



(51) International Patent Classification:
H04L 29/06 (2006.01)

(21) International Application Number:
PCT/EP2009/067829

(22) International Filing Date:
23 December 2009 (23.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08106030.3 23 December 2008 (23.12.2008) EP

(71) Applicant (for all designated States except US): **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HIETALA, Erkki Juhani** [FI/FI]; Haarakuja 5, FI-02320 Espoo (FI).

(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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

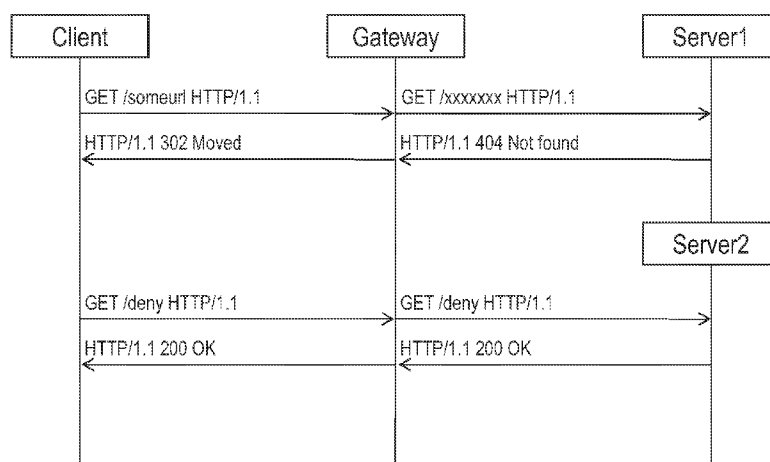
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, 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: METHOD AND DEVICE FOR PROCESSING DATA IN A NETWORK

Fig.1



(57) Abstract: A method and a device for processing data in a network are provided, said method comprising the steps of a gateway modifies a communication from a first network component to a second network component by indicating a reason for a service change and/or by indicating a change of the service. Furthermore, a communication system is suggested comprising said device.

DescriptionMethod and device for processing data in a network

5 The invention relates to a method and to a device for processing data in a network.

Deep Packet Inspection (DPI) is a form of computer network packet filtering that examines the data and/or header part of
10 a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. Deep Packet
15 Inspection (and filtering) enables advanced security functions as well as internet data mining, eavesdropping, and censorship.

A user surfing through the Internet may experience
20 unavailability of a particular service, site or network component, e.g. server, wherein the user is not aware of any reason as why the service requested is not available or denied. A reason may be a broken server or a server that has been moved to a different site or link.

25 The **problem** to be solved is to overcome the disadvantage stated before and in particular to provide an efficient approach to let a user experience a reason for a denial of a request.

30 This problem is solved according to the features of the independent claims. Further embodiments result from the depending claims.

35 In order to overcome this problem, a method for processing data in a network is provided comprising the step:

(a1) a gateway modifies a communication from a first network component to a second network component by

indicating a reason for a service change and/or by indicating a change of the service.

Hence, a user via a second network component (client device)
5 requesting a service from the first network component or from the network in general is informed about the reason as why the service is changed, in particular that the service is no longer reachable from this first network component. In addition, the client device (second network component) can be
10 informed about the change of the service, in particular it may obtain an information as how to access the service required from a different location.

Eventually, the client device (second network component) and
15 thus the user may be able to access the requested service from the network component that actually provides such service. The gateway may in particular forward information that can be used to access the correct network component.

20 The service requested may comprise any kind of service that can be provided by the network, in particular by a component or resource of a network, in particular of the Internet. Such service may be, e.g., an information, a site, a page, a program, a link (URL) or any other kind of content
25 information.

Advantageously, protocols of the first network component as well as of the second network component do not have to be amended or changed and the second network component (e.g.,
30 the client) may still become aware of a relocation of a service or content accessible, e.g., via a different server. This different server may be accessible by information provided by the gateway to the second network component (e.g., to the client).

