(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 May 2009 (07.05.2009)

PCT

(10) International Publication Number
WO 2009/058519 A1

(51) International Patent Classification:
G01R 31/08 (2006.01)

(21) International Application Number:
PCT/US2008/078984

(22) International Filing Date: 6 October 2008 (06.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/001,150	30 October 2007 (30.10.2007)	US
12/050,118	17 March 2008 (17.03.2008)	US
12/050,121	17 March 2008 (17.03.2008)	US

(71) Applicant *(for all designated States except US)*: **REDBACK NETWORKS INC.** [US/US]; 300 Holger Way, San Jose, CA 95134 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MEHTA, Rishi** [US/US]; 4459 Crocus Drive, San Jose, CA 95136 (US). **KINI, Sriganesh** [IN/US]; 373 River Oaks Circle Apartment 1704, San Jose, CA 95134 (US).

(74) Agents: **AMINI, Farzad** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 1279 Oakmead Parkway, Sunnyvale, CA 94085-4040 (US).

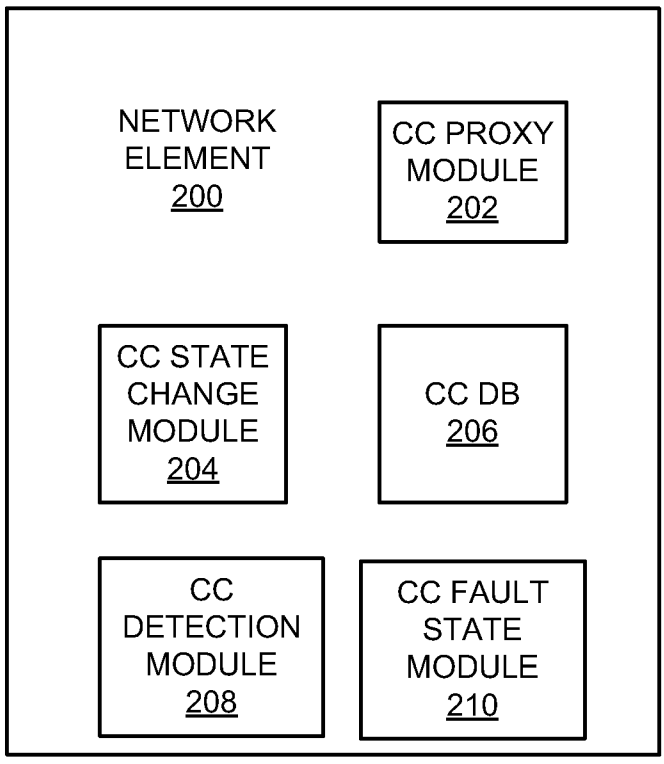
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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,

[Continued on next page]

(54) Title: SCALABLE CONNECTIVITY FAULT MANAGEMENT IN A BRIDGED/VIRTUAL PRIVATE LAN SERVICE ENVIRONMENT

FIGURE 2



(57) Abstract: A method and apparatus that proxies connectivity check messages and sends fault state changes messages across an MPLS/VPLS network is described. A network element proxies connectivity check messages for remote maintenance endpoints based on a local database. The network element updates the database based on received fault state change message that identify a fault state change of a remote maintenance endpoint. The network element detects fault state changes of local maintenance endpoints and sends a fault state change message to other network elements that proxy connectivity check message for the local maintenance endpoints.

WO 2009/058519 A1

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*

SCALABLE CONNECTIVITY FAULT MANAGEMENT IN A BRIDGED/VIRTUAL PRIVATE LAN SERVICE ENVIRONMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. provisional patent application number 61/001,150, entitled "SCALABLE CONNECTIVITY FAULT MANAGEMENT IN A BRIDGED/VIRTUAL PRIVATE LAN SERVICE ENVIRONMENT", filed October 30, 2007.

BACKGROUND

Field

[0002] Embodiments of the invention relate to the field of computer networking; and more specifically, supporting scalable connection fault management (CFM) in a bridged or virtual private local area network (LAN) service environment.

Background

[0003] Operation, Administration, and Maintenance (OAM) describes processes, activities, tools, standards, etc., involved with operating, administering, and maintaining computer networks. OAM is implemented for many different types of computer networks, such Ethernet, Internet Protocol (IP), multi-protocol label switching (MPLS), asynchronous transfer mode (ATM), virtual private LAN service (VPLS), etc. Each type of network will have a different type of OAM. For example, in an Ethernet network, 802.1ag Connectivity Fault Management (CFM) is used as an OAM management tool, and in a MPLS/VPLS network Virtual Circuit Connectivity Verification (VCCV) is used as an OAM tool. OAM tools are used, in part, to detect network connectivity faults, herein referred to as

faults. A fault can be when a network device loses connectivity to the network. OAM tools detect a fault state change, such when a device becomes active on the network, by connecting to the network or becoming active on the network. Furthermore, a fault state change can be when a network loses connectivity to the network.

[0004] Figure 1 illustrates one embodiment of network 100 CFM across a switched Ethernet and VPLS/MPLS environment. Network 100 is a heterogeneous network comprising two switched Ethernet networks 116A-B interconnected by a VPLS service provider network 106. In Figure 1, Ethernet networks 116A-B are geographically dispersed. VPLS is a way to provide Ethernet based multipoint-to-multipoint communication over IP/MPLS networks. It allows geographically dispersed sites, such as Ethernet networks 116A-B to share an Ethernet broadcast domain by connecting sites through psuedowires. In VPLS, the LAN of each Ethernet network 116A-B is extended to edge of service provider network 106 and service provider network 106 emulates a switch or bridge to connect the customer LANs of Ethernet networks 116A-B to create a single bridged LAN. Coupling switched Ethernet networks 116A-B and VPLS network 106 at the edge of each network are network elements 104A-B. While in one embodiment, network elements 104A-B are edge routers, in alternative embodiments, network elements 104A-B are the same and/or different type of network element (switch, router, core router, etc.) For example, network element 104A couples switched Ethernet network 116A and VPLS network 106, while network element 104B couples switched Ethernet network 116B and VPLS network 106.

