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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017618 A1

(51) International Patent Classification[7]: H04L 29/06, 12/24, H03M 7/30

(21) International Application Number: PCT/IT02/00533

(22) International Filing Date: 9 August 2002 (09.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO2001A000813 13 August 2001 (13.08.2001) IT

(71) Applicant *(for all designated States except US)*: **TELECOM ITALIA LAB S.P.A.** [IT/IT]; Via Reiss Romoli, 274, I-10148 Torino (IT).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GHIRARDI, Maurizio** [IT/IT]; Telecom Italia Lab S.p.a., Via Reiss Romoli, 274, I-10148 Torino (IT).

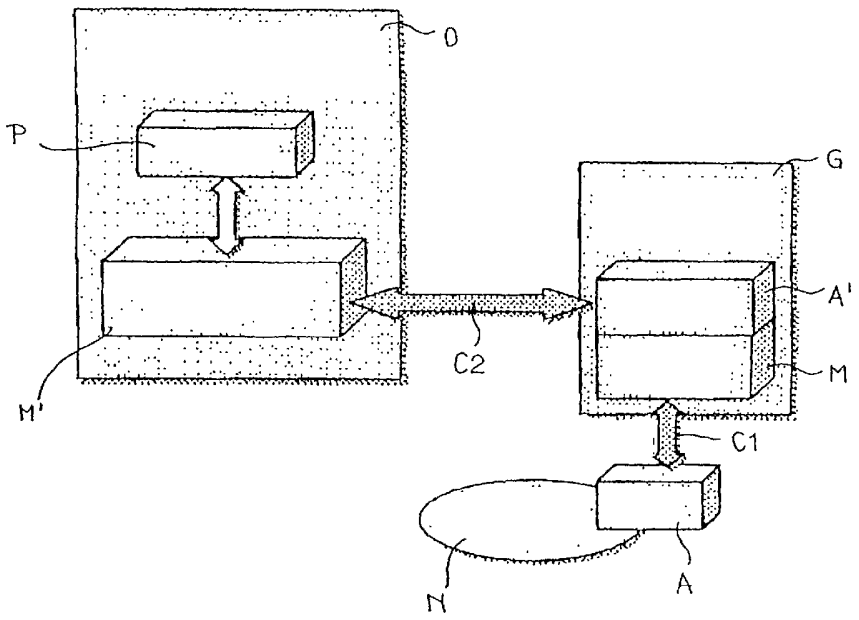
(74) Agent: **MASCIOPINTO, Gian, Giuseppe**; Telecom Italia Lab S.p.A., Via Reiss Romoli, 274, I-10148 Torino (IT).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR THE TRANSFER OF SNMP MESSAGES OVER UDP WITH COMPRESSION OF PERIODICALLY REPEATING SEQUENCES



(57) Abstract: The invention concerns the transfer of messages using an UDP transport. A typical example is offered by the SNMP messages, used to perform the communication (Cl, C2) between manager units (M, M') and agent units (A, A') within a system for the management of data communication networks, such as internet. The payload of messages and preferably the messages as a whole shall undergo a compression operation based on the recognition of sequences that periodically appear in the message.

WO 03/017618 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND DEVICE FOR THE TRANSFER OF SNMP MESSAGES OVER UDP WITH COMPRESSION OF PERIODICALLY REPEATING SEQUENCES

Technical Field

This invention concerns the transfer of messages using an UDP (short for User Datagram Protocol) transport, such as for instance the SNMP (Simple Network Management Protocol) messages.

These messages are generated and transmitted within data communication networks, such as internet. The architecture of the internet protocols is based on four logic layers, i.e. application, transport, network, and link.

The SNMP messages perform a simple communication mechanism between a Network Manager System (NMS) and the nodes being managed. This is made possible through specific applications located respectively at the NMS called "Network Manager" and at the nodes called "agents". The SNMP messages therefore take place at the UDP level, using it as a transport for such a purpose.

Background Art

The application called "agent" (hereinafter: agent) with its respective network manager over the SNMP messages has associated a database currently called "Management Information Base" or , short, MIB. Within such a database, the information is collected relating to the management and monitoring of the corresponding node or network element. In particular such information includes the following:

- MIB variables, that may be read by the Network Manager to derive information about the network element;
- MIB variables that may be written by the Network Manager to cause actions on the network element; and
- events (traps) that the same agent may cause towards the Network Manager (manager) with respect to specific situations.

The communication at SNMP level essentially includes therefore:

- messages required to read/write the above variables (GetRequest, GetNextRequest, SetRequest, GetBulk), sent out by the Network Manager, and

- response messages (GetResponse) and trap messages, transmitted by the agent.

The set of all the variables/traps managed by an agent are bound to the network element and specifically represent the relating MIB, i.e. they show the operation mode and the intrinsic characteristics of the network element to the Network Manager.

Each variable or trap is individually identified by a string in the ASN.1 notation (Abstract Syntax Notation One), called Object IDentifier or OID.

La framework of the string is, for instance, of "1.3.6.1.2.1.4.21" type, indicative of the fact that ASN.1 notation allows the representation of objects according to a hierarchical tree structure

A part of the MIB has been defined as a standard and is supported by any agent, whereas other variables and some traps are specific for each manufacturer and in some cases also characteristic of a particular apparatus typology.

The SNMP protocol, born in 1988, has undergone some evolutions during the years. In particular new messages typologies have been defined which the agents must be able to understand. The MIB standard, that each agent must be able to support, has been extended. On the filing date of this application, the versions being used are the 1st and the 2nd versions, whereas the standardisation of version 3 is currently under way.

The size of a MIB varies according to the apparatus type and can even be of the order of some hundred kBytes, corresponding to some hundred OIDs.

The diagram in Figure 1 of the attached drawings shows the typical components of an SNMP message. The content of each component is written in ASCII characters and its maximum permissible size is equal to the maximum size of an UDP message, the data entity that carries it, equal to 65,507 bytes or octets (of which about 64 kbytes are designed for the information to be carried).

In particular, in the same diagram of Figure 1 the presence may be noticed of a message header and of a PDU (Protocol Data Unit) part, of which the part denoted by 1 collects messages such as GetRequest, GetNextRequest, SetRequest and GetResponse, the part denoted by 2 collects GetBulk messages, whereas the part denoted by 3 generally concerns trap type messages.