35 According to an embodiment, the gateway performs deep packet inspection to determine whether or not modification of a communication, in particular redirection, is required.

Hence, the gateway may analyze IP packets by some sort of TCP flow tracking to determine whether or not an IP packet arriving at the gateway (from, e.g., a client) tries to access a service that matches a "denied rule". Such "denied rule" may be locally available at the gateway or it may be accessible to the gateway to find out whether a particular access service matches a denied criteria. In such case, the gateway could start dropping IP packets that fall under such "denied rule" or it may initiate redirection or it may initiate a reset of a TCP connection between the first network component and the second network component.

According to another embodiment, the gateway performs layer-4 processing, in particular without using TCP level processing. In particular, the packets are inspected on layer-4 and also the TCP level payload can be read to obtain the payload data on HTTP level (e.g., HTTP methods and headers).

Hence, no resource demanding layer-7 processing is required at the gateway. The suggested layer-4 processing can be conducted, e.g., by a kernel of the gateway, which leads to a much faster overall performance handling messages at the gateway.

According to just another embodiment, the gateway modifies the communication if a request from the second network component to the first network component is directed to a denied service.

Redirection may in particular be required in case a prepaid user runs out of memory and the access needs to be redirected to a self-service portal that allows the user to use a credit card. Redirection may also become necessary if access is not allowed to a specific URL (service) and the operator wants to inform the client as why the service is not allowed (wrong time or wrong profile). In addition, redirection may be necessary if the service is denied temporarily, e.g., for maintenance needs. In addition, the service may have been

moved to another server, which can be indicated to the client. Furthermore, a welcome page needed for the first service usage action can be provided by redirection means.

5

It is also an embodiment that the gateway initiates redirection and/or the gateway starts dropping data directed towards the first network component.

10 In an embodiment, the change of the service is indicated by conveying redirection information to access the service via a third network component.

Said redirection information may be a change of an address
15 (e.g., URL) that can be utilized by a client (e.g., the second network component) to access the required data or information via a different network component (another server than the server previously addressed).

20 In another embodiment, the first network component is a first server, the second network component is a client and the third network component is a second server.

Other than that, the first, second and third network
25 components can be any kind of components distributed throughout the network. Any of the network components may be a user's device or client or a server, e.g., operated by a service provider.

30 In a further embodiment, said communication from the first network component comprises a "Not found" message or an "OK message", optionally comprising the redirection information to access the service via said third network component.

35 In a next embodiment, the solution provided comprises the step:

(a2) the second network component accesses the third network component utilizing said redirection information.

5 Such access may be processed via said gateway. Hence, the client device may get access to the information required via said third network component (e.g., additional server).

It is also an embodiment that the network comprises the
10 Internet or is associated with the Internet.

Pursuant to another embodiment, said service comprises at least one of the following:

- 15 - a service provided by the network being addressable in the network;
- a site or a page of the network;
- a content of the network;
- an URL.

20 According to an embodiment, the solution provided comprises the following step prior to step (a1):

(a0) the gateway receives a request for the service from the second network component and changes this request into a message to be conveyed to the first
25 network component, pursuant to which the first network component provides a response without a message body.

Such a message to be conveyed to the first network component
30 may be a HEAD-message indicating that the first network component (server) must not return a message body in a response message. Only the HTTP headers are provided in such response and further conveyed to the second network component (the client), comprising e.g., a content-type, a content-
35 size, a date.

For example, the first network component may just return a "method not allowed" or a "200 OK" message.

The response from the first network component can be modified by the gateway, e.g., by providing a service or a service-relevant information.

- 5 According to another embodiment, the gateway receives a message without a message body from the first network component in return to the HEAD-message.