[0005] Each of switched Ethernet networks comprises maintenance endpoints (MEPs) coupled to the edge network elements. An MEPs is an actively managed CFM entity which can generate & receive CFM messages and track any responses such as personal computers, servers, bridges, switches, and other possible devices participating in Ethernet network. As illustrated in Figure 1,

Ethernet network 116A comprises maintenance endpoints 102A-C coupled to network element 104A and Ethernet network 116B comprises maintenance endpoints 102D-F coupled to network element 104B.

[0006] VPLS network 106 comprises network elements 108A-D, where network elements 108A and C couple to network element 104A and network elements 108B and D couple to network element 104B. Network elements 108A-B forward traffic between network elements 104A-B with pseudowire 110A. Network elements 108C-D forward traffic between network elements 104A-B with pseudowire 110B.

[0007] CFM is a standard that specifies protocols and protocol entities within virtual LAN (VLAN) aware bridges (such as network elements 104A-B) that provides capabilities for detecting, verifying, and isolating faults in VLANs. These capabilities can be used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment. CFM defines a maintenance domain that as a network or part of the network for which faults in connectivity can be managed. Within each maintenance domain, there are several MEPs. An MEP is an actively managed CFM entity, which initiates, terminates, and reacts to CFM flows associated within a specific maintenance domain. Periodically, each MEP sends connectivity check messages to the other MEP in the maintenance domain. The connectivity check message is a multicast, unidirectional heartbeat that signals that the MEP sending the connectivity check message is up and coupled to the network. An MEP sending an initial connectivity check message signifies to other MEPs in the maintenance domain that the MEP has become active in this domain. Lack of connectivity check message from a particular MEP indicates to the other MEPs that the particular MEP is down or not participating in the domain.

[0008] In Figure 1, MEPs 102A-C and D-F periodically send out connectivity check messages 112A-C and 114A-C, respectively. Each MEP can send out connectivity check messages every 3.3 milliseconds. These messages are

multicast to all the other MEPs in the maintenance domain. Because the MEPs of the different Ethernet networks 116A-B belong to the same maintenance domain, the connectivity check messages are transmitted across VPLS network 106 via network elements 104AB to the MEPs in different Ethernet networks 116AB. In addition, because the connectivity check messages are multicast, network elements 104AB broadcast these messages to each of the pseudowires coupled to the respective network element 104AB in VPLS network 106.

[0009] Although CFM can provide an end-to-end fault management scheme for heterogeneous network 100, CFM is not scalable because of the flooding of the connectivity check (CC) messages by network elements 104A-B. As the number of MEPs in the maintenance domain increase, the amount of CC messages transmitted across VPLS network increases dramatically.

BRIEF SUMMARY

[0010] A method and apparatus that proxies connectivity check messages and sends fault state changes messages across an MPLS/VPLS network is described. A network element proxies connectivity check messages for remote maintenance endpoints based on a local database. The network element updates the database based on received fault state change message that identify a fault state change of a remote maintenance endpoint. The network element detects fault state changes of local maintenance endpoints and sends a fault state change message to other network elements that proxy connectivity check message for the local maintenance endpoints.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Embodiments of the invention may be best understood by referring to the following description and accompanying drawings which illustrate such embodiments. The numbering scheme for the Figures included herein is such that the leading number for a given element in a Figure is associated with the number

of the Figure. However, element numbers are the same for those elements that are the same across different Figures. In the drawings:

[0012] Figure 1 (Prior Art) illustrates one embodiment of network supporting CFM across a switched Ethernet and VPLS/MPLS environment.

[0013] Figure 2 is a block diagram of a network element that supports proxying connectivity check messages for remote MEPs and sending VCCV messages to other network elements based on MEP fault state changes according to one embodiment of the invention.

[0014] Figure 3 is illustrates one embodiment of a network supporting scalable CFM across a switched Ethernet and VPLS/MPLS environment according to one embodiment of the invention.

[0015] Figure 4 is an exemplary flow diagram for proxying CC messages for remote MEPs according to one embodiment of the invention.

[0016] Figure 5 is an exemplary flow diagram for sending VCCV messages to other network elements based on MEP fault state changes according to one embodiment of the invention.

[0017] Figure 6 is a block diagram illustrating an exemplary network element that handles proxying CC messages and sending VCCV messages according to one embodiment of the system.

DETAILED DESCRIPTION

[0018] In the following description, numerous specific details such as network element, line card, fault, fault management, packet, maintenance endpoint, LAN, VPLS, MPLS and interrelationships of system components are set forth in order to provide a more thorough understanding of the invention. It will be appreciated, however, by one skilled in the art that the invention may be practiced without such specific details. In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in

order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

[0019] References in the specification to "one embodiment", "an embodiment", "an example embodiment", etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to affect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

[0020] In the following description and claims, the term "coupled," along with its derivatives, is used. "Coupled" may mean that two or more elements are in direct physical or electrical contact. However, "coupled" may also mean that two or more elements are not in direct contact with each other, but yet still co-operate or interact with each other. Exemplary embodiments of the invention will now be described with reference to Figures 2-6. In particular, the operations of the flow diagrams in Figures 4 and 5 will be described with reference to the exemplary embodiments of Figures 2, 3 and 6. However, it should be understood that the operations of these flow diagrams can be performed by embodiments of the invention other than those discussed with reference to Figures 2, 3 and 6 and that the embodiments discussed with reference to Figures 2, 3 and 6 can perform operations different than those discussed with reference to these flow diagrams.

