

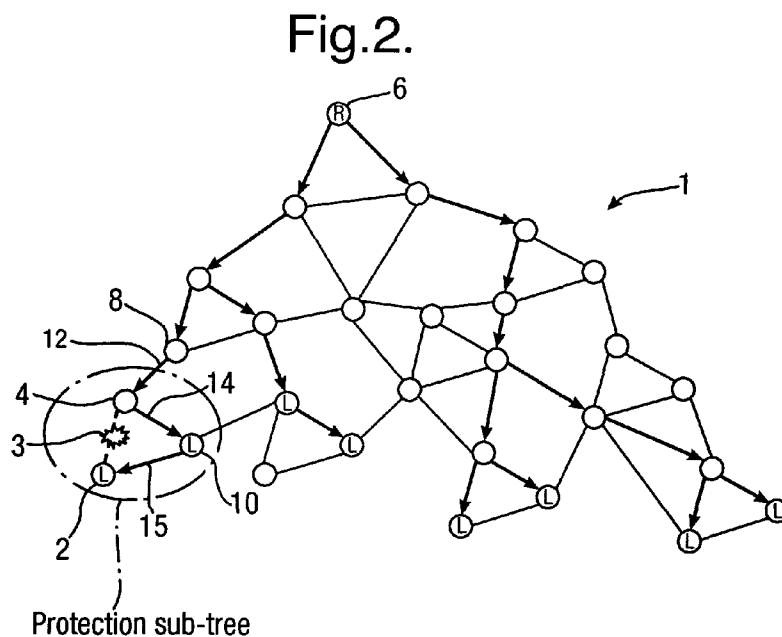


- (51) **International Patent Classification:**
H04L 12/56 (2006.01)
- (21) **International Application Number:**
PCT/EP2008/058844
- (22) **International Filing Date:**
8 July 2008 (08.07.2008)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
08156047.6 12 May 2008 (12.05.2008) EP
- (71) **Applicant (for all designated States except US):** TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; Torshamnsgaten 23, S-16483 Stockholm (SE).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** CORTI, Andrea [IT/IT]; Via degli Oleandri, 10/2, I-17019 Varazze (SV) (IT). FIORONE, Raoul [IT/IT]; Via Sbarbaro 3/17, I-16035 Rapallo (GE) (IT). MARTINOTTI, Riccardo [IT/IT]; Vico dei Gallico 1/B/4, I-17100 Savona (IT).
- (74) **Agent:** STASIEWSKI, Piotr; Ericsson Ltd, Maplewood, Chineham Business Park, Basingstoke Hampshire RG24 8YB (GB).

- (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, 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).

Published:
— with international search report (Art. 21(3))

(54) **Title:** RE-ROUTING TRAFFIC IN A COMMUNICATIONS NETWORK



(57) **Abstract:** Method of re-routing traffic in a communications network (1) in the event of a fault (3) on a path across the network, the method comprising, determining whether a first node (4), located between the fault and a network ingress node (6), is capable of switching traffic to an alternative path which avoids the fault, and if the first node is determined to be not so capable, then determining whether a second node (8), located upstream of the first node, is capable of switching traffic to an alternative path which avoids the fault.

WO 2009/138133 A1

RE-ROUTING TRAFFIC IN A COMMUNICATIONS NETWORK

TECHNICAL FIELD

The present invention relates generally to re-routing traffic in a communications
5 network.

BACKGROUND

Despite the publicity on multimedia services which require a point-to-multipoint
connectivity, like television streams multicast over Internet Protocol (IPTV), the
support of E-Tree services is a recent event in Connection Oriented – Packet
10 Switched (CO-PS) networks, like Multi Protocol Label Switching (MPLS),
Transport MPLS (T-MPLS) or Provider Backbone Bridging Engineering (PBB-
TE). The debate is still open on how to efficiently support E-Tree services and
provide the required network resiliency in CO-PS networks. Some doubt has been
instilled that CO-PS networks are not really as good as Connectionless – Packet
15 Switched (CL-PS) networks for such services. Currently, no finalized standard
solution exists.

Existing connectionless options like Ethernet-based networks (e.g. Provider Bridge
or Provider Backbone Bridge) still rely on very basic control plane solutions for
both loop avoidance and resiliency, like the few variants of the Spanning Tree
20 Protocol. Along with their limited capability to implement sophisticated traffic
engineering, this is one of the reasons why the move towards CO-PS networks is
ineluctably taking place, forcing the standard making bodies and the technical
community to face the issues related to the efficient support of E-Tree services.

Ultimately, solutions which completely rely on Layer 3 of the Open Systems
25 Interconnection (OSI) Basic Reference Model (i.e. the IP layer) are unsuitable,
cost inefficient and of inappropriate complexity, especially in relation to
metropolitan networks.

