



(51) International Patent Classification:
H04L 12/56 (2006.01)

(21) International Application Number:

PCT/CN2009/071524

(22) International Filing Date:

28 April 2009 (28.04.2009)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/048,396 28 April 2008 (28.04.2008) US

(71) Applicant (for all designated States except US):
HUAWEI TECHNOLOGIES CO., LTD. [CN/CN];
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **DUNBAR, Linda** [US/US]; 3813 Skyline Drive, Plano, Texas 75025 (US). **SULTAN, Robert** [US/US]; 211B Heritage Hills Drive, Somers, New York 10589 (US). **MACK-CRANE, T. Benjamin** [US/US]; 5616 Elinor Avenue, Downers Grove, Illinois 60516 (US). **YONG, Lucy** [US/US]; 5722 East 103 Street, Tulsa, Oklahoma 74137 (US). **LEE, Young** [US/US]; 1621 Tawakoni Lane, Plano, Texas 75075 (US).

(74) Agent: **UNITALEN ATTORNEYS AT LAW**; 7th Floor, Scitech Place, No. 22, Jian Guo Men Wai Ave., Chao Yang District, Beijing 100004 (CN).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

[Continued on next page]

(54) Title: TRANSPARENT BYPASS AND ASSOCIATED MECHANISMS

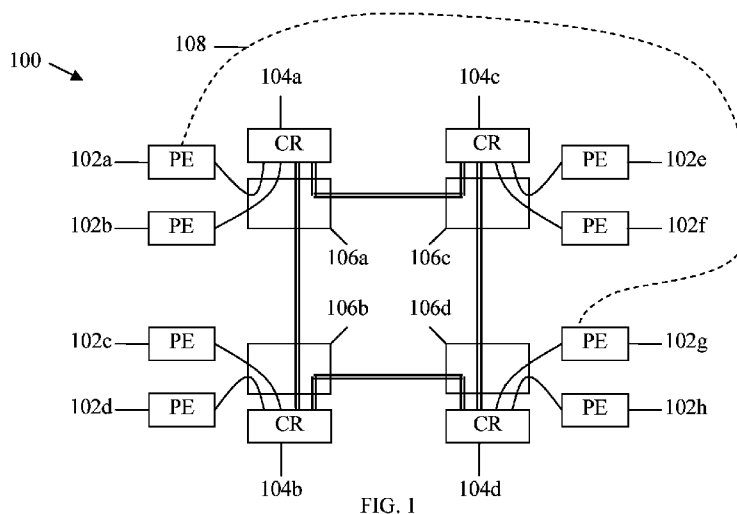


FIG. 1

(57) Abstract: A network component comprising at least one processor configured to implement a method comprising analyzing a path reservation message comprising a reserved path identifier, analyzing a plurality of frames each comprising a path identifier, and diverting at least some of the frames away from a router, wherein the path identifier in the diverted frames matches the reserved path identifier. Included is a system comprising a packet-aware transport box configured to receive a plurality of frames destined for a first router, snoop the frames, determine whether at least some of the frames should bypass the first router, and forward any frames that should bypass the first router to a second router without passing the frames to the first router.



Published:

— *with international search report (Art. 21(3))*

Transparent Bypass and Associated Mechanisms

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority to U.S. Provisional Patent Application No. 61/048,396, filed April 28, 2008 by Linda Dunbar et al., and entitled “Transparent By-Pass and the Mechanisms to Enable It,” which is incorporated herein by reference as if reproduced in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to the field of communications, and in particular, to transparent bypass and associated mechanisms.

BACKGROUND

[0003] Modern communications and data networks are comprised of nodes that transport data through the network. The nodes may include routers, switches, bridges, or combinations thereof that transport the individual data packets or frames through the network. Some networks may offer data services that forward data frames from one node to another node across the network without using pre-configured routes or bandwidth reservation on intermediate nodes. Other networks may forward the data frames from one node to another node across the network along pre-configured paths with each node along the route reserving bandwidth for the data frames, which is referred to as traffic engineered data services.

[0004] Bypasses are often used in networks to create a path between two nodes. For example, bypasses may be used when a fault is encountered in the network, to free capacity at intermediate nodes, or to improve the communications efficiency between two nodes. Unfortunately, bypasses change the topology of the network and can lead to undesirable changes in routing behavior within the network.

SUMMARY

[0005] In one embodiment, the disclosure includes a network component comprising at least one processor configured to implement a method comprising analyzing a path reservation message comprising a reserved path identifier, analyzing a plurality of frames each comprising a path identifier, and diverting at least some of the frames away from a router, wherein the path identifier in the diverted frames matches the reserved path identifier.

[0006] In another embodiment, the disclosure includes a system comprising a packet-aware transport box configured to receive a plurality of frames destined for a first router, snoop the frames, determine whether at least some of the frames should bypass the first router, and forward any frames that should bypass the first router to a second router without passing the frames to the first router.

[0007] In a third embodiment, the disclosure includes a method comprising configuring a bypass path by snooping a control frame comprising a label switched path (LSP) identifier, and routing a plurality of data frames associated with the LSP identifier to the bypass path without routing any subsequent control frames associated with the LSP identifier to the bypass path.