More specifically, in the header of SNMP messages the following information is present:

- Version Number: number of the SNMP version used for message composition (V1, V2, V3, ...), and

- Community Name: a kind of password that allows access through reading and writing to the objects contained in the MIB module.

The following information is available within the PDU

- PDU type: message typology that in the version 1 contains instructions such as GetRequest, GetNextRequest, SetRequest and Request, whereas version 2 may also contain instructions such as GetBulkRequest e InformRequest;

- Request id: individual identifier of the message assigned by the manager and utilised by the agent when answering, in order that the manager might associate the requested response with the appropriate reference;

- Error status: set to 0 in all message typologies, except for the response messages, wherein, if set to 1, it means that an error is present;

- Error Index: it indicates which one among the requested variables (OID) has caused the error, and

- Variable Bindings: these are OID/value pairs; the values are "null" in the case of requests, and compiled in the case of response messages.

In particular, the part just on the left side of Figure 1 shows a typical structure of the part collecting the above Variable Bindings.

In the present invention and in the captions appearing in some figures of the appended drawings, the choice has been made of mentioning - for the different elements being considered - the corresponding acronyms / names / initials in the English language.

This has been done for the sake of a clear and straightforward description. The above acronyms, names and initials are currently used at international level by those skilled in the art, since no translations into the different national languages have been developed during the years.

The transmission of the SNMP message, made possible over UDP, allows the data packet exchange between two computers linked to the network. The UDP message format namely consists of a header whose main data are the IP address of the computer transmitting the message, the IP address of the destination computer and the size of the PDU being transported. In turn, the PDU format is formed by a header part and by a data part currently called "Payload" or "Octet Data". The header therefore contains the following data: source port, destination port, size of the transported unit, integrity check (CHECKSUM) of the data unit.

The methodology currently adopted for transferring a SNMP messages over UDP (from the manager to the agent, and vice-versa) is based in essence on the fact that the complete SNMP message is coded by means of the BER (Basic Encoding Rules) methodology. This way of operating allows one to convert the bytes forming the SNMP message into a hexadecimal structure suitable to be used as a payload of the UDP message.

The UDP transfer service of the data thus obtained essentially envisages:

- at the transmission stage: reading of the SNMP message and subsequent hexadecimal coding (BER encode) of the message, for its transmission over UDP, and

- at the reception stage : after the reception over UDP, the hexadecimal decoding (BER decode) of the PDU and the subsequent reconstruction of the message.

The current application practice proves that in the data communication networks such as internet, the need arises of transferring a bulk of information in terms of requests/responses conveyed in the form of SNMP messages.

Owing to the total size of the information, the time required for the relating transfer and network traffic thus generated, the solutions conventionally adopted for transferring SNMP messages in a standard format generally exhibit a rather poor efficiency.

For this reason three IEFT specifications have already been proposed - at a draft level - to tackle the issue.

The first proposal (known as SNMP Object Identifier Compression, rev. April 2001 - draft-ietf-eos-oidcompression-00.txt) is based on the concept that the majority of the information contained in the MIB is referred to by OID, formed by a constant and rather large part and by a variable and very small part. Starting from this principle, the proposal aim is the encoding, according to an algorithm, of

the constant part of the OID through a shorter numbering. This solution optimises only in part the quantity of information being transferred, without considerably reducing its size.

The second proposal (known as "Efficient Transfer of Bulk SNMP Data, rev. April 2001 - draft-ietf-eos-snmpbulk-00.txt") faces the issue of the management of the GetBulk instruction that allows the simultaneous collection of a given set of information. The instruction introduced in the SNMP version 2 does not allow the optimisation of the collection, since the manager has to declare the number of elements to be collected, without knowing how many elements form the set of information requested. Amendments to the UDP protocols have been suggested with a modification of the encode algorithm of the message (from BER to PER, which stands for Packet Encoding Rules) or with resort to a transfer mode of FTP (acronym of File Transfer Protocol) type. The solution described in the above cited document, is the introduction of a new instruction at the agent side, called GetColsRequest, and of relating message at manager side, capable of recognising the number of elements to be transferred, identifying the end of the requested set and optimising therefore requests and network traffic. However, also this solution does not allow one to optmise the management of sizes and number of messages being sent.

The third solution taken into account (known as "SNMP Payload Compression - rev. April 2001 - draft-irtf-nmrg-snmp-compression-01.txt") is in principle similar to the first proposal, since it suggests a differential encoding algorithm called "OID Delta Compression" or ODC. Starting from an OID root, such a solution envisages to memorise the subsequent OID assigning to the OID a code associated to the OID root, followed by the varying part of OID. Substantially, the

variations are stored in terms of differential increments, as compared to the root element. This solution has the drawback of being incompatible with previous versions of the protocol. Further, it allows an estimated saving by about 30% for particularly recursive OID values, i.e. data arrays, and it is substantially inefficient in the event of a low number of recursive items.

Disclosure of the Invention

The aim of the present invention is to provide an alternative solution as compared to the solution set out before, so as to allow an optimised transfer over UDP of messages such as SNMP messages, without affecting the protocol and the performance at the agent's as well at the manager's side.

According to the present invention, such aim is attained by means of a method having the characteristics specifically recalled in the appended claims. The invention also concerns, in a separate way, the relating system and the data processing product, directly loadable into the internal memory of a computer and incorporating parts of software code to implement the method according to the invention, when the above data processing product runs on a computer.

In essence, the solution according to the invention is based on the compression of the whole message (header and PDU).

In particular two different transfer modes are foreseen.

The first one encapsulates the SNMP message into a new SNMP message of proprietary type, and sends it in a standard mode using UDP.

The second one directly drives UDP through a driver providing the result of the SNMP message compression as Data Octet.

The compression technique is essentially based on the recognition of sequences appearing periodically within the message.

In a particularly preferred embodiment of the invention, the compression technique being used is a variation of the technique known as LZ77 (see the work by Ziv. J., Lempel A., "A Universal Algorithm for Sequential Data Compression", IEEE Transactions on Information Theory, Vol. 23, No. 3, pp. 337-343), well-known in the UNIX environment and called gzip (gzip format - RFC 1952), also used by the more popular PKZIP. The specifications of such a technique are commonly known, and there are also source libraries available, that implement and use such a solution for different development environments and operating systems, such as HP-UX,Digital, BeOS, Linux, OS/2, Java, Win32, WinCE.