Standard-making bodies are currently working on a definition of a proper network infrastructure to support E-Tree services with the required degree of efficiency. No complete interoperable solution has been finalized so far for point-to-multipoint infrastructures, but there have been several attempts to solve this problem in CO-PS networks. The most efficient solutions make use of tree infrastructures built in the CO-PS network that connect an ingress or root node (which is a node where the E-Tree service enters the network/sub-network) to the several egress nodes (which are the destinations of the E-Tree service), with the aim of optimizing the overall use of network resources. Extensive literature is available on how to build an optimum tree for a particular network topology and possible constraints. In addition, resiliency is a basic requirement for this kind of service, because revenue generating applications, like IPTV, cannot be delivered to paying customers with poor quality or unacceptable interruptions. This tree infrastructure therefore needs to be protected against link or node failures, possibly in a non-traffic consuming way, like in 1:1 or restoration schemes, where the traffic is sent onto a backup path when the primary path has failed.

A few known solutions address this requirement, with local repair schemes, like Fast ReRoute (FRR) in MPLS, or with global repair schemes whose operation consist in providing a complete backup tree. A limitation of local repair schemes is that in the case of node failure the tree infrastructure needs to be locally modified, because some other node in the network needs to forward the traffic in a different way to make up for the failed node and ensure the E-Tree service traffic continuity. This can be difficult to implement, require a very high degree of complexity and result in a longer recovery time. In addition, traffic duplication is possible during fault conditions. Besides the need to actually configure a potentially very high number of alternative paths in order to avoid issues with single points of failure, the main limitation of FRR lies in its necessarily local repair nature, which is not particularly well suited for a potentially non-trivial tree infrastructure.

In the case of global repair schemes, irrespective of where and what the fault condition is in the active tree infrastructure, all of the traffic related to the E-Tree service is switched to the backup tree. This can be particularly problematic for the egress nodes, since even though the switching time is kept to a minimum, all such nodes will see an impact on the traffic, even those which are remote from where the fault has occurred. To add further complexity to such a scenario, E-Tree specific control plane protocols, like for instance IGMP in case of IPTV, can experience difficulties and may need to recover updated information on the backup tree before allowing the traffic to be forwarded normally again. This can lead to an even longer time for the protection scheme to finally converge and return to normal operation.

SUMMARY

According to one aspect of the invention there is provided a method of re-routing traffic in a communications network in the event of a fault on a path across the network. The method comprises, determining whether a first node, located between the fault and a network ingress node, is capable of switching traffic to an alternative path which avoids the fault. If the first node is determined to be not so capable, then determining whether a second node, located upstream of the first node, is capable of switching traffic to an alternative path which avoids the fault.

According to another aspect of the invention there is provided a communications network comprising a plurality of nodes which are connected by respective links to form a path for traffic across the network. The nodes comprising at least one re-routing node configured to determine that a fault has occurred between the re-routing node and a network egress node, and the re-routing node configured to determine if it is able to switch traffic onto an alternative path to avoid the fault. If it is not so able then the re-routing node configured to cause a fault notification signal to be

sent to an upstream node, and the upstream node configured to determine if it is able to switch traffic to an alternative path to avoid the fault.

According to a further aspect of the invention there is provided a node for use in a communications network. The node comprises a processor
5 configured to determine that a fault in the network has occurred and configured to determine whether it is capable causing traffic to be switched to an alternative path. In the event that the processor determines that it is not so capable, the processor configured to cause a fault notification signal to be transmitted for reception by a second node.

10 According to yet a further aspect of the invention there is provided a method of configuring a communications network to provide at least one alternative path in the event that a fault occurs in a path across the network. The method comprises configuring at least one re-routing node
15 of the network to determine that the fault has occurred, and configuring the at least one node to determine whether it is able to switch the traffic to an alternative path to avoid the fault. The method also comprises configuring the node such that if the node determines that it is not so able then the node issues a fault notification signal to another node.

According to another aspect of the invention there is provided machine-readable
20 instructions to configure a node, the instructions comprising instructions to cause a processor of the node to determine that a fault has occurred in a communications network in which the node is to be located, instructions to cause a processor to determine whether the node is capable of providing a switch to divert traffic onto an alternative path to avoid the fault, and instructions to cause the processor to
25 bring about the node issuing a fault notification signal if the node is determined not to be so capable

DESCRIPTION OF THE DRAWINGS

Various embodiments of the invention will now be described, by way of example only, in which:

Figures 1 to 4 show a communications network,

Figure 1a is a communications network node,

5 **Figure 5** is a flow diagram, and

Figure 6 is a flow diagram.

DETAILED DESCRIPTION

A network 1, which is configured to implement an embodiment of the present invention, is shown in Figure 1. The network 1 comprises a meshed
10 network and a tree structure has been identified and configured. Broadly, the network 1 comprises a plurality of nodes, shown as circular elements, and links providing communication between the nodes, the links shown by lines connecting the nodes. A root node, which is the node responsible for the distribution of an E-tree service within the network 1, and may be
15 termed a network ingress node is designated by the letter "R". The network 1 further comprises a plurality of leaf or egress nodes, which are the nodes attached to the destinations of the E-tree service, and are each designated by the letter "L". Each node of the network comprises a processor configured to cause received traffic to be forwarded as required. For
20 example, a node 4 comprises a processor 80, as shown in Figure 1a.