[0008] These and other features will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] For a more complete understanding of the present disclosure, reference is now made to the following brief description, taken in connection with the accompanying drawings and detailed description, wherein like reference numerals represent like parts.

[0010] FIG. 1 is a schematic diagram of an embodiment of a core network implementing express bypass.

[0011] FIG. 2 is a schematic diagram of an embodiment of a core network implementing transparent bypass.

[0012] FIG. 3 is a schematic diagram of another embodiment of a network implementing transparent bypass.

[0013] FIG. 4 is a schematic diagram of an embodiment of a method for establishing transparent bypass.

[0014] FIG. 5 is a schematic diagram of an embodiment of a general-purpose network component.

DETAILED DESCRIPTION

[0015] It should be understood at the outset that although an illustrative implementation of one or more embodiments are provided below, the disclosed systems and/or methods may be implemented using any number of techniques, whether currently known or in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, including the exemplary designs and implementations illustrated and described herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

[0016] Disclosed herein is a method for allowing routers to handle an increased volume of traffic without upgrading router's capacity. Specifically, a transparent bypass method is disclosed wherein packet-aware transport boxes associated with the routers snoop the control messages processed by the router to determine the paths that traverse the router. The packet-aware transport boxes build a table of associated paths and snoop the router's incoming data frames to determine whether any of the incoming data frames are associated with the paths in the table. Any data frames associated with the paths in the table are not sent to the router but are instead forwarded by

the packet-aware transport boxes to another destination, such as the next node on the path. In contrast, the packet-aware transport box forwards all control frames to the router, regardless of whether they are associated with the paths in the table or not. By doing so, the routers are able to maintain the paths in a normal fashion, but experience a reduced volume of frames.

[0017] FIG. 1 illustrates an embodiment of a network 100. The network may comprise a plurality of provider edges (PEs) 102a-102h (collectively, 102), a plurality of core routers (CRs) 104a-104d (collectively, 104), and a plurality of transport boxes 106a-106d (collectively, 106). The PEs 102 may be coupled to the CRs 104 as shown by the single solid lines in FIG. 1, while the CRs 104 may be coupled to each other as shown by the double solid lines in FIG. 1. The communications paths between the PEs 102 and the CRs 104 (including those between the CRs 104) may be electrical or optical communications paths. Typically, the communications paths between the CRs 104 have more capacity than the communications paths between the PEs 102 and the CRs 104. For example, the communications paths between the CRs 104 may be wavelength division multiplexed to create a capacity of about 200 gigabits per second (Gbps or G), while the communications paths between the PEs 102 and the CRs 104 may only be single wavelength channels having a capacity of about 10 Gbps.

[0018] The network 100 may be any communications system that may be used to transport data between PEs 102 and/or CRs 104. For example, the network 100 may be a wireline network or an optical network, such as a backbone, a provider, and an access networks. Such networks typically implement Synchronous Optical Networking (SONET), Synchronous Digital Hierarchy (SDH), Ethernet, Internet Protocol (IP), Asynchronous Transfer Mode (ATM), Frame Relay, or other protocols. Alternatively, the network 100 may be a wireless network. The network 100 may transport traffic using multi-protocol label switching (MPLS) LSPs and/or virtual local area

networks (VLANs) as described in IEEE 802.1Q. The traffic may comprise connectionless or switched traffic, also referred to as service instances or non-TE traffic, as described in IEEE 802.1ah. The traffic may also comprise connection-oriented or bridged traffic, also referred to as Provider Backbone Bridge-Traffic Engineering (PBB-TE) traffic or TE traffic, as described in IEEE 802.1. Each of the standards described herein is incorporated herein by reference.

[0019] The PEs 102 may be any devices, components, or networks that exchange data with the CRs 104. The PEs 102 may be routers, switches, or bridges, and may include provider core bridges (PCBs) and/or provider edge bridges (PEBs). The PEs 102 may implement one or more protocols, including MPLS, open shortest path first (OSPF), or border gateway protocol (BGP). The PEs 102 may establish MPLS LSPs with other devices, and as such may serve as the origin or termination point of a LSP. In embodiments, the PEs 102 may reside at the edge of or interface with devices that reside at the edge of a network provider's domain. Finally, the PEs 102 may comprise transport boxes similar to the transport boxes 106 described herein.

[0020] The CRs 104 may be any devices or components that exchange data with the PEs 102 and each other. For example, the CRs 104 may be routers, switches, or bridges, including backbone core bridges (BCBs) and/or backbone edge bridges (BEBs). In addition, the CRs 104 may implement one or more protocols, including MPLS, BGP, or OSPF. The CRs 104 may maintain MPLS LSPs, and as such may serve as an intermediate or transit node along a LSP. In embodiments, the CRs 104 may reside within the central region of a network provider's domain, e.g. not at the edge of the provider's domain.

[0021] Each CR 104 may comprise a transport box 106. The transport box 106, sometimes referred to as an optical transport box, may be a device that interfaces between a physical layer, such as an electrical or optical layer, and a higher layer, such as a media access control (MAC)

layer, MPLS layer, or IP layer. Specifically, the transport box 106 may receive physical layer communications destined for the CR 104, convert the communications into a higher layer format, and pass the communications to the CR 104. In addition, the transport box 106 may receive higher layer communications from the CR 104, convert the communications into a physical layer format, and transmit the communications to another CR 104 or a PE 102.

