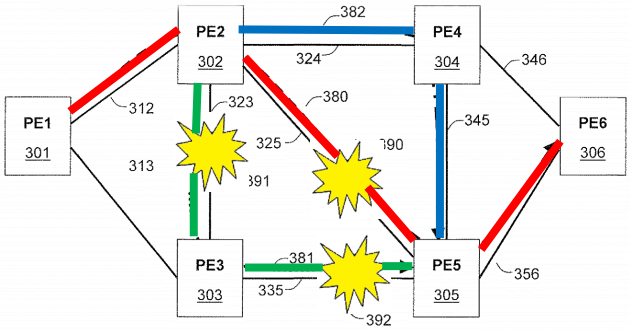
[2] I note that the prior art's disclosure of both backup paths protecting the same working path is consistent with the claim requirement of "*protecting the Primary LSP against dual failures."*

EDC_892, because it would allow for the nodes that receive the message to update the global allocation database. *See* Ex.1005, [0028] ("…global database 206 includes information for determining the existence of links having channels currently used for protection paths…"), [0030] ("Information regarding other links in the global allocation database may be compiled from allocation information provided by other nodes in the network domain."); Ex.1006, [0033] ("…messages for updating the global allocation database 26 are received by the nodes…"); *see* Reasons to Combine EDC_892 with EDC_525.

190. I note, as shown in the side-by-side comparison, that EDC_525's second backup path (which is used when the first backup path fails) provides the same protection as the '691 patent's disclosed embodiment:

primary path (380)

backup path (382)



bypass path (381)

Ex.1001, FIG. 3 (annotated).

first backup path (504)

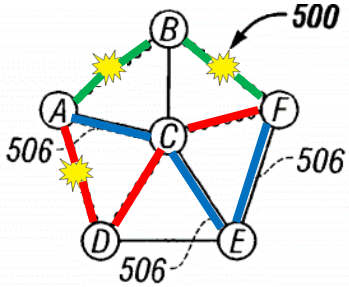


FIG. 5C

working path (502)

second backup path (506)

Ex.1005, FIG. 5C (annotated and modified to show exemplary failure condition).

'691 patent	EDC_525
A first fault 390 has disrupted facility 325, thus breaking Primary LSP 380. Bypass LSP 381 would normally compensate for the failure of facility 325 by providing an LSP connection from PE2 302 as a Point of Local Repair, to PE5 305 as its Merge Point. However, the presence of a second fault, namely fault 391 on facility 323 or fault 392 on facility 335 will break Bypass LSP 381. Backup LSP 382 connects to the same Point of Local Repair, namely PE2 302, and to the same Merge Point, namely PE5 305 as Bypass LSP 381. Thus, in the event of a fault on Bypass LSP 381, it may replace Bypass LSP 381 and provide protection for this LSP. Ex.1001, 5:48-58.	It should be appreciated that a diverse set of backup paths can provide better protection against multiple failure events in the network. For instance, in the example of a working path being protected by two backup paths, the probability of failure is intuitively low, as even after the failure of the working path and one of the protection paths it is still possible to restore the connection between the end nodes. A single backup path may also provide protection against multiple failures as long as the failures do not affect the working and protection paths simultaneously. Accordingly, having multiple backup paths advantageously decreases the probability of simultaneous interruption of all backups. Ex.1005, [0034].

191. Thus, EDC_525 in combination with EDC_892 and Hanif discloses transmitting a setup message to the nodes the second backup path (which is completely disjoint) as the backup path in the event that the first backup path fails, which renders obvious "*signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP*," as claimed.

7. Claim 2

a. [2.0] *A method as claimed in claim 1, wherein said path calculator is a constraint based shortest path first calculator.*

192. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious claim 2.

193. As discussed at element [1.4], the prior art instructions to compute a plurality of backup paths, taken separately and together with the processor, corresponds to a "*path calculator*." Further, EDC_525 discloses that the backup paths are calculated using "**resource-based cost constraints**" and "**based on a shortest path first algorithm**." Ex.1005, Claim 32; *see also* Ex.1005, [0008], [0032] ("…**cost/penalty constraints associated with sharing or non-sharing of protection links**."), [0033] ("Again, a protection path may be calculated within the resulting graph using any technique, e.g., Dijkstra's **Shortest Path First (SPF) algorithm**."). I further note that EDC_525's calculation is also constrained because

previously computed paths (e.g., nodes and/or links) are "logically removed" from the topology for calculation purposes or penalized by a "variable cost factor." *See* Ex.1005, [0032] ("In a complete link disjoint scheme, successive path computations involve network topologies wherein the links that make up previously computed paths are logically removed from the topology."), [0033] ("…removal of the intermediary nodes…all links associated therewith are also removed…"), [0040] ("…**variable cost factor may be employed to penalize the links and/or nodes already used for a connection…[when] computing multiple backup paths where the links are partially disjoint**.").

194. Additionally, EDC_892's computations use a "**shortest path algorithm**…to find the shortest path." Ex.1006, [0038]; *see also* Ex.1006, [0046] ("By assigning a lower factor, shorter protection paths will be encouraged."), [0047] ("**Prepare the constrained shared protection path…Let Protection Path be the shortest path to destination**…"), Abstract ("Costs are assigned to identified links where links that have at least one shareable channel are weighted differently that links that do not have a shareable channel. A protection path is determined using the found links based on the costs.").