The network 1 provides an active tree structure to support the E-tree service and an associated stand-by tree structure. The stand-by tree structure is arranged to be used in what may be termed as a "fractal" manner. This means that a type of hierarchy in the active tree is created
25 such that there is the possibility to identify sub-trees which can react

autonomously to fault conditions without needing the fault condition to be notified to the root node of the whole tree in order to switch all the traffic related to the E-tree service onto a stand-by tree. The active tree structure and the stand-by tree structure (both comprising of a number of sub-trees) are identified at the time of configuring the network or when the service which needs to be supported has to be rolled-out. Path diversity between the active and the stand-by tree structures and sub-tree structure have to be configured in order to limit to a minimum number, or indeed eliminate, single points of failure. Two logically disjoint trees can always be identified, each composed of a number of sub-trees. As will be described below, in the case of fault, the tree is “repaired” as close as possible to the fault itself, performing a protection switch operation only at the most appropriate sub-tree level, if any, and not necessarily at the whole-tree level (which will occur only when no sub-tree is able to deal with the specific fault). In this way the traffic impact is confined only to the minimum and unavoidable number of leaf nodes, and not necessarily to the complete tree.

Figure 1 shows the network 1 in normal working conditions. A tree, the links of which are shown by emboldened arrows, provided by the network, comprises two main portions. These are a left sub-tree portion and right sub-tree portion, as can easily be seen in Figure 1. As will be described below, some of the nodes of the tree are configured as re-routing nodes to route traffic to an alternative path to avoid a fault.

In Figure 2 a fault condition, shown at 3, has occurred in the network 1, to a link 13 attached to a leaf node 2. This part of the tree has been configured as a sub-tree, since, due to the physical topology of the network 1, is capable of autonomously recovering from a range of faults, included the fault 3 shown in Figure 2. A node 4 serves as a re-routing node, which is the node responsible for switching the traffic from an active sub-tree (i.e. the one used in normal operating conditions) to a stand-by sub-tree, and can be termed the root of that particular sub-tree. A re-routing node is a node that has been configured to be able to switch to a stand-by alternative path (i.e. a sub-tree) whenever the node detects a downstream fault or it is notified by a downstream node about a fault event. The node's responsibilities include filtering out fault notifications which are conveyed upstream of the tree (i.e. towards the root node 6, and between the fault and the node 6) in all those cases in which that node can itself perform the switch to divert the traffic to alternative path away from the downstream fault. In this way reaction to dealing with the fault can be kept as local as possible to the fault, and no other (upstream) node which is not directly involved in the switch operation will know anything about the fault.

On determining that a downstream fault has occurred, the re-routing node 4 switches traffic destined for the leaf node 2, to be sent over link 14 to a leaf node 10, and the leaf node 10 causes the traffic to be sent over link 15 to the leaf node 2.

As a consequence of the sub-tree switch performed by the node 4, the entire tree has not needed to have been made aware of the fault, and all the nodes of the tree, except the three nodes, 2, 4 and 10, in the circle shown as 'the protection sub-tree', have seen no increase in the E-tree traffic.

In Figure 3 a different fault condition has occurred. In this case, it is a fault of the node 4, shown at 30. The stand-by sub-tree which was able to react to and recover from the fault in Figure 2, is unable to cope with this fault condition, and therefore resolving the problem must be effected closer to the root node 6 of the complete tree. This is equivalent to say that a larger sub-tree, which comprises the sub-tree mentioned in Figure 2, has to take action to recover from the fault. The re-routing node 20 indicated in Figure 3, which may be termed the root node of the larger sub-tree, is notified and is operative to switch the traffic to the relevant stand by sub-tree. The re-routing node 20 determines that a fault has occurred by way of a fault notification signal being sent over the link 11 from the node 8, which is aware of the fault. It is to be noted here that node 8 is not a re-routing node and so the node 8 is operative to forward the fault signal to the upstream node, node 20. On receiving the signal, the node 20 is configured to switch received traffic across a link 27 to a node 21, the node 21 is configured to send the traffic across the link 28 to the node 22, the node 22 is configured to send the traffic across the link 29 to the node 10 and the node 10 is configured to send the traffic across the link 15 to the leaf node 2.

A further fault condition is shown in Figure 4. Compared to the fault conditions described above, the fault occurs closer to the root node 6 of the complete tree, and the sub-tree shown in Figure 3 is not able to deal with it. It should be clear that a larger sub-tree, if available, has to react to this fault, as indicated in Figure 4. The fault, shown at 50, has occurred in a link 36 connecting nodes 20 and 31. On determining that a fault has occurred, the (re-routing) node 31 is configured to switch traffic onto an alternative path to reach the leaf node 2. As is shown in Figure 4 the alternative path comprises nodes 32, 33, 34, 35, 28 and 10 and the links 37, 38, 39, 40, 41, 29 and 15. It should be clear that a larger sub-tree, if available, has to react to this failure, as indicated in Figure 4.

In case no sub-tree can be effective to recover from a fault condition, the whole tree may be involved in the protection switch, and in that situation the root node 6 of the complete tree performs the necessary switch to divert the traffic onto an alternative path.

- 5 It will also be appreciated that all the fault conditions which have been discussed above have no impact on the leaf nodes on the right end side part of the complete tree.

It will be appreciated that those nodes which are involved in providing an alternative path are suitably configured in an initial set-up procedure so
10 that diverted traffic arriving at those nodes is sent to the next node of the alternative path. This may be achieved in an initial set-up procedure by suitably configuring forwarding tables of each of the nodes.