[0022] In some cases, a network operator may implement express bypass in the network 100. For example, when traffic volume between two PEs 102, e.g. PE 102a and PE 102g, exceeds a threshold, a physical bypass 108 may be established between the PEs 102. The physical bypass 108 may comprise a new path between PE 102a and PE 102g. While the establishment of the physical bypass 108 is useful in reducing traffic flow through the CRs 104, express bypass is not without limitations. For example, the physical bypass 108 can only be established when the PEs 102 reside within the same administrative domain. In addition, the physical bypass 108 creates adjacency between PE 102a and PE 102g, which causes topology and route cost changes within the network. Such changes eventually lead to an unwanted increase in traffic on the physical bypass 108 and other undesirable changes to traffic within the network 100.

[0023] FIG. 2 illustrates an embodiment of a network 200 implementing transparent bypass. The network 200, PEs 202, and CRs 204 may be substantially the same as the network 100, PEs 102, and CRs 104 described above. However, the CRs 204 (and optionally the PEs 202) within the network 200 comprises packet-aware transport boxes 210a-210d (collectively, 210) instead of the transport boxes 106. The packet-aware transport boxes 210 may be similar to the transport boxes 106, but may comprise additional functionality, such as the ability to analyze and forward frames received from the PEs 202 and the CRs 204, e.g. without passing those frames to the CR 204. After analyzing the frames, the packet-aware transport boxes 210 may construct a forwarding table

-7-

and decide whether to implement transparent bypass on any subsequently snooped data frames. The transparent bypass may occur at the physical layer or at a higher layer, such as the MAC layer, the MPLS layer, or the IP layer. Finally, transparent bypass may be implemented at any time, but is particularly useful when the traffic volume going through CRs 204 is approaching or about to exceed the CRs' 204 capacity.

[0024] During transparent bypass, the packet-aware transport boxes 210 may analyze the frames received from the PEs 202 and the CRs 204 and determine whether the frames are control frames or data frames. If the frames are control frames, the packet-aware transport boxes 210 may forward the control frames to the CR 204 for routing and/or processing regardless of whether the control frames are associated with one the transparent bypass paths. Control frames may be used for establishing, maintaining, and removing paths, such as LSPs, in the network, and may comprise IP/MPLS control protocol data units (PDUs). Because the packet-aware transport boxes 210 have visibility into these frames, the packet-aware transport boxes 210 may maintain a forwarding database of paths associated with its CR 204. As such, when the packet-aware transport boxes 210 receive a data frame, they may determine whether the data frame is associated with one of the paths, and if so, forward the data frame to the next router or other node associated with the path, e.g. without ever forwarding the data frame to the CR 204. As such, the dashed line 212 may represent a data frame's path from PE 202a to PE 202g, e.g. the bypass of CRs 204a, 204c, and 204d. In contrast, the dotted line 214 may represent how a control frame's path from PE 202a to PE 202g deviates from the dashed line 212, e.g. the control frame's path goes through of CRs 204a, 204c, and 204d.

[0025] FIG. 3 illustrates an embodiment of a network 300 implementing transparent bypass. The network 300, PEs 302, CRs 304, and packet-aware transport boxes 310 may be substantially

the same as the network 200, PEs 202, CRs 204, and packet-aware transport boxes 210 described above. However, the network 300 may be a logical full mesh core IP network, and as such may allow the packet-aware transport boxes 310 to establish a one-hop transport path between any two CRs 304. For example, if the CRs 304 comprise Ethernet interfaces to the packet-aware transport boxes 310, sometimes called packet-optical transport platforms (P-OTP) as is the case in Ethernet over SONET/SDH applications, then VLANs can be used as channels between the CRs 304. Dashed lines 316 and 318 represent such one-hop transport paths between CRs 304. When implementing the transparent bypass in a full mesh network, the packet-aware transport boxes 310 may utilize these one-hop transport paths, which further reduces the traffic volume at the intermediate CRs 304, which act as intermediate label switched routers (LSRs) or transit routers. To the transit routers, the use of the one-hop transport paths is a double benefit because the transit routers see a traffic reduction on both their input ports and their output ports, e.g. when traffic is sent on path 318, CR 104c sees a reduction in traffic associated with ports connected to CR 304a and CR 304d. Note that while the benefit is realized for CR-CR ports, it does not affect the amount of traffic traversing PE-CR ports. As such, the CRs 304 adjacent to the PEs 302 will eventually have to upgrade their port capacity to handle the increased data to/from the PEs 302. Finally, most CR to P-OTP interfaces are 10 Gbps, which is usually required for any CR 304 interconnection. In order to show any significant advantage of logical mesh connections established by P-OTP, the CR to P-OTP interface may need to be as high as 40 Gbps or 100 Gbps, which is not currently commercially available in many networks.