In particular it is possible to use a porting of the algorithm on win32 by using a "zLib" library. For consultation, reference can be made to the site http://www.info-zip.org/pub/infozip/zlib/. The main feature of this library is to allow the runtime and on-memory compression of both binary data structures and strings, this being an important factor relating to the system performance.

Brief Description of Drawings

The invention will now be described by way of a non-limiting example, with reference to the attached drawings, wherein:

- Figure 1, relating to the background technique, has already been previously described;

- Figure 2 shows in the form of a general block diagram a typical application architecture of the solution according to the invention;

- Figures 3 to 5, each subdivided into two parts relating to transmission (part a) and to reception (part b)

respectively, illustrate different types of embodiments of the solution according to the invention in the form of a flow chart;

- Figure 6 is an additional flow chart illustrating the general characteristics of the solution according to the invention; and

- Figures 7 and 8 depict, according to modalities substantially similar to those adopted in Figure 1, the embodiment criteria of the solution according to the invention, illustrated in two possible variations.

Best mode for Carrying Out the Invention

Within the general diagram of Figure 2, reference N indicates a data communication network (as an immediate example, one may consider internet) defining the typical application environment of the solution according to the invention.

Reference A shows the module currently called "agent", that carries out the function of controlling and monitoring a corresponding element of the network N, operating in a - bi-directional - dialog mode with a corresponding manager M.

The latter defines, along with an additional agent A' of a higher hierarchical level, a port or gate G, that in turn interfaces with an additional manager M' of a higher hierarchical level.

The latter one defines along with a corresponding application, an observation module or observer O.

References C1 and C2 indicate two bi-directional communication channels that perform the communication - at a lower hierarchical level - between agent A and gate G, and - at a higher hierarchical level - between gate G and observer O.

The above-cited channels C1, C2 are those over which the transmission of SNMP messages takes place.

Flow charts of Figure 3 depict the modalities adopted for the compression (figure 3a) and decompression (figure 3b) of the SNMP message.

Flow charts of Figure 4 illustrate (still making reference to transmission - figure 4a - and to reception - figure 4b) a first solution which envisages the transfer of the compressed SNMP message through encapsulation over SNMP.

Flow charts of Figure 5 refer instead to a transfer solution through encapsulation over UDP. This still makes specific reference to transmission (Figure 5a) and reception (Figure 5b).

The diagrams of Figures 7 and 8 depict in relation to the OID representation the same formalism of Figure 1 and make reference to the set of compression and transmission operations, exemplified by part a) of Figures 3 and 4 (Figure 7) and part a) of Figures 3 and 5 (Figure 8), respectively.

By first examining the flow chart of Figure 3, reference 100 identifies the step during which the whole SNMP message (header + PDU) is read in order to be then converted or encoded into a hexadecimal format during a subsequent step denoted by 102. This is brought about by applying a coding of BER encode type.

The message thus encoded is then compressed by using a compression technique based on the recognition of recursive sequences, such as for instance the technique referred to in the zLib library, which has already been mentioned before.

This takes place during a step denoted by 104 so as to obtain during the step indicated by 106, a compressed Data Unit, ready for the transmission.

In a fully symmetrical way, the flow chart of part b of Figure 3 incorporates four steps, namely 206, 204, 202 and 200 (designed to be performed according to the indicated sequence), wherein the received compressed Data Unit (step

206) is subjected to decompression (step 204) with a view to the subsequent hexadecimal decoding (step 202), with a subsequent reconstruction of the entire SNMP message (step 200).

The fact of having assigned to the part b flow chart of Figure 3 numerical references sorted in an inverse way with respect to their performance sequence, has the only purpose of underlining the symmetrical character with steps 100 to 106 of the compression procedure. Similar choices have been made with reference to the flow charts of Figures 4 and 5.

As already shown, Figures 4 and 7 make reference to a transfer solution which envisages the encapsulation of the compressed Data Unit into a standard SNMP message, characterised by a proprietary or peculiar "Variable Binding", by a standard transmission modality over UDP.

The encapsulation modality of the compressed data Unit obtained during step 106 incorporates an initial step, denoted by 108, during which the compressed Data Unit is read by bytes and then converted into the corresponding set of ASCII characters, during a subsequent encoding step denoted by 110.

In the following step, denoted by 112 (which may be possibly preceded by auxiliary functions such as ACK TAB + NULL - see block 110a of Figure 7) the "Variable Binding" is generated of the message formed by a first OID with a proprietary or peculiar numbering (for instance 1.3.6.1.4.666.1) which contains in its value the string _ZIP_xxxx, wherein xxxx indicates the size of the original file. In the above cited example, the peculiar code 666.1 has been indicated which - at the moment - has not been registered at IANA (Internet Assigned Numbers Authority), but any other code not registered could be used.

The subsequent elements of the Variable Binding containing the compressed Data Unit, duly converted into ASCII characters, are formed by OID/value pairs. The value contains parts of the compressed Data Unit, converted into ASCII, having a maximum size of 255 characters.

Then the header information of the SNMP message is reconstructed. All this takes place during step 112, that is followed by a step denoted by 114, where an additional encoding according to the BER methodology is performed for generating a PDU payload of the UDP message (payload of PDU-UDP) to be used for data transmission (step 116).

Also in this case, steps denoted by 216, 214, 212, 210 and 208, reproduced in part b) of Figure 4 and designed to be performed according to the order by which they have been previously cited, represent the dual functions - to be carried out at the receiving side - of steps 108 to 116 relating to the transmission operation.

By adoption of the solution to which Figures 4 and 7 are referred, the compressed SNMP message has therefore a standard logic SNMP format, but a proprietary or peculiar content. Thus, it requires a functional extension - albeit minimal - of the agent's manager, such as to allow its recognition and encoding/decoding.

The experiments conducted by the Applicant prove that such a solution is fully feasible, without affecting the network architecture.

The alternative solution to which Figures 5 and 8 make reference, envisages the preparation of the compressed Data Unit starting from the SNMP message, according to the modalities shown in Figure 3, followed by the direct encapsulating of said Data Unit into the payload of PDU-UDP.

Obviously for a correct operation, this solution requires the use of a dedicated transmitter and receiver, for instance

under conditions which ensure the availability of a UDP port different from the standard one. The transmitter must therefore know the UDP port used by the receiver, and viceversa. The information about the ports being used may be exchanged at a higher level by means of a synchronisation message in a standard SNMP format, according to criteria to be better explained in the sequel.