195. It would have been obvious to a POSITA to implement EDC_525's path calculations as disclosed by EDC_892, in view of EDC_525's express citation to the exemplary path calculations of EDC_892. Ex.1005, [0031].

196. Thus, EDC_525 alone and in combination with EDC_892 and Hanif discloses that the instructions for computing backup paths is a constrained based SPF calculator, which renders obvious "*wherein said path calculator is a constraint based shortest path first calculator*," as claimed.

8. Claim 3

a. [3.0] ***A method as claimed in claim 1, wherein in response to determining that the fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is not available, in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, signaling, to at least one other MPLS label switch router, said partially disjoint path as the Backup LSP to said Bypass LSP.***

197. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious claim 3. For example, EDC_525 discloses that "[b]ecause of resource constraints and connectivity blocking in a network, **it may not be feasible to treat the links, nodes, or both, in a completely disjointed fashion for calculating the backup paths**." Ex.1005, [0040]. EDC_525's disclosure that it may not be feasible to treat links and nodes as completely disjoint renders obvious "*determining that the fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is not available*."

198. EDC_525 discloses that in instances where completely disjoint paths are not feasible, a "variable cost factor may be employed to penalize the links

and/or nodes already used for a connection…[when] computing multiple **backup paths where the links are partially disjoint**." Ex.1005, [0040], FIG. 8; *see also* 1005, [0041]. Further, as discussed at elements [1.4]-[1.5], the instructions for computing backup paths may be dynamically invoked and based on the result (which in this case would identify backup paths that are partially disjoint), appropriate setup and/or activation messages may be transmitted to the nodes along the path as discussed at element [1.6]. Accordingly, EDC_525 alone and in combination with EDC_892 and Hanif renders obvious "*in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, signaling, to at least one other MPLS label switch router, said partially disjoint path as the Backup LSP to said Bypass LSP.*"

9. Claim 4

b. [4.0] *A method as claimed in claim 3, wherein in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is not available, then signaling an error on the attempt to provide a Backup LSP.*

199. EDC_525 in combination with EDC_892 and Hanif renders obvious claim 3. For example, Hanif discloses that if "**a local repair path could not be found….An error condition may then be output indicating that a local repair LSP could not be established for the protected LSP**." Ex.1013, [0050]. A POSITA would have recognized that Hanif's disclosed situation (where a local

repair path cannot be found) is an example within the scope of claim 4's conditional language. If no local repair path is available (irrespective of disjointedness), then it necessarily follows that "*a partially disjoint path… is not available*." It would have been obvious to a POSITA to apply Hanif's teachings to EDC_525 and output an error if it is determined a second backup path connecting the ingress node and the egress node is unavailable, to notify a network administrator that corrective action should be taken. *See e.g.,* Ex.1020, 8:50-54 ("If no path exists [], then the appropriate warning can be displayed notifying the system administrator that…corrective action should be taken."). Accordingly, it would have been obvious to signal an error on the attempt if no backup path (regardless of disjointness) is available so that an administrator may take corrective action. *See also* Reasons to Combine Hanif with EDC_525.

200. Thus, EDC_525 in combination with EDC_892 and Hanif renders obvious "*wherein in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is not available, then signaling an error on the attempt to provide a Backup LSP."*

10. Claim 5

a. [5.0] *A method as claimed in claim 1 after said obtaining step, comprising further steps of: procuring a Shared Risk Link Groups (SRLG) associated with the nodes traversed by the end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node; and providing said Shared Risk Link*

Groups as part of said generating a request step to said calculator for use in calculating said disjoint path,

201. EDC_525 alone and in combination with EDC_892 and Hanif renders obvious claim 5. Consistent with the analysis at element [1.0.2], EDC_525 discloses a further embodiment where a SRLG is defined and used for early detection of potential failures and teaches that computed backup paths should not be part of that group:

> **As a further improvement, the multiple backup path computation schemes set forth above may be provided with the capability so as to be dynamically invoked based on network quality**…In one embodiment, a timer may be started with a duration in the order of a minute and all the subsequent degradations occurring on other links during the same time window may be used for **defining a Shared Risk Link Group (SRLG).** In other words, links that exhibit simultaneous degradation are more likely to fail at about the same time; which can help in early detection of multiple failures.

Ex.1005, [0042].

202. In the instance where the backup path computation scheme is dynamically invoked after establishing the first protection path and the working path, the defined SRLG would include the nodes traversed by the end-to-end path of the first backup path from the ingress node to the egress node (as discussed at [1.2]). Accordingly, EDC_525 renders obvious renders obvious "*procuring a Shared Risk Link Groups (SRLG) associated with the nodes traversed by the end-to-*

end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node."

203. Furthermore, EDC_525 discloses that backup paths are computed that do not belong to the defined SRLG:

> **To reduce the possibility of multiple failures, however, two links belonging to the same SRLG are not used for the same light-path connection** (i.e., spatial diversification). Once a degradation correlation profile is determined, an **appropriate multiple backup path computation scheme (e.g., the complete link disjoint methodology) may be used** to compute a predetermined number of backup paths based on failure prediction.

