

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Juniper Networks, Inc.
Petitioner

v.

Brixham Solutions, LTD.
Patent Owner

Case IPR2014-00425

DECLARATION OF TAL LAVIAN, Ph.D.

I, Tal Lavian, declare as follows:

1. I have personal knowledge of the facts stated in this declaration, and could and would testify to these facts under oath if called upon to do so.

I. INTRODUCTION

2. I have been retained by counsel for Juniper Networks, Inc. (“Juniper”) in this case as an expert in the relevant art.

3. I submitted a declaration dated February 11, 2014 in support of Juniper’s initial Petition for Inter Partes review of U.S. Patent No. 7,940,652 to Ping Pan (“the ’652 patent”). *See* Ex. 1003.

4. On October 10, 2014, Patent Owner Brixham Solutions, Ltd. (“BSL”) filed its response to Juniper’s petition. I have been asked to provide additional opinions in response to BSL’s response that are relevant to Juniper’s reply. The opinions discussed herein are my own. In formulating these opinions, I have reviewed a variety of materials and made use of my own personal knowledge. The materials I have relied on in formulating my opinions are identified in this report and/or in the Appendix List that was submitted with my February 11, 2014 declaration.

5. I am being paid \$400 per hour in connection with my work in this case. My compensation is not contingent on my reaching any particular findings or conclusions, or any outcome of the case.

II. EXECUTIVE SUMMARY

6. In sum, my opinions are as follows:

7. *First*, the Challenged Claims are obvious over Hofmeister in view of RFC 3386 and Owens.

8. As the Board recognized, Hofmeister discloses each element of the independent claims, other than the context of network failure (which the Board determined was part of the construction for the term “determining whether to preempt existing traffic on the standby Pseudowire”).

9. The motivation to combine Hofmeister with RFC 3386 and Owens—which disclose the use of priorities and preemption in the context of network failure—is abundant. Indeed, Hofmeister itself explicitly notes that a key advantage of the disclosed Pseudowire network is that it can perform better during network failure and can take advantage of prior art protection techniques from SONET, MPLS, and other networks.

10. *Second*, the Challenged Claims are either anticipated by or obvious over Halabi alone. The Board only identified one element that was missing from Halabi—the preemption of traffic on a standby path during network failure. As described in detail below, there are several passages of Halabi that disclose this concept.

11. To the extent that the Board believes these disclosures are not directed to Pseudowires (and instead relate to MPLS or GMPLS techniques), it is my opinion that it would have been obvious to a person having ordinary skill in the art (“PHOSITA”) that the disclosed MPLS and GMPLS techniques could be used with Pseudowires. Indeed, the background section of the ’652 patent itself discusses MPLS protection techniques as applying to Pseudowires.

12. *Third*, even if there were a need to combine Halabi with RFC 3386 and Owens, the motivation to combine the references is abundant. Halabi specifically notes that one of the key reasons for using Pseudowire technology is to take advantage of the reliability (i.e., protection) and scalability features of IP and MPLS networks. Accordingly, a PHOSITA would be motivated to apply protection techniques from those networks (which include the use of setup/holding priorities to make decisions about preemption during network failure) with Pseudowires.

13. To help illustrate the arguments that are detailed below and in Juniper’s reply, I have created a set of slides which is attached as Appendix A to this declaration.

III. BACKGROUND AND QUALIFICATIONS

14. I possess the knowledge, skills, experience, training and the education to form an expert opinion and testimony in this case. A detailed record of my

professional qualifications and relevant experience, including a list of patents and academic and professional publications, is set forth in my declaration dated February 10, 2014, and the curriculum vitae attached to that declaration as Appendix 1. *See* Ex. 1003.

IV. BASIS FOR OPINION

15. My opinions and views set forth in this declaration are based on my education, training, and experience in the relevant field, as well as the materials I reviewed in this case, and the scientific knowledge regarding the same subject matter that existed prior to the effective filing date of the '652 patent. In addition, they are informed by the legal principles outlined in my February 10, 2014 declaration. Ex. 1003 at ¶¶ 30-50.

V. CLAIM CONSTRUCTION

16. I understand that, for purposes of the accompanying petition for *Inter Partes* Review of the '652 patent ("Petition"), the Challenged Claims must be given their broadest reasonable interpretations in light of the specification of the '652 patent.

17. I understand that the Board determined it was not necessary to construe the claim terms "priority" and "receiving a Pseudowire configuration acknowledgement." I further understand that the Board construed the following terms:

Term	Board's Construction
standby Pseudowire	an emulation of a native service over a network that is used in the event of network failure
determining whether to preempt existing traffic on the standby Pseudowire	determining during the event of a network failure whether to drop network traffic that is carried by the standby Pseudowire

VI. ROUSKAS DECLARATION

18. I have reviewed the declaration of Dr. George Rouskas, which was submitted in support of BSL's response. I disagree with Dr. Rouskas's opinions.

19. For example, Dr. Rouskas states “[g]iven the Hofmeister reference’s teachings regarding the inventive application of certain parameters to admission control, notwithstanding the use of those parameters in other technologies [], it would not be obvious to extend such parameters from the Hofmeister reference to Pseudowire protection in the event of network failure.” Dr. Rouskas does not provide any factual support for this opinion. Nor does he identify any difficulty that a PHOSITA might have combining Hofmeister with the context of network failure, or any passage from the prior art purportedly teaching away from the combination. Moreover, he ignores the express statements in Hofmeister that a key advantage of the claimed Pseudowire system is that it can react quickly during network failure and that it can take advantage of protection schemes used in other networks, such as SONET. I discuss these issues in further detail below. This is illustrated in slides 14-15, 20 and 21 of Appendix A.

20. As another example, Dr. Rouskas’s description of RFC 3386 and Owens is inaccurate and overlooks various relevant passages, which are discussed in further detail below. This is illustrated in slides 17-18 of Appendix A.

21. As another example, Dr. Rouskas claims “that the authors of the Halabi reference did not think to apply the priority attributes expressly to Pseudowires is compelling evidence that one of ordinary skill in the art reading Halabi would not have thought of such application either.” There is no support for Dr. Rouskas’s claim, which ignores the background section of the ’652 patent itself that discusses the applicability of MPLS protection techniques to Pseudowires.

22. As another example, Dr. Rouskas provides no support for his conclusion that a PHOSITA would not be motivated to combine Hofmeister or Halabi with RFC 3386/Owens. As I explain below, the facts of this case demonstrate the exact opposite—there are many independent reasons that a PHOSITA would be motivated to combine the references.

VII. INVALIDITY OF THE CHALLENGED CLAIMS

A. Hofmeister in view of RFC 3386 and Owens renders the Challenged Claims of the ’652 patent obvious under § 103.

23. It is my understanding that the Board found—and Patent Owner does not dispute—that Hofmeister anticipates every limitation of the ’652 patent, other than the element of “*determining whether to preempt existing traffic on the standby*”

Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire.”

24. I further understand that the Board found that Hofmeister disclosed every aspect of the “determining whether to preempt existing traffic on the standby Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire” element other than the “context of network failure.”

25. In other words, the Board found that Hofmeister discloses “determining whether to preempt existing traffic on the standby Pseudowire” based on the priority for the standby Pseudowire in the context of network admission, but construed this term to require preemption *during a network failure*, and thus found that the context of a network failure was missing from Hofmeister. However, the Board determined that RFC 3386 and Owens disclosed the use of priorities and preemption in the context of network failure, and thus the combination of Hofmeister with RFC 3386 and Owens renders the claims obvious under § 103.

26. I agree with the Board that the combination of Hofmeister with RFC 3386 and Owens renders the Challenged Claims obvious.

Hofmeister

27. Hofmeister teaches a detailed method for signaling and managing Pseudowires over a SONET backbone. Ex. 1004 (Hofmeister) at Abstract, [0086]. Specifically, Hofmeister discloses that each Pseudowire is assigned “Setup

Priority” and “Holding Priority” attributes during the signaling process. These priority attributes are used to make decisions about whether a Pseudowire can preempt other Pseudowires, as well as whether the Pseudowire can be preempted by other Pseudowires. *Id.* at [0405]-[0408]. More specifically, Hofmeister provides a detailed explanation of how the “Setup Priority” and “Holding Priority” can be used with a preemption algorithm to make decisions about which Pseudowires are admitted to the network and whether or not to preempt existing Pseudowires to allow the admission of a new Pseudowire. In this respect, Hofmeister discloses “preempting existing traffic” in the context of network admission.

28. Hofmeister expressly notes that the disclosed invention “leverages [] conventional technologies” drawn from IETF Internet Drafts and RFCs, including the Martini draft regarding PWs (*id.* at [0010]), the Swallow draft regarding RSVP-TE for Fast-Reroute (*id.* at [0014]), and other technologies such as MPLS, OIF UNI, Virtual Concatenation, LCAS and GFP (*id.* at [0016]). Hofmeister further states that it utilizes configuration parameters from conventional IETF industry standards, such as CIR (RFC 2697/2698), Traffic Class (RFC 2475 on Internet DiffServ), and Setup/Holding Priorities (multiple RFCs regarding RSVP-TE protocol for MPLS). *Id.* at [0296]; *see also* App. 11 (RFC 2697); App. 12 (RFC 2698); App. 13 (RFC 2475); App. 9 (RFC 3209); App. 14 (RFC 4090).

29. In addition, Hofmeister notes that a key benefit of the claimed Pseudowire network is that it can take advantage of the “rich set of features for network resource allocation, traffic *restoration*, and link *protection*” (Ex. 1004 (Hofmeister) at [0257] (emphasis added)). Hofmeister explains that “[s]ince control messages traverse the same optical connections that data flows will traverse, it is easier and faster for the edge nodes to react to *network failures*” the invention is advantageous because it allows “*protection* mechanisms” to be “triggered much faster thereby preventing data loss” (*id.* at [0134], [0137] (emphasis added)). With respect to some of the disclosed embodiments, Hofmeister notes that it would be desirable to direct traffic to a **backup link**. *Id.* at [0397] (“direct existing traffic to a backup link (*e.g.* such as using protection bandwidth triggered via a conventional APS (automatic protection switch) protocol for SONET/SDH traffic”). Thus, Hofmeister expressly contemplates that prior art protection techniques can and should be used in combination with the claimed Pseudowire environment. This is illustrated in slides 14-15 of Appendix A.

30. Given that Hofmeister *explicitly suggests* that the claimed Pseudowire network can be implemented with legacy techniques for protecting data during network failure, it would have been obvious and natural for one of skill in the art to implement Hofmeister in combination with various well-known protection techniques.

RFC 3386 and Owens

31. Given that a number of the concepts in Hofmeister are drawn from IETF publications (see above), an obvious place to look for such protection techniques would be in IETF publications. RFC 3386 was published by the IETF. It describes various configuration parameters that can be used to provide traffic protection during network failure in a wide range of networks, including SONET, MPLS, GMPLS, and Pseudowire environments.

32. The protection techniques described in RFC 3386 *were widely-known* and utilized by the industry at the time of the Hofmeister patent. As a specific example of this, Owens (entitled “Protection/Restoration of MPLS Networks”) is a patent that was filed by a group of engineers from Tellabs who were involved in the IETF. It provides a more detailed description of how the protection techniques in RFC 3386 can be applied to an MPLS environment. For example, Owens teaches that, in an MPLS network, “a working path carries data from a starting point or node to a destination point or node via a working path MPLS system reliability is enhanced by way of a protection path, over which data can be carried from the starting point to the destination point upon a detected failure along the working path.” Ex. 1006 (Owens) at Abstract.