[0026] There are many methods by which the packet-aware transport boxes can implement the transparent bypass. For example, if LSPs are calculated by a path computation element (PCE), then the PCE can send the transparent bypass information to the packet-aware transport box. In

some instances, the PCE may comprise an upper layer PCE, such as a MPLS or IP layer PCE, and a lower layer PCE, such as a packet transport network (PTN), optical transport network (OTN), or a wavelength division multiplexed (WDM) layer PCE. In such cases, the upper layer PCE may consult the lower layer PCE for lower layer topology information. Alternatively, if there are pre-established LSPs, then the LSP forwarding table can be manually provisioned on the packet-aware transport boxes. However, it is expected that the transparent bypass will most often be implemented by allowing the packet-aware transport boxes to snoop the MPLS control protocol PDUs and establish LSP forwarding table accordingly.

[0027] FIG. 4 illustrates a method by which the packet-aware transport boxes snoop the MPLS control protocol PDUs and establish LSP forwarding table. Initially, a path reservation message 420 is sent from a first core router, e.g. CR 430, to a second core router, e.g. CR 442. The path reservation message 420 may be, for example, a resource reservation protocol – traffic engineering (RSVP-TE) session or path message sent using label distribution protocol (LDP). The path reservation message 420 may contain a specific keyword key, perhaps a wildcard, that triggers the below-described actions when it is detected during the snooping. The key may be an ASCII string or substring, and may be inserted at CR 430 by a network administrator. When the packet-aware transport box 432 receives the path reservation message 420, the packet-aware transport box 432 may ensure that the path reservation message 420 is requesting an appropriate object, such as a Record Route Object (RRO), and if so, forward the message to the CR 442.

[0028] After the CR 442 processes the path reservation message 420, the CR 442 may generate a path reserved (RESV) confirmation message 424 comprising the key, a RRO label (L2), and a RESV destination. Upon receiving the RESV message 424, the packet-aware transport box 440 programs its cross-connect fabric to map the L2 label used on the hop it is snooping to its direct

tunnel to the destination, which may be the packet-aware transport box 432. This action effectively sets up the transparent bypass. As such, the packet-aware transport box 440 will subsequently strip the L2 label off any data frames associated with the LSP and directs the data frames to a transport tunnel that terminates at the final snooping hop of the RSVP-TE path, namely the packet-aware transport box 432. The RESV message 424 will progress, hop by hop, across the intermediate CR 436 and its transport boxes 434, which may be packet-aware transport boxes.

[0029] When the packet-aware transport box 432 receives the final RESV message 424, the packet-aware transport box 432 may look at the RRO, find the label L2, for example by looking at the first recorded hop/label in the RRO, and program its cross-connect to forward label L2 from the tunnel to the packet-aware transport box 440 through its snooping interface. The packet-aware transport box 440 may also switch the label to the proper label (L1) for this hop as seen in the Label object of the RESV message 422. Thus, the RRO allows direct mapping of the first and last hops by the packet-aware transport boxes. As such, a multi-hop RSVP-TE path is turned into a three-hop path (442-440-432-430), the middle one of which is a direct detour bypassing all the inner hops.

[0030] When there are multiple optical links between two packet-aware transport boxes, there may be multiple options for mapping the LSPs to the transparent bypass path. For example, equal cost multi-path (ECMP) can be used to automatically map some LSPs to one of the transparent bypass paths. Alternatively, a network administrator may manually configure some LSPs to a fixed transparent bypass path.

[0031] Occasionally, faults may be detected along the bypass path. For example, a fault may be detected on a physical port of a packet-aware transport box. If a fault is detected, the packet-aware transport box may disable the transparent bypass function for the LSPs who have egress

ports associated with the faulty physical port. As such, the data frames associated with the LSPs whose transparent bypass is disabled will be forwarded to CRs as if the transparent bypass never existed. Such action may trigger fast re-route, which may cause the packet-aware transport boxes to forward the data frames along re-established LSPs. The packet-aware transport boxes may also establish forwarding entries for fast re-route paths. As such, when a CR sends data frames along the fast re-route paths, those data frames will be forwarded accordingly at each intermediate node. When any CR switches to the fast reroute path, there won't be any data frames on the normal or working LSP. As such, the packet-aware transport box may not need to do anything.

[0032] The packet-aware transport box may have many ports. For example, 20-40 ports are commonly used in transport boxes. When a failure occurs, only the data frames traversing through the faulty port may be sent to the CR. Even with the increase in traffic to the CR, the amount of frames sent to CR is still much less than the total amount of frames traversing all of the ports.

[0033] As described above, there are significant differences between express bypass and transparent bypass. Transparent bypass may generally be implemented for data frames on selected LSPs to reduce the data volume traversed through the CR's ports. As such, the traffic volume to and from the PEs can grow without increasing the port capacity on adjacent CRs. In addition, transparent bypass allows the PEs to continue peering with their original CRs. As such, there is no route or topology change to the routers, which means the transparent bypass does not affect the calculations for other routes. In other words, transparent bypass does not create any new adjacencies, and thus will not change the costs to other routes, cause any unexpected traffic switches to the newly established bypass, or cause other routers to change their forwarding tables. Finally, in transparent bypass all of the control data frames get sent to CRs, and as such when

transparent bypass is disabled, all of the data flows are defined at the CRs, and the network acts as if the packet-aware transport boxes did not exist.