[0021] A method and apparatus for proxying connectivity check (CC) messages for remote MEPs and sending MEP fault state changes across an MPLS/VPLS network is described. According to one embodiment of the invention, a network element proxies connectivity check messages by periodically sending out connectivity check messages to MEPs in the local network of the network

element. The network element transmits connectivity check messages for each of the active remote MEPs identified in a remote MEP database. The network element proxies the connectivity check message by creating the connectivity check message that mimics a message as if originated by one of the remote MEPs. According to another embodiment of the invention, the network element detects fault state changes of local MEP by the absence or appearance of connectivity check messages from local MEPs. The network element determines which local MEP had the fault state change and formats a VCCV message indicating the fault state change for that local MEP. The network element sends this VCCV message to other network elements that proxy connectivity check messages for remote MEPs.

[0022] Figure 2 is a block diagram of network element 200 that supports proxying connectivity check messages for remote MEPs and sending VCCV messages to other network elements based on MEP fault state changes according to one embodiment of the invention. A remote MEP is a MEP that reachable by traversing a VPLS network. A local MEP is part of the same Ethernet network as the proxying network element. For example and by way of illustration, in Figure 1, MEPs 102A-C are remote to network element 104B and local to network element 104A. MEPs 102D-F are remote to network element 104A and local to network element 104B.

[0023] In Figure 2, network element 200 comprises connectivity check proxy module 202, connectivity check state change module 204, connectivity check database 206, connectivity check module 208, and connectivity check fault state change module 210. Connectivity check proxy module 202 proxies connectivity check messages for remote MEPs by periodically transmitting connectivity check message representing remote MEPs to MEPs local to network element 200. For example and by way of illustration, network element 104A transmits connectivity check messages 114D-F representing MEPs 102D-F to MEPs 102A-C. In one embodiment, each of the connectivity check message transmitted is formatted to

appear as if the connectivity check message originated from one of the active remote MEPs. In one embodiment, each of the proxied connectivity check message comprises the MAC address of an active remote MEP and an identifier called MEPID that uniquely identifies the MEP. In one embodiment, connectivity check module 202 transmits a connectivity check message for each active remote MEP up to every 3.3 milliseconds.

[0024] Examples of the modules of network element 200 will be made with reference to Figure 3. Figure 3 is illustrates one embodiment of a network 300 supporting scalable CFM across a switched Ethernet and VPLS/MPLS environment according to one embodiment of the invention. Figure 3 is similar to Figure 1, in that MEPs 102A-C and D-F are sending to connectivity messages 112A-C and 114A-C, respectively. However, network elements 304A-B do not forward these messages to across VPLS network 306 as in Figure 1 as will be described below. Furthermore, in Figure 3, network elements 304A-B couple MEPs 102A-C and 102D-F, respectively, to service provider VPLS network 306. VPLS network 306 further comprises network elements 308A-D and pseudowires 310A-B. In addition, VCCV messages 318A-B are being transmitted and received by network elements 304A-B using pseudowires 310A-B.

[0025] In Figure 3, instead of forwarding connectivity check messages 112A-C and 114A-C, network elements 304A-B proxy these connectivity check messages. In one embodiment, connectivity check proxy module 202 of network elements 304A-B transmits connectivity check messages 314D-F and 312D-F, respectively, to MEPs local to these network elements. In this embodiment, MEPs 102A-C are local to network element 304A and MEPs 102D-F are local to network element 304B. In one embodiment, network elements 304A-B do not need to forward connectivity check messages 112A-C and 114A-C across VPLS network 306 because network elements 304A-B are proxying these messages. Thus, the traffic for end-to-end fault management is greatly reduced because connectivity fault state change messages are transmitted across VPLS network

306 instead of the connectivity messages constantly transmitted by MEPs 112A-C and 114A-C.

[0026] Returning to Figure 2, in one embodiment, network element determines which remote MEPs are active with connectivity state change module 204. In one embodiment, network element 200 receives a fault state change message from another network element that indicates that a remote MEP has had a fault state change. In one embodiment, connectivity check state change module 204 determines a remote MEP fault state change by receiving a VCCV message indicating a remote MEP fault state change. VCCV is a control channel between a pseudowire's ingress and egress points over which connectivity verification messages can be sent. VCCV messages can traverse the network in-band with the pseudowire's data or out-of-band. VCCV message are not forwarded past network elements on the edge of the MPLS/VPLS network. Thus, connectivity proxy module 202 proxies fault information of one protocol (e.g., CFM) based on receiving fault state updates on another protocol (e.g., VCCV).

[0027] In reference to Figure 3, network element 304A determines which of remote MEPs 102D-F are active by receiving messages indicating fault state changes of MEPs in Ethernet network 316B. In one embodiment, network element 304A of network elements receives and processes the fault state change messages. In this embodiment, network element 304B transmits fault state change messages regarding MEPs 102D-F to network element 304A across VPLS network 306. In one embodiment, network element 304B transmits these messages as VCCV messages 318B over pseudowire 310B as described in reference with Figure 2, block 204.

[0028] Returning to Figure 2, connectivity check detection module 208 detects whether fault state change associated with a local MEP. In this embodiment, connectivity check module 208 detects the fault state change by receiving a connectivity check message from a newly active MEP or the lack of a connectivity check message from an active MEP. In one embodiment,

connectivity check fault state change module 210formats a message indicating the fault state change and transmits it to other network elements that are proxying the connectivity check messages. While in one embodiment, this is a VCCV message carried over the pseudowire between the network elements, in alternate embodiments, other signaling mechanisms in the art can be used. The other network elements use this message to update their remote MEP database and to proxy connectivity check messages to the MEP local to that network element. By sending fault state changes and proxying connectivity check messages, network element 200 provides that end-to-end fault management for MEP without flooding the service provider network interconnecting the two Ethernet networks with constant connectivity checks messages. Furthermore, by detecting local fault state changes of MEP and transmitting these changes to other network elements proxying connectivity check messages, the other network element can automatically build connectivity check databases of remote MEPs.

