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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/142710 A1

(51) International Patent Classification:
H04L 12/26 (2006.01) *H04L 12/56* (2006.01)

(21) International Application Number:
PCT/EP2010/058051

(22) International Filing Date:
9 June 2010 (09.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09305529.1 10 June 2009 (10.06.2009) EP

(71) Applicant *(for all designated States except US)*: **ALCATEL LUCENT** [FR/FR]; 3, avenue Octave Gréard, F-75007 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAN EWIJK, Adrianus** [NL/BE]; Pinksterbloemlaan 60, B-2180 Ekeren (BE). **DAVIES, Paul** [US/BE]; Grote Hondstraat 44, B-2018 Antwerp (BE). **SOLD, Haran** [NL/FR]; 48 avenue Kléber, F-75116 Paris (FR).

(74) Agent: **Bell Patent Attorneys (No 365)**; Copernicuslaan 50, B-2018 Antwerp (BE).

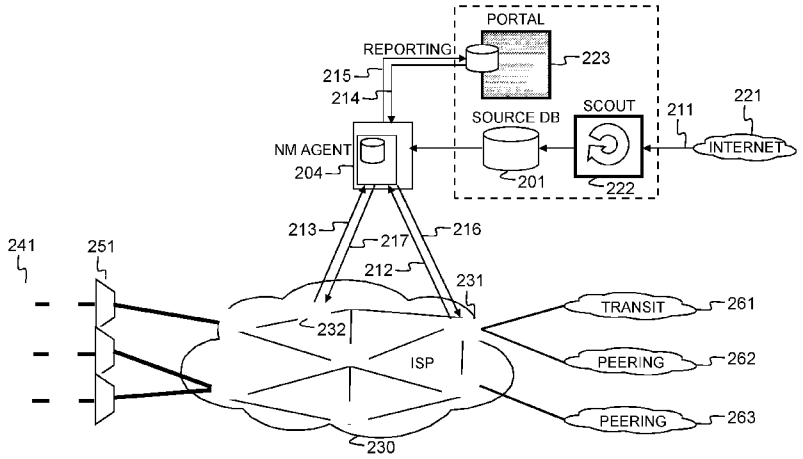
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: NETWORK MANAGEMENT METHOD AND AGENT



(57) Abstract: In the network management method according to the invention network flow information (102) is obtained from network management probes (231, 232) and application traffic profile information (101) is obtained from a source database (201). The network flow information (102) and the application traffic profile information (101) are correlated. Based on the correlation results, traffic policy rules are generated and installed in network elements via network management signals (216, 217).

WO 2010/142710 A1

NETWORK MANAGEMENT METHOD AND AGENT

Field of the Invention

[01] The present invention generally relates to communication networks like for instance the Internet. The invention more particularly concerns network or traffic management, i.e. controlling or influencing traffic flows in a network using a-priory knowledge on sources of traffic and applications or services delivered over the network.

Background of the Invention

[02] Network operators and Internet Service Providers (ISPs) are facing an increasing need to monitor and control traffic and applications that are delivered over their networks by specific sources. Identification and a better understanding of the applications that cause traffic increases in the operator's network will enable the operator or ISP to negotiate and install source specific traffic policies in its network.

[03] An existing tool for monitoring and controlling traffic is called Deep Packet Inspection (DPI) or Complete Packet Inspection, described for instance in Wikipedia at the following URL:

http://en.wikipedia.org/wiki/Deep_packet_inspection

DPI consists in creating a packet inspection point in the data path where packet inspection hardware can identify the type of traffic where a packet belongs to. Knowing the traffic category where a packet belongs to, for instance TCP (Transmission Control Protocol) or HTTP (Hypertext Transfer Protocol), does not enable to identify the source of the traffic, let aside the application that delivers the packet. Further, DPI devices are installed in the data path and therefore have to inspect and process the packets within very tight delay constraints, i.e. real-time processing at typical speeds of 10 to 40 Gbps (Gigabits per second) in today's networks. DPI devices hence require a high processing power and are therefore rather costly hardware solutions that do not meet the network operator's requirements in terms of identifying the sources and applications of traffic such that

policy rules for routing or policing traffic can be derived and applied per source or application.