In the above described three fault conditions, three re-routing nodes, 4, 20 and 31
15 at different levels in the tree infrastructure have been mentioned. Each of those nodes corresponds to what may be termed as a respective sub-root node of three protected sub-trees (i.e. each sub-tree comprises an active and a stand-by tree), and plays a special role in providing an alternative path.

The re-routing nodes are responsible for two possible courses of action:

- 20 - to provide fault recovery by way of a switch operation, with no further notification signal towards upstream nodes

or

- to delegate protection to an upper sub-tree by sending a fault notification signal.

- It is to be noted that the fault notification signal is conveyed upstream of the tree, because this allows an effective realization of the method of re-routing. Provided that the re-routing nodes are not in a fault condition, they are responsible for determining whether a fault notification signal which they receive in response to a
- 5 fault condition (however they may also, or alternatively, detect a fault condition directly) can be locally repaired, by switching the traffic onto a stand-by sub-tree, of which they are the root, or whether, instead, they need to forward a fail notification signal to an upper layer of the tree, which can be a larger sub-tree (which includes their own sub-tree) or the complete tree.
- 10 Fault notification signals can conveniently be implemented using known techniques, such as Operation Administration and Maintenance (OAM) packets or Control Plane protocols (also depending on the actual technology which has been used for the CO-PS network) or by a proprietary message set.
- 15 Figure 5 is a flow diagram showing the overall re-routing method effected by the network 1. At 100, a fault has occurred in the network. At step 101, the fault is detected by a node. If the node is a re-routing node then the procedure proceeds to step 104. If the node is not a re-routing node then, as shown at step 103, a fault notification signal is sent upstream. At the
- 20 point at which a re-routing node is reached, as shown at step 104, the node determines whether it can recover the fault by a switching the traffic to an alternative path. If it can, then, as shown at step 105, a switch operation is effected (so as to recover the fault), and no fault notification signal is sent upstream to another node. If, however, the re-routing node is unable to
- 25 recover the fault, then at step 106 it is determined whether the node is in fact the root node of the tree. If that node is the root node, then a disjoint protection path is not available. If the node is not the root node then the procedure returns to step 103.

Figure 6 is a flow diagram of the steps taken by a re-routing node. At 200, a fault notification signal is sent by a downstream node to the re-routing node. On receipt of the signal, step 201 requires that the re-routing node determines whether the node is able to recover the fault by switching the traffic to alternative path. If the re-routing node determines that it is so able, then the node performs the step 202 to divert the traffic to an alternative path. This results in the outcome 203. If the re-routing node determines that it is not so able, then as shown at steps 204 and 205, the node does not perform a switch operation to divert the traffic to an alternative path, rather it sends a fault notification signal to an upstream node. From the re-routing node's perspective this results in the outcome 206. It is to be noted that a reason why a re-routing node may not be able to switch traffic onto an alternative path is that a link, which forms part of a stand-by tree connected to the node may be faulty or another node at the opposite end of that link may be faulty. In that scenario an upstream re-routing node would be sought, in accordance with the steps shown in Figure 5. It will be appreciated that that re-routing nodes can be suitably configured by way of machine-readable instructions, whether in the form of a signal, a data structure or a software product.

There are numerous advantages to the network 1. Fault recovery is capable of being performed by each sub-tree close to the failure point, so that only the minimum number of components of the network are affected by the re-routing method. In the case of a failure affecting a node or a portion of the tree where protection locally would require high complexity, fault recovery is “scaled” to an upper level sub-tree where the fault can be simply bypassed by an alternative path. This may be viewed as a tree infrastructure composed of a set of sub-trees hierarchically organized. The desired behavior can be deterministically achieved because the re-routing nodes are configured to react to a failure in a pre-determined 1:1 fashion, i.e. in the case of fault traffic is switched from an active sub-tree to a stand-by sub-tree.

In this way, by suitably configuring the protected tree and the protected sub-trees, thanks to the re-routing method, traffic disturbances to an E-tree service due to a fault are minimized and confined locally as far as is possible (or as locally as it is considered beneficial by a network operator). Given that every standby sub-tree is configured prior to any fault condition, a switch operation to divert the traffic to an alternative path can take place very quickly. This is particularly advantageous over known local repair schemes which require a node to be re-configured ‘on the fly’ when a fault occurs. Advantageously, the re-routing method performed by the network 1 is not limited to any particular connection orientated technology.

Path protection provided by the re-routing method in the network 1 is advantageously not limited in its application to any specific connection-oriented technology.

It is to be noted that even in the case of single points of failure, due to physical topology constraints active and stand-by trees and sub-trees remain logically separate, so that there is no risk of erroneous forwarding of the traffic.

It will be appreciated that although the above network implements a multicast solution, the method of re-routing traffic implemented by the network 1 is also applicable to unicast scenarios.