[0034] In some embodiments, the network may require special configuration to implement the transparent bypass. For example, the packet-aware transport box may need to be able to differentiate control frames, e.g. IP/MPLS control PDUs, from data frames, e.g. data PDUs. In addition, the packet-aware transport box may only transparently bypass data frames associated with paths that are implementing transparent bypass. In other words, data frames associated with paths not implementing transparent bypass, control frames, and other types of frames continue to be sent to the CR. Finally, the packet-aware transport box may have to act as a transit router in that it may have to swap the MPLS labels on the data frames as if the data frames went through CR.

[0035] The network components described above may be implemented on any general-purpose network component, such as a computer or network component with sufficient processing power, memory resources, and network throughput capability to handle the necessary workload placed upon it. FIG. 5 illustrates a typical, general-purpose network component 500 suitable for implementing one or more embodiments of the components disclosed herein. The network component 500 includes a processor 502 (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage 504, read only memory (ROM) 506, random access memory (RAM) 508, input/output (I/O) devices 510, and network connectivity devices 512. The processor 502 may be implemented as one or more CPU chips, or may be part of one or more application specific integrated circuits (ASICs).

[0036] The secondary storage 504 is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM 508 is not large enough to hold all working data. Secondary storage 504 may be used to store

programs that are loaded into RAM 508 when such programs are selected for execution. The ROM 506 is used to store instructions and perhaps data that are read during program execution. ROM 506 is a non-volatile memory device that typically has a small memory capacity relative to the larger memory capacity of secondary storage 504. The RAM 508 is used to store volatile data and perhaps to store instructions. Access to both ROM 506 and RAM 508 is typically faster than to secondary storage 504.

[0037] At least one embodiment is disclosed and variations, combinations, and/or modifications of the embodiment(s) and/or features of the embodiment(s) made by a person having ordinary skill in the art are within the scope of the disclosure. Alternative embodiments that result from combining, integrating, and/or omitting features of the embodiment(s) are also within the scope of the disclosure. Where numerical ranges or limitations are expressly stated, such express ranges or limitations should be understood to include iterative ranges or limitations of like magnitude falling within the expressly stated ranges or limitations (e.g., from about 1 to about 10 includes, 2, 3, 4, etc.; greater than 0.10 includes 0.11, 0.12, 0.13, etc.). For example, whenever a numerical range with a lower limit, R_l , and an upper limit, R_u , is disclosed, any number falling within the range is specifically disclosed. In particular, the following numbers within the range are specifically disclosed: $R = R_l + k * (R_u - R_l)$, wherein k is a variable ranging from 1 percent to 100 percent with a 1 percent increment, i.e., k is 1 percent, 2 percent, 3 percent, 4 percent, 5 percent, ..., 50 percent, 51 percent, 52 percent, ..., 95 percent, 96 percent, 97 percent, 98 percent, 99 percent, or 100 percent. Moreover, any numerical range defined by two R numbers as defined in the above is also specifically disclosed. Use of the term “optionally” with respect to any element of a claim means that the element is required, or alternatively, the element is not required, both alternatives being within the scope of the claim. Use of broader terms such as comprises, includes, and having

should be understood to provide support for narrower terms such as consisting of, consisting essentially of, and comprised substantially of. Accordingly, the scope of protection is not limited by the description set out above but is defined by the claims that follow, that scope including all equivalents of the subject matter of the claims. Each and every claim is incorporated as further disclosure into the specification and the claims are embodiment(s) of the present disclosure. The discussion of a reference in the disclosure is not an admission that it is prior art, especially any reference that has a publication date after the priority date of this application. The disclosure of all patents, patent applications, and publications cited in the disclosure are hereby incorporated by reference, to the extent that they provide exemplary, procedural, or other details supplementary to the disclosure.

[0038] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods might be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted, or not implemented.

[0039] In addition, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as coupled or directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and

-15-

alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

CLAIMS

What is claimed is:

1. A network component comprising:
at least one processor configured to implement a method comprising:
analyzing a path reservation message comprising a reserved path identifier;
analyzing a plurality of frames each comprising a path identifier; and
diverting at least some of the frames away from a router, wherein the path identifier in the diverted frames matches the reserved path identifier.
2. The network component of claim 1, wherein the path reservation message is a multi-protocol label switching (MPLS) control message.
3. The network component of claim 1, wherein the path reservation message is a resource reservation (RSVP) control message.
4. The network component of claim 1, wherein none of the diverted frames are control frames.
5. The network component of claim 4, wherein all of the diverted frames are data frames.
6. The network component of claim 1, wherein the diverted frames are forwarded on a label switched path.

7. The network component of claim 1, wherein the diverted frames are forwarded on a virtual local area network.

8. A system comprising:

a packet-aware transport box configured to receive a plurality of frames destined for a first router, snoop the frames, determine whether at least some of the frames should bypass the first router, and forward any frames that should bypass the first router to a second router without passing the frames to the first router.

9. The system of claim 8, wherein the packet-aware transport box is configured to receive the frames at a physical layer, and wherein the packet-aware transport box is configured to communicate with the first router at a media access control (MAC) layer, a multi-protocol label switching (MPLS) layer, or an Internet Protocol (IP) layer.