[04] Known improvements of DPI consist in correlating the contents or behaviour of multiple packets in order to obtain more detailed information on the HTTP or TCP flows. By correlating certain re-directs, or by correlating the content of data packets with the URL that was used to retrieve an HTTP service or with the IP (Internet Protocol) address and MAC (Medium Access Control) address of the subscriber's residential gateway, more advanced DPI devices may be able to obtain or reconstruct more detailed information on the HTTP or TCP flows. However, such correlation techniques further increase the real-time processing requirements for DPI devices, making these devices even more complex and costly, and still do not enable to identify the exact source of traffic, the application that delivers the traffic, or the content of the traffic.

[05] In summary, although DPI devices enable to categorize traffic in some categories, like HTTP, P2P, etc., they do not meet today's requirements for identifying traffic, sources, and applications, and they involve complex and costly hardware for real-time packet processing in the data path. Network or traffic management solutions based on DPI consequently cannot determine and apply policy rules for routing or policing traffic of individual sources or applications.

[06] It is an objective of the present invention to provide a network management method and agent that resolve the above mentioned drawbacks of existing solutions. In particular, it is an objective to provide a network management method and agent that enable network operators and ISPs to install and apply source specific policies in their networks.

Summary of the Invention

[07] According to the present invention, the above mentioned drawbacks of the prior art are overcome by a network management method as defined in claim 1, comprising the steps of:

- obtaining network flow information from network management probes;

- obtaining application traffic profile information from a source database;
- correlating the network flow information with the application traffic profile information; and based thereon:
- generating traffic policy rules; and
- installing the traffic policy rules in network elements via network management signals.

[08] Thus, by using specific a priori knowledge on the traffic sources and applications, i.e. the application traffic profile information available from a source database, and by correlating the information extracted from this source database with network flow information from probes in the network, the traffic can be influenced at the network layer and/or transport layer via traffic policy rules that can be source and/or application specific. In case of the Internet, the network flow information can for instance be the IP 5-tuple (IP source address, IP destination address, IP source port, IP destination port, protocol) that may be extracted from the packets by a probe in the network, e.g. a DPI device. The source database stores addresses, ports, protocols and application traffic profiles for every important traffic source, e.g. server, on the network, and is supposed to be populated and maintained by a dedicated scout agent that contacts popular or important traffic sources in the network to collect this information. In case of the Internet, the address information stored in the source database corresponds to the IP address of the traffic source, the port information corresponds to the source port number, and the protocol information corresponds to TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). The application traffic profile information contains all important cross-layer information of the IP traffic sources and must therefore at least identify the application(s) supported by the IP traffic source, the codecs used, and a description of the temporal properties of the sourced IP traffic such as the average bit rate, burst size, jitter, etc. The network management method according to the current invention, based on correlation of network flow information with information extracted from a source database, has increased specificity of the traffic sources and applications. As a consequence, its accurateness in identifying and characterizing traffic sources and applications is much better. An advantage thereof is that traffic policing rules for individual traffic sources or traffic sources from a specific service provider can be generated and installed in network elements such as routers, policing functions, etc.

[09] Optionally, as defined by claim 2, the network management signals in the method according to the present invention may take the form of an Access Control List or ACL.

[10] Indeed, one way to install the traffic policy rules in network elements such as routers or policing functions, is by generating an Access Control List and forwarding the Access Control List to the network element that has to apply the traffic policy rules. The Access Control Lists may be equipment vendor specific.

[11] Further optionally, as defined by claim 3, the traffic policy rules may comprise a rule for upgrading a Quality of Service marking or QoS marking of certain traffic in a router.

[12] Thus, the application traffic profile information obtained from the source database may be used to define Quality of Service or QoS marking rules that are installed in routers, e.g. edge IP routers. The information from the source database, after correlation with the network flow information, thereto may be translated automatically and dynamically into a limited set of QoS marking rules or Access Control Lists for specific applications. For instance, one rule can instruct a router to change the QoS marking of packets with a specific IP source address and IP source port that pass the router. Based on that rule, the router will then mark traffic that matches the criterion. This way, the packets that match the criterion will receive a specific QoS treatment in the ISP's network.