CLAIMS

1. Method of re-routing traffic in a communications network (1) in the event of a fault (3) on a path across the network, the method comprising,
5 determining whether a first node (4), located between the fault and a network ingress node (6), is capable of switching traffic to an alternative path which avoids the fault, and if the first node is determined to be not so capable, then determining whether a second node (8), located upstream of the first node, is capable of switching traffic to an alternative path which
10 avoids the fault.
2. Method as claimed in claim 1 in which at least one further node determines whether it is capable of switching the traffic to an alternative path in the event that the second node (8) determines that it is not so capable.
- 15 3. Method as claimed in claim 1 or in claim 2 in which the first node (4) neighbours the fault (3).
4. Method as claimed in claim 1, 2 or 3 in which the first node (4) determines that the fault (3) has occurred.
5. Method as claimed in any preceding claim in which the second node (8)
20 neighbours the first node.
6. Method as claimed in any preceding claim in which if the first node (4) determines that it is unable to switch traffic to an alternative path, then said first node sends a fault notification signal to the second node (8).

7. Method as claimed in any preceding claim in which if the first node (4) determines that it is able to switch traffic to an alternative path, then a fault notification signal is not sent to the second node (8).
8. A communications network (1) comprising a plurality of nodes (4, 6, 8, 10) which are connected by respective links (11, 12, 13, 14, 15) to form a path for traffic across the network, the nodes comprising at least one re-routing node (4) configured to determine that a fault (3) has occurred between the re-routing node and a network egress node (2), and the re-routing node configured to determine if it is able to switch traffic onto an alternative path to avoid the fault, and if it is not so able then the re-routing node configured to cause a fault notification signal to be sent to an upstream node (8), and the upstream node configured to determine if it is able to switch traffic to an alternative path to avoid the fault.
9. Communications network as claimed in claim 8 in which the at least one re-routing node (4) is configured to switch traffic to at least one alternative path.
10. Communications network as claimed in claim 8 or claim 9 in which the at least one re-routing node (4) is connected to at least three links (13, 8, 14).
11. Communications network as claimed in any of claims 8 to 10 in which if the at least one re-routing node (4) determines that it is able to switch traffic to an alternative path, then the re-routing node is configured not to send fault notification signal is not sent to the second node (8).
12. Communications network as claimed in any of claims 8 to 11 which is a connection-orientated network

13. A node (4) for use in a communications network (1), the node comprising a processor (80) configured to determine that a fault (3) in the network has occurred and configured to determine whether it is capable causing traffic to be switched to an alternative path, and in the event that the processor determines that it is not so capable, the processor configured to cause a fault notification signal to be transmitted for reception by a second node (8).
14. A node (4) as claimed in claim 13 in which if the processor (80) determines that the node is capable of causing traffic to be switched to another path then the processor configured to cause that the fault notification signal is not sent.
15. Method of configuring a communications network (1) to provide at least one alternative path in the event that a fault (3) occurs in a path across the network, the method comprising configuring at least one re-routing node (4) of the network to determine that the fault has occurred, and configuring the at least one node to determine whether it is able to switch the traffic to an alternative path to avoid the fault, and configuring the node such that if the node determines that it is not so able then the node issues a fault notification signal to another node (8).
16. Machine-readable instructions to configure a node (4), the instructions comprising instructions to cause a processor (80) of the node to determine that a fault (3) has occurred in a communications network in which the node is to be located, instructions to cause a processor to determine whether the node is capable of providing a switch to divert traffic onto an alternative path to avoid the fault, and instructions to cause the processor to bring about the node issuing a fault notification signal if the node is determined not to be so capable.

Fig. 1.

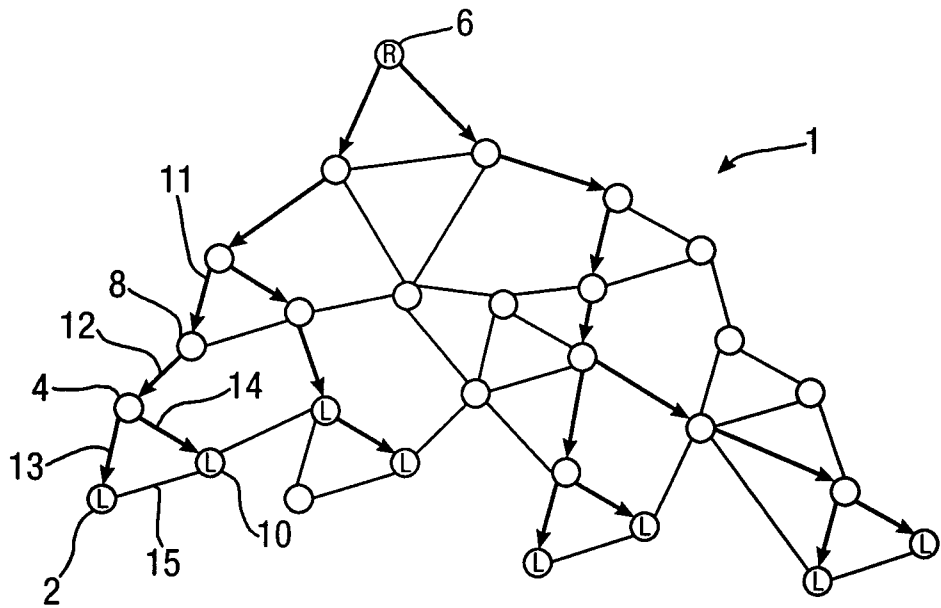


Fig. 1a.