Ex.1005, [0042].

204. It would have been obvious for a POSITA to provide the defined SRLG as part of the generated request to the instructions for computing backup paths (see analysis at element [1.4]) because this information would allow for computing backup paths with links that do not belonging to the same SRLG (e.g., a "complete link disjoint methodology,") to thereby reduce the possibility of multiple failures. Thus, EDC_525 in combination with EDC_892 and Hanif renders obvious "*providing said Shared Risk Link Groups as part of said generating a request step to said calculator for use in calculating said disjoint path*." as claimed.

11. Claim 6

a. [6.0.1] *A non-transitory machine readable storage medium encoded with instructions for execution by a network processor of a Multiprotocol Label Switching (MPLS) label switch*

205. To the extent limiting, consistent with the analysis at element [1.0.1], EDC_525 alone and in combination with EDC_892 and Hanif discloses a processor of a node in an MPLS network, which renders obvious "*a network processor of a Multiprotocol Label Switching (MPLS) label switch.*" Ex.1003, ¶205. EDC_525's node also performs "**switching**." Ex.1005, [0025]. Additionally, Hanif discloses that the network node "**may be embodied as a network device such as a switch or router.**" Ex.1013, [0066]. It would have been obvious to a POSITA to implement EDC_525's network node as a switch, per Hanif, because this this merely a simple substitution of one known element for another (EDC_525's node for Hanif's switch) to obtain predictable results (perform switching in the network). The combination is also merely a combination of prior art elements (Hanif's switch with EDC_525's network node) according to known methods (it was known how to implement switches) to yield predictable results (perform switching). *See also* Reasons to combine Hanif with EDC_525.

206. The prior art combination also renders obvious "*non-transitory machine readable storage medium encoded with instructions for execution*." Consistent with knowledge in the art, it would have been obvious to a POSITA for

EDC_525 processor-accessible medium to be implemented as "*non-transitory*" medium (e.g., CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive), because such an implementation would allow for retaining the instructions after a power down. Ex.1011, 6:24-30 ("The computer system 84 includes memory 88 which can be utilized to store and retrieve software programs incorporating computer code… Exemplary computer readable storage media include CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive."), Claim 12 ("A non-transitory computer readable storage medium encoded with computer executable instructions…"). Furthermore, consistent with the analysis at element [1.0.1], it would have been obvious to a POSITA for EDC_525 instructions to be for "*execution*" by a processor, as was conventional and well known in the art. Ex.1012, Claim 17 ("A nontransitory computer readable medium comprising a computer program comprising machine-readable **instructions which when executed by a processor** cause the processor to perform.").

207. Moreover, Hanif discloses that the memory includes "**instructions that are executed by processor**." *See e.g.,* Ex.1013, [0074] ("Memory 410 may also store programs comprising software code or instructions that are executed by processor 408 and/or by the other modules of node 400. For example, code or instructions which when executed by a processor cause the processor (or modules 404 and 406) to determine local repair LSPs and optimize local paths, as described

above, may be stored in memory 410."); *see also* Ex.1013, [0060],[0073]. It would have been obvious to a POSITA to apply Hanif's teachings and implement EDC_525's instructions so that they are executable by a processor to facilitate the computations of multiple backup paths and other network operations, thereby furthering EDC_525's objectives. *See e.g.,* Ex.1005, [0034]; *see also* Reasons to Combine Hanif with EDC_525.

208. Accordingly, EDC_525 alone and in combination with EDC_892 and Hanif renders obvious "*non-transitory machine readable storage medium encoded with instructions for execution by a network processor of a Multiprotocol Label Switching (MPLS) label switch*."

b. [6.0.2] *for providing a Backup Label Switched Path (LSP) to a Bypass LSP already established for a Protected Primary LSP, the medium comprising:*

209. See analysis at elements [1.0.2], [6.0.1].

c. [6.1] *instructions for protecting the Primary LSP against dual failures, comprising:*

210. See analysis at elements [1.1], [6.0.1]-[6.0.2].

d. [6.2] *instructions for establishing the Bypass LSP for the Protected Primary LSP having a Point of Local Repair node and a Merge Point node;*

211. See analysis at elements [1.2], [6.0.1]-[6.0.2].

e. [6.3] ***instructions for obtaining the nodes traversed by an end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node;***

212. See analysis at elements [1.3], [6.0.1]-[6.0.2].

f. [6.4] ***instructions for generating a request to a path calculator using the nodes traversed by said end-to-end path of said Bypass LSP for a disjoint path connecting said Point of Local Repair Node to said Merge Point node;***

213. See analysis at elements [1.4], [6.0.1]-[6.0.2].

g. [6.5] ***instructions for receiving a response from said path calculator; and***

214. See analysis at elements [1.5], [6.0.1]-[6.0.2].

h. [6.6] ***in response to determining that a fully disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, instructions for signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP.***

215. See analysis at elements [1.6], [6.0.1]-[6.0.2].

12. Claim 7

a. [7.0] ***A non-transitory machine readable storage medium as claimed in claim 6, wherein the instructions specify that said path calculator is a constraint based shortest path first calculator.***

216. See analysis at elements [6.0.1]-[6.6], [2.0].

13. Claim 8

a. [8.0] ***A non-transitory machine readable storage medium as claimed in claim 6, wherein in response to determining that the fully disjoint path connecting said***