[13] Alternatively, as is indicated by claim 4, the traffic policy rules may comprise criteria for re-routing certain traffic in a router.

[14] Thus, as an alternative to influencing the QoS marking, the traffic policy rules may cause packets from a specific source and/or application to take a specific route in the ISP's network.

[15] In another alternative, defined by claim 5, the traffic policy rules comprise traffic policing criteria for a policing function.

[16] Thus, instead of imposing QoS marking rules and/or re-routing criteria on the routers, the network management method according to the current invention may generate policing criteria, i.e. conditions to drop packets, and impose these policing criteria on one or more policing functions in the network.

[17] As is indicated by claim 6, the application traffic profile information in the network management method according to the current invention at least comprises:

- information indicative for an application supported by a traffic source,
- information indicative for a codec used to encode/decode content delivered by the traffic source; and
- information indicative for temporal properties of traffic delivered by the traffic source.

[18] The information indicative for the supported application may for instance identify the type of application, e.g. video or audio, or may be more specific and identify for instance the exact video application like Hulu, Youtube, iTunes, Bittorent, etc. The information indicative for the codec used may for instance identify the encoding mechanism, like mp4, h264, etc. in case of video traffic, or mp3, wav, etc. in case of audio. The information indicative for temporal properties of the traffic can be extracted from the Quality of Service profile of the traffic source, and will typically contain parameters like the average video bit rate, the burst size, jitter, etc.

[19] As is indicated by claim 7, the network flow information in the method according to the current invention may comprise:

- source address information and destination address information for a traffic flow;
- source port information and destination port information for the traffic flow;
- protocol information for the traffic flow;
- Quality of Service marking for the traffic flow; and
- information indicative for a physical interface whereon the traffic flow traversed.

[20] In case of the Internet, the source address will be the source IP address in the header of IP packets belonging to the traffic flow under consideration. The destination address will be the destination IP address that can be extracted from the same IP packet header. The source and destination port information will correspond to the IP source port number and IP destination port number used by that flow. The protocol information protocol information corresponds to TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). The foregoing information extracted from the IP packets by a probe or packet inspection function in the network, constitutes the IP 5-tuple. Further, the QoS marking like for instance the TOS (Type Of Service) bit can be extracted from the packet header through packet inspection, and the physical interface whereon the IP packet traversed can be identified by the probe in the network that extracts the network flow information.

[21] Optionally, as is defined by claim 8, the method according to the invention may further comprise:

- generating traffic reports accessible by a network operator via a dedicated portal.

[22] Indeed, by correlating the network flow information with the information obtained from the source database, detailed traffic reports may be built for network operators or service providers. In particular when the source database also stores application metadata such as the name of the application or service, the company offering the service, the content delivery network, the domain offering the service, the URLs or links involved in delivering the service, the applications involved in delivering the service, the geographical location of the servers involved in delivering the service, the delivered content, the company that is the source of the content, etc., the results of the correlation will not only be useful for generating and installing traffic policy rules, but will also be useful to build and deliver detailed reports on the traffic from specific sources or applications, that can be made accessible to the network operator or service providers via a dedicated portal or interface.

[23] In addition to a network management method as defined by claim 1, the current invention also relates to a corresponding network management agent as defined by claim 9, comprising:

- means for obtaining network flow information from network management probes;

- means for obtaining application traffic profile information from a source database;

- means for correlating the network flow information with the application traffic profile information;

- means for generating traffic policy rules; and

- means for installing the traffic policy rules in network elements via network management signals.

[24] The network management agent can for instance be a set of computer programs installed in a network management platform of the network operator or ISP.

Brief Description of the Drawings

[25] Fig. 1 illustrates the obtaining of data in an embodiment of the network management method according to the present invention; and

[26] Fig. 2 illustrates the sequence of steps in an embodiment of the network management method according to the present invention.

Detailed Description of Embodiment(s)

[27] Fig. 1 shows information 101 obtained from a source database, SOURCE DB, and network flow information, 102 or NETWORK FLOW DATA, that lie at the basis of the invention. Fig. 1 further shows information 103 obtained from an ASN (Autonomous System Number) database, ASN DB, and obtained from geographic databases, IP GEO DB, that may optionally be used in embodiments of the current invention as supplemental information.