10 In yet another embodiment, the solution provided comprises the following step prior to step (a1):

- (a0) the gateway receives a request for the service from the second network component and changes this request into a GET-message, a PUT-message or a POST-message to be conveyed to the first network component.
- 15

According to a next embodiment, the gateway receives a "200 OK" message in return to the GET, PUT- or POST-message in particular indicating the change of the service within a message body.

20

The problem stated above is also solved by a device comprising a and/or being associated with a processor unit and/or a hard-wired circuit and/or a logic device that is arranged such that the method as described herein is executable thereon.

25

According to an embodiment, the device is a or is associated with a communication device, in particular a network component, a gateway, a server or a client device.

30

The problem stated supra is further solved by a communication system comprising the device as described herein.

35 Embodiments of the invention are shown and illustrated in the following figures:

Fig.1 shows an exemplary message sequence chart between a client, a gateway, a Server1 and a Server2, wherein a reason of a service change or a change of service, in particular a redirection information, is conveyed to the client device;

Fig.2 shows an alternative message sequence chart between a client, a gateway, a Server1 and a Server2, wherein a reason of a service change or a change of service, in particular a redirection information, is conveyed to the client device;

Fig.3 shows a message sequence chart based on Fig.1 in more detail.

The approach provided herein in particular enables an HTTP redirection transparently processed in an IP gateway that is analyzing the IP traffic, e.g., on layer-4 (L4).

For example, in case of a proxy mode deep packet inspection (DPI), TCP sessions are terminated in a gateway node so that a user space (on layer-7 (L7)) application in the gateway is able to process the HTTP requests and inspect the payload data. If the HTTP request is allowed to its final destination, the gateway will make the connection towards the destination server and it will send the original request to such destination server. If a response arrives from the server, the gateway sends the response to the client using the existing connection. In this kind of communication, if the access needs to be redirected, the gateway does not need to connect to the destination server at all. Instead, the gateway may immediately after having received the HTTP request from the client send the redirection response back to the client. However, such kind of direct processing bears the disadvantage of the proxy mode gateway requiring a lot of processing capacity, because the TCP session terminates at the gateway and it is processed by the gateway's user space application on L7 (i.e. L7 is required at such gateway).

Hence, a TCP handshake is being processed between the client and gateway and also between the gateway and the server. So each connection from the client is processed locally in the gateway user space, which results in heavy operation

5 (compared to mere L4 level processing).

For example, the network gateway being able to route IP packets in kernel level (L4) up to 1GBits/s may only process about 100MBit/s in user space (L7). TCP stream processing in
10 application space requires IP packet reassembly, handling of the TCP window, sequence number processing, retransmissions, etc., which results in a lot of processing capacity all done by said gateway.

15 The approach provided herein allows for a gateway to operate, e.g., in a kernel mode DPI on layer-4 (L4). Such kernel mode DPI gateway may advantageously investigate IP packets having some sort of TCP flow tracking (e.g., state full inspection). The purpose of this kind of flow tracking may comprise
20 denying service access that matches a so-called 'deny' rule. Hence, if the client connects to the HTTP service the TCP session is established between the client and the server (TCP handshake between the client and server). The DPI gateway located in the path between the client and the server may
25 inspect, route and forward the IP packets. If the HTTP request arriving at the gateway does have the service access to a denied service, the gateway will start dropping the IP packets or it will send the TCP reset to the client and to the server for terminating the TCP session.

30 Hence, the approach described herein allows making a redirection in the kernel space (L4 of the gateway) without using TCP level processing. By providing redirection as described herein, the DPI gateway does not have to break the
35 TCP connection between the server and client.

It is however noted, that prior to the client being able to send the request to the server via the gateway providing DPI

services, the connection may have to be established, e.g., via TCP handshake. Hence, when the client sends the packet containing an HTTP request in a TCP payload which does match the deny/redirect rule, the gateway performs DPI and is thus able to provide redirection as described herein. If TCP retransmission is required, the server will be able to handle it - the DPI gateway may only rewrite the data as described herein.