10. The system of claim 8, wherein the packet-aware transport box is configured to determine whether at least some of the frames should bypass the first router by snooping multi-protocol label switching (MPLS) control protocol data units (PDUs).

11. The system of claim 8, wherein the packet-aware transport box is configured to determine whether at least some of the frames should bypass the first router by receiving a command from an external path computation element (PCE).

12. The system of claim 11, wherein the PCE comprises a higher layer PCE and a lower layer PCE, and wherein the higher layer PCE consults the lower layer PCE for lower layer topology information.
13. The system of claim 12, wherein the lower layer is a packet transport network layer, an optical transport network layer, or a wavelength division multiplexed layer.
14. The system of claim 8, wherein the packet-aware transport box is configured to determine whether at least some of the frames should bypass the first router by manual configuration.
15. The system of claim 8, wherein the packet-aware transport box is configured to separate any data frames that should bypass the first router from any remaining data frames.
16. The system of claim 8, wherein no control frames bypass the first router.
17. The system of claim 8, wherein the packet-aware transport box is configured to determine that none of the frames should bypass the first router when a fault is detected in a port associated with the frames.
18. A method comprising:
 configuring a bypass path by snooping a control frame comprising a label switched path (LSP) identifier; and

routing a plurality of data frames associated with the LSP identifier to the bypass path without routing any subsequent control frames associated with the LSP identifier to the bypass path.

19. The method of claim 18, wherein the control frame is distributed using label discovery protocol.

20. The method of claim 18 further comprising: disabling the bypass path when a fault is detected in a port associated with the bypass path.