[28] The basic insight underlying the embodiment illustrated by Fig. 1 is that traffic flows in an IP network can be influenced by correlating specific a-priory knowledge 101 on application sources contained in an IP source database with network flow data 102 received from probes in the network, for instance NetFlow or other IP flow

data (e.g. IPFIX, CFLOWD, SFLOW, etc.) received from a NetFlow traffic analyzer, routers, policing functions, packet inspection devices, etc.

[29] The IP source database from which information 101 is obtained is a database of IP addresses and ports of every important computer (e.g. server) on the Internet and of the applications that are delivered from these IP addresses. It stores all important cross-layer information of IP sources and applications in the application traffic profile of a traffic source. This includes, besides network address and protocol information, information about the source, about the network, about the application(s) or service(s) delivered, about the content delivered, and about the companies that are involved in the full delivery chain of the application.

[30] "Source" information includes the IP source address, the source port number, the protocol used (e.g. UDP, TCP) and eventually the geographic location of the source. The latter geographic information may be obtained from the IP GEO DB database. "Network" information includes an identification of the content delivery network and its assigned address range that can be obtained from the ASN DB database. "Application" information includes the name of the application or service (e.g. iTunes, YouTube, Joost, Hulu, etc.), the traffic class and traffic type (video, audio, etc.). "Content" information includes for instance the file name and the name of the company that created or owns the content (e.g. NBC, RTL, etc.). "Company" information may include the name of companies offering applications or services (e.g. Google, Apple, etc.), the name of companies operating the content delivery network (e.g. Akamai, Limelight, etc.), and the name of companies creating content (e.g. NBC, RTL, etc.), if not yet included in the foregoing.

[31] The network flow data 102 obtained from probes in the network like NetFlow traffic analyzers includes the IP 5-tuple consisting of source IP address of a flow, destination IP address of a flow, source port number, destination port number, and Layer 3 or transmission layer protocol (e.g. TCP or UDP). In addition the network flow data 102 also contain the Quality of Service or QoS marking, like for instance the Type Of Service (TOS) bit or the Differentiated Services Code Point (DSCP) value extracted from the packets in the flow. Further, the network flow data 102 contain an identification of the logical or physical interface traversed by the flow.

Other examples of network flow data besides NetFlow are CFLOWD, IPFIX and for instance SFLOW.

[32] By correlating the information 101 in the IP source database SOURCE DB with the network flow data 102 as is indicated by 104 in Fig. 1, traffic policy rules can be generated and traffic in the IP network can be influenced in real time at the network and/or transport layer. As will be illustrated in the following paragraphs with reference to Fig. 2, the correlation result can be used to generate network management signals (e.g. SNMP or Simple Network Management Protocol traps) based on the application traffic without having to install expensive network appliances in the network.

[33] Fig. 2 shows an ISP's network 230 over which video applications, i.e. streaming video and peer-to-peer video applications are delivered to clients 241 that connect with the ISP's network 230 via an access network 251, e.g. a DSL (Digital Subscriber Line) network. Fig. 2 shows transit clouds, 261 or TRANSIT, and peering clouds, 262 and 263 or PEERING. The applications are delivered across these clouds.

[34] Fig. 2 illustrates with arrow 211 a process wherein a scout agent, 222 or SCOUT, collects info on important video sources in the Internet 221 by emulating clients and determines domain names associated with these video sources. The scout agent 222 thereupon collects IP source and application traffic profile information for these video sources and builds the IP source database, 201 or SOURCE DB. The process of populating and maintaining the IP source database 201 is described in more detail in a counterpart patent application from the same applicant, entitled "Method and Scout Agent for Building a Source Database" that is incorporated herein by reference.

[35] As a result, the IP source database 201 contains network information like IP addresses, ports and protocol information (UDP/TCP) of important video sources, and also information about the video applications that are delivered from these IP addresses, the type of traffic they deliver (e.g. streaming video or peer-to-peer video), the delivered video content, the domain and the geographic location of the

server(s) that deliver the content, the companies that are the source of the video content, and the content delivery network (CDNs) that deliver the video content.

