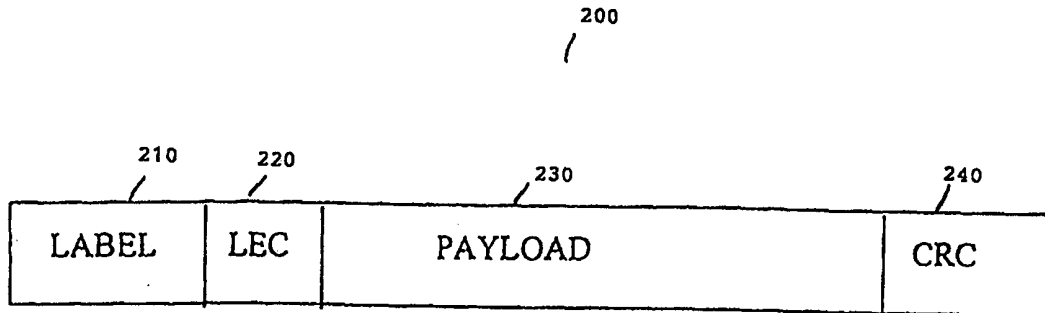




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁷ : H04L 12/56</p>	<p>A1</p>	<p>(11) International Publication Number: WO 00/54465 (43) International Publication Date: 14 September 2000 (14.09.00)</p>
<p>(21) International Application Number: PCT/IB00/00253 (22) International Filing Date: 9 March 2000 (09.03.00) (30) Priority Data: 09/264,758 9 March 1999 (09.03.99) US (71) Applicant: NOKIA INTERNET COMMUNICATIONS INC. [US/US]; Robert C. Rolnik, IPR, 313 Fairchild Drive, Mountain View, CA 94043 (US). (71)(72) Applicants and Inventors: RAVIKANTH, Rayadurgam [IN/US]; 26 Beacon Street, Apt. 28B, Burlington, MA 01803 (US). STRANDBERG, Ove [FI/US]; 22045 Regnart Road, Apt. B, Cupertino, CA 95014 (US). VAANANEN, Pasi [FI/US]; 25 Linden Avenue, Apt. 25, Sommerville, MA 02143 (US). (74) Agent: ROLNIK, Robert; Nokia Inc., 6000 Connection Drive, 1-4-755, Irving, TX 75039 (US).</p>		<p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p>

(54) Title: GENERIC LABEL ENCAPSULATION PROTOCOL



(57) Abstract

A method for encapsulation of labeled datagrams over serial communications links, and a method for extracting the datagrams on the receiving end of the link. The encapsulation method includes adding a label (210) and a label error correction (220) to the front of a datagram, the label error correction (220) being derived using the label (210) and adding a cyclic redundancy check (240) at a trailing end of the datagram, the cyclic redundancy check (240) being derived using the datagram. The end of a packet encapsulating the datagram with a label (210), a label error correction field (220) and a cyclic redundancy check field (240) is identified by analyzing incoming bits for a packet until a pattern of bits is detected that matches a number of previous bits of the packet coded with a predetermined coding formula and identifying the end of the packet based upon the detection of the match and the predetermined coding formula.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

GENERIC LABEL ENCAPSULATION PROTOCOL

Field of the Invention.

5 This invention relates in general to serial communications systems, and more particularly to a generic label encapsulation protocol for carrying label switched packets over serial links.

Description of Related Art.

10 Demand for bandwidth is skyrocketing in data service provider networks. With this demand comes a need for efficient bandwidth utilization, higher performance and simplicity. Fullest traffic an Internet Protocol (IP) traffic volumes are expected to continue to increase at substantially higher rates. With the rise of IP throughout global networks, many high volume links are trying to sidestep the additional burden required by ATM cells. Most carriers use SONET (Synchronous Optical Network) as the OSI layer I
15 specification for data transmission over optical fibers in the public network, and ATM is then used as the OSI layer II link. However, the extra data that must be added to a packet to traverse an ATM link can eat up more than 10 percent of ATM's raw bandwidth. Further, there are many other packet protocols for bundling data for transmission. While SONET will be mentioned herein as a primary example, those skilled in the art will
20 recognize that the concepts discussed here is valid for any serial link.

 SONET is a family of transmission rates from 51.84 Mbps (the base rate) to 13.22 Gbps that was created to provide the flexibility needed to transport many digital signals with different capacities, and to provide a design standard for manufacturers. Despite the name, it is not limited to optical links. SONET development began as a suggestion to
25 the Exchange Carriers Standards Association and ultimately came to rest at the American National Standards Institute (ANSI). SONET has also been adopted by the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T). The ITU-T version is know as Synchronous Digital Hierarchy (SDH), which varies slightly in that SDH levels begin at 155 Mbps.