Point of Local Repair Node to said Merge Point node is not available,

217. See analysis at elements [6.0.1]-[6.6], [3.0].

b. [8.1] ***in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is available, signaling, to at least one other MPLS label switch router, said partially disjoint path as the Backup LSP to said Bypass LSP.***

218. See analysis at element [3.1].

14. Claim 9

a. [9.0] ***A non-transitory machine readable storage medium as claimed in claim 6, wherein in response to determining that a partially disjoint path connecting said Point of Local Repair Node to said Merge Point node is not available, signaling an error on the attempt to provide a Backup LSP.***

219. See analysis at elements [6.0.1]-[6.6], [4.0].

15. Claim 10

b. [10.0] ***A non-transitory machine readable storage medium as claimed in claim 6, wherein the instructions specify after said obtaining step further steps of:***

220. See analysis at elements [6.0.1]-[6.6].

c. [10.1] ***procuring a Shared Risk Link Groups (SRLG) associated with the nodes traversed by the end-to-end path of said Bypass LSP from said Point of Local Repair Node to said Merge Point node; and*** **providing said Shared Risk Link Groups as part of said generating a request step to said calculator for use in calculating said disjoint path.**

221. See analysis at element [5.0].

B. Ground 2: Claims 1-10 are obvious over EDC_525 in view of EDC_892, Hanif, and Li

222. The combination of EDC_525, EDC_892, Hanif, and Li renders obvious claims 1-10 as discussed below.

1. Summary of Li

223. Chinese patent publication CN 101645848 A to Li et al. ("Li," Ex.1030) is titled "Traffic Protection Method and Apparatus, and System." Ex.1030, Title.

224. Like the '691 patent, generally pertains to "networks having an MPLS function." Ex.1030, Abstract. In the context of FIGS. 3 and 4, Li discloses prioritizing backup LSPs such that a higher priority backup LSP is initially utilized when a primary (or master) LSP fails and a lower priority LSP is utilized in case the higher priority LSP fails:

> A master LSP for carrying traffic and at least one backup LSP playing a protective role existing between label switched routers (LSRs) of an ingress interface and an egress interface; and Setting priorities for the master LSP and the backup LSP, wherein when the state of the master LSP carrying the traffic is abnormal, the backup LSP having a relatively high priority is preferably selected as an LSP carrying the traffic. In the embodiment of the present invention, the traffic protection method is specifically illustrated by an instance that the at least one backup LSP playing a protective role includes two backup LSPs.

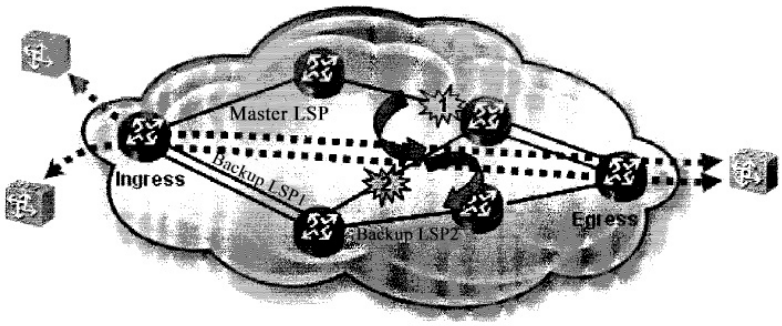
Ex.1030, 6.

225. In the context of FIG. 4, Li discloses the sequence for path utilization:

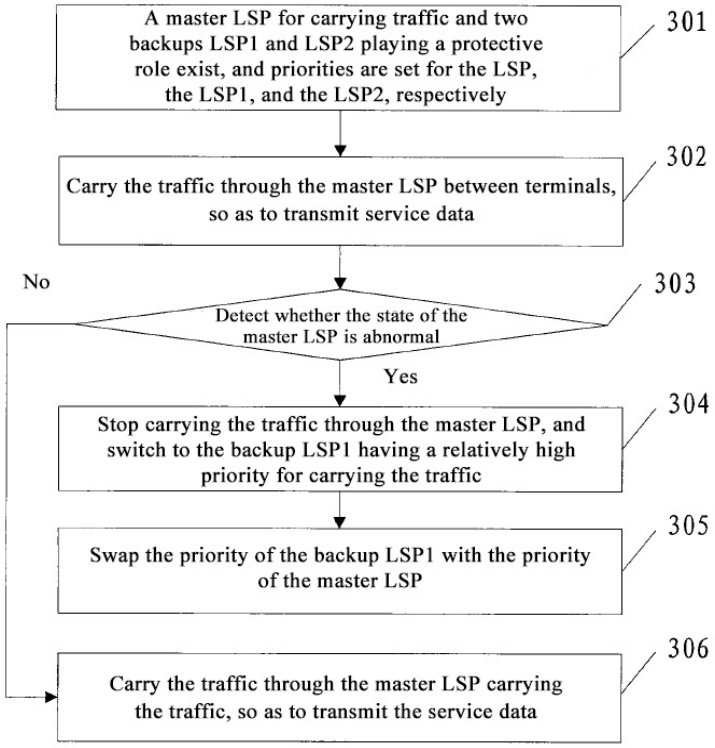
> 301. A master LSP for carrying traffic and two backups LSP1, LSP2 playing a protective role exist between the LSRs of the ingress interface and the egress interface, wherein priorities are set for the master LSP, the backup LSP1, and the backup LSP2, respectively; and specifically, the master LSP is set to have the highest priority, which is set as master, and the priorities of the backup LSP1 and the backup LSP2 are set from high to low as backup 1 and backup 2.
>
> …
>
> 303. The state of the master LSP is detected, wherein if it is detected that the state of the master LSP is abnormal, step 304 is performed, and if it is detected that the state of the master LSP is not abnormal, step 306 is performed. An abnormality in the state of the master LSP may be in, but not limited to, the following forms, including: link failure, data packet loss, transmission interruption, etc.; and there is no limitation for this in the embodiment of the present invention.
>
> …
>
> In the embodiment of the present invention, the priority level of the backup LSP1 is higher than the priority level of the backup LSP2, such that the link carrying the traffic is switched from the master LSP to the backup LSP1, and the backup LSP1 carrying the traffic transmits the service data.
>
> If an abnormality also occurs in the high-priority backup LSP1, the link carrying the traffic is switched from the master LSP to the backup LSP2, that is, according to the priorities of the backup LSP1 and the