[36] The network management agent, 204 or NM AGENT, collects IP flow data from network management probes in an ISP's network 230, e.g. a NetFlow traffic probe 232, a DPI device integrated in router 231, etc. It is noticed that alternatively, the Netflow data can also come directly from a router without integrated DPI device or without using a dedicated NetFlow agent. This is illustrated by the arrows 212 and 213 in Fig. 2. The IP flow information will indicate IP 5-tuples (IP source address, IP destination address, IP source port, IP destination port, protocol), plus the QoS marking and physical interface on which the IP flow traversed. This IP 5-tuple info can be correlated with the information in the IP source database 201 to determine what service is being used. The correlation may involve querying the source database 201 using the IP 5-tuple. This can be done manually or automatically. In the scenario where it is done manually, the ISP will use the IP source DB 201 to define what application sources he would like to manage. For instance if an ISP wants to manage hulu.com traffic, the operator can query the IP source DB 201 to retrieve the IP source information that is relevant for his network situation, e.g. depending on the geographic location. The IP source database 201 will provide the IP source information relevant for hulu.com.

[37] The information contained in the database 201 is thereupon used by the network management agent 204 to define QoS marking rules (e.g. Access Control Lists or ACLs) that are installed in network elements like edge router 231 and the NetFlow traffic probe 232. The IP source database information is automatically and dynamically translated into a limited set of QoS marking rules or ACLs for specific subscribers, IP sources or applications. For example, a rule can instruct the router 231 and the NetFlow traffic probe 232 to mark each packet with a specific source IP address and port that passes the router 231 or NetFlow traffic probe 232. The rule is installed in router 231 and NetFlow traffic probe 232 through network management signaling as is indicated by arrows 216 and 217. Based on such rule the router 231 and NetFlow traffic probe 232 will mark traffic that matches the criterion. The traffic QoS marking may cause the packets to take a specific route in the ISP's network 230 or to receive specific QoS treatment.

[38] As an alternative to QoS marking, the network management agent 204 may define rules for route optimization (e.g. changing the next hop address in routing tables for certain sources or applications), or rules for dropping/accepting packets to be installed in policing functions in the network 230.

[39] Fig. 2 further shows that the network management agent 204 retrieves network flow information in 212 and 213, and correlates this with the IP source database 201 to generate reports, referenced by REPORTING. A dedicated portal, 223 or PORTAL, thereto sends management request to the network management agent 204, as indicated by arrow 214. The network management agent 204 thereupon reports source and/or application performance to the portal 223, as is indicated by arrow 215.

[40] It is further noticed that the QoS marking rules installed according to the current invention by the network management agent 204 can also be used for accounting and billing.

[41] Although the present invention has been illustrated by reference to specific embodiments, it will be apparent to those skilled in the art that the invention is not limited to the details of the foregoing illustrative embodiments, and that the present invention may be embodied with various changes and modifications without departing from the scope thereof. The present embodiments are therefore to be considered in all respects as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein. In other words, it is contemplated to cover any and all modifications, variations or equivalents that fall within the scope of the basic underlying principles and whose essential attributes are claimed in this patent application. It will furthermore be understood by the reader of this patent application that the words "comprising" or "comprise" do not exclude other elements or steps, that the words "a" or "an" do not exclude a plurality, and that a single element, such as a computer system, a processor, or another integrated unit may fulfil the functions of several means recited in the claims. Any reference signs in the

claims shall not be construed as limiting the respective claims concerned. The terms "first", "second", third", "a", "b", "c", and the like, when used in the description or in the claims are introduced to distinguish between similar elements or steps and are not necessarily describing a sequential or chronological order. Similarly, the terms "top", "bottom", "over", "under", and the like are introduced for descriptive purposes and not necessarily to denote relative positions. It is to be understood that the terms so used are interchangeable under appropriate circumstances and embodiments of the invention are capable of operating according to the present invention in other sequences, or in orientations different from the one(s) described or illustrated above.