30 To deliver efficient network manageability and scalability, today's data networks are based on a hierarchical architecture that includes the backbone as well as the service node layers. The major function of a router and a backbone is to provide performance and scalability, to switch millions of packets per second, and to scale to high rates. At

the service nodes or the distribution layer, the main goal of an edge router is to provide features such as security access control, and support for differentiated services through class of service (CoS) offering. For example, most carriers transport their router traffic through the SONET/SDH platforms for long distances. The SONET/SDH hardware forms the main infrastructure amending telecommunication providers and enterprises worldwide. Therefore, it is imperative for the data equipment to inter operate with this infrastructure seamlessly.

IP over SONET/SDH is gaining popularity as a way to reduce the ATM overhead burden described above and squeeze more bandwidth out of a link. IP over SONET/SDH removes ATM from the transmission picture, foregoing the traditional method of encapsulating IP packets into an ATM cell, which is then mapped into a SONET frame. Instead, this technology maps the IP package straight into a SONET frame.

Packet data over SONET/SDH is the servo transmission of data over SONET frames through the use of point-to-point protocol (PPP). PPP was designed as a standard method of communicating over point-to-point links. Initial deployment was designed for short local lines, lease lines and plain-old-telephone-service (POTS) using modems. As new packet services and higher speed lines are introduced, point-to-point protocol is easily deployed in these environments as well.

PPP treats SONET transports as octet oriented synchronous links. PPP presents an octet interface to the physical layer and there is no provision for sub-octets to be supplied or accepted. The octet stream is mapped into the SONET synchronous payload envelope (SPE), with the octet boundaries aligned with the SPE octet boundaries. SONET provides substantial overhead information, allowing simpler multiplexing and greatly expended operations, administration, maintenance and provisioning (OAM&P) capabilities.

SONET includes multiplexing principles such as mapping, aligning, multiplexing and stuffing. One of the benefits of SONET is that it can carry large payloads (above 50 Mbps). Nevertheless, the digital hierarchy signals can be accommodated as well by subdividing STS (Synchronous Transport Signals) SPE into smaller components of structures known as virtual tributaries (VTs), for the purpose of transporting and switching payloads smaller than the STS-1 rate.

Accordingly, packet over SONET/SDH is an ideal feature for networks that are built for providing Internet or IP data. Packet over SONET/SDH provides superior bandwidth utilization and efficiency over other transport methods. However, not all networks can reap the benefits of IP over SONET/SDH. First, all data traversing the

link must be IP. Because 155 Mbps over IP data is not easy to come by, this requirement is a major drawback of using IP over SONET/SDH. ATM can be more easily statistically multiplexed than IP over SONET/SDH. However, ATM can be run on lower speed links. But, as mentioned above, ATM carries the additional overhead that must be added to each packet to traverse the ATM link.

As the convergence towards delivery of audio, data, images and video through diverse transmission switching systems that supply high speed transportation over any medium to any location, SONET is gaining momentum as the transport network for transmitting packets due to its reduced overhead is compared to IP over ATM-type solutions. However, as stated above, the current approach to packet over SONET/SDH using point-to-point protocol encapsulation.

There is an ongoing effort in the IETF to provide easy switching for packet traffic over servo links by using labels and label switching routers (LSR). The multi-protocol label switching (MPLS) groups work is directed at solving the complexity involved label-switching and presenting a standard-based interoperability testing proposal. Label switching adds connections to connectionless protocols such as Transport Control Protocol/Internet Protocol (TCP/IP). By calculating routes across the network and assigning "tags" or "labels" to those routes, frame forwarding is simplified to the point where it also can be implemented in hardware. Given this architecture, labels switching can, in theory, operate equally well over ATM and non-ATM environments. In ATM networks, the label already exists; it is the virtual channel (VC) address. In non-ATM environments, such as Ethernet, new protocols have to be developed to accomplish this. The main advantage of using labels is improved forwarding capability to elimination of layer three look-up and the traffic engineering capabilities brought by the use of labels.

However, as mentioned above, the only approach currently used for carrying packet traffic over SONET/SDH uses point-to-point encapsulation. A definition as to how labels can be encapsulated has not yet been proposed. Further, even if labels are used for carrying packet traffic over servo links, the problem of detecting the end of packet without having to look inside the payload has now been solved.

It can be seen then that there is a need for encapsulation for carrying label switch packet over servo links.

It can be seen then that there is a need for a method to detect the end of packets without having to look inside the payload.