[0029] In reference to Figure 3, network element 304A detects fault state changes in local MEPs 102A-C and transmits faults state change messages to network elements 306B. In this embodiment, network element 304A detects the fault state changes and transmits the appropriate messages as described in reference with Figure 2.

[0030] Returning to Figure 2, in one embodiment, connectivity check proxy module 202 transmits the connectivity check messages based on the active MEPs identified in the connectivity check database 206. While in one embodiment, the connectivity check database 206 comprises local and remote MEPs and stores the connectivity status of each MEP in the database, in alternative embodiments, connectivity check database 206 comprise the same and/or different information (e.g., different combinations of active MEPs, local MEPs, remote MEPs, status of MEPs, etc.).

[0031] Figure 4 is an exemplary flow diagram of a method 400 for proxying connectivity check messages for remote MEPs according to one embodiment of

the invention. In one embodiment, network element 200 performs method 400 to proxy connectivity check messages. In Figure 4, at block 402, method 400 receives fault state change messages, indicating a fault state change of a remote MEP. In one embodiment, method 400 receives a VCCV message that indicates the fault state change.

[0032] At block 404, method 400 processes the received fault state change message. In one embodiment, method 400 extracts the information from the fault state change message regarding the remote MEP that triggered the fault state change. While in one embodiment, method 400 extracts the MAC address of the remote MEP and whether the remote MEP became active or lost connectivity, in alternate embodiments, method 400 extracts other information such as MEPID, MAC-address, CC-interval, RDI (remote defect indicator) bit.

[0033] Method 400 uses the processed information from block 404 to update the connectivity check database at block 406. While in one embodiment, method 400 adds a new entry in the connectivity check database 206 for a remote MEP that becomes active, in alternate embodiments, method 400 can take some other action for a remote MEP that becomes active (update an existing remote MEP entry in connectivity check database 206 to indicate that MEP is active, etc.). In addition, method 400 updates the connectivity check database if the received fault state changes message indicates a remote MEP has lost connectivity. While in one embodiment, method 400 deletes the entry associated with the remote MEP that the message indicated had lost connectivity, in alternate embodiments, method 400 can take some other action (mark that remote MEP as lost connectivity, etc.

[0034] At block 408, method 400 proxies the connectivity check messages by periodically transmitting connectivity check messages to local MEPs based on the updated connectivity check database. In one embodiment, method 400 transmits a connectivity check message for each active remote MEP as indicated in the

connectivity check database 206 as described in reference to connectivity check proxy module 202 in Figure 2 and/or network elements 304A-B in Figure 3.

[0035] Figure 5 is an exemplary flow diagram of a method 500 for sending VCCV messages to other network elements based on MEP fault state changes according to one embodiment of the invention. In one embodiment, network element 200 performs method 500 to send VCCV messages to other network element based on MEP fault state changes. In Figure 5, at block 502, method 500 detects a fault state change from one of the local MEPs.

[0036] At block 504, method 500 formats a fault state change message for the service provider network interconnecting two geographically disperse Ethernet networks. In one embodiment, method 500 formats a fault state change message as a VCCV message sent over one or more of the pseudowires of VPLS network 306. Alternatively, method 500 could format the fault state change message to another suitable OAM protocol for a VPLS network or other type of network interconnecting networks where the MEPs are coupled. In one embodiment, method 500 stores the information about the fault change (source MAC, MEP active, MEP not connected, etc.) in fields of the VCCV message. For example and by way of illustration, a VCCV payload can indicate a message formatted in a way to accommodate multiple CC messages, by using optional and/or custom fields of the VCCV payload. In this way, method 500 transforms fault detection of one protocol (CFM) and carries this information over another protocol (VCCV, etc.).

[0037] At block 506, method 500 transmits the formatted fault state message according to the OAM protocol of the service provider network. While in one embodiment, method 500 transmits the fault state change message according to the VCCV protocol (either in-band or out of band), in alternate embodiments, method 500 transmits the fault state change message according to some other protocol appropriate to the service provider network.

[0038] Figure 6 is a block diagram illustrating an exemplary network element 600 that handles proxying connectivity check messages and sending VCCV messages according to one embodiment of the system. In Figure 6, backplane 606 couples to line cards 602A-N and controller cards 604A-B. While in one embodiment, controller cards 604A-B control the processing of the traffic by line cards 602A-N, in alternate embodiments, controller cards 604A-B perform the same and/or different functions (reprogram the line cards, upgrade software, handle operator requests, collect statistics, etc.). Line cards 602A-N process and forward traffic according to the policies received from controller cards 604A-B. In one embodiment, line cards 602A-N proxy connectivity check messages and transmit fault state change messages as described in Figures 2-5.

[0039] This implementation of the proxy connectivity check messages and transmit fault state change messages is an example, and not by way of limitation. Thus, network elements having other architectural configurations can incorporate embodiments of the invention. Examples of other network elements that could incorporate embodiments of the invention could have multiple line cards or have a single line card. Moreover, a network element having proxy connectivity check messages and transmit fault state change messages distributed across the traffic cards could incorporate embodiments of the invention.

[0040] Controller cards 604A-B as well as line cards 602A-N included in the different network elements include memories, processors and/or Application Specific Integrated Circuits (ASICs). Such memory includes a machine-readable medium on which is stored a set of instructions (i.e., software) embodying any one, or all, of the methodologies described herein. Software can reside, completely or at least partially, within this memory and/or within the processor and/or ASICs. For the purposes of this specification, the term "machine-readable medium" shall be taken to include any mechanism that provides (i.e., stores and/or transmits) information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory (ROM);

random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; etc.

Alternative Embodiments

[0041] For example, while the flow diagrams in the figures show a particular order of operations performed by certain embodiments of the invention, it should be understood that such order is exemplary (e.g., alternative embodiments may perform the operations in a different order, combine certain operations, overlap certain operations, etc.)