CLAIMS

1. A network management method, said method comprising the steps of:

- obtaining network flow information (102) from network management probes (231, 232);

- obtaining application traffic profile information (101) from a source database (201);

- correlating said network flow information (102) with said application traffic profile information (101); and based thereon:

- generating traffic policy rules; and

- installing said traffic policy rules in network elements via network management signals (216, 217).

2. A network management method according to claim 1, wherein said network management signals (216, 217) take the form of an Access Control List or ACL.

3. A network management method according to claim 1, wherein said traffic policy rules comprise a rule for upgrading a Quality of Service marking or QoS marking of certain traffic in a router.

4. A network management method according to claim 1, wherein said traffic policy rules comprise criteria for re-routing certain traffic in a router.

5. A network management method according to claim 1, wherein said traffic policy rules comprise traffic policing criteria for a policing function.

6. A network management method according to claim 1, wherein said application traffic profile information (101) comprises:

- information indicative for an application supported by a traffic source,

- information indicative for a codec used to encode/decode content delivered by said traffic source; and

- information indicative for temporal properties of traffic delivered by said traffic source.

7. A network management method according to claim 1, wherein said network flow (102) information comprises:

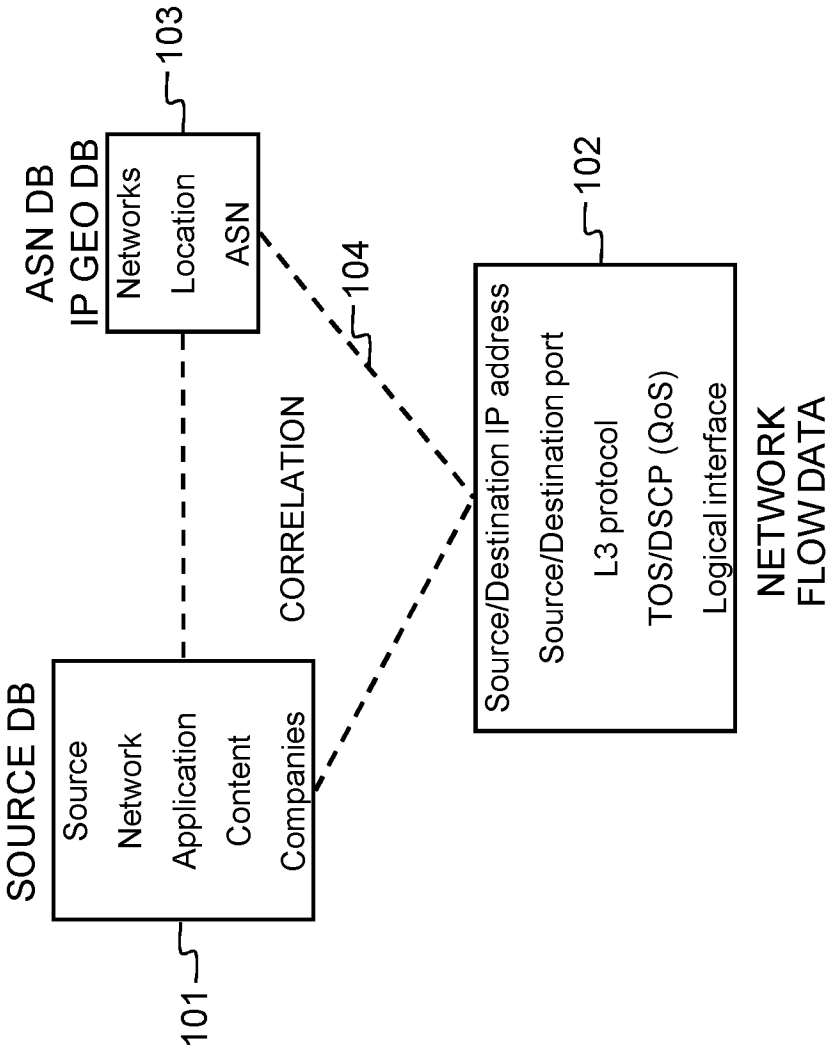
- source address information and destination address information for a traffic flow;
- source port information and destination port information for said traffic flow;
- protocol information for said traffic flow;
- a Quality of Service marking for said traffic flow; and
- information indicative for a physical interface whereon said traffic flow traversed.