SUMMARY OF THE INVENTION

To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present

specification, the present invention discloses a generic label encapsulation protocol for carrying label switched packets over serial links.

The present invention solves the above-described problems by providing a label encapsulation protocol and a method for detecting the end of variable length packets.

5 A method in accordance with the principles of the present invention includes adding a label and a label error correction to the front of a datagram, the label error correction being derived using the label and adding a cyclic redundancy check at a trailing end of the datagram, the cyclic redundancy check being derived using the datagram.

10 Other embodiments of a method in accordance with the principles of the invention may include alternative or optional additional aspects. One such aspect of the present invention is that the label includes three bytes.

Another aspect of the present invention is that the label error correction is obtained according to D^8+D^2+D+1 .

Another aspect of the present invention is that the datagram is scrambled.

15 Another aspect of the present invention is that the datagram is scrambled according to $D^{43}+1$.

Another aspect of the present invention is that the cyclic redundancy check is obtained using a polynomial $D^{16}+D^{15}+D^2+1$.

Another aspect of the present invention is that the datagram is an IPv4 packet.

20 Another aspect of the present invention is that the datagram is an IPv6 packet.

Another aspect of the present invention is that the label comprises a plurality of bits, wherein a bit in the label is a label significant bit for indicating that no payload is being carried.

25 In another embodiment of the present invention a method is provided for identifying an end of a packet encapsulating the datagram with a label, a label error correction field and a cyclic redundancy check field, the method including analyzing incoming bits for a packet until a pattern of bits is detected that matches a number of previous bits of the packet coded with a predetermined coding formula and identifying the end of the packet based upon the detection of the match and the predetermined coding formula.

30 Another aspect of the present invention is that the predetermined coding formula comprises a cyclic redundancy check polynomial and the analyzing comprises coding incoming bits according to the cyclic redundancy check polynomial to produce a calculated cyclic redundancy check until the calculated cyclic redundancy check matches the cyclic redundancy check field.

35 Another aspect of the present invention is that the selecting further comprises the identifying the end of the current packet based upon the detection of the match.

Another aspect of the present invention is that the predetermined coding formula comprises a label error correction polynomial and the analyzing comprises coding incoming bits according to the label error correction polynomial to produce a calculated label error correction until the label error correction matches the label error correction field.

5 Another aspect of the present invention is that the selecting further comprises the identifying the end of the previous packet based upon the detection of the match.

Another aspect of the present invention is that the predetermined coding formula comprises a combination of a cyclic redundancy check polynomial and a label error correction polynomial, wherein the analyzing comprises coding incoming bits according to the cyclic redundancy check polynomial and the label error correction polynomial, wherein the cyclic redundancy check polynomial produces a calculated cyclic redundancy check until the calculated cyclic redundancy check matches the cyclic redundancy check field and the label error correction polynomial produces a calculated label error correction until the label error correction matches the label error correction field.

15 These and various other advantages and features of novelty which characterize the invention are pointed out with particularity in the claims annexed hereto and form a part hereof. However, for a better understanding of the invention, its advantages, and the objects obtained by its use, reference should be made to the drawings which form a further part hereof, and to accompanying descriptive matter, in which there are illustrated and described specific examples of an apparatus in accordance with the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

Fig. 1 illustrates a network system that is applicable to the generic label encapsulation protocol according to the present invention for carrying label switched packets over serial links;

Fig. 2 illustrates a generic label encapsulation protocol (GLEP) packet according to the present invention;

Fig. 3 illustrates a stream 300 of variable size packets; and

30 Fig. 4 is a flow chart illustrating the method for detecting the end of a variable size packets having a label encapsulated according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description of the exemplary embodiment, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration the specific embodiment in which the invention may be practiced. It is to be

understood that other embodiments may be utilized as structural changes may be made without departing from the scope of the present invention.

Fig. 1 illustrates a network system 100 that is applicable to the generic label encapsulation protocol according to the present invention for carrying label switched packets over serial links. In Fig. 1, a local user 110 is sending packets to a remote user 120 via a serial link 130. The packets cross the network 140 via routers 150, 152 at each end thereof. For example, the packets may be transported over SONET/SDH. Packet over SONET/SDH has been gaining momentum, due to its reduced overhead as compared to IP over ATM type solutions. Label switching in IP networks has up to now dealt with link layer technologies such as ATM and Frame Relay. However, ATM and Frame Relay have more natural ways to map label switched traffic to the link layer technologies than packet over SONET/SDH. The current approach to packet over SONET/SDH uses PPP encapsulation for this purpose. However, the manner in which labels can be encapsulated in packet over SONET/SDH has not yet been defined.