When the alternative solution depicted in Figures 5 and 8 is adopted, the compressed Data Unit, made available during step 108 and designed to replace the BER of the message, becomes the payload of the PDU-UDP message.

The relating operation is schematised by the steps denoted by 118 and 120 in Figures 5 and 8, said steps preceding transmission step 122, designed for the respective dedicated port (generally called port X) of the receiver.

Also in this case, the complementary operation incorporates three steps, denoted by 222 (reception at port Y of the module acting at that moment as a receiver), 220 (extraction of the payload of PDU-UDP), and 218 (getting of the received compressed Data Unit, designed to be transferred toward step 206 of the part b) flow chart of Figure 3), respectively.

Also in this case steps 222, 220 and 218 are carried out according to the order by which they have been mentioned.

The synchronisation message referred to previously is sent out by the manager to the SNMP agent according to a general principle "application-to-application" using the standard SNMP format containing a proprietary or peculiar "Variable Binding".

The information being transferred may be of the type:

OID	Value
1.3.6.1.4.666.2	<UDP_TX_Port>
1.3.6.1.4.666.3	<UDP_RX_Port>

The manager sends to the SNMP manager a proprietary message compiling the value <UDP_TX_Port> with the number of the port designed to be used for the UDP transmission (for instance 1024) as well as a value <UDP_RX_Port> with the number of the port that it uses for the UDP reception (for instance 1224).

The agent replies to the manager sending a similar message containing its own information. This method reduces the processing time by improving the solution efficiency.

The block diagram of figure 6 additionally shows how the described solution may be generalised so as to be applied to any message typology using UDP as a transport (for instance SNMP, PING, etc.). This generalisation makes it possible to implement an UDP driver capable of replacing those presently used.

This solution is capable of evaluating the size of the payload to be transferred, and further proceeding (provided the size is adequate (for instance: more than 20 Bytes) by using the method herein described. To declare the compact nature of the UDP message to the receiver, use can be made of the 8 bits included from bit 62 to bit 69 of the header of the UDP message (at present such bits are not used and are set by default to 0) setting to 1 for instance one or more of such bits.

In particular, in the diagram of Figure 6, reference 300 indicates any step wherein the need arises of sending a message capable of being transported over UDP, followed by a compression step 302 of the payload, performed according to the modalities described in Fig.3.

A subsequent step 304 envisages the generation of the UDP message header according to the above-recalled terms, while a subsequent step denoted by 306 corresponds to the creation of

the entire UDP message, with a view to its IP transmission, to be performed during a step denoted by 308.

The described methodology allows the implementation of a general purpose solution, capable of supporting any type of application which makes use of the UDP-IP protocol stack.

Said solution is particularly suitable for the implementation of hardware or "on chip" solutions.

A functional extension of the described solution, applicable independently of the methodology being used for the data transfer, and the encoding of the message or its equivalent BER or Data Octet UDP. In this regard a safe and effective method appears to be the one currently termed as "block cipher Rijndael", also called "AES".

The solution described herein has the advantage of allowing the compression of SNMP messages - beyond the drawbacks described in the introduction of this description - making reference to a flexible compression technique, in a consolidated way, but also to other compression techniques (such as MPEG). Such a technique and its algorithm can be used in several operating systems, making such a solution a re-usable and re-implementable solution. Further, said solution has a minimum impact both on the manager and the agent, since it requires the set-up of a simple superstructure for compression and decompression of messages.

The solution also proves efficient, since it allows the optimisation of the network traffic, by transferring, time intervals being equal, a larger quantity of information or the same quantity of information through a lower number of messages. It is also a safe solution, since being compressed and encoded the information travels within the network in a clear text.

Obviously, while the principle of the invention remains unchanged, the details of the implementation of the invention

and its embodiments might be varied considerably with respect to what has been herein described and illustrated, without departing from the spirit and scope of the invention as defined by the appended claims.

5

CLAIMS

1. Method for the transfer over UDP (User Datagram Protocol) of messages incorporating a payload (OID), characterised in that it comprises the step of submitting at least said payload to a compression step (302, 104, 204) based on the recognition of sequences that periodically appear in the messages.

2. Method according to claim 1, characterised in that said compression step is performed according to a technique of gzip type, such as zLib.

3. Method according to claim 1 or claim 2, characterised in that it comprises the step of indicating the executed compression step into the message transferred over UDP.

4. Method according to claim 3, characterised in that it uses a bit field of the UDP header to indicate the executed compression step (302).

5. Method according to claim 4, characterised in that the bits from bit 62 to bit 69 of the UDP header are used to indicate the executed compression step (302).

6. Method according to claim 5, characterised in that it comprises the step of setting to 1 at least one among the bits 62 to 69 of the header of the UDP message.

7. Method according to any of the claims 1 to 6, applied to the transfer of SNMP messages, characterised in that the compression step comprises the following operations:

- reading (100) an entire SNMP message,
- encoding (102) the read message in hexadecimal format, and
- submitting the message encoded in the hexadecimal form to a compression (104).

8. Method according to any of the claims 1 to 7, applied to the transfer of SNMP messages, characterised by a reception step comprising the operations of :

- submitting a received message to a de-compression step (204) complementary to said compression step, so that the message submitted to the de-compression step can be obtained in hexadecimal format,

- decoding (202) the message submitted to the de-compression step (204) starting from the hexadecimal format, and

- reconstructing (200) the entire SNMP message starting from the decoded message.

9. Method according to claim 7 or claim 8, characterised in that it comprises an encapsulating operation into a standard SNMP message of the message submitted to said compression step (104).

10. Method according to claim 9, characterised in that it comprises the operations of :

- reading by bytes (108) the message submitted to said compression step (104) and converting (110) it into a corresponding message in ASCII characters,

- generating (112) a set of Variable Bindings, including a first OID indicative of the size of the original file and subsequent OID/value pairs carrying parts of said message submitted to said compression step (104), converted into ASCII characters,

- reconstructing a header information of the SNMP message,

- encoding (114) the SNMP message so obtained into a hexadecimal format so as to generate the UDP payload, and

- transferring (116) over UDP the payload so generated.