33. Owens also describes various specific protection features in greater detail. For example, Owens teaches that the protection path can be configured

using “dynamic” protection (which is akin to the “cold” mode discussed in the ’652 patent) or “pre-negotiated” protection (which is akin to the “hot” or “warm” mode discussed in the ’652 patent). *Id.* at 5:1-29. Owens also discloses various “protection modes,” such as revertive or non-revertive, as well as a number of “protection switching options, such as “1+1 protection,” and “1:1, 1:n and n:m Protection.” *Id.* at 6:16 – 7:15.

34. RFC 3386 discloses “preempting existing traffic” based on the “relative priority” assigned to the Pseudowire in the context of a network failure. Ex. 1005 (RFC 3386) at § 2.2.2 (“Extra traffic, also referred to as preemptable traffic, is the traffic carried over the protection entity while the working entity is active. Extra traffic is not protected, *i.e.*, ***when the protection entity is required to protect the traffic that is being carried over the working entity, the extra traffic is preempted.***”); § 2.3 (“In the 1:n protection architecture . . . [w]hen multiple working entities have failed simultaneously, only one of them can be restored by the common protection entity. This contention could be resolved by ***assigning a different preemptive priority*** to each working entity.”). (Emphasis added.)

35. RFC 3386 further discloses that priorities should be assigned to both working and protection connections. Ex. 1005 (RFC 3386) at § 3.2.1 (“There should be the ability to maintain relative restoration priorities between working and protection connections . . . Some distinction between working and protection

connections is likely, either through explicit objects, or preferably through implicit methods such as general classes or *priorities*.”). (Emphasis added.) This is illustrated in slides 17-18 of Appendix A.

36. Owens also discloses “preempting existing traffic on a standby” based on a “priority” in the context of network failure. For example, Owens teaches that, in a 1+1 protection scheme, the backup path “could be used to transmit *an exact copy of the working traffic*, with a *selection between the traffic* on the working and protection paths being made at the PML.” App. 15 (Owens) at 6:56-59 (emphasis added). Owens further teaches that, in a 1:1 protection scheme, “the working traffic normally travels only on the working path, and is switched to the protection path only when the working entity is unavailable. *Once the protection switch is initiated, all the low priority traffic being carried on the protection path is discarded to free resources for the working traffic.*” *Id.* at 7:1-6 (emphasis added); *see also* 5:23-29; 1:34-36 (“[A] protection priority could be used as a differentiating mechanism for premium services.”).

Motivations to Combine

37. Given the prominence of the protection methods discussed in RFC 3386 and Owens, and their close relationship to the protocols from which the Hofmeister invention explicitly derives, it would have been obvious to apply the

protection techniques and parameters described in RFC 3386 and Owens to the specific Pseudowire environment described by Hofmeister.

38. Indeed, because Hofmeister already discloses assigning relative priorities (Setup/Holding) to a Pseudowire during configuration (which are the same examples of “priority” discussed in the ’652 specification), it would have been an obvious and predictable step for a PHOSITA to use those priorities to make decisions about Pseudowire preemption during a network failure, as taught by RFC 3386 and Owens, and as commonly done in other types of data networks.

39. Moreover, it is my opinion that a PHOSITA would have been motivated to combine Hofmeister with RFC 3386 and/or Owens, as evidenced by the fact that the combination falls within several of the “Exemplary Rationales” identified by the Supreme Court in the *KSR* case and outlined in the Manual of Patent Examining Procedure, which were identified and explained to me by counsel. In this case, “Exemplary Rationales” A, C, D and G are the most relevant. I discuss them in turn below.

Rationale A

40. It would have been obvious to combine Hofmeister with the context of network failure described in RFC 3386 and Owens because it would merely involve “[c]ombining prior art elements according to known methods to yield predictable results.” MPEP § 2143(I).

41. As noted above, Hofmeister discloses a Pseudowire system where each Pseudowire is assigned a Setup and Holding Priority, and those priorities are used to make preemption decisions during network admission.

42. Also as noted above, RFC 3386/Owens disclose the element of using priority attributes and preempting lower priority traffic during a network failure to protect higher priority traffic according to a 1+1, 1:1, 1:n, or m:n scheme.

43. It would have been straightforward for a PHOSITA to combine these prior art elements—namely, (1) the Pseudowire system from Hofmeister where each Pseudowire is assigned a Setup and Holding Priority, and (2) the context of network protection using various protection schemes that employ priorities and preemption from RFC 3386 and Owens—using known methods for network design to yield the predictable result of a data network with robust and efficient protection that takes into account the priority of the different traffic when making decisions about how to allocate network resources. This is illustrated in slide [x] of Appendix A.

44. This is particularly true because Setup and Holding Priority attributes were commonly used by network designers in other systems to make decisions about preemption during network failure.

45. For example, Halabi—a book that summarizes the state of the art in the areas of MPLS, Pseudowires, and other similar data networks—notes that

“[t]he SESSION_ATTRIBUTE object allows RSVP-TE to set different LSP priorities, preemption, and fast-reroute features. *These are used to select alternate LSPs in case of a failure in the network.* The SESSION_ATTRIBUTE . . . includes fields such as Setup Priority and Holding Priority, which affect whether this session can preempt or can be preempted by other sessions.” Ex. 1008 (Halabi) at 144. Halabi’s description of Setup Priority and Holding Priority as attributes that could be used to select alternate paths in the event of a network failure is representative of the general understanding and use of these attributes in the industry at the time of the ’652 patent, thus evidencing that a PHOSITA would have been motivated to combine the priority and preemption techniques of Hofmeister with the context of network failure.

46. Indeed, in such a combination, the Setup and Holding Priorities would continue to perform their function of dictating decisions about finite network resource allocation, and the underlying concept of network protection would continue to protect data and provide redundancy in the event of a failure. This is illustrated in slide 27 of Appendix A.

Rationale C

47. It also would have been obvious for the network environment disclosed in Hofmeister to employ the protection techniques in the context of network failure described in RFC 3386 and Owens because the combination would

have involved nothing more than the “*use of a known technique to improve similar devices (methods, or products) in the same way.*” MPEP § 2143(I).

48. RFC 3386 describes various configuration parameters for providing traffic protection applicable to several types of networks, including SONET, MPLS, GMPLS, and PW. These protection techniques were well-known and commonly utilized by the networking industry at the time of Hofmeister. Owens, for example, is a detailed application of RFC 3386 to the MPLS environment.

49. It was also *well-known* at the time that protection concepts applicable to MPLS environments mapped easily to PW environments.

50. It would have been *straightforward* for a PHOSITA to improve the particular PW environment described in Hofmeister (a PW network that uses Setup and Holding Priority attributes to make admission decisions) using the *well-known protection techniques* in RFC 3386 and Owens (which teach the use of priority attributes to make preemption decisions during network failure) in the same way that those techniques improve other types of data networks. More specifically, it would have been nothing more than the use of the well-known preemption and priority attribute techniques from RFC 3386/Owens to improve the Pseudowire environment in Hofmeister in the same way—i.e., by providing an efficient and robust way to protect the data network while still achieving high utilization.

51. Indeed, the improvement to Hofmeister would be identical to the improvement that those protection techniques offer to other types of networks—i.e., increased efficiency during network failure via service differentiation and prioritization. This is illustrated in slide 27 of Appendix A.

Rationale D

52. It would have been obvious to apply the protection techniques in the context of network failure described in RFC 3386 and Owens to the Hofmeister Pseudowire system to provide protection during a network failure because it would merely be “*applying a known technique to a known device (method, or product) ready for improvement to yield predictable results.*” MPEP § 2143(I) (emphasis added).

53. BSL has claimed to improve upon prior art networks by using the Setup Priority and Holding Priority attributes to make determinations about whether to preempt traffic on a standby PW during a network failure. But the use of Setup and Holding Priorities to manage decisions during a network failure in various network environments (including MPLS networks) had been known for years. *See, e.g.*, Ex. 1008 (Halabi) at 144.

54. Moreover, the Hofmeister Pseudowire network was ready for improvement, as evidenced by the express statements in Hofmeister that one of the key advantages of the claimed invention is that it can take advantage of the prior

art protection techniques used to address network failure. Ex. 1004 (Hofmeister) at [0137] and [0257]).

55. As such, a PHOSITA would have recognized that applying the known protection techniques of RFC 3386 and Owens to the particular Pseudowire network of Hofmeister would have yielded predictable results (an efficient process to deal with network failures) to improve Hofmeister. This is illustrated in slide 29 of Appendix A.

Rationale G

56. It would have been obvious to combine Hofmeister with RFC 3386 and/or Owens because there were “*teaching[s], suggestion[s], or motivation[s] in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.*” MPEP § 2143(I) (emphasis added).

57. Specifically, those designing network environments at the time of the ’652 patent recognized that it was crucial for data networks to incorporate a mechanism for protecting data during network failure events and therefore **almost every network designer would incorporate** some type of data protection when building a network. This is the normal and expected way to design a network in almost every large network.

58. In addition, Hofmeister and Owens teach this feature. *See, e.g.*, Ex. 1004 (Hofmeister) at [0137] (noting that a key advantage of the invention is that “protection mechanisms can be triggered much faster thereby preventing data loss”); Ex. 1006 (Owens) at 1:33-35 (“It is imperative that MPLS be able to provide protection and restoration of traffic.”).

59. Furthermore, network designers recognized the need to balance fast recovery times with better resource utilization when implementing protection mechanisms. *See, e.g.*, Ex. 1005 (RFC 3386) at § 2.3 (noting trade-offs between protection and restoration techniques, and describing the spectrum of techniques). Moreover, the industry recognized that network user needs vary such that some users (e.g., those transmitting mission critical data) might be willing to pay more for a premium service with more bandwidth and better redundancy/protection, whereas other users may want to pay less for a network with greater utilization with less robust protection. *See, e.g.*, Ex. 1006 (Owens) at 1:34-36 (noting that a “protection priority” could be used as a “differentiating mechanism for premium services that require high reliability”).

60. Thus, in order to allow greater control of and differentiation between network resources to accomplish these goals, **it was common** for networks to employ “SESSION_ATTRIBUTE” Objects, such as the Setup and Holding Priority attributes described by Hofmeister.

61. While Hofmeister focuses on the use of the Setup Priority and Holding Priority attributes in the context of network admission, these very same attributes were commonly used by network designers to make decisions about preemption during network failures, as well. *See, e.g.*, Ex. 1008 (Halabi) at 144 (noting that Setup and Holding Priority can be “used to select alternate LSPs in case of a failure in the network” and “affect whether this session can preempt or be preempted by other sessions”).

62. Moreover, Hofmeister notes that the disclosed invention “leverages [] conventional technologies” and utilizes configuration parameters from IETF Internet Drafts, RFCs, and standards. Ex. 1003 (Hofmeister) at [0010], [0014], [0016], [0296].

63. Given this body of teaching in the prior art, the historical use of Setup and Holding Priorities to make preemption decisions during network failure, and the incorporation of numerous other concepts from IETF documents, it would have been a natural fit and a predictable step for a PHOSITA to use the Setup and Holding Priorities described in Hofmeister to make preemption decisions during network failure, just as those particular priorities had been used in other, related network environments (e.g., MPLS, martini PW, etc.) and other IETF documents, including RFC 3386.