The present invention provides a generic label encapsulation protocol that enables the carrying of a label and the associated packet in a fashion that will enable easy switching by a label switching router (LSR) 150, 152. Further, the present invention provides a method for extracting the datagram from the label at the remote end.

Fig. 2 illustrates a generic label encapsulation protocol (GLEP) packet 200 according to the present invention. As shown in Fig. 2, 24 bits or 3 bytes are allocated for the label 210 information. Since this is the primary header that the label switching will be based upon, a 1 byte Label Error Correction (LEC) field 220 is used to detect errors in the label header of this GLEP packet 200. For example, the LEC field 220 may be obtained using the polynomial D^8+D^2+D+1 . The GLEP packet 200 also includes the original payload 230 and a Cyclic Redundancy Check (CRC) field 240.

The original payload is a variable size packet. Fig. 3 illustrates a stream 300 of variable size packets 310-320. Each of the variable size packets 310-320 includes a header 330 and a data field 340. For example, the variable size packets 310-320 may be IPv4 or IPv6 packets or they may be based on any other network layer protocol.

Referring again to Fig. 2, the payload 230 is the field adjacent to the LEC field 220. The payload 230 may be scrambled, e.g., using the $D^{43}+1$ polynomial which is the ATM scrambler. Those skilled in the art will recognize that the generic label encapsulation protocol according to the present invention is truly multi-protocol in the fact that the payload 230 being carried could be any network layer protocol. This ensures that the generic label encapsulation protocol according to the present invention is consistent with the work of the MPLS working group. The fourth and final field in the

proposed scheme is the CRC field 240. The CRC 240 may be 2 bytes in length. Further, the CRC 240 may be obtained using the CRC-16 polynomial $D^{16}+D^{15}+D^2+1$.

However, those skilled in the art will recognize that the present invention is not meant to be limited to the above-described label space partitioning, field dimensions and coding polynomials. Those skilled in the art will also recognize that in addition to the MPLS label identifier, fields like MAC bits, Class of Service bits, congestion indication bits, etc. may be included, and that in such a case, the label field 210 indicated above could be more than 3 bytes. In addition, one of the bits of the label field 210 may be reserved for a "label significant bit." This is to indicate the fact that no payload 230 is being carried. Actually there are three options for this:

1. When there is no data to send, this bit is set as "label insignificant", and consecutive labels marked with "label insignificant" are sent as long as there is no data to send.
2. It may even be unnecessary to have bit for this, these can be discarded on basis of the reception of consecutive matching labels back-to-back.
3. Other alternative is to reserve special label codepoint such as 00000000 00000000 xxxxxxxx for this function (bits are expensive).

Having described the encapsulation protocol, the method for extracting the payload from the label will be described next. The extraction needs to be examined as to whether the present invention can effectively be used to label switch GLEP packets 200, without too much processing (such as IP level processing) overhead.

One of the primary advantages to the ATM approach is the fact that the ATM cells are of fixed sizes and the virtual path indicator/virtual channel indicator (VPI/VCI) fields are in fixed positions in the cell. While even in the current GLEP case, it is true that the labels 210 are placed in a fixed location and only a fixed length lookup is required, it still remains a problem that the GLEP packets 200 are variable size in nature since the datagrams 230 themselves are of variable length as shown in Fig. 3. The task then is to detect the end of packet without having to look inside the payload. This can be achieved using the CRC field 240 and the LEC field 220.

Fig. 4 is a flow chart 400 illustrating a method for detecting the end of a variable size packets having a label encapsulated according to the present invention. In Fig. 4, the end of a frame may be identified two ways. The end of a previous frame may be identified by detecting the beginning of the label of the current frame using the LEC, or the end of the current frame may be detected by using the CRC. First, the method is

chosen 410. If the end the current frame method is chosen 412, the CRC for the bits of the payload is calculated 414. The typical implementation of the CRC is in the form of shift registers. In keeping with the example described above with reference to Fig. 2, as the bits of the payload come in, the 16-bit CRC operation is performed in hardware. This
5 calculated CRC is then checked with the trailing 16 bits 416. Monitoring for a match takes place 418, wherein a match indicates the end of the current GLEP frame 420. Otherwise, the process recycles 422.

If the end the previous frame method is chosen 440, the LEC for the bits of the label is calculated 442. As the bits of the label come in, the LEC operation is performed
10 in hardware. This calculated LEC is then checked until a match with the LEC field is identified 444. Monitoring for a match takes place 446, wherein a match indicates the beginning of the current frame and consequently the end of the previous GLEP frame 448. Otherwise, the process recycles 450.