11. Method according to claim 8 and 9 or 10, characterised in that the reception step comprises the operations of:

- receiving the message submitted to said compression step as a UDP payload (216),

- submitting the payload so received to a hexadecimal decoding operation (214),

- recognising and assembling (212) the Variable Binding of the message submitted to hexadecimal decoding, and

- submitting the message recognised and assembled in the recognising and assembling operation (212) to a decoding operation from ASCII to binary (210),

- submitting the message decoded in binary form to said de-compression step (204).

12. Method according to claim 7 or claim 8, characterised in that it comprises the step of integrating the message submitted to said compression step (104) through encapsulation over UDP.

13. Method according to claim 12, characterised in that it comprises the steps of :

- configuring said message submitted to said compression step (104) as PDU payload of an UDP message (payload of PDU-UDP), and

- transferring the payload of PDU-UDP created in this way from a given transmission port of a transmitter to a given reception port of a receiver.

14. Method according to claim 13, characterised in that it includes the steps of :

- receiving said message as a payload of a PDU-UDP received at the reception port, and

- extracting said payload from said UDP message.

15. Method according to claim 13 or claim 14, characterised in that it comprises the step of transmitting between a transmission terminal (M, M'; A, A') and a receiving terminal (A, A'; M, M') a synchronisation message of SNMP type, identifying said transmission port and/or said reception port.

16. System for managing data communication networks, including at least one manager unit (M, M') and at least one agent unit (A, A'), communicating with one another over at least one channel (C1, C2) through the transmission of messages, characterised in that said messages are transferred over UDP following the method based on anyone of the claims 1 to 15.

17. Data processing product, directly loadable into the internal memory of a digital processor and including parts of software code to perform the method according to anyone of the claims 1 to 15, when the product is run on a digital processor.

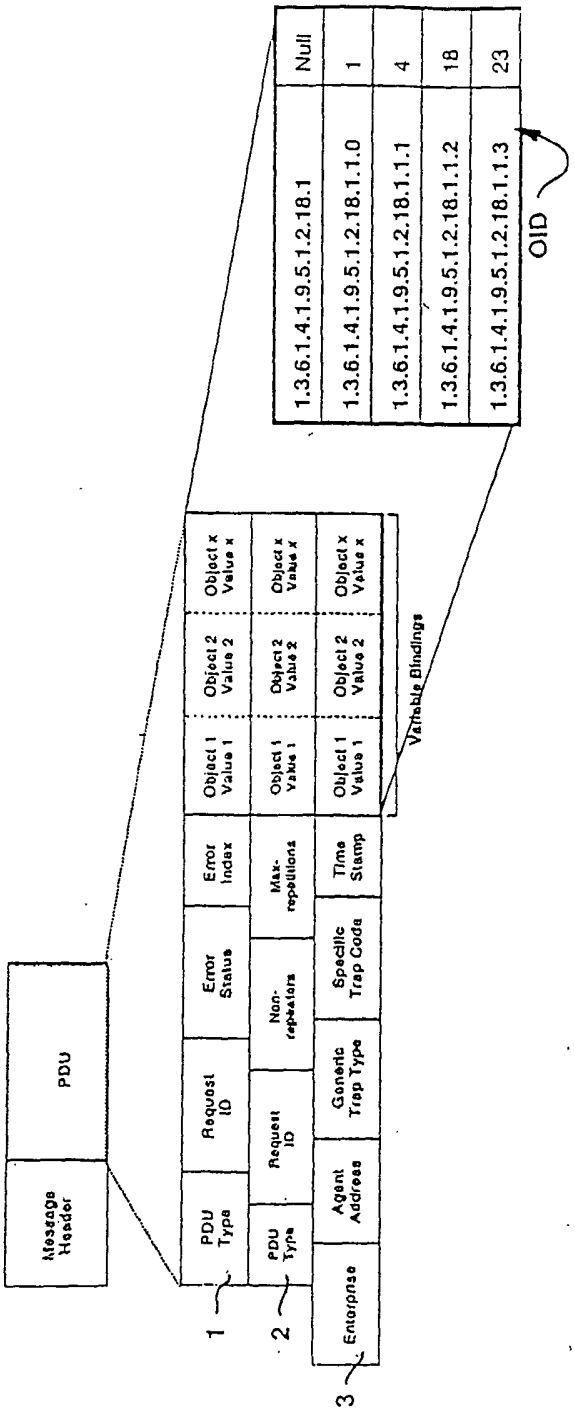

Message Header
PDU
PDU Type
Request ID
Error Status
Error Index
Object 1 Value 1
Object 2 Value 2
Object x Value x
PDU Type
Request ID
Non-repeaters
Max-repetitions
Object 1 Value 1
Object 2 Value 2
Object x Value x
Agent Address
Generic Trap Type
Specific Trap Code
Time Stamp
Object 1 Value 1
Object 2 Value 2
Object x Value x
Enterprise
Variable Bindings
1
2
3
1.3.6.1.4.1.9.5.1.2.18.1
1.3.6.1.4.1.9.5.1.2.18.1.1.0
1.3.6.1.4.1.9.5.1.2.18.1.1.1
1.3.6.1.4.1.9.5.1.2.18.1.1.2
1.3.6.1.4.1.9.5.1.2.18.1.1.3
OID
Null
1
4
18
23