backup LSP2, the traffic is switched to and carried through the normal backup path having a high priority.

Ex.1030, 6-7, FIGS. 3 and 4.



Ex.1030, FIG. 3.



Ex.1030, FIG. 4.

226. Li further discloses an additional embodiment in the context of FIGS. 5-6, where "if it is detected that the state of the master tunnel P is abnormal… the

traffic through the master tunnel P is stopped, and according to the priorities of the backup tunnels, the traffic is switched to the backup tunnel." Ex.1030, 9, FIG. 5-6. "In the embodiment of the present invention, the priority level of the backup tunnel P1 is higher than the priority of the backup tunnel P2, wherein if the state of the backup tunnel P1 is not abnormal, the traffic is switched from the master tunnel to the backup tunnel P1, and if the state of the backup tunnel P1 is abnormal, the traffic is switched from the master tunnel to the backup tunnel P2, and the backup tunnel transmits the service data." Ex.1030, 9.

2. Reasons to Combine Li with EDC_525

a. *Li is Analogous Art*

227. Li, like EDC_525 and the '691 patent, discloses providing a backup path for a primary (or master) path in an MPLS network and are therefore analogous art. Ex.1001, 1:6-10, Abstract; Ex.1005, [0001]- [0009], Abstract, FIGS. 4, 6-9, Claims 1, 31; Ex.1030, 6-7, Abstract, FIGS. 3-4. Additionally, like EDC_525 and the '691 patent, Li addresses the problem of using multiple backup paths to protect against multiple failures. Ex.1001, 1:6-10, Abstract; Ex.1005, [0008], [0031]-[0034], Abstract, FIGS. 4, 6-9, Claims 1, 31; Ex.1030, 6-9, FIGS. 3-6.

b. *Motivation to combine with Li*

228. A POSITA would have been motivated to combine the teachings of Li and EDC_525 (as modified in view of EDC '829 and Hanif) to produce numerous predictable and beneficial results.

229. EDC_525 teaches that two backup paths provide protection for each other in case of multiple simultaneous failures. *See e.g.,* Ex.1005, [0034]. EDC_525, however, leaves it to a POSITA to determine the sequence of backup path utilization. As such, a POSITA looking to implement EDC_525's teachings would have looked to other relevant teachings for this purpose. In that regard, Li discloses prioritizing two backup paths and using the higher priority backup path first and then using the lower priority backup path in case that path also fails. *See* Ex.1030, 6. For example, in the context of FIGS. 3 and 4, Li discloses that a higher priority backup path (backup LSP1) is initially utilized when a primary path (master LSP) fails and, in the event that the higher priority path subsequently fails, then a lower priority backup path (backup LSP2) is utilized. Ex.1030, 6-7, FIGS. 3 and 4; *see also* Ex.1030, 9-10, FIGS. 5-6 (disclosing an additional embodiment that also has LSPs with different priorities).

230. It would have been obvious to a POSITA to apply Li's teachings when implementing multiple backup paths, per EDC_525, such that failover sequence would be controlled based on priority (i.e., with a higher priority backup path being

used first in case of failure and a lower priority backup path being used only after the higher priority path has also failed). Such an implementation would beneficially give greater control over path failover selection.

231. Also, a POSITA would have been motivated to apply Li's priority teachings, when implementing two backup paths per EDC_525, because it may reduce the probability that the selected backup path is preempted. For example, it was known in the art to include priority fields when a path is setup for FRR (or local protection) such that a path with a higher priority has less likelihood that it would be preempted by other paths, as compared with a backup path having a lower priority:

> FIG. 2 is a format of a FAST_REROUTE object used for setup of a backup LSP for fast rerouting…. A Setup Priority field 200 contains a value representing priority of a backup LSP. This value is for deciding whether the backup LSP can preempt another LSP by comparison of the priority of the backup LSP and that of another LSP. A Holding Priority field 202 contains a value representing holding priority of a backup LSP. **This value is for deciding whether the backup LSP can be preempted by another LSP by comparison of the priority of the backup LSP and that of another LSP**.