Thus, it is possible to accurately identify the variable length GLEP frame. The
15 LEC allows the forwarding of a GLEP frame based on the label that is carried in the header, which is a fixed length lookup. Thus, this generic label encapsulation protocol according to the present invention allows for easy deployment of MPLS over serial links such as SONET. Nevertheless, those skilled in the art will readily recognize that the present invention is not meant to be limited to separately using CRC and LEC. Those
20 skilled in the art will recognize that more complex methods in accordance with the present invention may be used to increase performance. For example, a combination of the two approaches, i.e., some combination using both LEC and CRC, may be used to detect the end of the GLEP packets.

Returning again to Fig. 1, according to the present invention, a packet entering
25 the network cloud 140 would have a label attached at the ingress LSR 150. The egress LSR 152 would then extract the label according to the method described above with reference to Fig. 4.

In summary, the present invention describes a new method for encapsulation of
30 labeled datagrams over serial communications links, and a method for extracting the datagrams on the receiving end of the link. The key advantage of the present invention over the currently available label encapsulation methods, such as ATM and Frame Relay is the simplicity and efficiency of the method over the other alternatives. While SONET and MPLS are key technologies in Internetworking, there are benefits to combining these two. The approach outlined herein represents the first effort in carrying MPLS packets in
35 SONET. This eliminates the additional overhead of running ATM on SONET, while still maintaining the MPLS switching capability. Further, all the associated benefits of MPLS

can be obtained. Since packet over SONET is already in use, the present invention further enhances the capabilities of such a network. Specifically, QoS can be enabled on IP over SONET backbones through the use of MPLS. While SONET has been mentioned as the primary example above, those skilled in the art will recognize that the present invention described herein is valid for any serial link, and thus enables MPLS over any serial link.

The foregoing description of the exemplary embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not with this detailed description, but rather by the claims appended hereto.

WHAT IS CLAIMED IS:

1. A method for encapsulating a label in a packet enabling label switching of the packet over serial links, comprising:
 - adding a label and a label error correction to the front of a datagram, the
 - 5 label error correction being derived using the label; and
 - adding a cyclic redundancy check at a trailing end of the datagram, the cyclic redundancy check being derived using the datagram.
2. The method of claim 1 wherein the label includes three bytes.
3. The method of 1 wherein the label error correction is obtained
- 10 according to D^8+D^2+D+1 .
4. The method of claim 1 wherein the datagram is scrambled.
5. The method of claim 4 wherein the datagram is scrambled according to $D^{43}+1$.
6. The method of claim 1 wherein the cyclic redundancy check is
- 15 obtained using a polynomial $D^{16}+D^{15}+D^2+1$.
7. The method of claim 1 wherein the datagram is an IPv4 packet.
8. The method of claim 1 wherein the datagram is an IPv6 packet.
9. The method of claim 1 wherein the label comprises a plurality of bits, wherein a bit in the label is a label significant bit for indicating that no payload is
- 20 being carried.
10. A method for identifying an end of a packet encapsulating the datagram with a label, a label error correction field and a cyclic redundancy check field, comprising:
 - analyzing incoming bits for a packet until a pattern of bits is detected that
 - 25 matches a number of previous bits of the packet coded with a predetermined coding formula; and

identifying the end of the packet based upon the detection of the match and the predetermined coding formula.

11. The method of claim 10 wherein the predetermined coding formula comprises a cyclic redundancy check polynomial and the analyzing comprises coding incoming bits according to the cyclic redundancy check polynomial to produce a calculated cyclic redundancy check until the calculated cyclic redundancy check matches the cyclic redundancy check field.
12. The method of claim 11 wherein the selecting further comprises the identifying the end of the current packet based upon the detection of the match.
13. The method of claim 10 wherein the predetermined coding formula comprises a label error correction polynomial and the analyzing comprises coding incoming bits according to the label error correction polynomial to produce a calculated label error correction until the label error correction matches the label error correction field.
14. The method of claim 13 wherein the selecting further comprises the identifying the end of the previous packet based upon the detection of the match.
15. The method of claim 10 wherein the predetermined coding formula comprises a combination of a cyclic redundancy check polynomial and a label error correction polynomial, wherein the analyzing comprises coding incoming bits according to the cyclic redundancy check polynomial and the label error correction polynomial, wherein the cyclic redundancy check polynomial produces a calculated cyclic redundancy check until the calculated cyclic redundancy check matches the cyclic redundancy check field and the label error correction polynomial produces a calculated label error correction until the label error correction matches the label error correction field.
16. The method of claim 15 wherein the selecting further comprises the identifying the end of the current packet based upon the detection of the match.
17. A packet network, comprising:

an ingress entity for receiving a datagram and encapsulating the datagram with a label for controlling the processing of the datagram, a label error correction field and a cyclic redundancy check field to produce a labeled packet, and forwarding the labeled packet to a next hop; and

- 5 an egress entity for identifying an end of a packet encapsulating the datagram with the label, the label error correction field and the cyclic redundancy check field.