10 An example could be summarized as follows:

In case redirection is done, the format of the headers may be as follows:

15 The client sends:

```
GET /someurl HTTP/1.1
Host: www.server1.com
Accept: */*
Connection: keep-alive
```

20

The server responds with:

```
HTTP/1.1 302 Moved
Location: http://www.server2.com/deny
Content-length: 0
Connection: close
```

25

Based on the server's response, the client can launch a new request:

```
GET /deny HTTP/1.1
Host: www.server2.com
Accept: */*
Connection: keep-alive
```

30

Also, a response code 301 may be applicable for most web browsers. Accordingly, the following redirection response from the server may work in a similar manner:

35

```
HTTP/1.1 301 Moved
Location: http://www.server2.com/deny
```

Content-length: 0

Connection: close

Hence, the IP gateway may modify an HTTP URL received via an
5 IP packet to point to a nonexistent URL. The destination
server may return an HTTP response "404 Not found".

Such response is received at the IP gateway, which modifies
it into a "302 Moved" message. In addition, the IP gateway
10 modifies HTTP response headers to carry a 'Location' header
comprising the redirection URL. After such changes, the TCP
CRC is recalculated and the IP packet is sent to the HTTP
client.

15 Hence, the client is able to send a HTTP GET request to
another server utilizing the redirection URL conveyed by the
IP gateway.

Fig.1 shows an exemplary message sequence chart between a
20 client, a gateway, a Server1 and a Server2.

The messages exchanged can be describes as follows:

(1) A connection between the client and the Server1 is
25 established via the gateway. After a TCP three way
handshake, the client sends a HTTP request comprising in
particular

30 GET /someurl HTTP/1.1
Host: www.server1.com
Accept: */*
Connection: keep-alive

35 to the gateway. The gateway analyzes the incoming HTTP
request, e.g., utilizing DPI to find out whether or not
it matches the deny/redirect rule. In the affirmative,
the gateway performs DPI and is thus able to provide
redirection. If TCP retransmission is required, the

server will be able to handle it - the DPI gateway just needs to rewrite the data. The gateway changes the destination URL, e.g., such that an TCP packet sequence number is not changed and forwards a message

5

```
GET /xxxxxxx HTTP/1.1
Host: www.server1.com
Accept: */*
Connection: keep-alive
```

10

to the Server1.

- (2) Because the destination URL "/xxxxxxx" does not exist, the Server1 responds with a HTTP response

15

```
HTTP/1.1 404 Not found.
Content-length: 250
Connection: keep-alive
```

20

The response code from the Server1 may also comprise or be "302". Some HTTP services provide a missing service notification by redirecting the access to an own service from where the status can be retrieved.

25

The gateway modifies this response into

```
HTTP/1.1 302 Moved
Location: http://www.server2.com/deny
Content-length: 0
Connection: close
```

30

and replaces the HTTP headers to comprise a location information of a redirect URL ".../deny". For example, a information "http://www.server2.com/deny" could be provided to indicate that the content can be found via a redirection information "http://www.server2.com".

35

Such modified data packet is forwarded from the gateway to the client.

- (3) The client closes the existing TCP connection to the Server1 and establishes a new connection to the Server2. Furthermore, the client uses the redirect URL ".../deny" via a GET request

```
5      GET ".../deny" HTTP/1.1.  
10     Host: www.server2.com  
      Accept: */*  
      Connection: keep-alive
```

15 The gateway forwards this request directly to the Server2.

- (4) The Server2 responds with a message

```
20     HTTP/1.1 200 OK  
      Content-length: 500  
      Connection: keep-alive  
      <html><p>Your service is denied ...</html>
```

25 and conveys the data requested to the client via the gateway. Said gateway just forwards the data to the client.