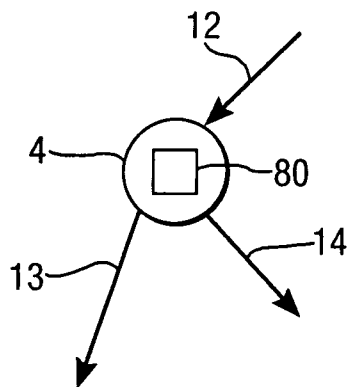


Fig.2.

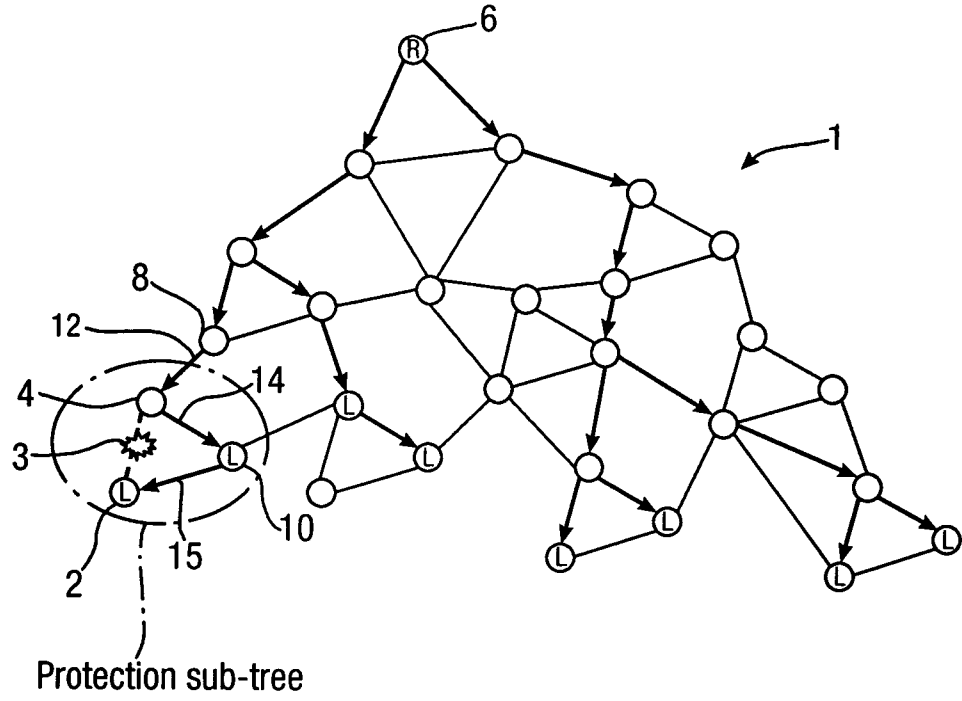


Fig.3.

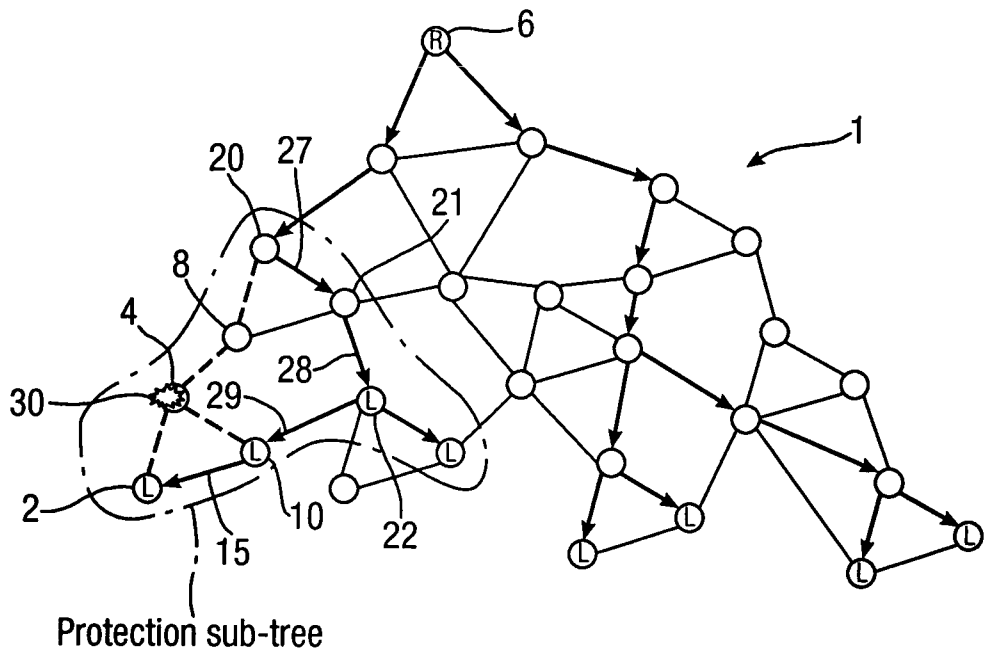


Fig.4.