18. The packet network of claim 17 wherein the ingress entity encapsulates the datagram by adding a label and a label error correction derived using the label to the front of a datagram and adding a cyclic redundancy check derived using the datagram at a trailing end of the datagram.

19. The packet network of claim 18 wherein the label includes three bytes.

20. The packet network of claim 18 wherein the label error correction is obtained according to D^8+D^2+D+1 .

21. The packet network of claim 18 wherein the datagram is scrambled.

22. The packet network of claim 21 wherein the datagram is scrambled according to $D^{43}+1$.

23. The packet network of claim 18 wherein the cyclic redundancy check is obtained using a polynomial $D^{16}+D^{15}+D^2+1$.

24. The packet network of claim 18 wherein the datagram is an IPv4 packet.

25. The packet network of claim 18 wherein the datagram is an IPv6 packet.

26. The packet network of claim 18 wherein the label comprises a plurality of bits, wherein a bit in the label is a label significant bit for indicating that no payload is being carried.

27. The packet network of claim 17 wherein the egress entity identifies
5 an end of a packet encapsulating the datagram with the label, the label error correction field and the cyclic redundancy check field by analyzing incoming bits for a packet until a pattern of bits is detected that matches a number of previous bits of the packet coded with a predetermined coding formula and identifying the end of the packet based upon the detection of the match and the predetermined coding
10 formula.

28. The packet network of claim 27 wherein the predetermined coding formula comprises a cyclic redundancy check polynomial, the egress entity coding incoming bits according to the cyclic redundancy check polynomial to produce a calculated cyclic redundancy check until the calculated cyclic redundancy check
15 matches the cyclic redundancy check field.

29. The packet network of claim 28 wherein the selecting further comprises the identifying the end of the current packet based upon the detection of the match.

30. The packet network of claim 27 wherein the predetermined coding
20 formula comprises a label error correction polynomial, the egress entity coding incoming bits according to the label error correction polynomial to produce a calculated label error correction until the label error correction matches the label error correction field.

31. The packet network of claim 30 wherein the selecting further
25 comprises the identifying the end of the previous packet based upon the detection of the match.

32. The packet network of claim 27 wherein the predetermined coding formula comprises a combination of a cyclic redundancy check polynomial and a label error correction polynomial, the egress entity coding incoming bits according

to the cyclic redundancy check polynomial and the label error correction polynomial, wherein the egress entity uses the cyclic redundancy check polynomial to produce a calculated cyclic redundancy check until the calculated cyclic redundancy check matches the cyclic redundancy check field and the label error

5 correction polynomial to produce a calculated label error correction until the label error correction matches the label error correction field.