[0042] While the invention has been described in terms of several embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described, can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of limiting.

CLAIMS

What is claimed is:

1. A computerized method, comprising:

receiving a message of a first protocol indicating a fault state change for one of a plurality of remote maintenance endpoints, the fault state change determined by a second protocol;

updating a local database based on the received message, the local database comprising the fault status of at least some of the plurality of remote maintenance endpoints; and

proxying connectivity check messages to local maintenance endpoints based on the updated local database, wherein the proxying comprises periodically sending connectivity check messages for each maintenance endpoint identified as active in the local database.

2. The computerized method of claim 1, wherein each of the proxied connectivity check messages are formatted to appear as if that message originated from one of the plurality of remote maintenance endpoints.

3. The computerized method of claim 1, wherein the updating comprises:

storing the fault status of the remote maintenance endpoint associated with the received message.

4. The computerized method of claim 1, wherein the first protocol is Virtual Circuit Connectivity Verification protocol.

5. The computerized method of claim 1, wherein the second protocol is Connectivity Fault Management protocol.

6. The computerized method of claim 1, wherein a managed endpoint is one of a personal computer, a server, a bridge, and a switch.

7. The computerized method of claim 1, wherein each of proxied connectivity check messages comprises an address and a unique identifier of a remote managed endpoint associated with that message.

8. A machine-readable medium that stores instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

receive a message of a first protocol indicating a fault state change for one of a plurality of remote maintenance endpoints, the fault state change determined by a second protocol;

update a local database based on the received message, the local database comprising the fault status of at least some of the plurality of remote maintenance endpoints; and

proxy connectivity check messages to local maintenance endpoints based on the updated local database, wherein the proxying comprises periodically sending connectivity check messages for each maintenance endpoint identified as active in the local database.

9. The machine-readable medium of claim 8, wherein each of the proxied connectivity check messages are formatted to appear as if that message originated from one of the plurality of remote maintenance endpoints.

10. The machine-readable medium of claim 8, wherein the machine-readable medium further causes the set of processors to:

store the fault status change of the remote maintenance endpoint associated with the received message.

11. The machine-readable medium of claim 8, wherein the first protocol is Virtual Circuit Connectivity Verification protocol.

12. The machine-readable medium of claim 8, wherein the second protocol is Connectivity Fault Management protocol.

13. The machine-readable medium of claim 8, wherein a remote managed endpoints is one of a personal computer, a server, a bridge, and a switch.

14. An apparatus comprising:

a connectivity check state change module to receive messages indicating fault state changes from a plurality of remote maintenance endpoints, the fault state change determined by a second protocol;

a connectivity check database to store the fault status changes for the plurality of remote maintenance endpoints; and

a connectivity check proxy module to proxy connectivity check messages to local maintenance endpoints based on the updated local database, wherein the proxying comprises periodically sending connectivity check messages for each maintenance endpoint identified as active in the local database.

15. The apparatus of claim 14, wherein each of the proxied connectivity check messages are formatted to appear as if that message originated from one of the plurality of remote maintenance endpoints.

16. The apparatus of claim 14, wherein the first protocol is Virtual Circuit Connectivity Verification protocol.

17. The apparatus of claim 14, wherein the second protocol is Connectivity Fault Management protocol.

18. A network element comprising:

a controller card that controls functions of the network element;

a set of one or more line cards, wherein at least one of the line cards configured to

receive a message of a first protocol indicating a fault state change for one of a plurality of remote maintenance endpoints, the fault state change determined by a second protocol;

update a local database based on a received message, the local database comprising the fault status of at least some of the plurality of remote maintenance endpoints; and

proxy connectivity check messages to local maintenance endpoints based on the updated local database, wherein the proxying comprises periodically sending connectivity check messages for each maintenance endpoint identified as active in the local database.

19. The network element of claim 19, wherein each of the proxied connectivity check messages are formatted to appear as if that message originated from one of the plurality of remote maintenance endpoints.

20. The network element of claim 18, wherein line cards are further configured to:

store the fault status change of the remote maintenance endpoint associated with the received message.

21. A computerized method comprising:

detecting according to a first protocol a fault state change of one of a set of one or more local maintenance endpoints;

creating a fault state change message according to a second protocol based on the detected fault state change; and

sending the fault state change message according to the second protocol to at least one of a plurality of network elements proxying connectivity check messages.

22. The computerized method of claim 21, wherein the fault state change indicates a connectivity change for the one of the set of one or more local maintenance endpoints, the change is one of connecting to a network, becoming active on the network, and losing connectivity to the network.

23. The computerized method of claim 21, wherein the first protocol is Connectivity Fault Management protocol.

24. The computerized method of claim 21, wherein the second protocol is Virtual Circuit Connectivity Verification protocol.

25. The computerized method of claim 21, wherein information about the fault state change is stored in fields of a VCCV message.

26. The computerized method of claim 21, wherein a managed endpoint is one of a personal computer, a server, a bridge, and a switch.

27. A machine-readable medium that stores instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising: detect, according to a first protocol, a fault state change of one of a set of one or more local maintenance endpoints;

create a fault state change message according to a second protocol based on the detected fault state change; and

send the fault state change message according to the second protocol to at least one of a plurality of network elements that proxies connectivity check messages.

28. The machine-readable medium of claim 27, wherein the fault state change indicates a connectivity change for the one of the set of one or more local maintenance endpoints, the change is one of connecting to a network, becoming active on the network, and losing connectivity to the network.

29. The machine-readable medium of claim 27, wherein the first protocol is Connectivity Fault Management protocol.

30. The machine-readable medium of claim 27, wherein the second protocol is Virtual Circuit Connectivity Verification protocol.

31. The machine-readable medium of claim 27, wherein information about the fault state change is stored in fields of a VCCV message.