It is noted that the ".../deny" expression can have different meaning. For example, a client may be configured to use a HTTP proxy, i.e. the client is connected via the gateway and further via said HTTP proxy to the Server2 (e.g., "www.server2.com"):

```
35     GET http://www.server2.com/deny HTTP/1.1.  
      Host: www.server2.com  
      Accept: */*  
      Connection: keep-alive
```

As an alternative, the client may not use such HTTP proxy, but have a direct connection to the destination (e.g., to Server2) via said gateway:

```
5      GET /deny HTTP/1.1.  
      Host: www.server2.com  
      Accept: */*  
      Connection: keep-alive
```

10 Both such formats may be adapted by changing the method line path accordingly. The location header may be the same for both, the direct mode and the proxy mode server redirection response (location according to the example:
http://www.server2.com/deny.

15

Fig.3 shows a message sequence chart based on Fig.1 in more detail. Hence, TCP message flags SYN, SYN ACK, ACK, FIN, FIN ACK are shown indicating synchronization (SYN), acknowledgement (ACK) and an end of a connection (FIN).

20

A first connection is established between the client and the Server1 and a second connection is established between the client and the Server2 after the redirection response 101 has been provided to the client.

25

Hence, the redirection can be provided, e.g., by the kernel of the gateway without using any TCP level processing. This enables redirection without the gateway having to break up the TCP connection between the Server1 and the client.

30

It is noted that before the client is able to send a request to the Server1 via said DPI gateway, the connection needs to be established, i.e. via TCP handshake, comprising SYN, SYN ACK and ACK messages.

35

When the client sends a packet containing the HTTP request in TCP payload, which does match the deny/redirect rule, the DPI gateway is able to do the redirection as described. If the

TCP retransmission is required due to such matching entry regarding said deny/redirect rule, the Server1 may handle it and the DPI gateway may just rewrite the data to be forwarded. Redirection status codes as indicated, e.g., 301 or 302, may both work for most web clients.

Alternative Embodiment

As an alternative, the approach provided herein enables HTTP redirection transparently in the IP gateway that is analyzing the IP traffic by modifying the accessed HTTP method "HEAD" instead of methods "GET", "PUT" or "POST" so that the destination server may return a HTTP response "200 OK" or any other valid HTTP response.

Such response, received by the IP gateway, is modified into a "302 Moved" message. In addition, the IP gateway also modifies the HTTP response headers to carry a 'Location' header having the redirection URL. After such changes, the TCP CRC is recalculated and the IP packet is sent to the HTTP client.

Hence, the client is able to send an HTTP GET request to another server utilizing the redirection URL conveyed by the IP gateway.

Fig.2 shows a different embodiment visualized by a message sequence chart comprising a client, a gateway, a Server1 and a Server2.

The messages exchanged can be describes as follows:

(1) A connection between the client and the Server1 is established via the gateway. After a TCP three way handshake, the client sends a HTTP request

```
GET /someurl HTTP/1.1
Host: www.server1.com
```

Accept: */*
Connection: keep-alive

to the gateway. The gateway analyzes the incoming HTTP
request and the gateway knows that the service accessed
would be denied and that redirection is needed. The
gateway changes the HTTP method to a "HEAD" message such
that a TCP packet sequence number is not changed and
forwards a message

HEAD /someurl HTTP/1.1
Host: www.server1.com
Accept: */*
Connection: keep-alive

to the Server1.

- (2) The HEAD message is similar to the GET message except
that the server's response does not provide a message-
body.

The server responds with HTTP response

HTTP/1.1 200 OK
Content-length: 0
Content-type: text/html
Server: Apache/1.3
Last-Modified: Sat, 29 Oct 2007 19:43:31 GMT
Connection: keep-alive

The gateway modifies this response into

HTTP/1.1 302 Moved
Location: http://www.server2.com/deny
Content-length: 0
Connection: close

and replaces the HTTP headers to comprise a location information of a redirect URL ".../deny". Such modified data packet is forwarded from the gateway to the client.