64. A PHOSITA would have been particularly motivated to combine the Setup and Holding Priority of Hofmeister with the context of network failure because an express goal of Hofmeister is to take better advantage of the available and well-known protection mechanisms, such as those described in RFC 3386/Owens. This is illustrated in slides [x-y] of Appendix A.

65. In fact, it would have been highly inefficient and unusual *not* to use the Setup Priority and the Holding Priority to make determinations about preemption during a network failure.

66. Given the costs of running a network, service providers are motivated to make sure that the network is utilized in the most efficient way. As a result, market forces generally cause service providers to ensure that no parts of a network are idle and that all resources and bandwidth are being used as much as possible at any one time. It is and was common practice for service providers to over-subscribe a network.

67. Because of this, the use of backup paths for “extra” or “low priority” traffic is and was commonplace and “preempting existing traffic” when there is a failure or when the network is or was oversubscribed is the most reasonable and efficient way to operate the network.

68. Another factor that supports a motivation to combine Hofmeister with RFC 3386 and Owens is that all of these references were authored by members of

the tight-knit IETF community, which was working together to create industry standards and advance the industry's knowledge base regarding data networks. For example, RFC 3386 was drafted by IETF members from the service provider side (*i.e.*, W. Lai of AT&T and D. McDysan of Worldcom) and Hofmeister and Owens were drafted by members from the network product provider side (Tad Hofmeister and Ping Pan of CIENA Corp. and K. Owens, S. Makan, C. Huang, and V. Sharma of Tellabs).

69. Because these IETF members were working together on a regular basis and coordinating to provide consumers a complete networking solution, it would have been natural for those skilled in the art to look at and consider the entire body of IETF publications when reviewing and considering concepts related to Pseudowires, including RFC 3386 and Owens.

70. This is illustrated in slide 31 of Appendix A.

B. Halabi and/or Halabi in view of RFC 3386 and Owens renders the Challenged Claims obvious under 35 U.S.C. § 103.

71. It is my understanding that the Board found—and Patent Owner does not dispute—that Halabi anticipates every limitation of the '652 patent, other than the element of “*determining whether to preempt existing traffic on the standby Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire.*”

72. I further understand that the Board found that Halabi discloses every aspect of the disputed limitation other than “the context of preemption of traffic on a standby path during network failure,” but that this aspect is disclosed by RFC 3386 and Owens. Based on BSL’s response to the Board’s decision, it appears that **BSL’s only argument is that there is no motivation to combine Halabi.**

73. In my opinion, Halabi actually does disclose “the context of preemption of traffic on a standby path during network failure.”

74. Halabi is a part of the Cisco Press series of books, which includes a variety of industry text books and treatises that summarize the state of the art on particular topics. The Cisco Press books generally discuss mainstream topics that are part of the curriculum for networking classes and used also as study guides for

Cisco Certifications. The Cisco Press books are also used by engineers who use Cisco products to learn about the available features and configuration options.

75. Halabi discusses the adoption of Metro Ethernet services, as well as how those services have led carriers to deliver Metro Data Services. The book delves into the role of virtual private networks (VPN), virtual private local area networks (VLAN), virtual private LAN services (VPLS), traffic engineering, and MPLS and Generalized MPLS (GMPLS) in the Metro Ethernet.

76. More specifically, the book examines the concepts of Virtual Private LAN Service (VPLS), SONET/SDH, Resilient Packet Ring (RPR), Pseudowire concept, Pseudowire via Layer 2 Tunneling Protocol (L2TP), Ethernet transport, and Ethernet over MPLS (“Draft Martini”).

77. It also covers various issues pertaining to the configuration and protection of hybrid Layer 2/Layer 3 IP/MPLS networks, along with the emulation of Layer 2 Ethernet services over MPLS networks, and the emulation of Layer 2 VPN over an IP network. This emulation of native services over a packet-switched network is also referred to as a “Pseudowire” environment.

78. Halabi also contains specific chapters that cover the concepts of RSVP-TE (RSVP signaling for traffic engineering) and MPLS Fast-Reroute, which were well-known techniques that allowed for greater control of network set-up and operation (as described above).

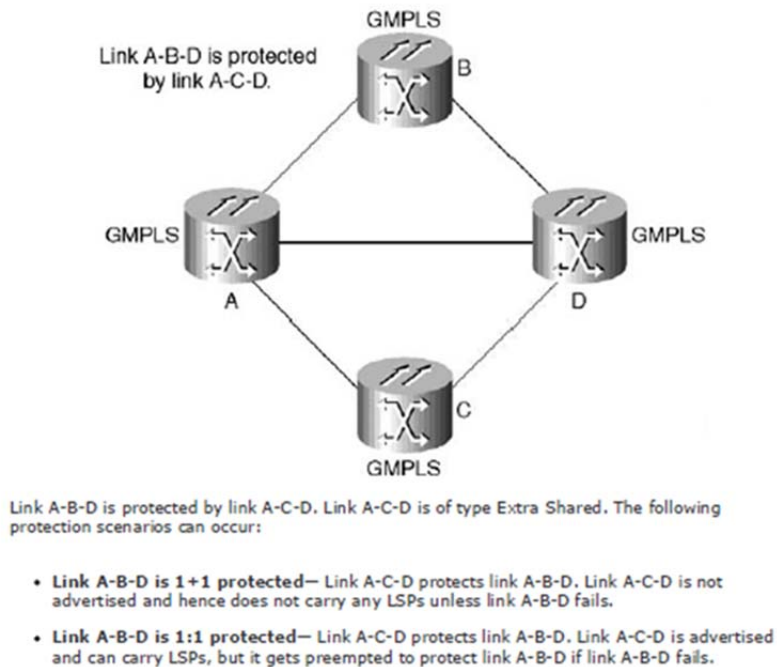
79. Halabi also covers the topic of Generalized MPLS (GMPLS), which is a protocol that allows various additional network resources (e.g., SONET, SDH, DWDM, and optical fibers) to be sent over an MPLS-like backbone.

80. Halabi is rich with information regarding MPLS, Pseudowires, and various protection techniques. Indeed, the book is a summary of approximately 3-5 years of mainstream knowledge in the field, referencing RFC documents, industry publications, Metro Ethernet Forum, IETF, ITU, and ETSI references related to Metro Ethernet.

81. Throughout Halabi, there are several disclosures of “the context of preemption of traffic on a standby path during network failure” that the Board found to be missing from Halabi. For example, Halabi teaches that “[t]he resources allocated for a secondary [Label Switched Path “LSP”] may be used by other LSPs until the primary LSP ***fails over*** to the secondary LSP. At that point, any set of LSPs that are using the resources for the secondary LSP must be ***preempted***.” Ex. 1008 (Halabi) at 184 (emphasis added). This is illustrated in slide 35 of Appendix A.

82. Halabi also teaches a number of “different link protection types,” including an “Extra Traffic” link that “protects another link or links” where “[i]n case of failure of the protected links, all LSPs on this link are lost” and a “Dedicated 1:1” link that is “protected by a disjoint link of the type Extra Traffic.”

Id. at 174. This implementation is depicted in Figure 8.5 and also illustrated in slides 36-37 of Appendix A:



83. As a result, as originally noted in my February 11, 2014 declaration, it is my opinion that Halabi alone either anticipates the Challenged Claims or renders them obvious under § 103.

84. Even if there were a need to combine Halabi with RFC 3386 or Owens, however, it is my opinion that a PHOSITA would have been motivated to combine these references for a multitude of reasons.

85. For example, Halabi teaches that the whole point of employing Pseudowire technology is to allow native Layer 2 services to take advantage of the scalability and **reliability** (that is, protection) mechanisms of MPLS: “hybrid

Layer 2 (L2) and Layer 3 (L3) IP and MPLS networks [*i.e.*, Pseudowire networks] have emerged as a solution that marries Ethernet’s simplicity and cost effectiveness” with the “scalability and **reliability**” that “exist only in IP and Multiprotocol Label Switching (MPLS) control planes.” Ex. 1008 (Halabi) at xv (emphasis added). Thus, combining Halabi with RFC 3386 and Owens is not only obvious, but also specifically encouraged by Halabi.

86. To the extent that BSL is arguing that Halabi’s disclosure of priority and preemption attributes are limited to LSPs and it would not be obvious to apply these concepts to Pseudowires, this ignores Halabi’s express teaching that the whole point of Pseudowires is to take advantage of the traffic engineering techniques available in an MPLS network (including those that pertain to reliability/protection). Ex. 1008 (Halabi) at xv. This is illustrated in slide 38 of Appendix A.

87. It is also contrary to the ’652 patent itself, which acknowledges that it is obvious to apply protection schemes from MPLS/LSP to Pseudowires in that it describes the existing protection methods for Pseudowires as including “MPLS Fast Reroute.” Ex. 1001 (’652 patent) at 1:49-64 (discussing prior art MPLS protection schemes as being applicable to PWs); 3:14-37 (noting that LSP protocols can be used to set up PWs); 6:20-30 (“In a system implementing a 1:1 protection scheme, one Pseudowire is used to protect another Pseudowire.

Similarly, a 1:N system (e.g. **MPLS Facility Backup**), one Pseudowire is used to protect N other Pseudowires, and not in a M:N system M Pseudowires are used to protect N other Pseudowires. This is illustrated in slide 39 of Appendix A.

88. Moreover, the Examiner found in the original prosecution of the '652 patent that, at the time of the invention, it would have been obvious to a PHOSITA to apply the protection/restoration mechanisms used in the context of MPLS and/or GMPLS to a Pseudowire environment because both MPLS/GMPLS and Pseudowire are in the narrow field of point-to-point virtual links. I agree with the Examiner that this would be an obvious and predictable combination. I also note that the Patent Owner did not contest that combining MPLS/GMPLS protection/restoration mechanisms with Pseudowire and Pseudowire protection concepts was obvious when traversing the Examiner's rejection of the claims that ultimately issued as claims 1, 9 and 14. Ex. 1002 (File History) at 113-15, 106-07, 103-04, 90-93.

89. The close connection between MPLS and Pseudowire is further evidenced by the fact that concepts pertaining to MPLS/GMPLS and Pseudowire are all described in the same *Metro Ethernet* book. Moreover, the whole point of Halabi is to discuss concepts, protocols, and traffic engineering techniques that will allow consistency and resiliency in hybrid Layer 2 and Layer 3 networks that use Pseudowire, which Halabi teaches are necessary to deploy Ethernet in the Metro.

90. And, Halabi itself notes that “[w]hen traffic moves from one site to another across the carrier’s backbone [via PW], it follows the MPLS label switched path (LSP) assigned for that traffic . . . *the LSP could be traffic-engineered* . . . many mechanisms can be used for traffic rerouting in case of failure.” Ex. 1008 (Halabi) at 80 (emphasis added). Thus, Halabi itself expressly contemplates that the disclosed MPLS and GMPLS traffic engineering techniques (**including preemption and priority**) can be used in connection with Pseudowire protection, not just LSP tunnel protection. *Id.*

91. In addition, there are numerous independent reasons that a PHOSITA would be motivated to combine Halabi with RFC 3386 or Owens. In particular, the combination would fall within a number of “Exemplary Rationales” that are outlined in the MPEP.

Rationale A

92. It would have been obvious to combine Halabi with RFC 3386 and Owens because it would merely involve “[c]ombining prior art elements according to known methods to yield predictable results.” MPEP § 2143(I).