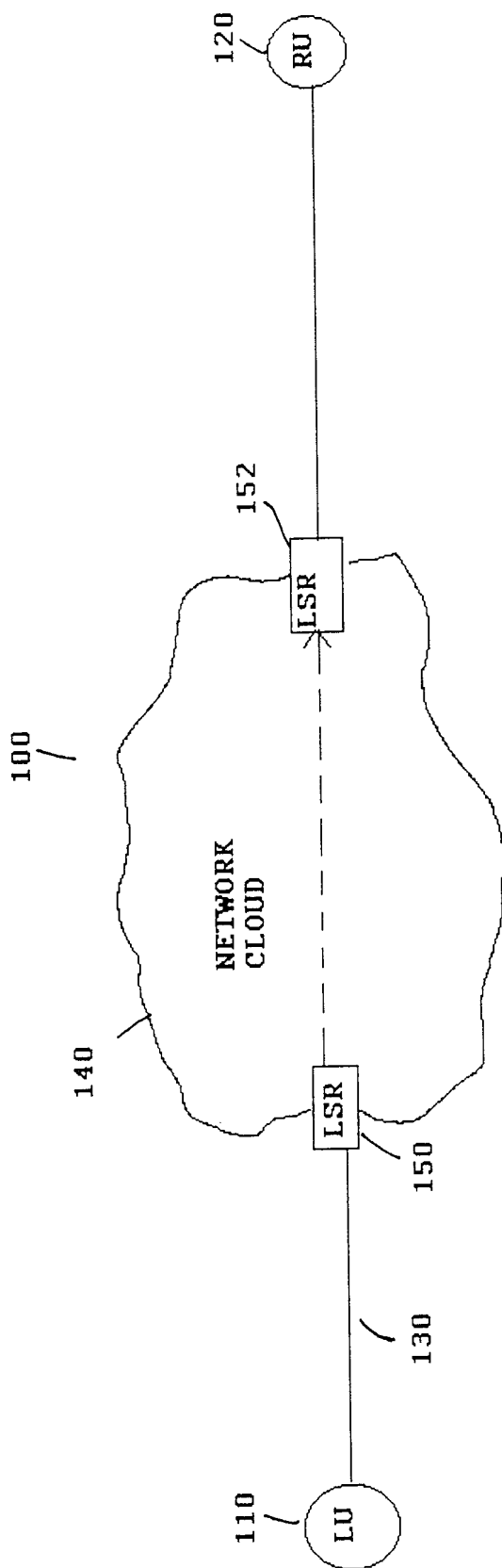


Figure 1

200 /

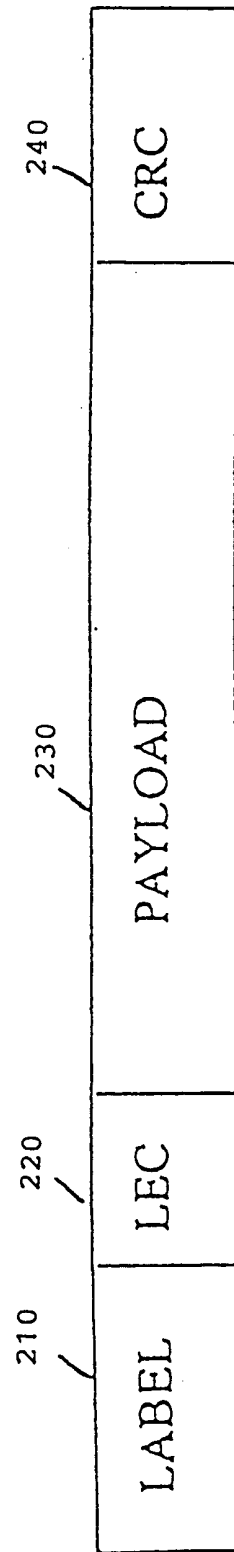


Figure 2

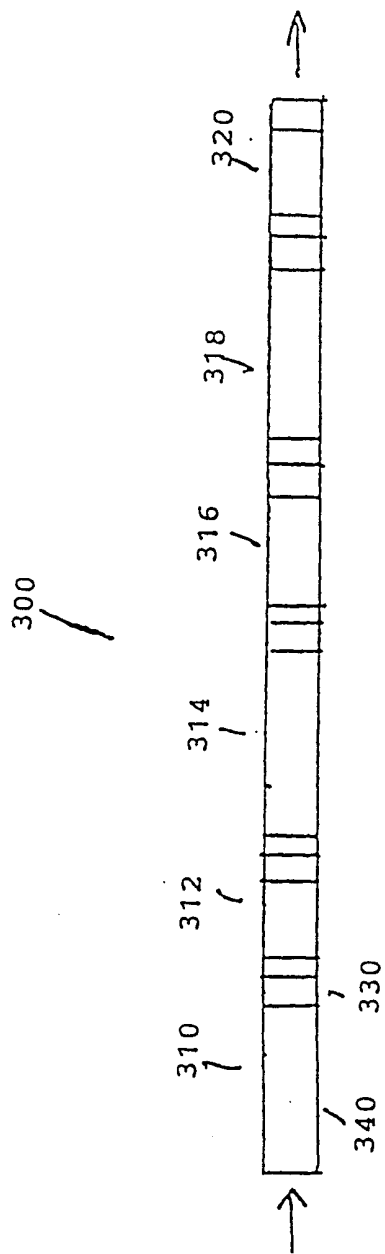


Figure 3

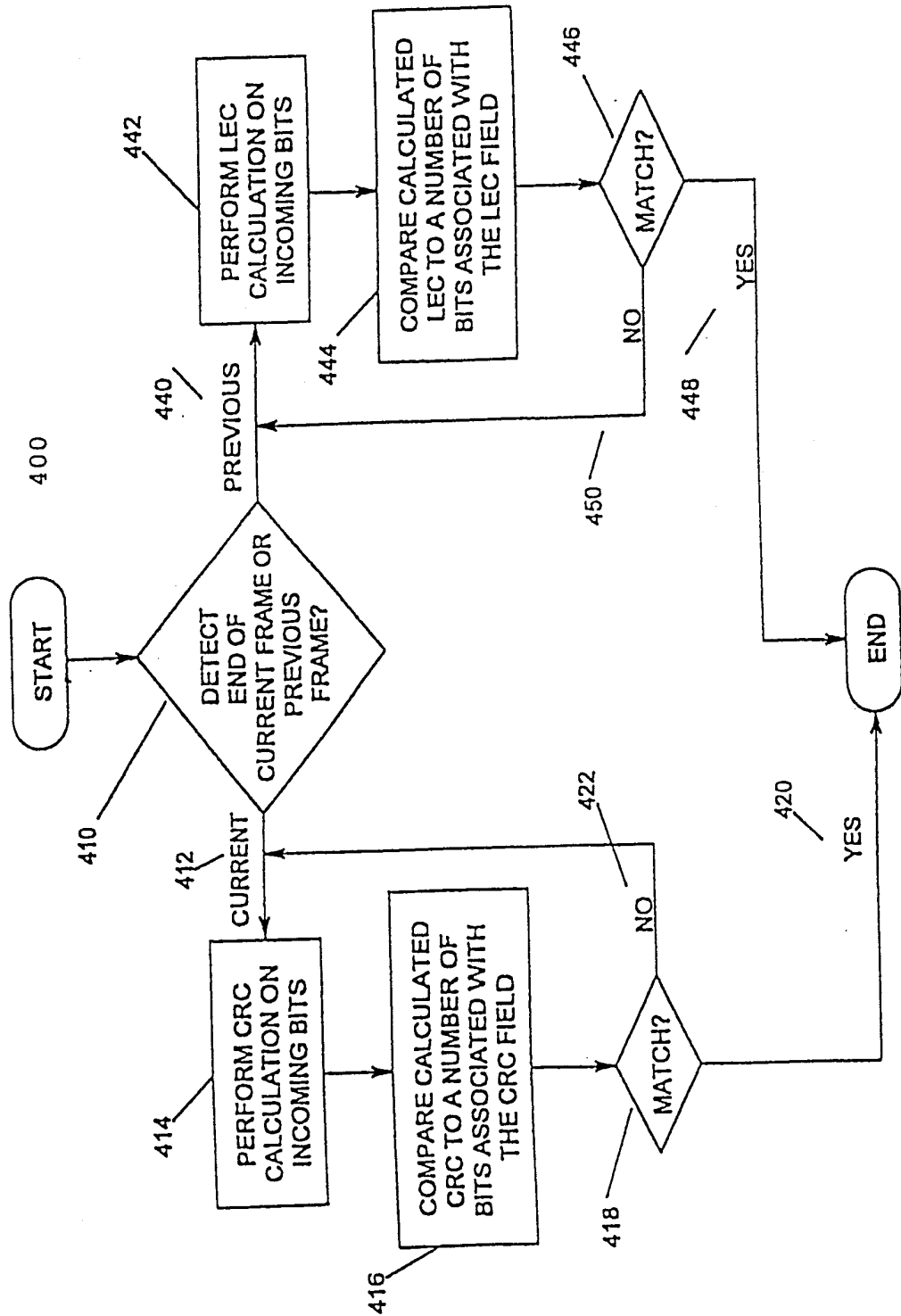


Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB00/00253

A. CLASSIFICATION OF SUBJECT MATTER IPC(7) : HO4L 12/56 US CL : 370/392, 401, 467, 474, 449 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) U.S. : 370/392, 401, 467, 474, 449 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) EAST		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,099,517 A (GUPTA et al.) 24 March 1992, (entire document)	1-32
A	US 5,430,715 A (CORBALIS et al.) 04 July 1995, (entire document)	1-32
A	US 5,841,776 A (CHEN) 24 November 1998, (entire document)	1-32
A	US 5,878,044 A (FRISCHKNECHT et al.) 02 March 1999, (entire document)	1-32
A	US 5,878,045 A (TIMBS) 02 March 1999, (entire document)	1-32
Y	US 5,594,732 A (BELL et al.) 14 January 1997, (col 9, lines 35-40; col 9, lines 7-9; col 15, lines 44-67)	1, 17
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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 document 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 20 JUNE 2000	Date of mailing of the international search report 19 JUL 2000	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer MITCHELL SL <i>James R. Matthews</i> Telephone No. (703) 305-3900	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB00/00253

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,763,319 A (ROZENBLIT) 09 August 1988, (col 18, lines 1-2; Fig 3)	1, 10, 17