- 5 (3) The client closes the existing TCP connection to the Server1 and establishes a new connection to the Server2. Furthermore, the client uses the redirect URL ".../deny" via a GET request

10 GET ".../deny" HTTP/1.1
 Host: www.server2.com
 Accept: */*
 Connection: keep-alive

- 15 The gateway forwards this request directly to the Server2.

- (4) The Server2 responds with a message

20 HTTP/1.1 200 OK
 Content-length: 500
 Connection: keep-alive
 <html><p>Your service is denied ...</html>

- 25 and conveys the data requested to the client via the gateway. Said gateway just forwards the data to the client.

- 30 It is noted that the ".../deny" expression can have different meaning as explained with regard to the example above. Hence, a client may be configured to use a HTTP proxy or it may utilize a direct connection.

35 Further Advantages:

Hence, pursuant to the approach provided herein, TCP level packet retransmission is handled by the client and by the

server, wherein the gateway does not have to modify any TCP sequence and/or acknowledge numbers. In particular, the gateway does not have to buffer IP packets which have not yet been acknowledged either by the client or by the server.

5

Usually the "404 Not found" response provided by the Server1 may not comprise any payload data to be sent to the client. However, the space in the IP packet that could otherwise be used for payload data could be utilized by conveying a
10 redirection URL, in particular with additional data.

Also, HTTP servers and/or clients may send other HTTP headers 'Server' and 'Content-Type' which can be replaced to contain a redirection header with additional data. If IP packet
15 retransmission occurs, the gateway needs only to rewrite the IP packet as it has done previously. The TCP/IP session information and/or termination are handled by the original client and by the server. The IP gateway may in particular only forward the TCP/IP signaling packets.

20

This is of advantage as this approach does not require the IP gateway to terminate all HTTP sessions transparently within its own TCP/IP stack or a partial implementation thereof.

25

Claims:

1. A method for processing data in a network, comprising the step:
 - 5 (a1) a gateway modifies a communication from a first network component (Server1) to a second network component (Client) by indicating a reason for a service change and/or by indicating a change of the service.
- 10 2. The method according to claim 1, wherein the gateway performs deep packet inspection to determine whether or not modification of a communication, in particular redirection, is required.
- 15 3. The method according to claim 2, wherein the gateway performs layer-4 processing, in particular without using TCP level processing.
- 20 4. The method according to any of claims 1 to 3, wherein the gateway modifies the communication if a request from the second network component to the first network component is directed to a denied service.
- 25 5. The method according to claim 4, wherein the gateway initiates redirection and/or the gateway starts dropping data directed towards the first network component (Server1).
- 30 6. The method according to any of the preceding claims, wherein the change of the service is indicated by conveying redirection information to access the service via a third network component (Server2).
- 35 7. The method according to claim 6, wherein the first network component (Server1) is a first server, the second network component (Client) is a client and the third network component is a second server (Server2).

8. The method according to any of claims 6 or 7, wherein said communication from the first network component comprises a "Not found" message or an "OK message",
5 optionally comprising the redirection information to access the service via said third network component.
9. The method according to any of the preceding claims, comprising the step:
10 (a2) the second network component (Client) accesses the third network component (Server2) utilizing said redirection information.
10. The method according to any of the preceding claims,
15 wherein the network comprises the Internet or is associated with the Internet.
11. The method according to any of the preceding claims, wherein said service comprises at least one of the
20 following:
- a service provided by the network being addressable in the network;
- a site or a page of the network;
- a content of the network;
25 - an URL.
12. The method according to any of the preceding claims, comprising prior to step (a1) the step:
(a0) the gateway receives a request for the service from
30 the second network component (Client) and changes this request into a message to be conveyed to the first network component (Server1), pursuant to which the first network component (Server1) provides a response without a message body.
35
13. The method according to claim 12, wherein the gateway receives a message without a message body from the first

network component (Server1) in return to the HEAD-message.