Ex. 1025, [0043]-[0044]; *see also* Ex.1019, 8-9 ("…The FAST_REROUTE object is used to control the backup used for the protected LSP. This specifies the setup and hold priorities."); Ex.1024, [0055] ("The Path message carries…establishment

priority, hold priority…"). Accordingly, it would have been obvious to a POSITA implementing two backup paths, per EDC_525, to assign priorities to backup paths and upon a failure of a working path use a backup path with the highest priority (as Li teaches) because this would reduce the probability that the backup path is preempted by another path during operation. If a backup path with a lower priority would be initially used, the probability of preemption would be greater, which would have been recognized as undesirable.

232. Additionally, a POSITA would have been motivated to utilize Li's priority scheme for backup path selection, when implementing two backup paths per EDC_525, because it would allow for assigning a first backup path a high priority when it has the same (or greater) quality of service ("QoS") as the working path, thereby ensuring that the QoS is maintained even though failure has occurred. Maintaining QoS would have been recognized as important by a POSITA for paths that carry voice data, among other sensitive data. *See* Ex.1026, 7 ("Backup bandwidth protection allows you to give LSPs carrying certain kinds of data (such as voice) priority for using backup tunnels… Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained."); Ex.1021, 1:22-26 ("As the Internet becomes a multi-media communications medium that is expected to reliably handle voice and video traffic, network protocols must also evolve to support quality of-service (QoS)

requirements."); Ex.1027, 6 ("Table 9 shows the different protection strategies proposed, according to the QoS requirements. They are sorted based on priority."); Ex.1030, 1 ("In telecommunications networks, high reliability is always the most basic and critical performance requirement, especially for voice services."). As such, it would have been obvious to apply a priority scheme to select backup paths, as Li teaches, when implementing two backup paths per EDC_525, because it would allow for maintaining QoS using a first backup path that has the same QoS as the failed working path and only using the second backup path (which may not support the same QoS) in the event that the first backup path also fails.

233. Yet another reason to combine the teachings of Li with EDC_525 is that prioritization allows for using the priority levels of the different paths to minimize frequent switching when the primary path is restored to a normal state. *See* Ex.1030, 1 ("In the process of implementing the foregoing traffic switching, the inventor found that there is at least the following problem in the prior art: when the master path fails, a backup path immediately replaces the master path to protect the traffic. Once the master path is restored to a normal state, the traffic is switched back to the master path. The traffic needs to be switched twice for one link flapping. If a network is complex and not stable enough, frequent switching of traffic in the network will occur, which will cause unnecessary burden on a system and affect the reliability of the traffic."). Path prioritization "solve[s] the problem of severe impact

on traffic reliability caused by frequent traffic switching when a network is unstable" because the traffic can be "locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path." Ex.1030, 1-2.

234. Each above noted reason, separately and together would have motivated a POSITA to apply Li's priority teachings to EDC_525.

235. Furthermore, as discussed in Ground 1 element [1.0.2] and [1.2], EDC_525 teaches that the path computations may be performed at a central node. Ex.1005, [0025] ("…centrally…"); *see also* Ex.1005, [0042] ("…centralized…"). It would have been obvious to a POSITA, in implementing the combination of Li with EDC_525 where the path computations are performed centrally to include this information in a signal sent by the central node to the ingress node (point of local repair). *See* Ex. 1025, [0043]-[0044] ("…a FAST_REROUTE object used for setup of a backup LSP for fast rerouting [includes]…. A Setup Priority field 200 contains a value representing priority of a backup LSP…A Holding Priority field 202…"); Ex.1019, 8-9 ("…The FAST_REROUTE object is used to control the backup used for the protected LSP. This specifies the setup and hold priorities."); Ex.1024, [0055] ("The Path message carries…establishment priority, hold priority…"). The signal would inform the ingress node of the calculated backup paths that need to be setup and the sequence of backup path failover.

236. The combination of Li with EDC_525 represents a simple combination of known elements (e.g., path priority per Li with EDC_525's paths) to yield predictable results (e.g., informing an ingress node which backup path to use first in case that a working path fails). The proposed combination also merely represents the application of a known technique (e.g., assigning path priority, per Li, to EDC_525's paths) to yield predictable and beneficial results (e.g., informing the ingress node which backup path to use first, and obtaining one or more of the noted benefits discussed immediately above).

c. *Reasonable expectation of success*

237. The results would have been predictable and there would have been a reasonable expectation of success in the combination since EDC_525 and Li address the same technology, as analyzed above. Also, path prioritization was well-known in the art, and it was known how to provide path priority information in signals, which further supports reasonable expectation of success. A POSITA would have possessed the skills required to make the proposed combination, including being able to implement the combined teachings of Li and EDC_525 in corresponding hardware and software.

3. Claim 1

238. Other than the below identified element, the remaining Claim 1 analysis in Ground 1 remains the same in Ground 2.

239. To the extent argued that "*signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP*" is not rendered obvious per the Ground 1 analysis, the further combination with Li renders this element obvious.