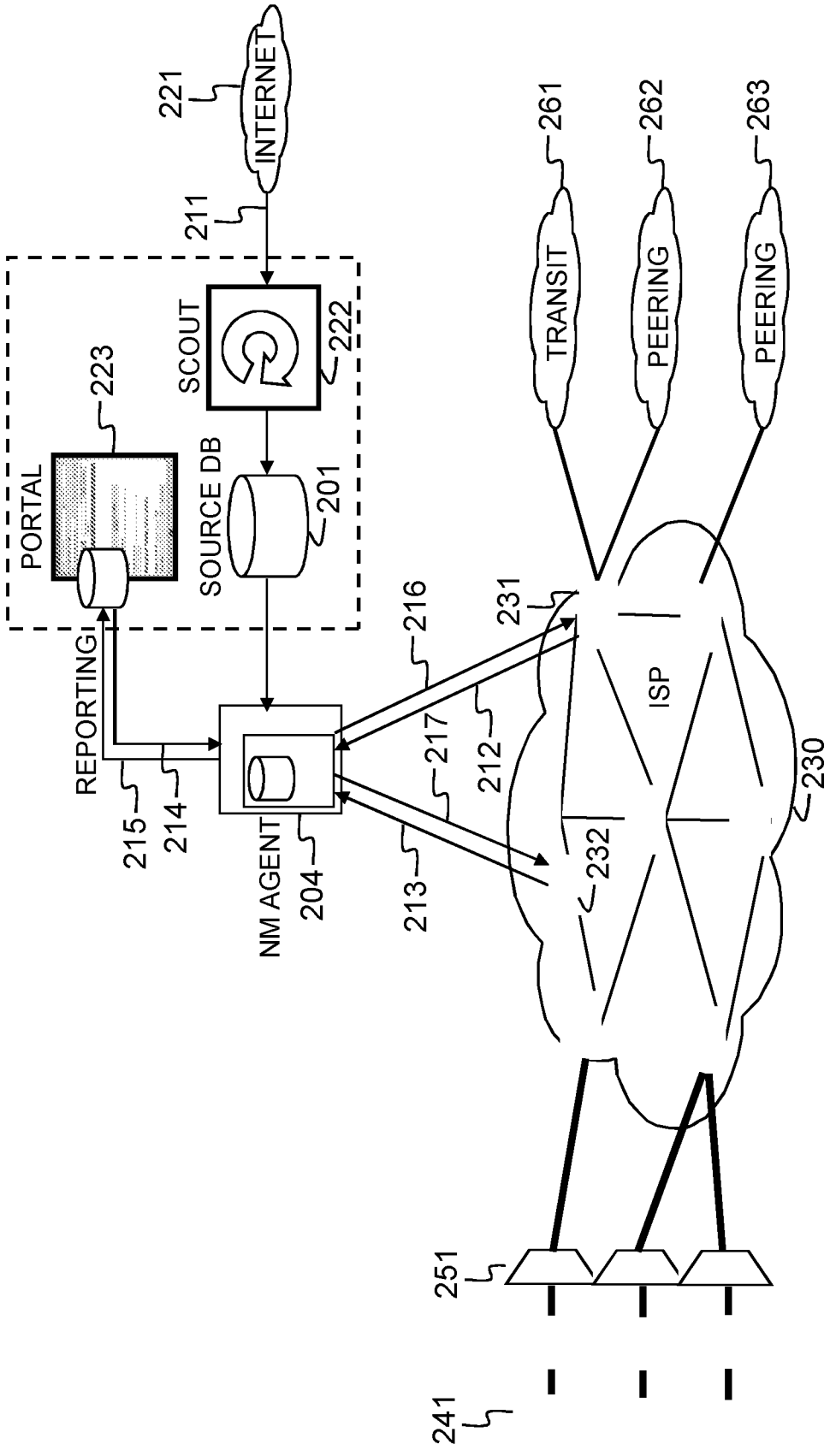
8. A network management method according to claim 1, said method further comprising:

- generating traffic reports accessible by a network operator via a dedicated portal (223).