Fig. 1

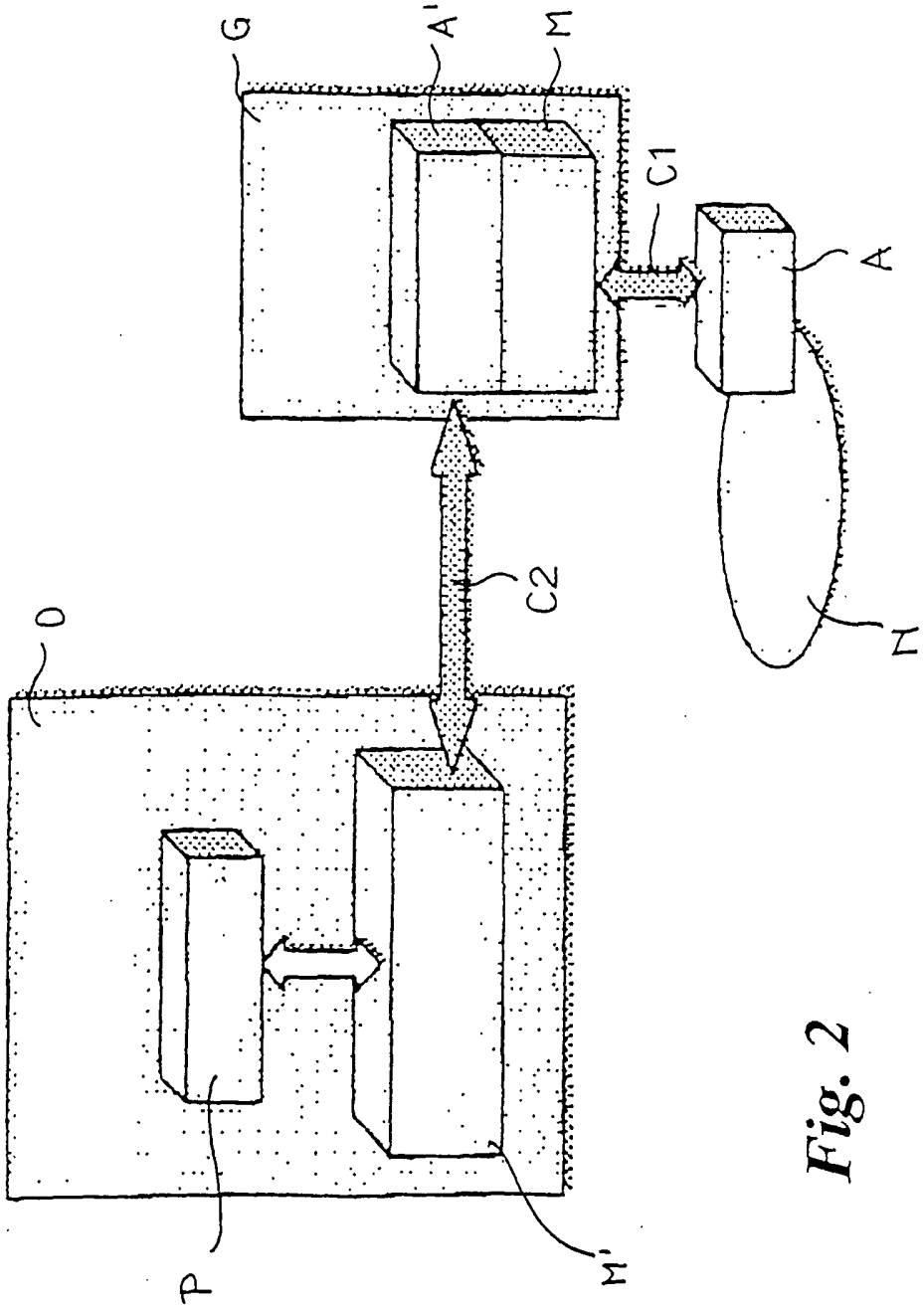


Fig. 2

Fig. 3

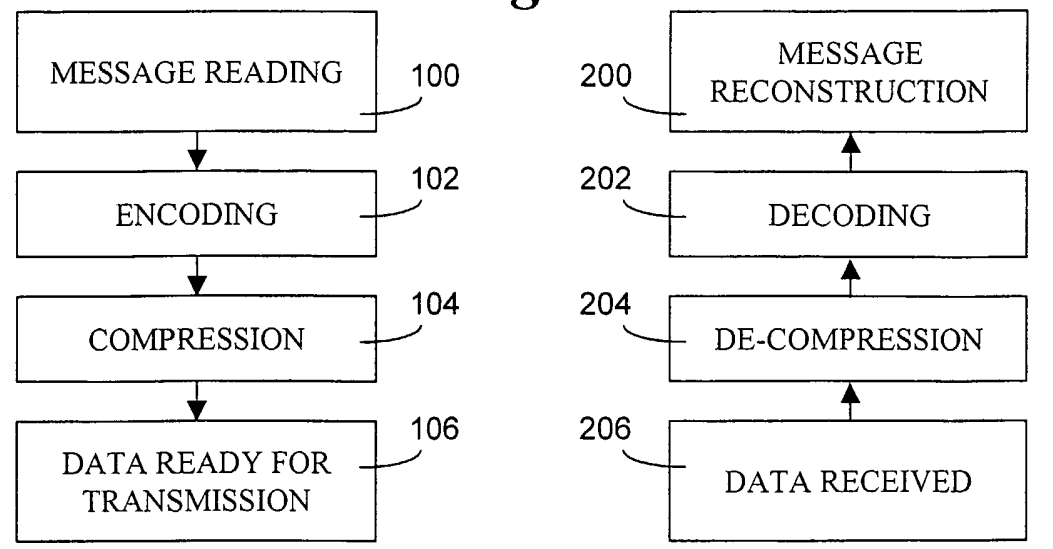


Fig. 4

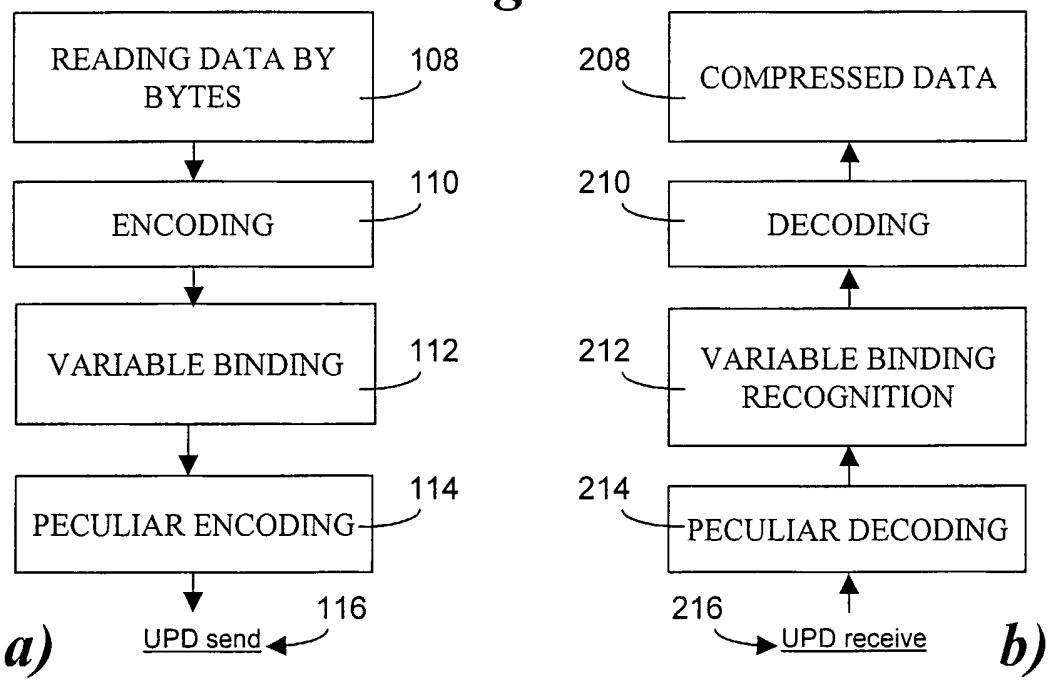
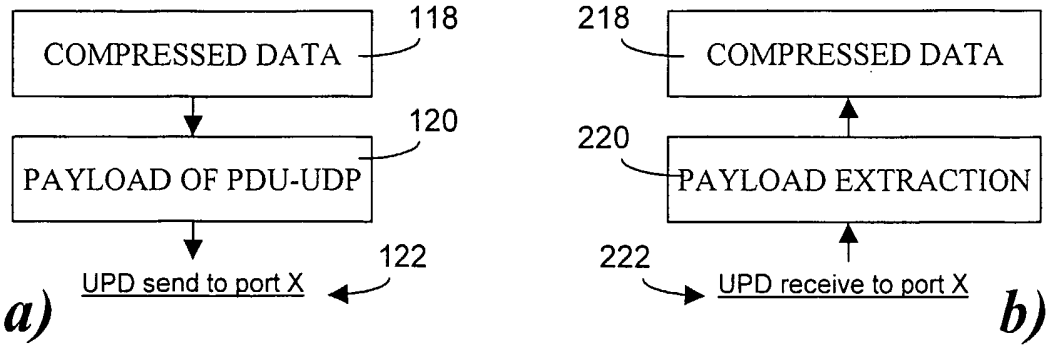