-1/3-

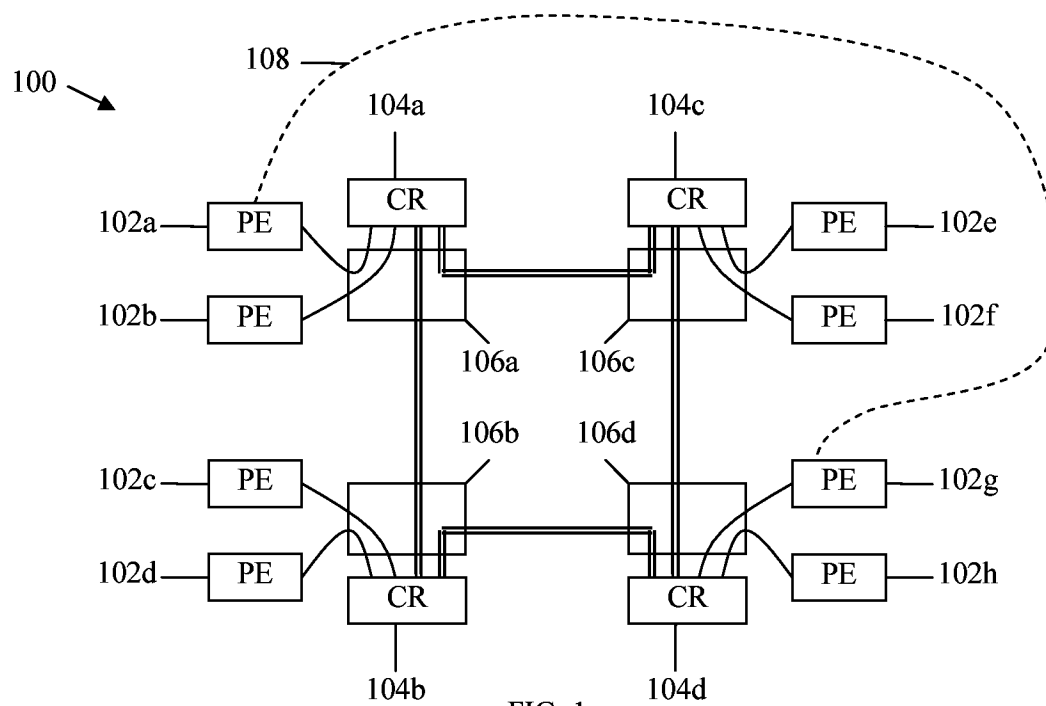


FIG. 1

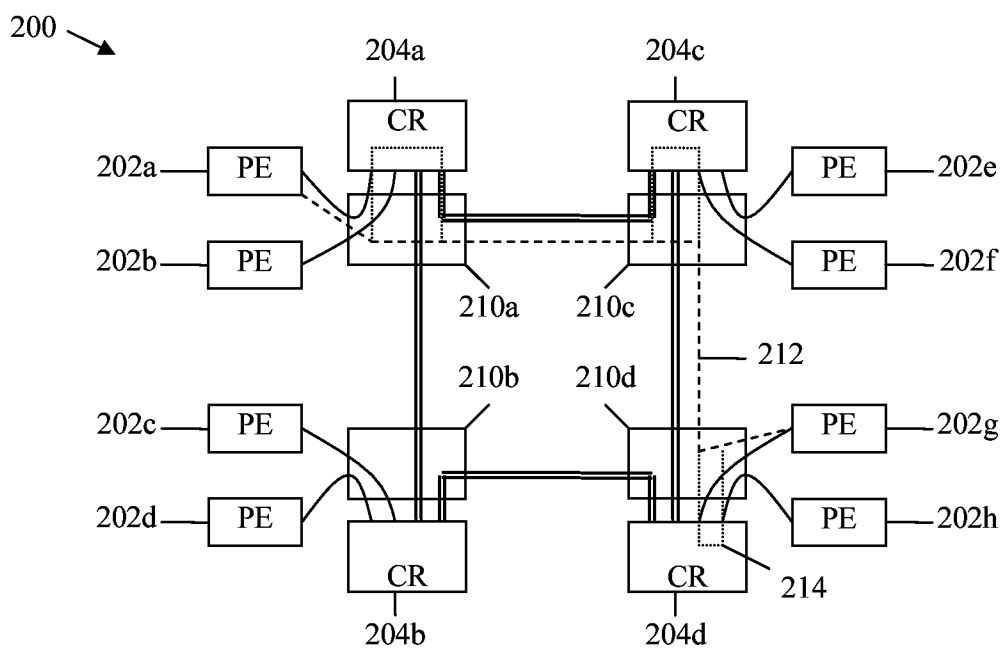
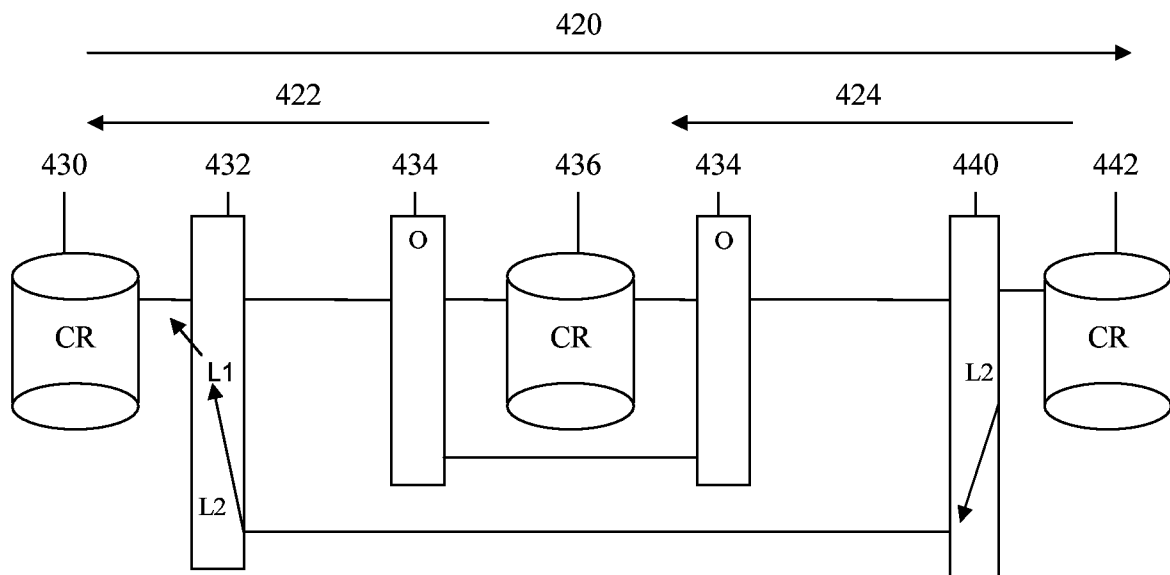
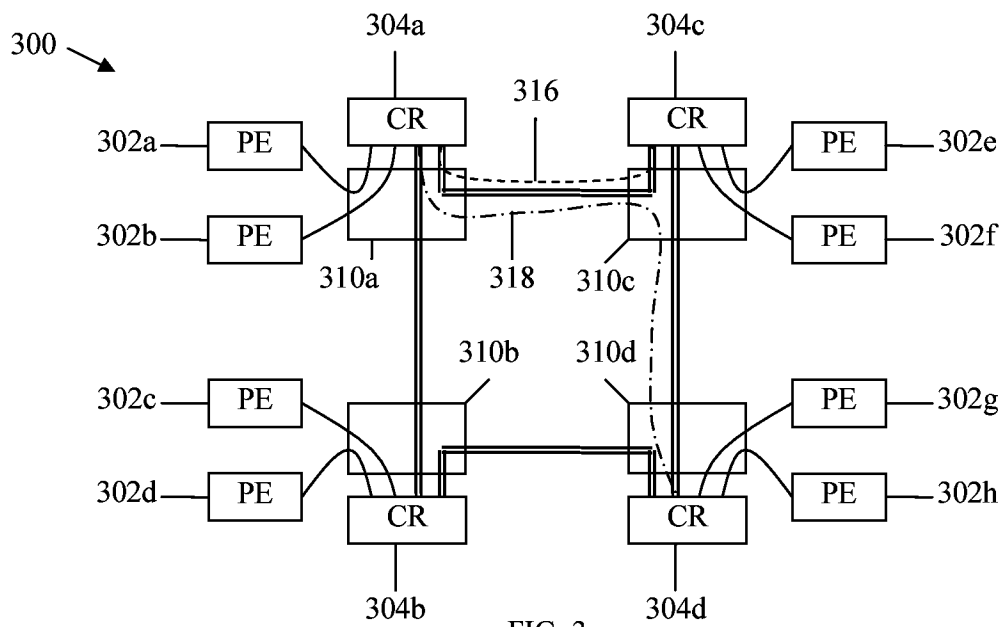