93. As noted above, Halabi discloses a Pseudowire system that includes a primary Pseudowire that is protected by a secondary Pseudowire. It also discloses the use of priority and preemption attributes, Setup/Holding priorities, and a variety of protection schemes. Also as noted above, RFC 3386/Owens disclose the

element of using priority attributes and preempting lower priority traffic during a network failure to protect higher priority traffic according to a 1+1, 1:1, 1:n, or m:n scheme. It would have been straightforward for a PHOSITA to combine these prior art elements using a known method for network design to yield the predictable result of a data network with robust and efficient protection that takes into account the priority of the different traffic when making decisions about how to allocate network resources.

94. This is illustrated in slide 42 of Appendix A.

Rationale C

95. It also would have been obvious for the network environment disclosed in Halabi to employ the protection techniques described in RFC 3386 and Owens because the combination would have involved nothing more than the “*use of a known technique to improve similar devices (methods, or products) in the same way.*” MPEP § 2143(I).

96. It would have been straightforward for a PHOSITA to improve the particular network environments described in Halabi (a Pseudowire network with a primary/backup protection scheme, priority and preemption attributes, Setup/Holding priorities, and the preemption of extra traffic on a backup when there is a failure) with the well-known protection techniques in RFC 3386 and Owens (which teach the use of priority attributes to make preemption decisions

during network failure) in the same way that those techniques improve other types of data networks.

97. Indeed, the improvement to Halabi would be **identical** to the improvement that those protection techniques offer to other types of networks—i.e., increased efficiency during network failure via service differentiation and prioritization.

98. This is illustrated in slide 44 of Appendix A.

Rationale D

99. It would have been obvious to apply the protection techniques described in RFC 3386 and Owens to the network environments disclosed in Halabi to provide protection during a network failure because it would merely be “*applying a known technique to a known device (method, or product) ready for improvement to yield predictable results.*” MPEP § 2143(I).

100. BSL has claimed to improve upon prior art networks by using the Setup Priority and Holding Priority attributes to make determinations about whether to preempt traffic on a standby Pseudowire during a network failure. But the use of Setup and Holding Priorities to manage decisions during a network failure in various network environments (including MPLS networks) had been known for years. *See, e.g.,* Ex. 1008 (Halabi) at 144.

101. Moreover, the Halabi Pseudowire network was ready for improvement, as evidenced by the express statements in Halabi that a key purpose of Pseudowires is to take advantage of the rich set of scalability and reliability (i.e., protection) mechanisms that are available to MPLS networks.

102. As such, a PHOSITA would have recognized that applying the known protection techniques of RFC 3386 and Owens to the particular Pseudowire network described in Halabi would have yielded predictable results (an efficient process to deal with network failures) to improve Halabi.

103. This is illustrated in slide 46 of Appendix A.

Rationale G

104. It would have been obvious to combine Halabi with RFC 3386 and/or Owens because there were *“teaching[s], suggestion[s], or motivation[s] in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.”* MPEP § 2143(I) (emphasis added).

105. Specifically, those designing network environments at the time of the '652 patent recognized that it was crucial for data networks to incorporate a mechanism for protecting data during network failure events and therefore almost every network designer would incorporate some type of data protection when

building a network. *See, e.g.*, Ex. 1006 (Owens) at 1:33-35 (“It is imperative that MPLS be able to provide protection and restoration of traffic.”).

106. In addition, network designers recognized the need to balance fast recovery times with better resource utilization when implementing protection mechanisms. *See, e.g.*, Ex. 1005 (RFC 3386) at § 2.3 (noting trade-offs between protection and restoration techniques, and describing the spectrum of techniques). Moreover, the industry recognized that network user needs vary such that some users (e.g., those transmitting mission critical data) might be willing to pay more for a premium service with more bandwidth and better redundancy/protection, whereas other users may want to pay less for a network with greater utilization with less robust protection. *See, e.g.*, Ex. 1006 (Owens) at 1:34-36 (noting that a “protection priority” could be used as a “differentiating mechanism for premium services that require high reliability”).

107. Thus, in order to allow greater control of and differentiation between network resources to accomplish these goals, it was common for networks to employ “SESSION_ATTRIBUTE” Objects, such as the Setup and Holding Priority attributes described by Halabi.

108. Given this body of teaching in the prior art, it would have been a natural fit and a predictable step for a PHOSITA to combine Halabi with RFC 3386 and Owens to include any element that is allegedly missing from Halabi.

109. The close relationship between Halabi and the prior art is illustrated in slide 48 of Appendix A.

110. Based on BSL's response to the Board's decision, it appears that BSL's only argument is that there is no motivation to combine Halabi with RFC 3386 and Owens. The above paragraphs show many motivations to combine.

111. In sum, because Halabi already generally teaches the concepts of preemption of existing traffic (*see, e.g.*, Ex. 1008 (Halabi) at 128 (discussing preemption attribute); 175 (noting that in 1:1 protection, the protection link "gets preempted to protect [the primary link if it fails]"), as well as assigning relative priorities (*id.* at 128 (discussing priority attribute); 144-145 (discussing Setup/Holding Priorities)), it would have been an obvious and predictable step to use those priorities to make decisions about preemption during a network failure and to preempt existing traffic on the standby path, as taught by RFC 3386 and Owens.

VIII. CONCLUSION

For the reasons stated herein, it is my opinion that the Challenged Claims of the '652 patent are anticipated or obvious. This declaration is based on my present assessment of materials and information currently available to me. My investigation and assessment may continue, which may include reviewing documents and other information that may yet be made available to me.

Accordingly, I expressly reserve the right to continue my study in connection with this case and to expand or modify my opinions and conclusions as my study continues.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Respectfully submitted,

Dated: 12/18/2014

By: Tal Lavian
TAL LAVIAN, Ph.D.

APPENDIX A

Juniper Networks, Inc. v. Brixham Solutions Ltd., IPR 2014-00425

'652 Patent

JUNIPER[®]
NETWORKS

Overview

1

'652 Patent

2

Claim Construction

3


Invalidity

- **Hofmeister in view of RFC 3386/Owens**
- **Halabi**
- **Halabi in view of RFC 3386/Owens**

JUNIPER
NETWORKS

The '652 Patent

The '652 Patent



US007940652B1

(12) **United States Patent**
Pan

(10) **Patent No.:** US 7,940,652 B1
(45) **Date of Patent:** May 10, 2011

(54) **PSEUDOWIRE PROTECTION USING A STANDBY PSEUDOWIRE**

(75) Inventor: **Ping Pan**, San Jose, CA (US)

(73) Assignee: **Brixham Solutions Ltd.**, Tortola (VG)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 861 days.

(21) Appl. No.: **11/054,569**

(22) Filed: **Feb. 14, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/653,065, filed on Feb. 14, 2005.

(51) **Int. Cl.** *H04L 3/14* (2006.01)

(52) **U.S. Cl.** 370/228; 370/216; 370/225; 709/220

(58) **Field of Classification Search** 370/216, 370/225, 228; 709/220
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,920,705 A	7/1999	Lyon et al.
6,167,051 A	12/2000	Nagami et al.
6,347,088 B1	2/2002	Katou et al.
6,430,184 B1	8/2002	Robins et al.
6,546,427 B1	4/2003	Eklach
6,574,477 B1*	6/2003	Rathunde 455/453
6,621,793 B2	9/2003	Walgren et al.
6,665,273 B1	12/2003	Geogon et al.
6,680,943 B1	1/2004	Gibson et al.
6,751,684 B2	6/2004	Owen et al.
6,813,271 B1	11/2004	Cable
6,845,380 B1	1/2005	Sen et al.
6,985,488 B2	1/2006	Pan et al.
7,050,206 B1	5/2006	Cohen et al.
7,206,104 B2*	4/2007	Salch et al. 370/216

OTHER PUBLICATIONS

Ziyang Chen: "The LSP Protection/Restoration Mechanism in GMPLS," Internet Draft (Online) Oct. 2002 (Oct. 1, 2002), XP00223952 Retrieved from the internet URL: <http://www.ietf.org/wotawa.ca/~bochmann/dsrg/PublicDocuments/Master-theses/Chen,%20Ziyang%20-%20-%202002.pdf>.

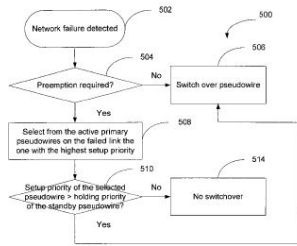
(Continued)

Primary Examiner — William Trost, IV
Assistant Examiner — Siming Liu

(57) **ABSTRACT**

Providing protection to network traffic includes sending a Pseudowire protection configuration parameter for configuring a standby Pseudowire between a source node and a destination node, receiving a Pseudowire configuration acknowledgment indicating whether the Pseudowire protection configuration parameter has been accepted by the destination node, and in the event that the Pseudowire protection configuration parameter has been accepted by the destination node, using the standby Pseudowire, wherein the standby Pseudowire is configured based at least in part on the Pseudowire protection configuration parameter.

17 Claims, 7 Drawing Sheets



JUNIPER
Exhibit 1001-1

Title: Psuedowire Protection Using a Standby Psuedowire

Priority Date: February 14, 2006

Challenged Claims: 1-5, 8-11, 13-15, 17

'652 Patent

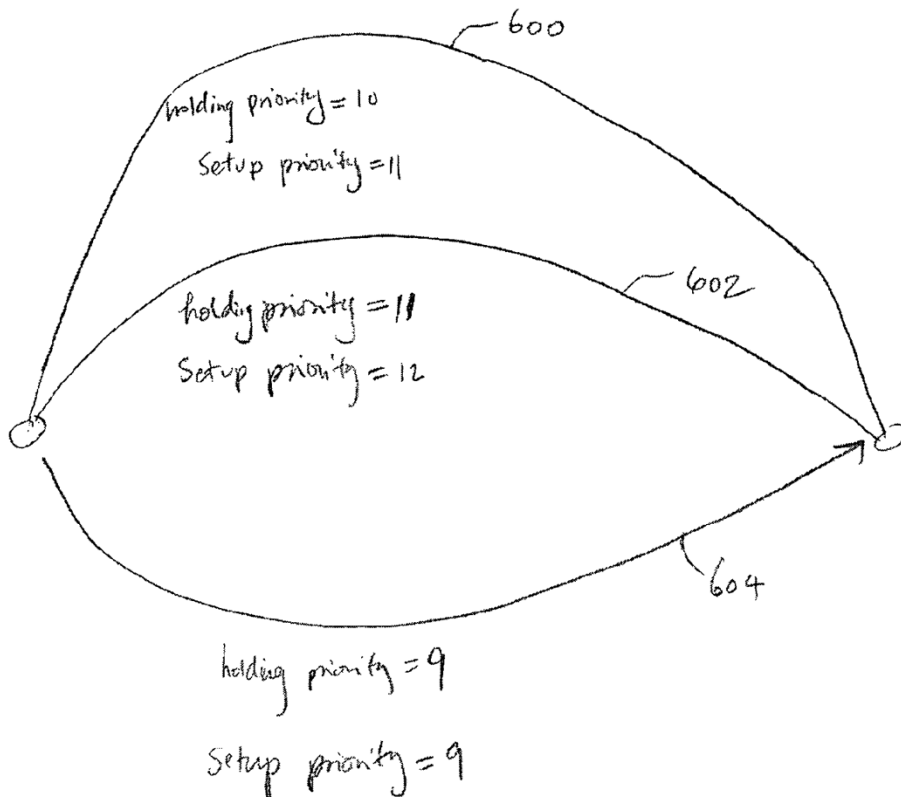


FIG. 6

- A “standby” Pseudowire with a “protection configuration parameter” is established.
- The “protection configuration parameter” configures Pseudowire properties, including protection type, scheme & priority.