Fig. 5



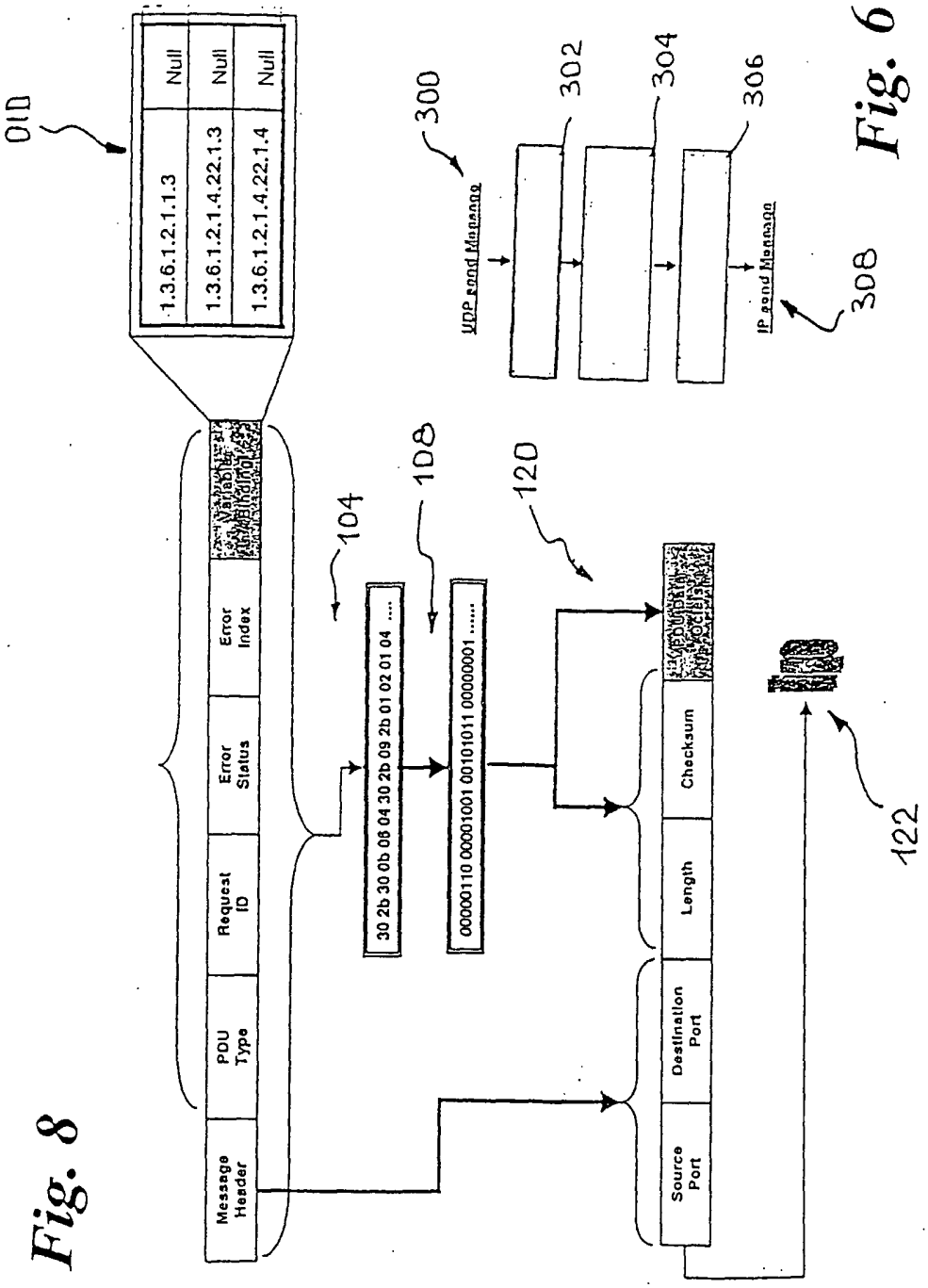
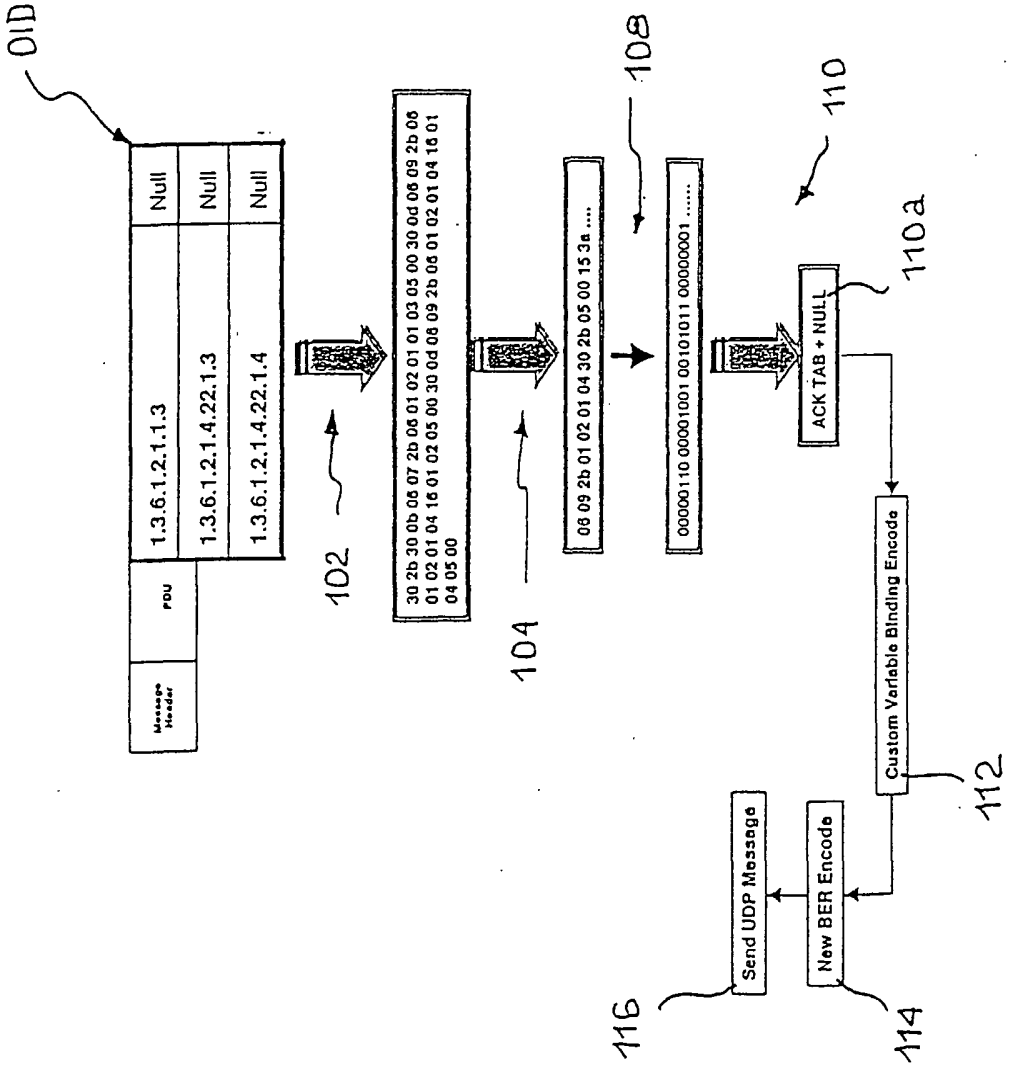