240. EDC_525 teaches that two backup paths provide protection for each other in case of multiple simultaneous failures:

> It should be appreciated that a diverse set of backup paths can provide better protection against multiple failure events in the network. For instance, in the example of a working path being protected by two backup paths, the probability of failure is intuitively low, as even after the failure of the working path and one of the protection paths it is still possible to restore the connection between the end nodes. A single backup path may also provide protection against multiple failures as long as the failures do not affect the working and protection paths simultaneously. Accordingly, having multiple backup paths advantageously decreases the probability of simultaneous interruption of all backups.

Ex.1005, [0034].

241. EDC_525, however, leaves it to a POSITA to determine the sequence of backup path utilization in the circumstance where there is only a single or sequential failure. As such, a POSITA looking to implement EDC_525's teachings would have looked to other relevant prior art teachings on backup path sequence for

utilization. In that regard, Li discloses prioritizing two backup paths and using the higher priority backup path first:

> A master LSP for carrying traffic and at least one backup LSP playing a protective role existing between label switched routers (LSRs) of an ingress interface and an egress interface; and setting priorities for the master LSP and the backup LSP, wherein when the state of the master LSP carrying the traffic is abnormal, the backup LSP having a relatively high priority is preferably selected as an LSP carrying the traffic.

Ex.1030, 6.

242. Li provides an example, in the context of FIGS. 3 and 4, where a higher priority backup path (backup LSP1) is initially utilized when a primary path (master LSP) fails and, in the event that the higher priority path subsequently fails, then a lower priority backup path (backup LSP2) is utilized:

> 301. A master LSP for carrying traffic and two backups LSP1, LSP2 playing a protective role exist between the LSRs of the ingress interface and the egress interface, wherein priorities are set for the master LSP, the backup LSP1, and the backup LSP2, respectively; and specifically, the master LSP is set to have the highest priority, which is set as master, and the priorities of the backup LSP1 and the backup LSP2 are set from high to low as backup 1 and backup 2.
>
> …
>
> 303. The state of the master LSP is detected, wherein if it is detected that the state of the master LSP is abnormal, step 304 is performed, and if it is detected that the state of the master LSP is not abnormal, step

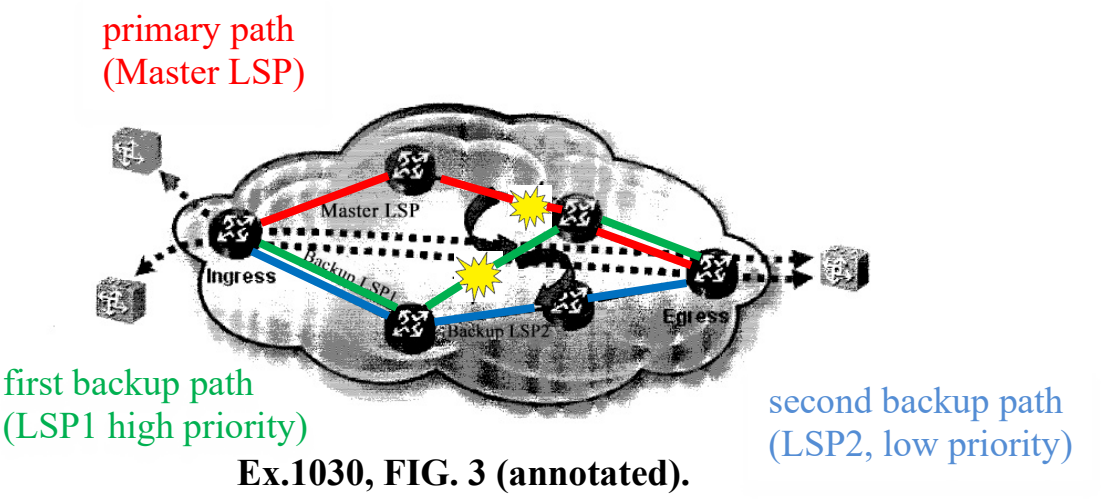
306 is performed. An abnormality in the state of the master LSP may be in, but not limited to, the following forms, including: link failure, data packet loss, transmission interruption, etc.; and there is no limitation for this in the embodiment of the present invention.

…

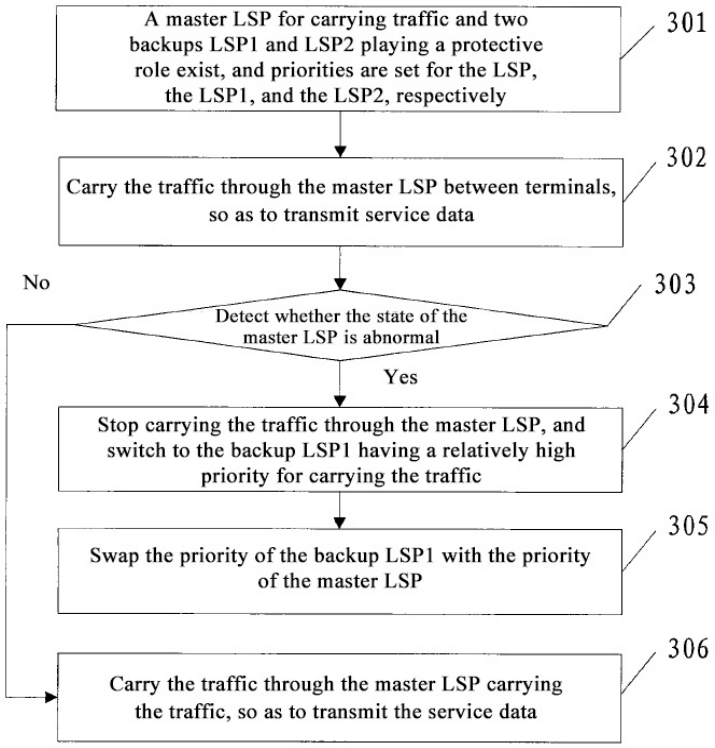
In the embodiment of the present invention, the priority level of the backup LSP1 is higher than the priority level of the backup LSP2, such that the link carrying the traffic is switched from the master LSP to the backup LSP1, and the backup LSP1 carrying the traffic transmits the service data.