'652 Patent

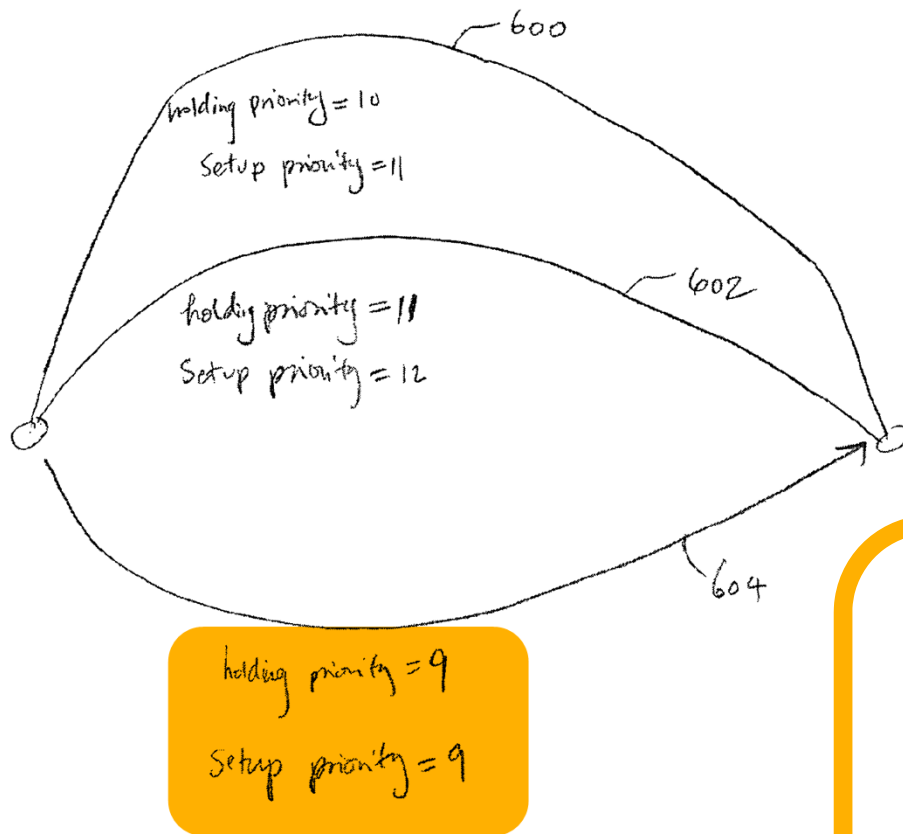


FIG. 6

- When protected Pseudowire fails, existing traffic on the “standby” Pseudowire is preempted based on the priority assigned to it.

holding priority = 9
Setup priority = 9

Single Disputed Element

Claim 1

1. A method of providing protection to network traffic, comprising:
 - a) sending a Pseudowire protection configuration parameter for configuring a standby Pseudowire between a source node and a destination node, the Pseudowire protection configuration parameter indicating a protection property associated with the standby Pseudowire, the protection property including a priority for the standby Pseudowire;
 - b) receiving a Pseudowire configuration acknowledgement indicating whether the Pseudowire protection configuration parameter has been accepted by the destination node;
 - c) accepting the Pseudowire protection configuration parameter by the destination node;
 - d) using the standby Pseudowire that is configured based at least in part on the Pseudowire protection configuration parameter; and
 - e) determining whether to preempt existing traffic on the standby Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire.

Claim Construction

Claim Construction

Term	Construction
standby Pseudowire.	an emulation of a native service over a network that is used in the event of a network failure.

Claim Construction

Term	Construction
determining whether to preempt existing traffic on the standby Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire.	determining <u>during the event of a network failure</u> whether to preempt existing traffic on the standby Pseudowire, wherein the determination is based, at least in part, on the priority for the standby Pseudowire.

Invalidity

**Hofmeister in View of RFC 3386/Owens
Renders the Challenged Claims Obvious**

BSL's Arguments

1

Hofmeister has “nothing to do with protecting traffic in the event of a network failure”

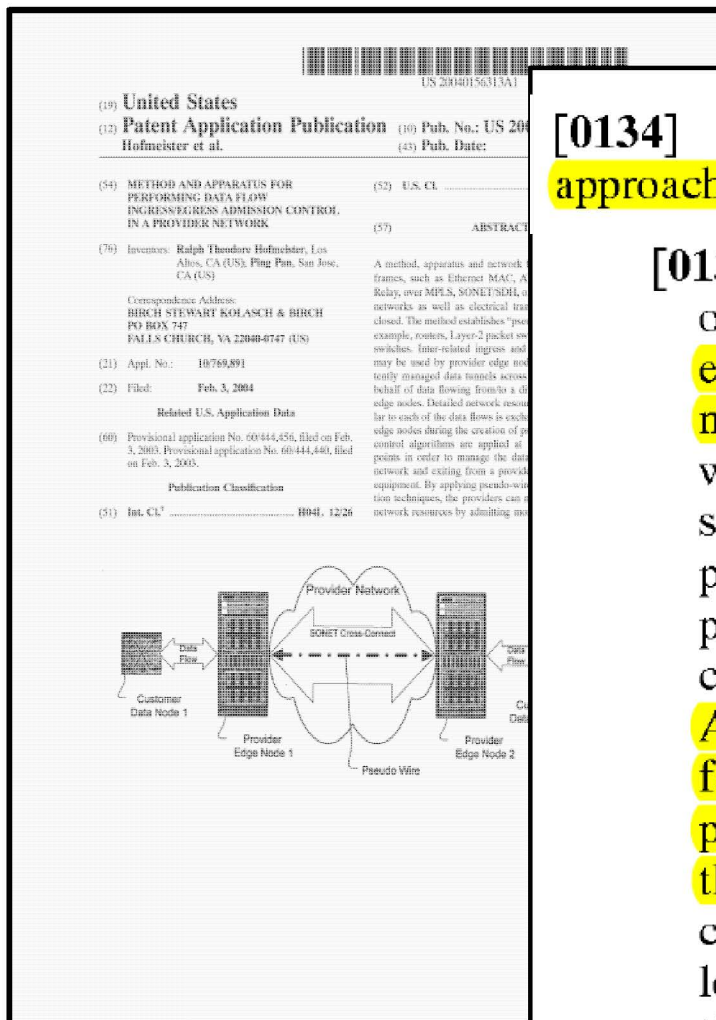
2

RFC 3386/Owens don't disclose “prioritization”

3

No motivation to combine

Hofmeister: Better Performance During Network Failure Is An “Advantage” Of Invention

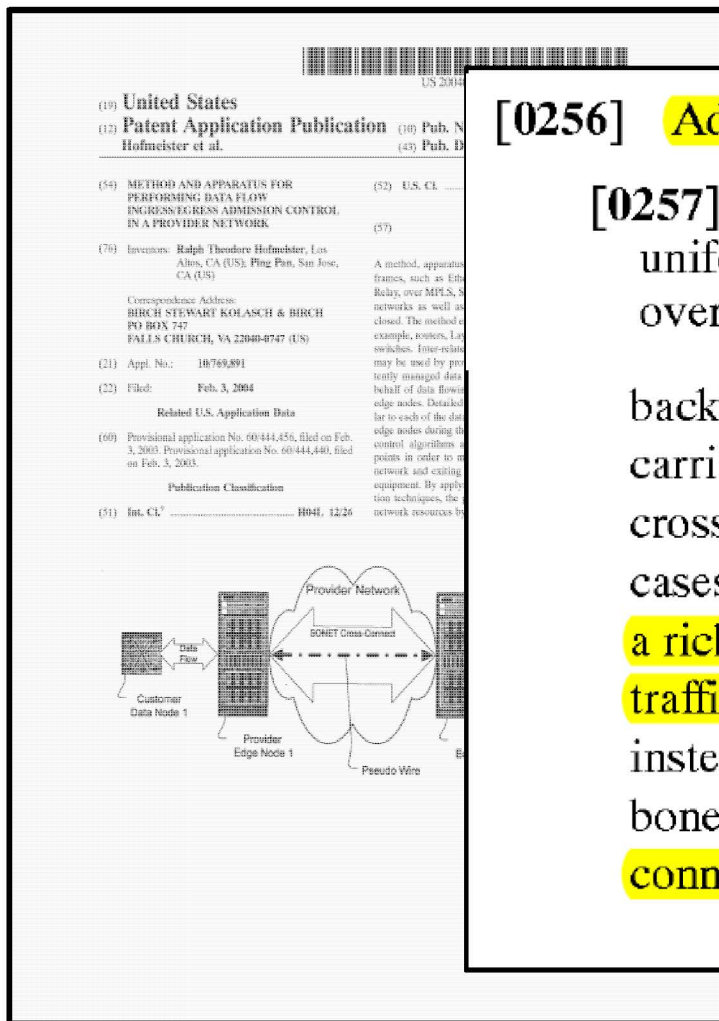


[0134] There are a number of advantages in the inventive approach described herein including:

[0137] 3. Since control messages traverse the same optical connections that data flows will traverse, it is easier and faster for the edge nodes to react to network failures. In comparison, in MPLS networks, when there is a failure on the data plane, it will take seconds before the control plane will be aware of the problem—likely to be notified from the routing protocol updates. In the inventive approach, the control-plane and the data-plane share the same fate. As a result, the control-plane can respond to failures faster. This is a huge advantage particularly because protection mechanisms can be triggered much faster thereby preventing data loss. At modern line rates currently approaching 40 gigabits/seconds per wavelength activating protection mechanisms in a shorter time will prevent the loss of tremendous amounts of data.

Ex. 1004 (Hofmeister) at [0134], [0137]

Hofmeister: Better Performance During Network Failure Is An “Advantage” Of Invention



[0256] Advantages Of Invention:

[0257] Martini’s pseudo-wire approach provides a uniformed method to carry all types of layer-2 traffic over a carrier’s backbone network. However, the backbone must be MPLS/IP-enabled. Traditionally, carriers are very careful with setting up SONET cross-connections inside their networks. In many cases, SONET connections are well provisioned with a rich set of features for network resource allocation, traffic restoration, and link protection, etc. Thus, instead of building pseudo-wires over a MPLS backbone, it would be desirable to use SONET cross-connects to carry pseudo-wire traffic directly.

Ex. 1004 (Hofmeister) at [0256] – [0257]

BSL's Arguments

1

~~Hofmeister has “nothing to do with protecting traffic in the event of a network failure”~~

2

RFC 3386/Owens don't disclose “prioritization”

3

No motivation to combine

RFC 3386: Priorities Are Assigned To Both Working And Protection Connections

Network Working Group
Request for Comments: 3386
Category: Informational

W. Lai, Ed.
AT&T
D. McOyuan, Ed.
worldcom

Status
This
not
mem
Copyri
Cop
Abstra
This
rep
ser
Conven
The
*SH
doc

3.2.1 1:1 Path Protection with Pre-Established Capacity

In this protection mode, the head end of a working connection establishes a protection connection to the destination. There should be the ability to maintain relative restoration priorities between working and protection connections, as well as between different classes of protection connections.