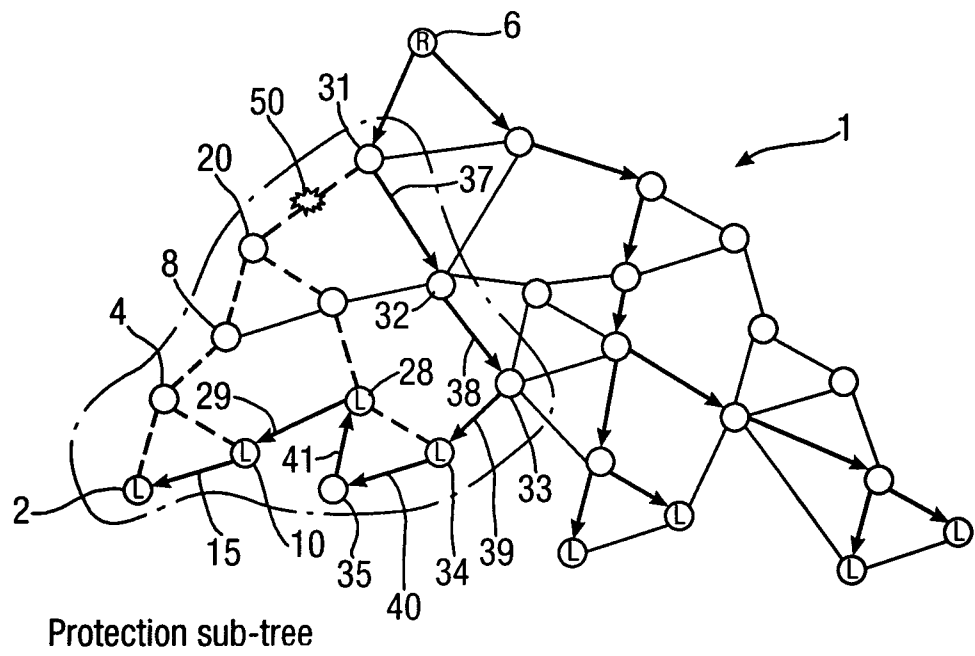


Fig.5.