32. The machine-readable medium of claim 27, wherein a managed endpoint is one of a personal computer, a server, a bridge, and a switch.

33. An apparatus comprising:

a connectivity check detection module to detect, according to a first protocol, a fault state change of one of a set of one or more local maintenance endpoints; and

a connectivity check fault state change module to create a fault state change message according to a second protocol based on the detected fault state

change and send the fault state change message according to the second protocol to at least one of a plurality of network elements that proxies connectivity check messages.

34. The apparatus of claim 33, wherein the fault state change indicates a connectivity change for the one of the set of one or more local maintenance endpoints, the change is one of connecting to a network, becoming active on the network, and losing connectivity to the network.

35. The apparatus of claim 33, wherein the first protocol is Connectivity Fault Management protocol.

36. The apparatus of claim 33, wherein the second protocol is Virtual Circuit Connectivity Verification protocol.

37. The apparatus of claim 33, wherein information about the fault state change is stored in fields of a VCCV message.

38. The apparatus of claim 33, wherein a managed endpoint is one of a personal computer, a server, a bridge, and a switch.

39. A network element comprising:

a controller card that controls functions of the network element;

a set of one or more line cards, wherein at least one of the line cards configured to

detect, according to a first protocol, a fault state change of one of a set of one or more local maintenance endpoints,

create a fault state change message according to a second protocol based on the detected fault state change, and

send the fault state change message according to the second protocol to at least one of a plurality of network elements that proxies connectivity check messages.

40. The network element of claim 39, wherein the first protocol is Connectivity Fault Management protocol.

41. The network element of claim 39, wherein the second protocol is Virtual Circuit Connectivity Verification protocol.

42. The network element of claim 39, wherein information about the fault state change is stored in fields of a VCCV message.

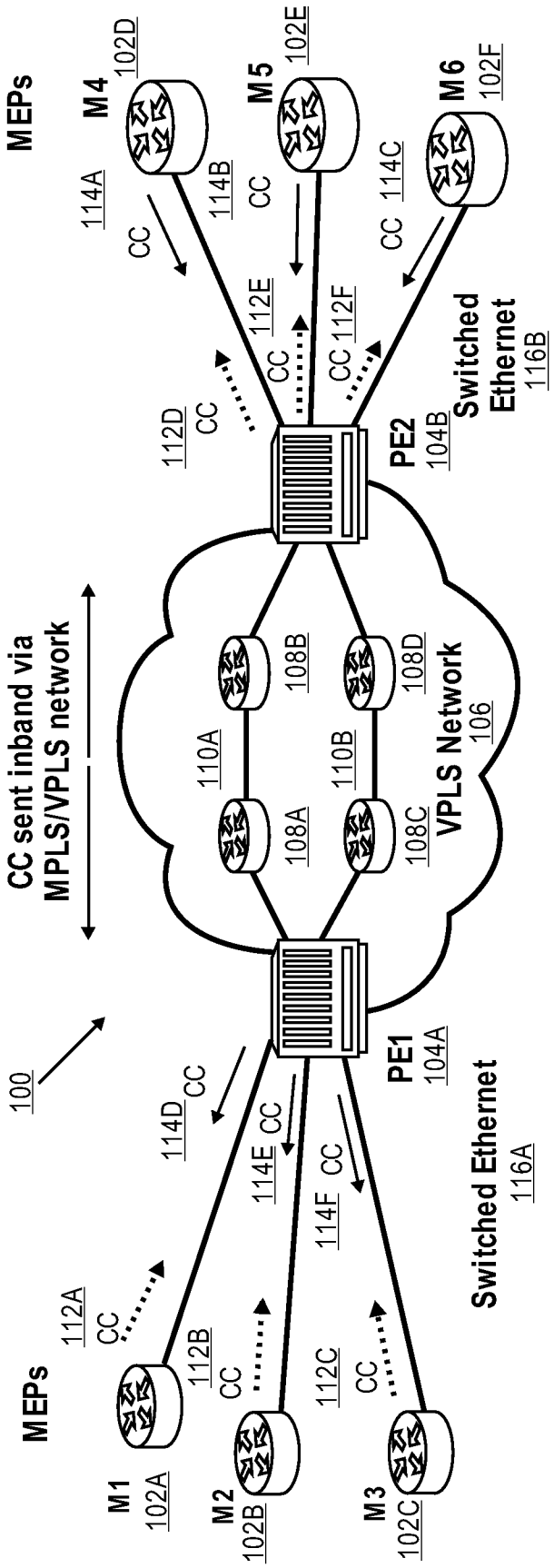
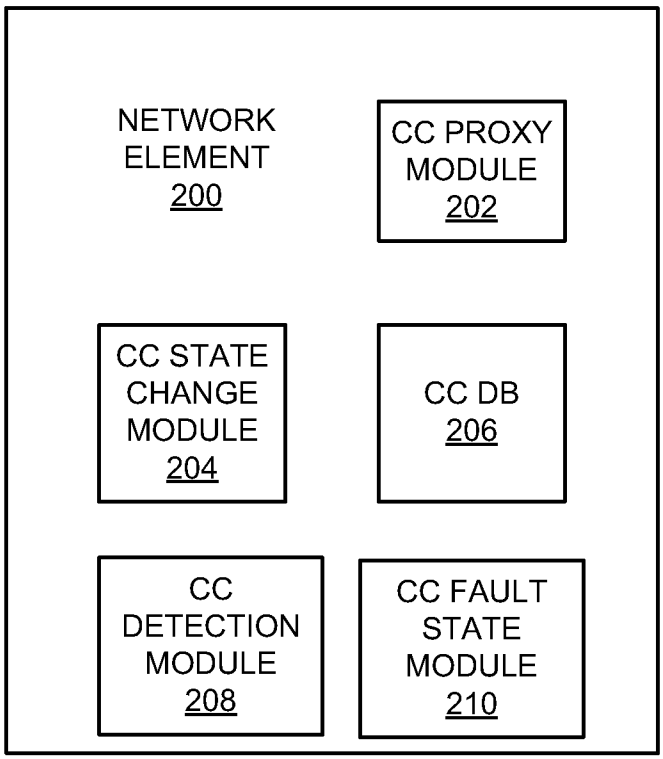