Lai, et. al. Informational (Page 1)

Ex. 1005 (RFC 3386) at section 3.2.1

RFC 3386: Priorities Are Assigned To Both Working And Protection Connections

Network Working Group
Request for Comments: 3386
Category: Informational

W. Lai, Ed.
ATA&T
D. McTyman, Ed.
worldcom

Status
This
not
men
Copyri
Cop
Abstra
This
req
ser
Conven
The
*SH
doc

In normal operation, traffic is only sent on the working connection, though the ability to signal that traffic will be sent on both connections (1+1 Path for signaling purposes) would be valuable in non-packet networks. Some distinction between working and protection connections is likely, either through explicit objects, or preferably through implicit methods such as general classes or priorities. Head ends need the ability to create connections that are as failure disjoint as possible from each other. This requires SRG information

Lai, et. al. Informational [Page 1]

Ex. 1005 (RFC 3386) at section 3.2.1

BSL's Arguments

1

~~Hofmeister has “nothing to do with protecting traffic in the event of a network failure”~~

2

~~RFC 3386/Owens don't disclose “prioritization”~~

3

No motivation to combine

Conclusory Expert Declaration Is Insufficient



Dr. George
Rouskas

“Given the Hofmeister reference’s teachings regarding the inventive application of certain parameters to admission control, notwithstanding the use of those parameters in other technologies (Juniper Ex. 2004 [sic] ¶ 296), it would not be obvious to extend such parameters from the Hofmeister reference to Pseudowire protection in the event of network failure.”

Ex. BX2002 at 2

Conclusory Expert Declaration Is Insufficient



Dr. George
Rouskas

Does not identify:

- ✘ Any facts to support conclusion
- ✘ Any reason why one could not combine Hofmeister with RFC 3386/Owens
- ✘ Any difficulties one skilled in the art would have combining Hofmeister with RFC 3386/Owens
- ✘ Any passages that teach away from the combination

Ex. BX2002

Conclusory Expert Declaration Is Insufficient



“Affidavits expressing an opinion of an expert must disclose the underlying facts or data upon which the opinion is based.”

Numerous Exemplary Rationales From *KSR*/*MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D


Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

G

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale A

Combining **prior art elements** according to **known methods** to yield **predictable results**

	<u>Prior Art Elements</u>	<u>Known Method</u>	<u>Predictable Results</u>		
Dr. Tal Lavian UC Berkeley	Hofmeister: Pseudowire System With Setup and Holding Priorities RFC 3386/Owens: network failure	+	Known network design principles	=	Robust/efficient network that can differentiate classes of traffic

Ex. 1027 (Lavian Declaration) at ¶ 40-46

Exemplary Rationale A

Combining prior art elements according to known methods to yield predictable results

SESSION_ATTRIBUTE Object

The **SESSION_ATTRIBUTE object** allows RSVP-TE to set different LSP priorities, preemption, and fast-reroute features. These are used to select alternate LSPs in case of a **failure in the network**. The SESSION_ATTRIBUTE is carried in the PATH message. It includes **fields such as Setup Priority and Holding Priority**, which affect whether this session can preempt or can be preempted by other sessions. A Flag field is also used to introduce options such as whether transit routers can use local mechanisms that would violate the ERO and cause local

Result = Efficient Network Protection

Ex. 1008 (Halabi) at 144

Numerous Exemplary Rationales From *KSR/MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D

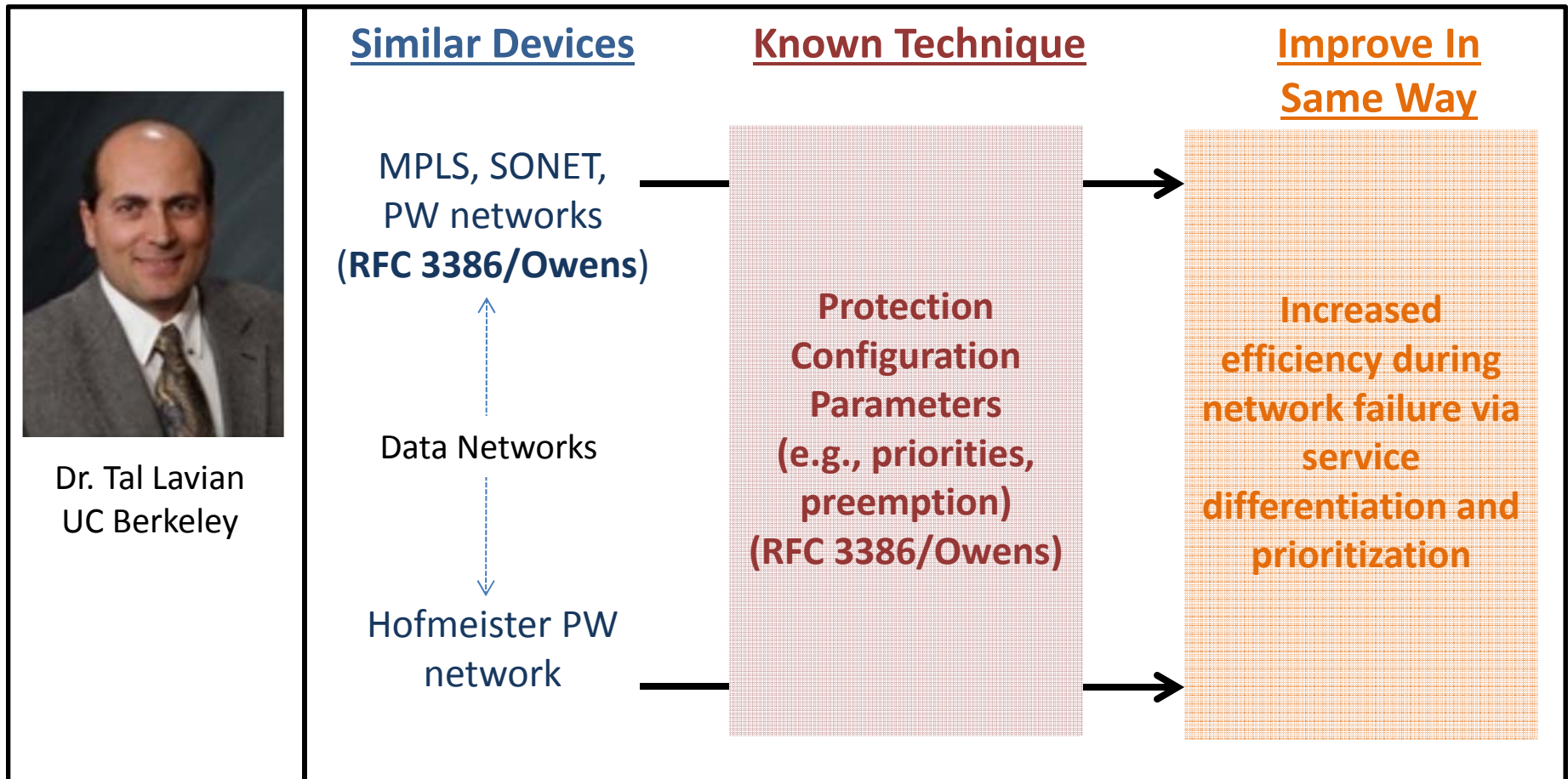
Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

E

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale C

Use of a **known technique** to improve **similar devices** (methods or products) in the **same way**

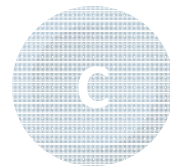


Ex. 1027 (Lavian Declaration) at ¶ 48-52

Numerous Exemplary Rationales From *KSR/MPEP* Apply



Combining prior art elements according to known methods to yield predictable results



Use of known technique to improve similar devices (methods or products) in the same way



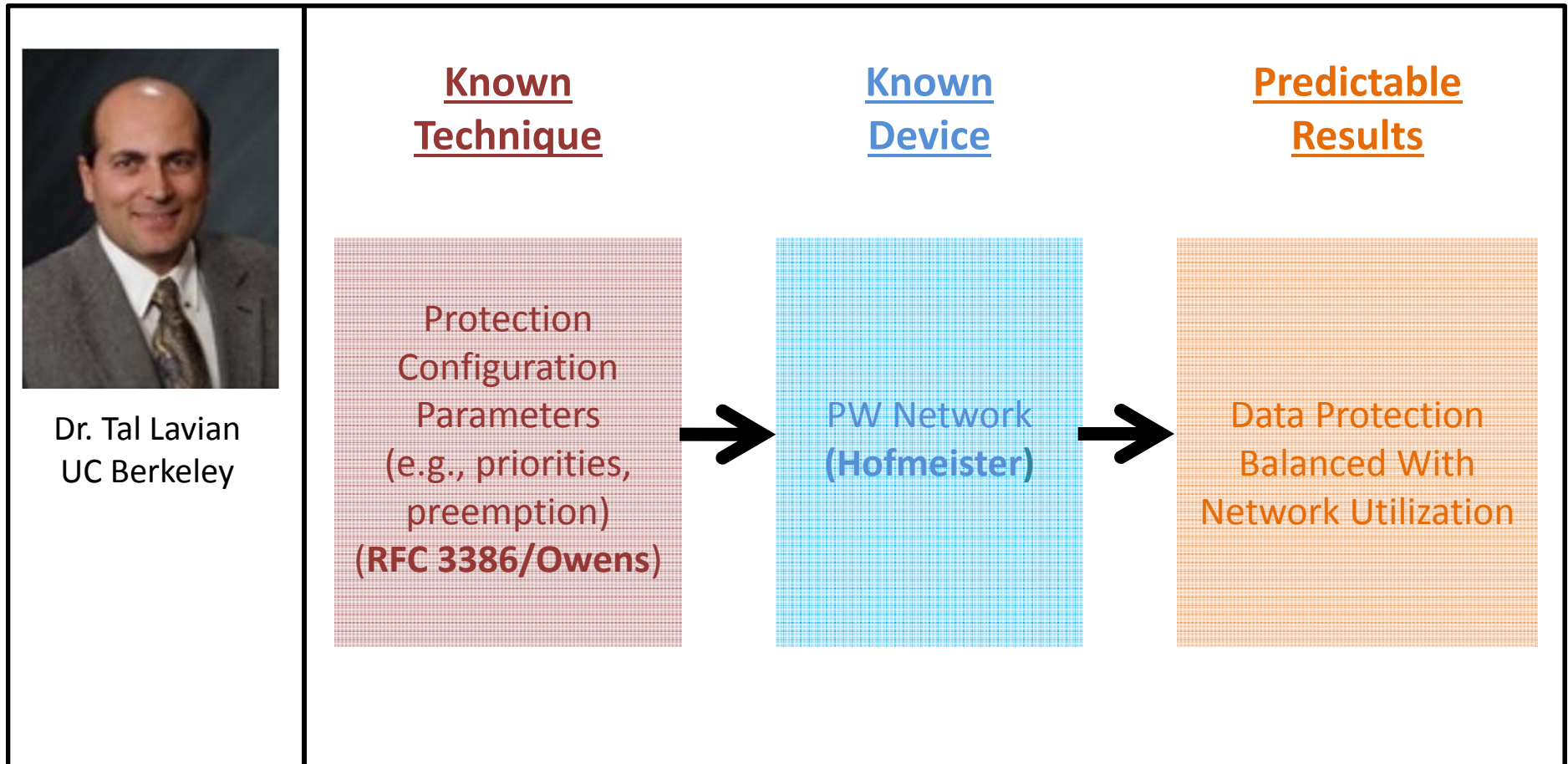
Applying a known technique to a known device (method or product) ready for improvement to yield predictable results



Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale D

Applying a **known technique** to a **known device** (method or product) ready for improvement to yield **predictable results**

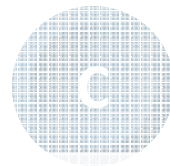


Ex. 1027 (Lavian Declaration) at ¶ 54-57

Numerous Exemplary Rationales From *KSR/MPEP* Apply



Combining prior art elements according to known methods to yield predictable results



Use of known technique to improve similar devices (methods or products) in the same way



Applying a known technique to a known device (method or product) ready for improvement to yield predictable results



Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale G

Teachings, suggestions, or motivations in the prior art that would have led one of ordinary skill to modify the prior art reference teachings to arrive at the claimed invention



Dr. Tal Lavian
UC Berkeley

- **Crucial for networks to provide data protection (Hofmeister/Owens/Halabi/RFC 3386)**
- **Balance between fast recovery and resource utilization (RFC 3386)**
- **Service differentiation (Owens)**
- **Common configuration parameters, such as “SESSION_ATTRIBUTE” Objects (e.g., Setup/Holding Priorities) (Hofmeister/Halabi/Owens)**
- **Standardization across protocols**

Ex. 1027 (Lavian Declaration) at ¶ 59-72

BSL's Arguments

1

~~Hofmeister has “nothing to do with protecting traffic in the event of a network failure”~~

2

~~RFC 3386/Owens don't disclose “prioritization”~~

3

~~No motivation to combine~~

**Halabi Anticipates and/or Renders the
Challenged Claims Obvious**

Halabi



“On this record, we are persuaded that Halabi teaches all of this limitation other than the context of preemption of traffic on a standby path during network failure.”

Halabi Discloses “Preemption of Traffic On A Standby Path During Network Failure”



Protection Information

GMPLS uses a new object type length value (TLV) field to carry LSP protection information. The use of this information is optional. Protection information indicates the LSP's link protection type. When a protection type is indicated, the connection request is processed only if the desired protection type can be honored. A link's protection capabilities may be advertised in routing.

Protection information also indicates whether the LSP is a primary or secondary LSP. A secondary LSP is a backup to a primary LSP. The resources of a secondary LSP are not used until the primary LSP fails. **The resources allocated for a secondary LSP may be used by other LSPs until the primary LSP fails over to the secondary LSP. At that point, any set of LSPs that are using the resources for the secondary LSP must be preempted.**

Halabi Discloses “Preemption of Traffic On A Standby Path During Network Failure”

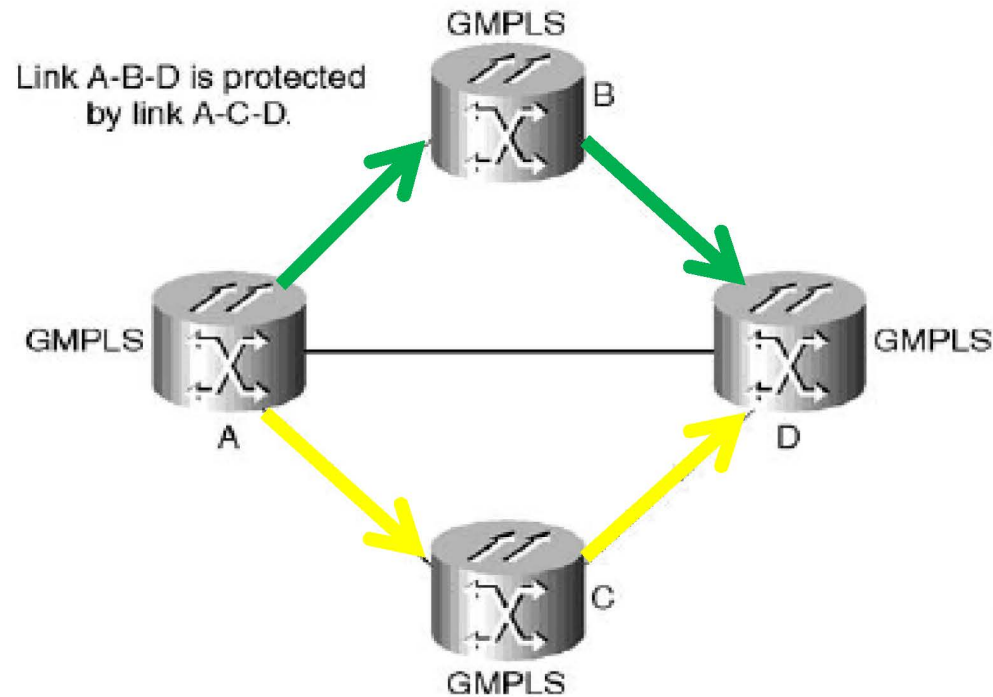


Link Protection Types

GMPLS introduces the concept of a *link protection type*, which indicates the protection capabilities that exist for a link. Path computation algorithms use this information to establish links with the appropriate protection characteristics. This information is organized in a hierarchy where typically the minimum acceptable protection is specified at path instantiation and a path selection technique is used to find a path that satisfies at least the minimum acceptable protection. The different link protection types are as follows:

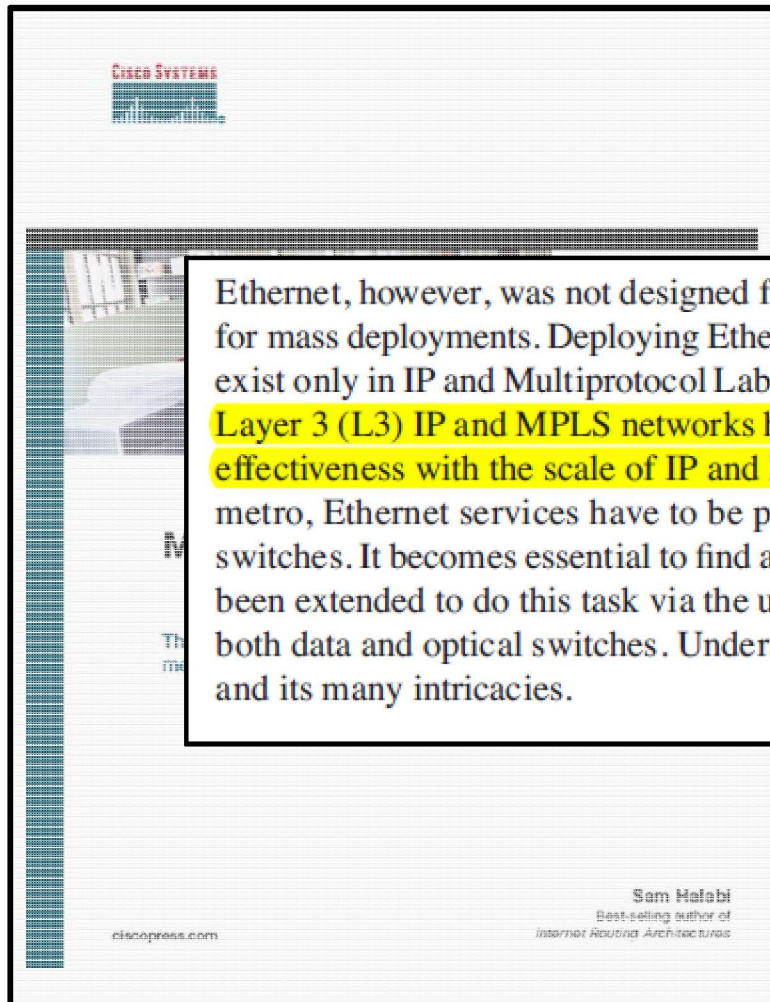
- **Extra Traffic**—This type of link protects another link or links. In case of failure of the protected links, all LSPs on this link are lost.
- **Unprotected**—This type of link is simply not protected by any other link. If the unprotected link fails, all LSPs on the link are lost.
- **Shared**—This type of link is protected by one or more disjoint links of type Extra Traffic.
- **Dedicated 1:1**—This type of link is protected by a disjoint link of type Extra Traffic.

Halabi Discloses “Preemption of Traffic On A Standby Path During Network Failure”



- **Link A-B-D is 1+1 protected**— Link A-C-D protects link A-B-D. Link A-C-D is not advertised and hence does not carry any LSPs unless link A-B-D fails.
- **Link A-B-D is 1:1 protected**— Link A-C-D protects link A-B-D. Link A-C-D is advertised and can carry LSPs, but it gets preempted to protect link A-B-D if link A-B-D fails.

Halabi – Motivation to Combine



Ethernet, however, was not designed for metro applications and lacks the scalability and reliability required for mass deployments. Deploying Ethernet in the metro requires the scalability and robustness features that exist only in IP and Multiprotocol Label Switching (MPLS) control planes. As such, hybrid Layer 2 (L2) and Layer 3 (L3) IP and MPLS networks have emerged as a solution that marries Ethernet's simplicity and cost effectiveness with the scale of IP and MPLS networks. With many transport technologies deployed in the metro, Ethernet services have to be provisioned and monitored over a mix of data switches and optical switches. It becomes essential to find a control plane that can span both data and optical networks. MPLS has been extended to do this task via the use of the Generalized MPLS (GMPLS) control plane, which controls both data and optical switches. Understanding these topics and more will help you master the metro space and its many intricacies.

Ex. 1008 (Halabi) at xv

It Is Obvious To Apply MPLS Protection Techniques To Pseudowires

(12) **United States Patent**
Pan

(54) **PSEUDOWIRE PROTECTION USING A STANDBY PSEUDOWIRE**

(75) Inventor: **Ping Pan**, San Jose, CA (US)

(73) Assignee: **Brixham Solutions Ltd.**, Tortola (VG)

(*) Notice: Subject to any disclaimer, the term of patent is extended or adjusted under U.S.C. 154(b) by 861 days.

(21) Appl. No.: **11/954,569**

(22) Filed: **Feb. 14, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/653,065, filed on 14, 2005.

(51) **Int. Cl.**
H04L 3/14 (2006.01)

(52) **U.S. Cl.** **370/228; 370/216; 370/225; 709**

(58) **Field of Classification Search** **370**
..... **370/225, 228; 709**

See application file for complete search history.

(56) **References Cited**

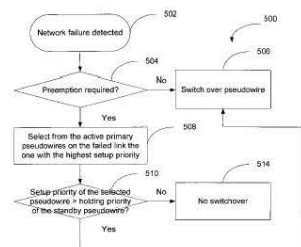
U.S. PATENT DOCUMENTS

5,930,705	A	7/1999	Lyon et al.
6,167,051	A	12/2000	Nagami et al.
6,347,088	B1	2/2002	Katou et al.
6,430,184	B1	8/2002	Robins et al.
6,546,427	B1	4/2003	Ehrlich
6,574,477	B1*	6/2003	Rathunde
6,621,793	B2	9/2003	Wiegren et al.
6,665,273	B1	12/2003	Geogon et al.
6,680,943	B1	1/2004	Gibson et al.
6,751,684	B2	6/2004	Owen et al.
6,813,271	B1	11/2004	Cable
6,845,389	B1	1/2005	Sen et al.
6,985,488	B2	1/2006	Pan et al.
7,050,396	B1	5/2006	Cohen et al.
7,206,104	B2*	4/2007	Salah et al.