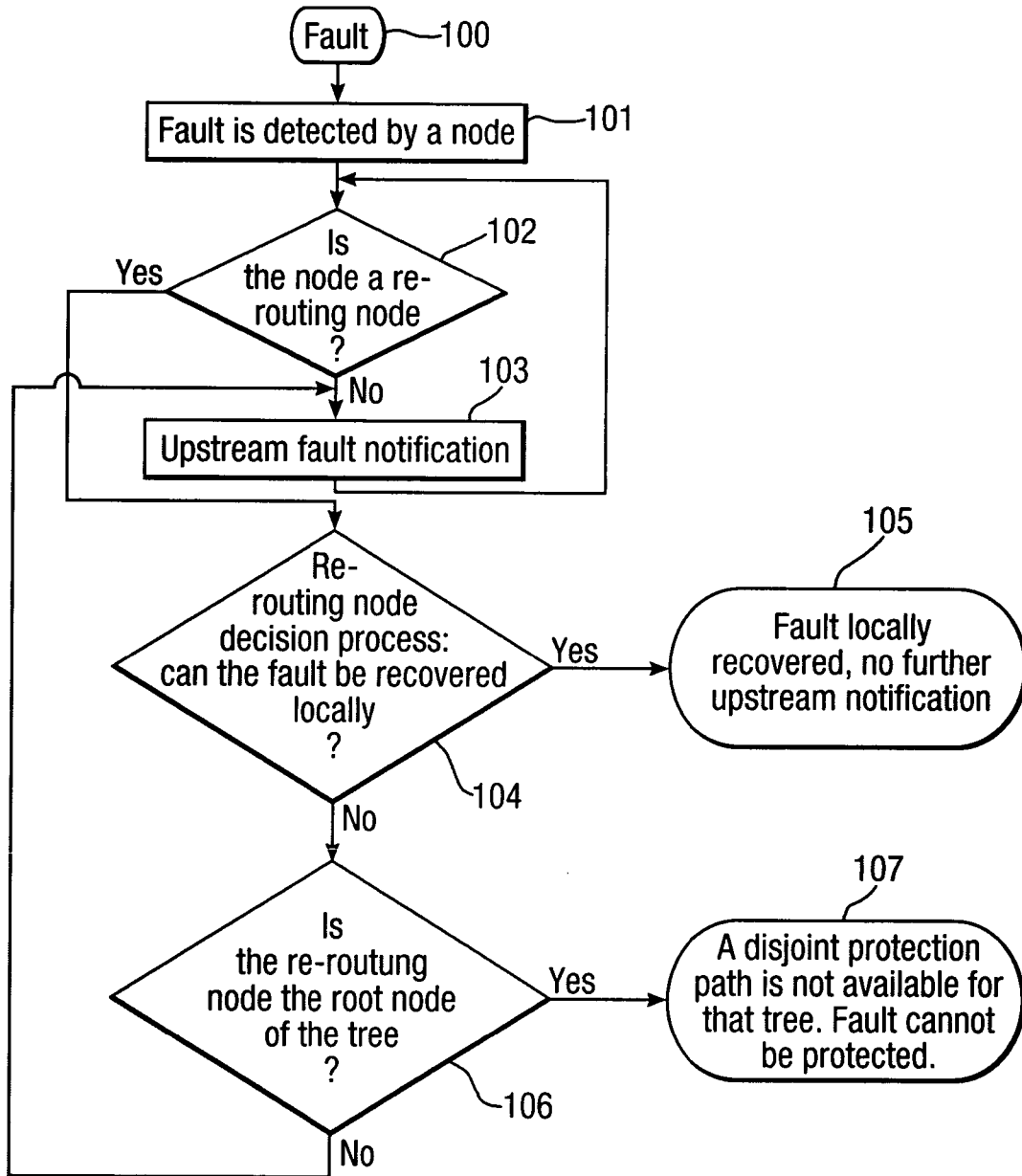
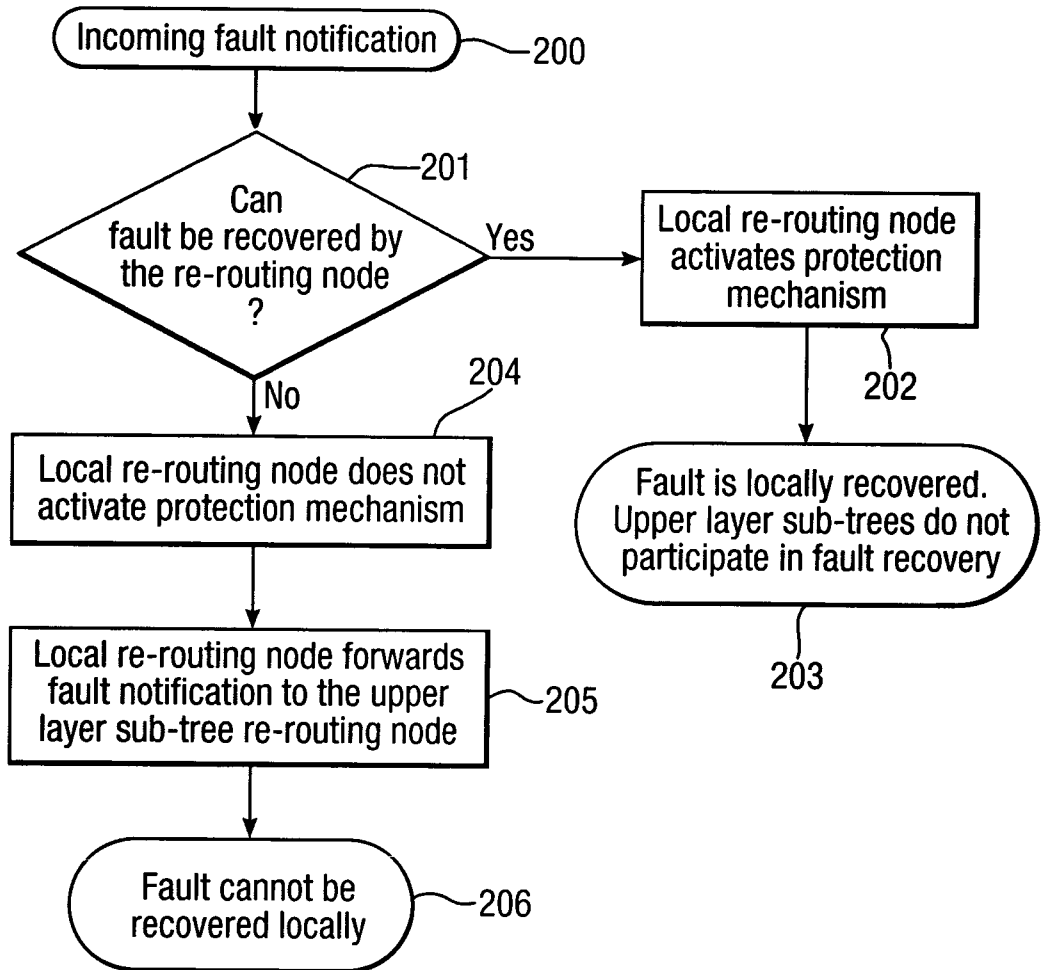


Fig.6.



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/058844

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/56

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)
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 practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 859 491 A (ALSTHOM CGE ALCATEL [FR] CIT ALCATEL [FR]) 19 August 1998 (1998-08-19) column 1, lines 1-4, 41-47 column 3, lines 49-51 column 9, lines 31-45 column 10, lines 4-12	1-16
X	EP 1 608 111 A (SONY CORP [JP]) 21 December 2005 (2005-12-21) paragraph [0013] paragraph [0015]	1-16

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *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)
- *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

- *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
- *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
- *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.
- *Z* document member of the same patent family

Date of the actual completion of the international search 12 August 2008	Date of mailing of the international search report 21/08/2008
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Clemente Lafuente, G

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2008/058844

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
EP 0859491	A	19-08-1998	AT 315861 T	15-02-2006
			AU 740234 B2	01-11-2001
			AU 5300798 A	20-08-1998
			CA 2227111 A1	18-08-1998
			DE 69735084 T2	31-08-2006
			JP 10243029 A	11-09-1998
			US 6115753 A	05-09-2000
EP 1608111	A	21-12-2005	WO 2004082225 A1	23-09-2004
			KR 20050114654 A	06-12-2005
			US 2006268688 A1	30-11-2006