FIG. 2

-2/3-



-3/3-

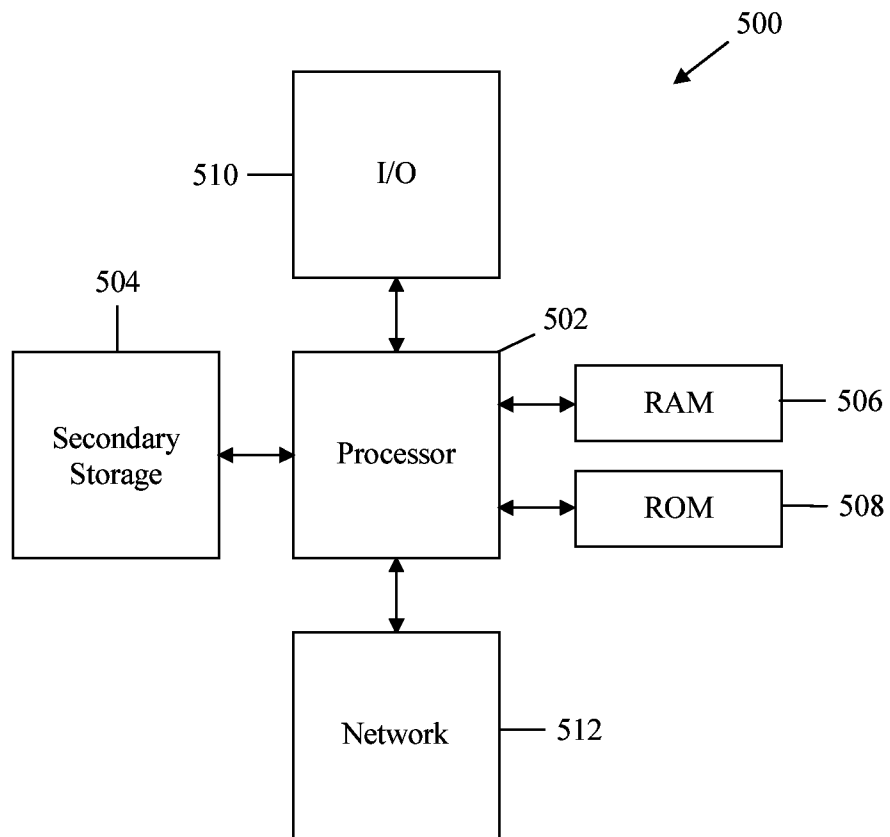


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/071524

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/56(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS,CNKI,WPI,EPODOC,PAJ: MESSAGE?, INFORMATION, FRAME?, LABEL, IDENTIFIER?, ROUT+, PATH, DIVERT+,
TRANSMIT+, TRANSPORT+, RESERV+, BYPASS+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN101035081A(HANGZHOU HUASAN COMMUNICATION TECHNOLOGY) 12 Sep. 2007(12.09.2007) the whole document	1-20
A	CN1747456A(MICROSOFT CORP) 15 Mar. 2006(15.03.2006) the whole document	1-20
A	JP2006129359A(NTT COMMUNICATIONS KK) 18 May 2006(18.05.2006) the whole document	1-20
A	EP1379036A1(ALCATEL et al.) 07 Jan. 2004(07.01.2004) the whole document	1-20

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 17 Jul. 2009(17.07.2009)	Date of mailing of the international search report 06 Aug. 2009 (06.08.2009)
---	--

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer

CHAO Lulin

Telephone No. (86-10)62411499

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2009/071524

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The independent claim 1 and the independent claims 8,18 disclose two inventions:

The independent claim 1 requests for a network component comprising at least one processor, which analyzes a path reservation message comprising a reserved path identifier and analyzes a plurality of frames each comprising a path identifier and diverts the frames away from a router, wherein the path identifier in the diverted frames matches the reserved path identifier. The independent claim 8 requests for a system comprising a packet-aware transport box configured to forward any frames that should bypass the first router to a second router. The independent claim 18 requests for a method comprising configuring a bypass path and routing a plurality of data frames to the bypass path.

There is no same or corresponding special technical feature between the independent claim 1 and the independent claims 8,18. They don't belong to a single invention concept. Therefore, the claims 1-7 and the claims 8-20 lack unity of invention and don't comply with PCT Rules 13.1, 13.2 and 13.3.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/071524

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101035081A	12.09.2007	None	
CN1747456A	15.03.2006	US2006050648A1	09.03.2006
		EP1635521A1	15.03.2006
		JP2006094488A	06.04.2006
		KR20060092859A	23.08.2006
JP2006129359A	18.05.2006	None	
EP1379036A1	07.01.2004	US2004004955A1	08.01.2004
		DE60304082E	11.05.2006
		EP1379036B1	22.03.2006
		AT321403T	15.04.2006