FIG. 1
(PRIOR ART)

FIGURE 2


NETWORK ELEMENT 200
CC PROXY MODULE 202
CC STATE CHANGE MODULE 204
CC DB 206
CC DETECTION MODULE 208
CC FAULT STATE MODULE 210

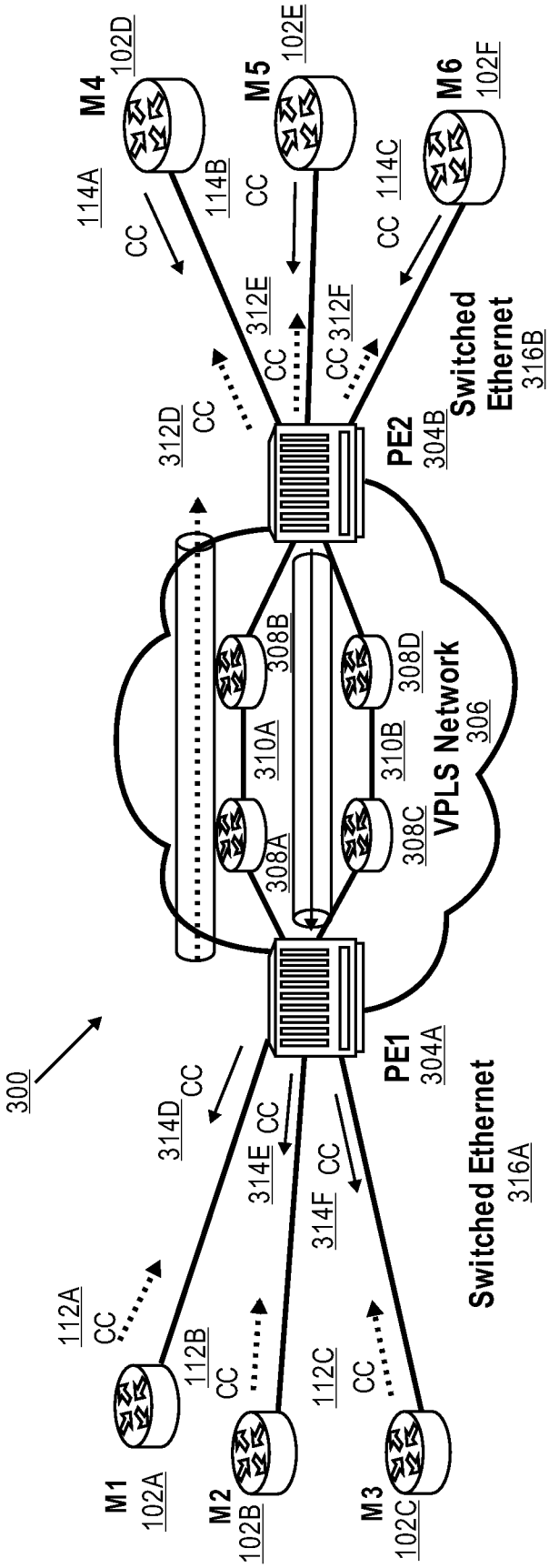

300
M1
102A
M2
102B
M3
102C
M4
102D
M5
102E
M6
102F
PE1
304A
PE2
304B
VPLS Network
306
Switched Ethernet
316A
Switched Ethernet
316B
112A
112B
112C
114A
114B
114C
308A
308B
308C
308D
310A
310B
312D
312E
312F
314D
314E
314F
CC

FIG. 3

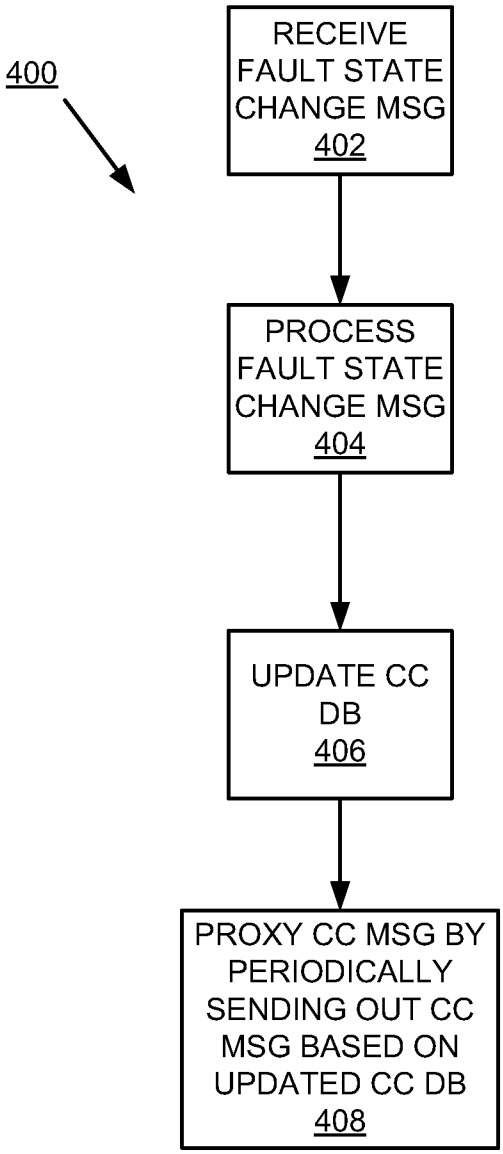

400
RECEIVE FAULT STATE CHANGE MSG 402
PROCESS FAULT STATE CHANGE MSG 404
UPDATE CC DB 406
PROXY CC MSG BY PERIODICALLY SENDING OUT CC MSG BASED ON UPDATED CC DB 408