Some MPLS devices implement schemes such as MPLS Fast Reroute to provide limited data protection. These existing schemes, however, often do not provide adequate protection. Take the following scenario as an example: between two provider edges (PEs), a first tunnel comprising multiple Pseudowires is protected by a second tunnel. Due to network topology constraints, the two tunnels may have different bandwidth. This is a possible scenario in an MPLS Fast Reroute operation. In this example, the second tunnel may have lower bandwidth than that of the first one. If the first tunnel should fail, the amount of data that needs to be redirected through the second tunnel may be greater than the bandwidth of the second tunnel. Furthermore, existing schemes do not provide a way of determining whether other less critical data may pass through the second tunnel.

- 20 A specific protection scheme corresponds to a field value. For example, 1+1 maps to 0, 1:1 maps to 1, and so on. In a system implementing a 1+1 protection scheme, the same traffic is sent over two parallel Pseudowires and the receiver selects one traffic stream at a time. In a system implementing a 1:1 protection scheme, one Pseudowire is used to protect another Pseudowire. Similarly, in a 1:N system (e.g. MPLS Facility Backup), one Pseudowire is used to protect N other Pseudowires, and in a M:N system M Pseudowires are used to protect N other Pseudowires.
- 25



JUNIPER
Exhibit 1001-1

Ex. 1001 ('652 Patent) at 1:49-64, 6:20-30

**Halabi in View of RFC 3386/Owens Renders the
Challenged Claims Obvious**

Numerous Exemplary Rationales From *KSR*/*MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D


Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

G

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale A

Combining **prior art elements** according to **known methods** to yield **predictable results**

	<u>Prior Art Elements</u>	<u>Known Method</u>	<u>Predictable Results</u>		
Dr. Tal Lavian UC Berkeley	<p>Halabi: Pseudowire protection and preemption/ priority attributes</p> <p>RFC 3386, Owens, Halabi: preemption during network failure</p>	+	Known network design principles	=	Robust/efficient network that can differentiate classes of traffic

Ex. 1027 (Lavian Declaration) at ¶ 95-96

Numerous Exemplary Rationales From *KSR/MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D

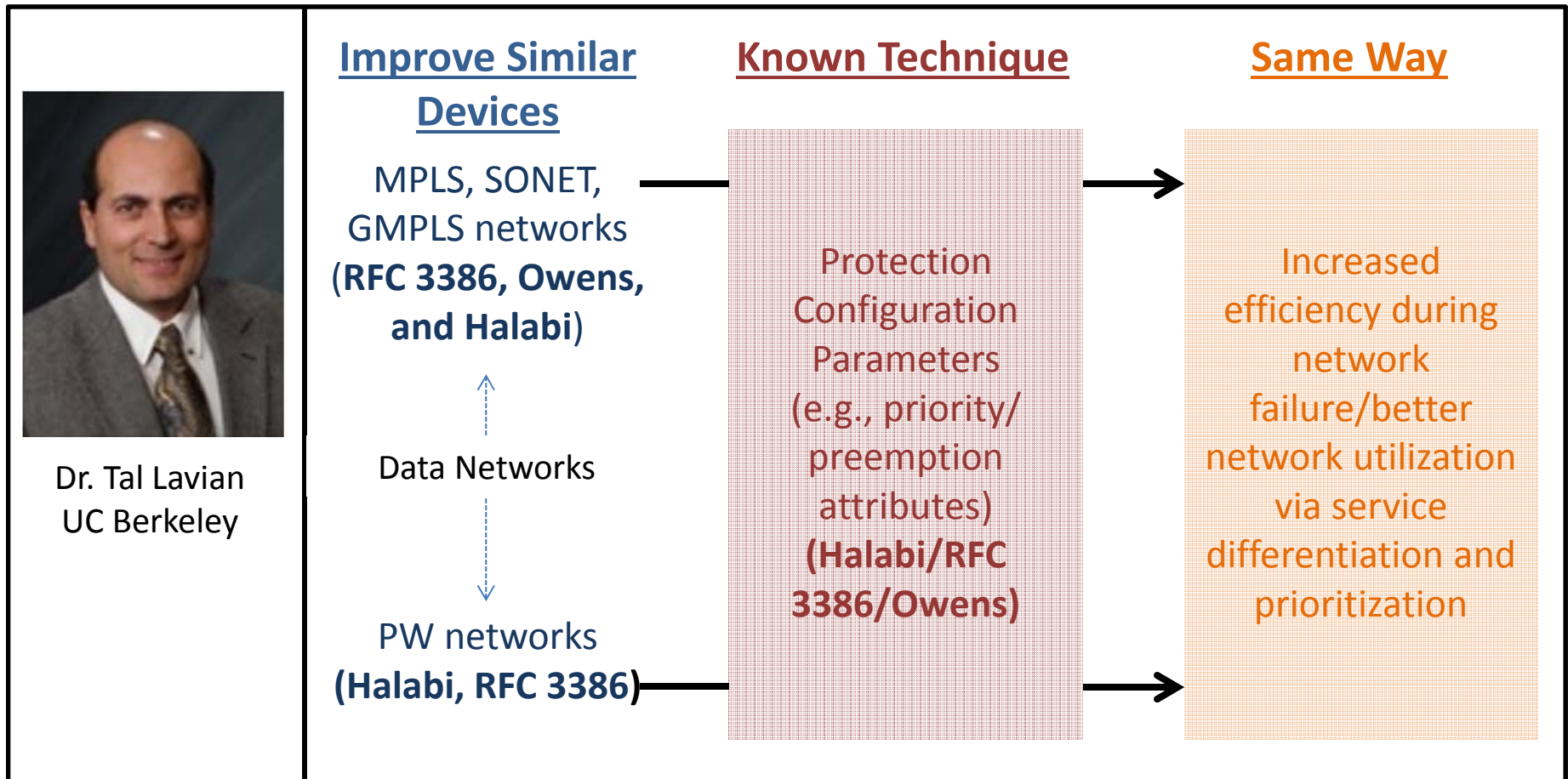
Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

G

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale C

Use of a **known technique** to improve **similar devices** (methods or products) in the **same way**



Dr. Tal Lavian
UC Berkeley

Ex. 1027 (Lavian Declaration) at ¶ 98-100

Numerous Exemplary Rationales From *KSR*/*MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D

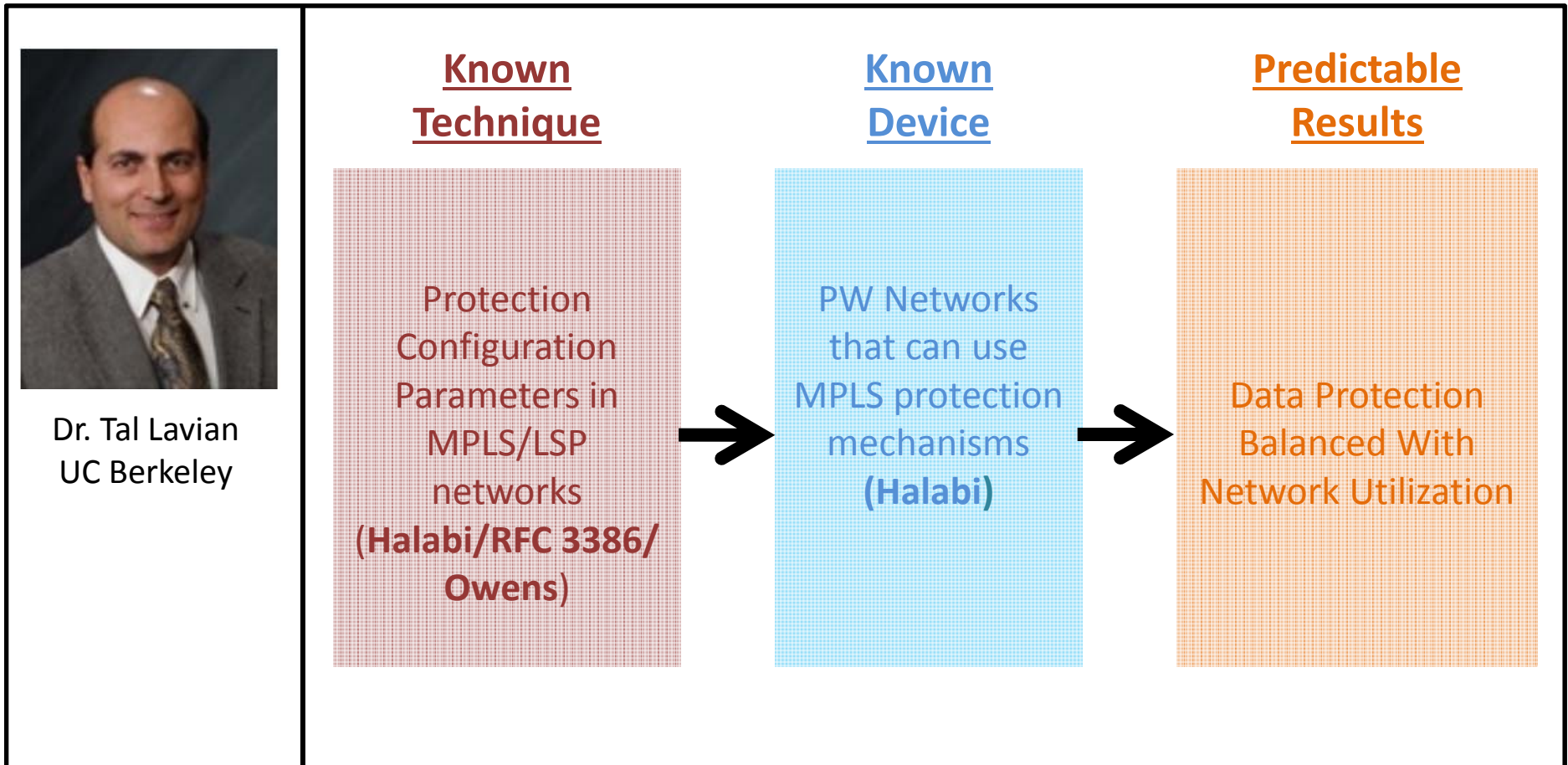
Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

G

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

KSR Exemplary Rationale D

Applying a **known technique** to a **known device** (method or product) ready for improvement to yield **predictable results**



Ex. 1027 (Lavian Declaration) at ¶ 102-105

Numerous Exemplary Rationales From *KSR/MPEP* Apply

A

Combining prior art elements according to known methods to yield predictable results

C

Use of known technique to improve similar devices (methods or products) in the same way

D

Applying a known technique to a known device (method or product) ready for improvement to yield predictable results

G

Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or combine prior art reference teachings to arrive at the claimed invention

Exemplary Rationale G

Teachings, suggestions, or motivations in the prior art that would have led one of ordinary skill to modify the prior art reference teachings to arrive at the claimed invention



Dr. Tal Lavian
UC Berkeley

- **Crucial for networks to provide data protection (Hofmeister/Owens/Halabi/RFC 3386)**
- **Balance between fast recovery and resource utilization (RFC 3386)**
- **Service differentiation (Owens)**
- **Common configuration parameters, such as “SESSION_ATTRIBUTE” Objects (e.g., Setup/Holding Priorities) (Hofmeister/Halabi/Owens)**
- **Standardization across protocols**

Ex. 1027 (Lavian Declaration) at ¶ 107-114

'652 Patent

JUNIPER[®]
NETWORKS