9. A network management agent (204) comprising:

- means for obtaining network flow information (102) from network management probes (231, 232);
- means for obtaining application traffic profile information (101) from a source database (201);
- means for correlating said network flow information (102) with said application traffic profile information (101);
- means for generating traffic policy rules; and
- means for installing said traffic policy rules in network elements via network management signals (216, 217).


SOURCE DB
Source
Network
Application
Content
Companies
101
ASN DB
IP GEO DB
Networks
Location
ASN
103
CORRELATION
104
Source/Destination IP address
Source/Destination port
L3 protocol
TOS/DSCP (QoS)
Logical interface
102
NETWORK
FLOW DATA


INTERNET
221
211
SCOUT
222
223
PORTAL
SOURCE DB
201
REPORTING
215
214
NM AGENT
204
213
216
217
212
231
232
ISP
230
TRANSIT
PEERING
PEERING
261
262
263
251
241

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/058051

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/26
ADD. H04L12/56

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, 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	WO 2008/119930 A (BRITISH TELECOMM [GB]; WITTGREFFE JOHN PETER [GB]) 9 October 2008 (2008-10-09) * abstract figures 3,4A,6,7 page 1, lines 1-5 page 2, lines 6-9 page 5, lines 12-17 page 6, lines 3-7,14-19 page 8, lines 16-30 page 9, lines 25-32 page 10, lines 1-12,29-33 page 11 page 12, lines 12,13,30-33 page 13, lines 5-24 page 17, lines 9-31 page 18, lines 1-9,24-30 page 19, lines 1-26	1-9

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2010	04/08/2010

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, Fax: (+31-70) 340-3016	Volpato, Andrea

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/058051

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/088529 A1 (KLINKER ERIC [US] ET AL) 8 May 2003 (2003-05-08) * abstract figures 1C,2-6,7A paragraphs [0010], [0011] paragraph [0017] paragraph [0057] paragraph [0059] paragraph [0066] paragraphs [0069] - [0071] paragraphs [0075] - [0077] paragraphs [0079], [0080] paragraphs [0087], [0089] paragraphs [0092] - [0100] paragraphs [0112], [0113] paragraphs [0118], [0119] paragraphs [0125] - [0130] paragraphs [0132], [0134], [0137], [0138] paragraphs [0156] - [0160]	1-9
X	US 6 502 131 B1 (VAID ASEEM [US] ET AL) 31 December 2002 (2002-12-31) * abstract figures 1-9,16-18 column 1, lines 19-23 column 2, lines 15-17,56-58 column 3, lines 6-26 column 4, lines 35-40 columns 5-6 column 7, lines 5,6,61-67 column 8, lines 10-26 column 9, lines 64-67 column 10 column 12, lines 44-47 column 13, lines 35-67 columns 14-20 column 22, lines 30-67 columns 23-28 column 29, lines 34-67 column 30, lines 1-3	1-9
A	US 2007/011317 A1 (BRANDYBURG GORDON [US] ET AL) 11 January 2007 (2007-01-11) * abstract figures 1-6 paragraphs [0007], [0008] paragraph [0010] paragraphs [0018] - [0020] paragraphs [0022] - [0025] paragraphs [0028] - [0044] paragraph [0049] paragraph [0052] paragraph [0059]	1-9

-/--

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/058051

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 054 529 A (LUCENT TECHNOLOGIES INC [US]) 22 November 2000 (2000-11-22) * abstract figures 1,2,7-9 paragraph [0013] paragraph [0015] paragraphs [0021] - [0025] paragraph [0028] paragraph [0030] paragraphs [0039], [0040] paragraphs [0050], [0051]	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/058051

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008119930 A	09-10-2008	EP 2140610 A1	06-01-2010
		US 2010177650 A1	15-07-2010
US 2003088529 A1	08-05-2003	AU 2002363519 A1	19-05-2003
		EP 1449106 A1	25-08-2004
		JP 2005508596 T	31-03-2005
		WO 03040947 A1	15-05-2003
US 6502131 B1	31-12-2002	US 6578077 B1	10-06-2003
US 2007011317 A1	11-01-2007	NONE	
EP 1054529 A	22-11-2000	CA 2308696 A1	20-11-2000
		JP 2001044992 A	16-02-2001