FIGURE 4

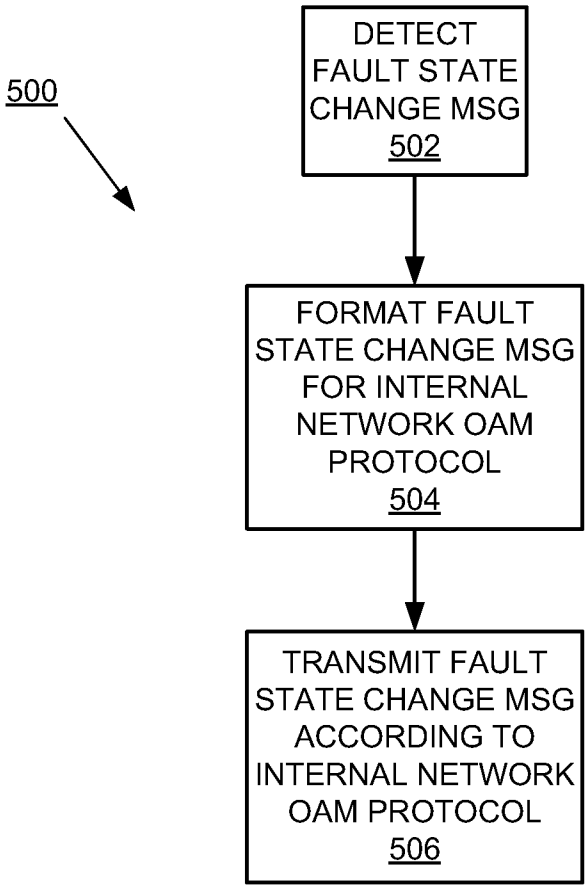

500
DETECT FAULT STATE CHANGE MSG 502
FORMAT FAULT STATE CHANGE MSG FOR INTERNAL NETWORK OAM PROTOCOL 504
TRANSMIT FAULT STATE CHANGE MSG ACCORDING TO INTERNAL NETWORK OAM PROTOCOL 506

FIGURE 5

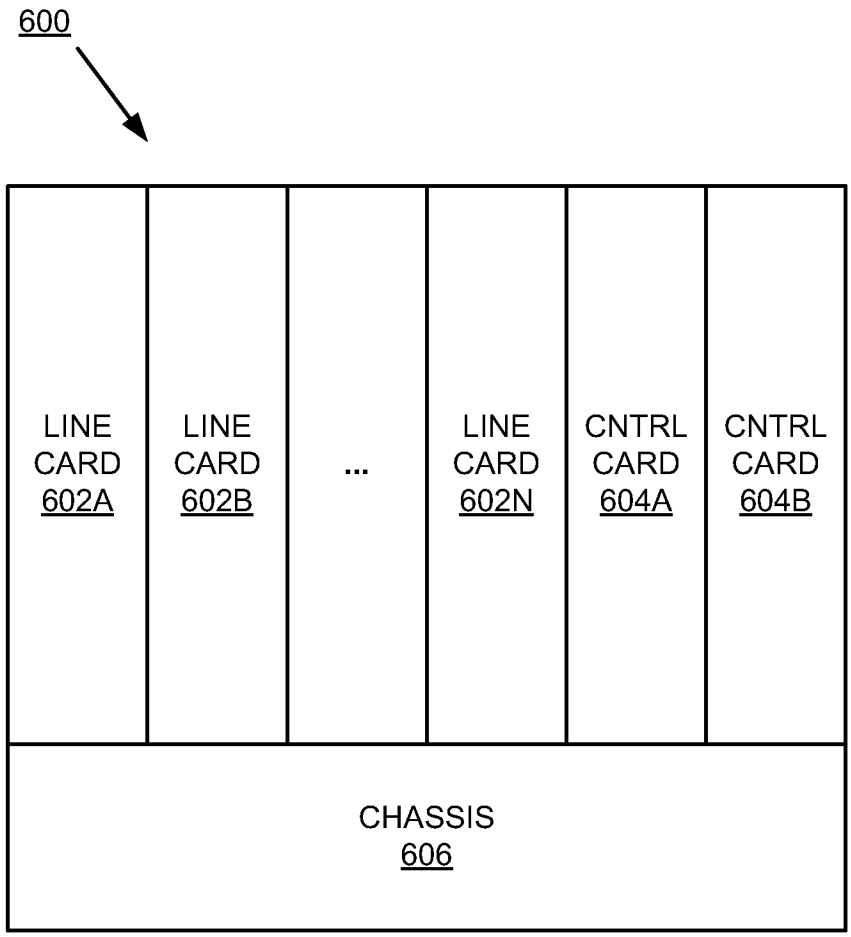

600
LINE CARD 602A
LINE CARD 602B
...
LINE CARD 602N
CNTRL CARD 604A
CNTRL CARD 604B
CHASSIS 606

FIGURE 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/078984

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G01R 31/08 (2008.04)
USPC - 370/236.2
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(8) - G01R 31/08 (2008.04)
USPC - 370/236.2

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)
USPTO (US, USPG-PUB, EPO, DERWENT), Google Patents, Google Scholar

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/0025256 A1 (HERTOGHS et al) 01 February 2007 (01.02.2007) entire document	1-42
Y	US 2006/0159008 A1 (SRIDHAR et al) 20 July 2006 (20.07.2006) entire document	1-42
Y	US 7,240,364 B1 (BRANSCOMB et al) 03 July 2007 (03.07.2007) entire document	4, 11, 16, 18-20, 24, 30, 36, 39-42

☐ Further documents are listed in the continuation of Box C. ☐

* 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 application or patent 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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 2008	12 DEC 2008
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)