OID
1.3.6.1.2.1.1.3
1.3.6.1.2.1.4.22.1.3
1.3.6.1.2.1.4.22.1.4
Null
Null
Null
300
302
304
306
UDP send Message
IP send Message
308
Message Header
PDU Type
Request ID
Error Status
Error Index
Variable Bindings
104
108
120
122
30 2b 30 0b 06 04 30 2b 09 2b 01 02 01 04 ....
00000110 00001001 00101011 00000001 .....
Source Port
Destination Port
Length
Checksum

Fig. 8

Fig. 6

Fig. 7


OID
Message Header
PDU
1.3.6.1.2.1.1.3
1.3.6.1.2.1.4.22.1.3
1.3.6.1.2.1.4.22.1.4
Null
Null
Null
102
30 2b 30 0b 06 07 2b 06 01 02 01 01 03 05 00 30 0d 06 09 2b 06 01 02 01 04 16 01 02 05 00 30 0d 06 09 2b 06 01 02 01 04 16 01 04 05 00
104
06 09 2b 01 02 01 04 30 2b 05 00 15 3a ....
108
00000110 00001001 00101011 00000001 .....
110
ACK TAB + NULL
110a
Custom Variable Binding Encode
112
New BER Encode
114
Send UDP Message
116

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IT 02/00533

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/24 H03M7/30

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 7 H04L H03M

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, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DEGERMARK, NORDGREN, PINK: "IP header compression" 'Online! February 1999 (1999-02) , IETF XP002221120 Retrieved from the Internet: <URL: www.ietf.org> 'retrieved on 2002-11-15!	1-6
A	abstract page 7, line 15 -page 9, line 15	7-17

X	SANDRA MCLEOD: "OID compression" 'Online! April 2001 (2001-04) , IETF XP002221121 Retrieved from the Internet: <URL: http://www.ietf.org/proceedings/01aug/I-D/draft-ietf-eos-oidcompression-00.txt> 'retrieved on 2002-11-15! cited in the application	1-9
A	the whole document	7-17

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 November 2002	09/12/2002

Name and mailing address of the ISA	Authorized officer
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	Grimaldo, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	SAYTEN CHANDRAGIRI: "Eifficient transfer of bulk SNMP data" 'Online! April 2001 (2001-04) , IETF XP002221122 Retrieved from the Internet: <URL: http://www.ietf.org/proceedings/01aug/I-D/draft-ietf-eos-snmpbulk-00.txt> 'retrieved on 2002-11-15! cited in the application	1-6
A	the whole document	7-17
X	J. SCHOENWAELDER: "SNMP payload compression" 'Online! April 2001 (2001-04) , IETF XP002221123 Retrieved from the Internet: <URL: http://www.ibr.cs.tu-bs.de/projects/nmrg/draft-irtf-nmrg-snmp-compression-01.txt> 'retrieved on 2002-11-15! cited in the application	1-6
A	the whole document	7-17
A	WO 00 72517 A (GRAVES DAVID ;TOTH JOE (CA); EDGE NETWORKS CORP (CA); SCHELLENBERG) 30 November 2000 (2000-11-30) page 9, line 11 -page 10, line 23; figure 6	1-17

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IT 02/00533

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0072517 A	30-11-2000	AU 2652800 A	12-12-2000
		AU 2652900 A	12-12-2000
		AU 2653000 A	12-12-2000
		WO 0072599 A1	30-11-2000
		WO 0072602 A1	30-11-2000
		WO 0072517 A1	30-11-2000