If an abnormality also occurs in the high-priority backup LSP1, the link carrying the traffic is switched from the master LSP to the backup LSP2, that is, according to the priorities of the backup LSP1 and the backup LSP2, the traffic is switched to and carried through the normal backup path having a high priority.

Ex.1030, 6-7, FIGS. 3 and 4; *see also* Ex.1030, 9-10, FIGS. 5-6 (disclosing an additional embodiment that also has LSPs with different priorities).



Ex.1030, FIG. 3 (annotated).



Ex.1030, FIG. 4.

243. It would have been obvious to a POSITA to apply Li's teachings when implementing multiple backup paths, per EDC_525, such that failover sequence can be controlled by assigning each backup path a priority (i.e., with a higher priority backup being used first in case of failure and a lower priority backup used only after the highest priority path has also failed). Such an implementation would beneficially give greater control over path failover. Also, a POSITA would have been motivated to utilize Li's priority scheme teachings, when implementing two backup paths per EDC_525, because it would reduce the probability that a first backup path (which would be utilized when there is a primary path failure) is preempted by other paths. Additionally, a POSITA would have been motivated to

utilize Li's priority scheme for backup path selection, when implementing two backup paths per EDC_525, because it would allow for assigning a first backup path a higher priority when it has the same QoS as the primary path, thereby ensuring that the QoS is maintained even though failure has occurred. Yet another reason to combine the teachings of Li with EDC_525 is that the prioritizing scheme allows for using the priority levels of the different paths to minimize frequent switching when the master path is restored to a normal state. *See also* Reasons to Combine Li with EDC_525.

244. Furthermore, consistent with the analysis in Ground 1 element [1.0.2] and [1.2], EDC_525 teaches that the path computations may be performed at a central node. Ex.1005, [0025] ("…centrally…"); *see also* Ex.1005, [0042] ("…centralized…"). It would have been obvious to a POSITA implementing the combination of Li with EDC_525, when the path computations for the second backup path are performed centrally, for the central node to send a signal (e.g., setup signal, see Ground 1 element [1.6]) to the ingress node (point of local repair) that informs that a fully disjoint second backup path needs to be setup. It also would have been obvious to a POSITA, consistent with knowledge in the art, to include priority information so that the ingress node is informed about the backup path's priority and the sequence to use the backup paths in case the working path fails. *See, e.g.,* Ex. 1025, [0043]-[0044] ("…a FAST_REROUTE object used for setup of

a backup LSP for fast rerouting [includes]…. A Setup Priority field 200 contains a value representing priority of a backup LSP…A Holding Priority field 202…"); Ex.1019, 8-9 ("…The FAST_REROUTE object is used to control the backup used for the protected LSP. This specifies the setup and hold priorities."); Ex.1024, [0055] ("The Path message carries…establishment priority, hold priority…").

245. For example, the second backup path may have a lower QoS and therefore be given a lower priority than the first backup path (already established) and in the case that the working path fails, the first backup path would initially provide protection at the same QoS and the second backup path would be used only in the circumstance where the first backup path also fails. *See* Ex.1026, 7 ("Backup bandwidth protection allows you to give LSPs carrying certain kinds of data (such as voice) priority for using backup tunnels… Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained."); Ex.1021, 1:22-26 ("As the Internet becomes a multi-media communications medium that is expected to reliably handle voice and video traffic, network protocols must also evolve to support quality of-service (QoS) requirements."); Ex.1027, 6.

246. Thus, EDC_525 in combination with EDC_892, Hanif, and Li discloses transmitting a setup message from a central node to the ingress node that identifies that the fully disjoint second backup path has a lower priority than the

first backup path, which renders obvious "*signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP*," as claimed.

4. Claims 2-5

247. See analysis at Claim 1 Ground 2 and Claims 2-5 Ground 1.

5. Claim 6

248. Other than the below identified element, the remaining Claim 6 analysis in Ground 1 remains the same in Ground 2.

249. EDC_525 in combination with EDC_892, Hanif, and Li renders obvious "*signaling, to at least one other MPLS label switch router, said fully disjoint path as the Backup LSP to said Bypass LSP*" for the same reasons discussed above at Claim 1 Ground 2.

6. Claims 7-10

250. See analysis at Claim 6 Ground 2 and Claims 7-10 Ground 1.

IX. DECLARATION

251. I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code.

Dated: November 14, 2024

Henry H. Houh

_____

Henry H. Houh, Ph.D.