14. The method according to any of claims 1 to 11,
5 comprising prior to step (a1) the step:

(a0) the gateway receives a request for the service from
the second network component (Client) and changes
this request into a GET-message, a PUT-message or a
POST-message to be conveyed to the first network
10 component (Server1).

15. The method according to claim 14, wherein the gateway
receives a "200 OK" message in return to the GET-, PUT-
or POST-message from the first network component
15 (Server1) in particular indicating the change of the
service within a message body.

16. A device comprising a and/or being associated with a
processor unit and/or a hard-wired circuit and/or a
20 logic device that is arranged such that the method
according to any of the preceding claims is executable
thereon.

17. The device according to claim 16, wherein said device is
25 or is associated with a network component, in particular
a gateway, a server of a client device.

18. Communication system comprising the device according to
any of claims 16 or 17.

Fig.1

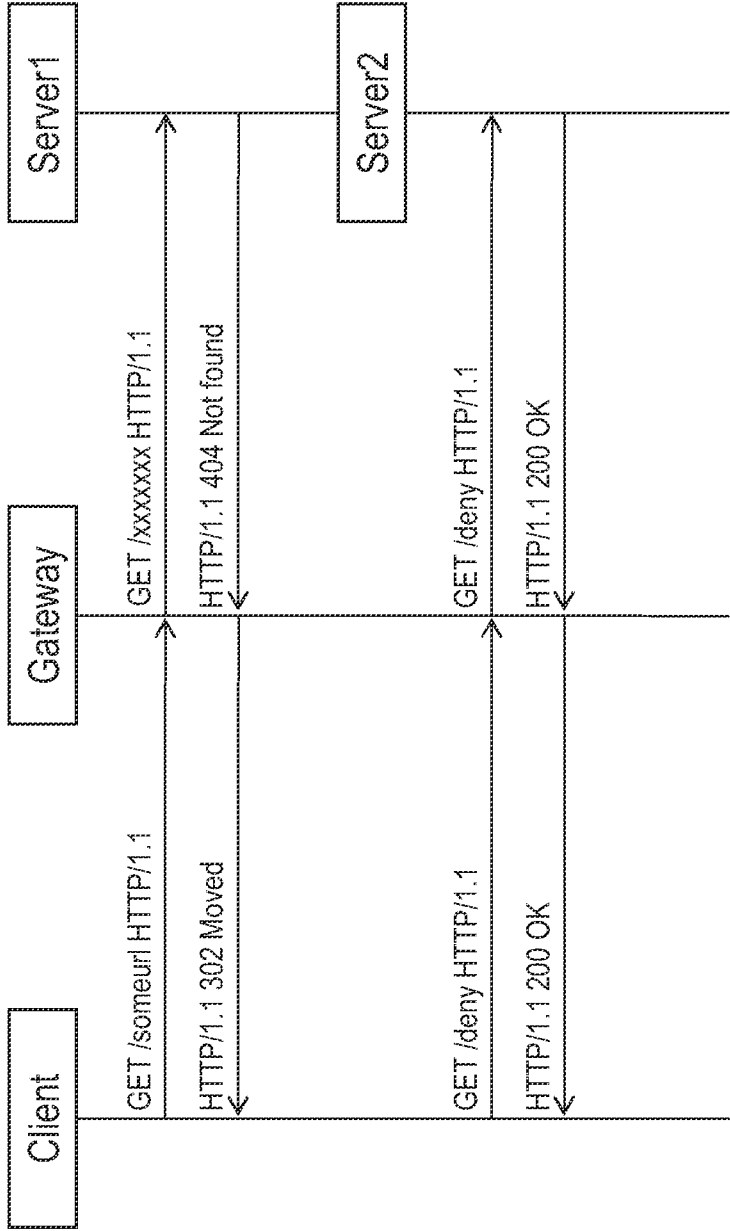


Fig.2

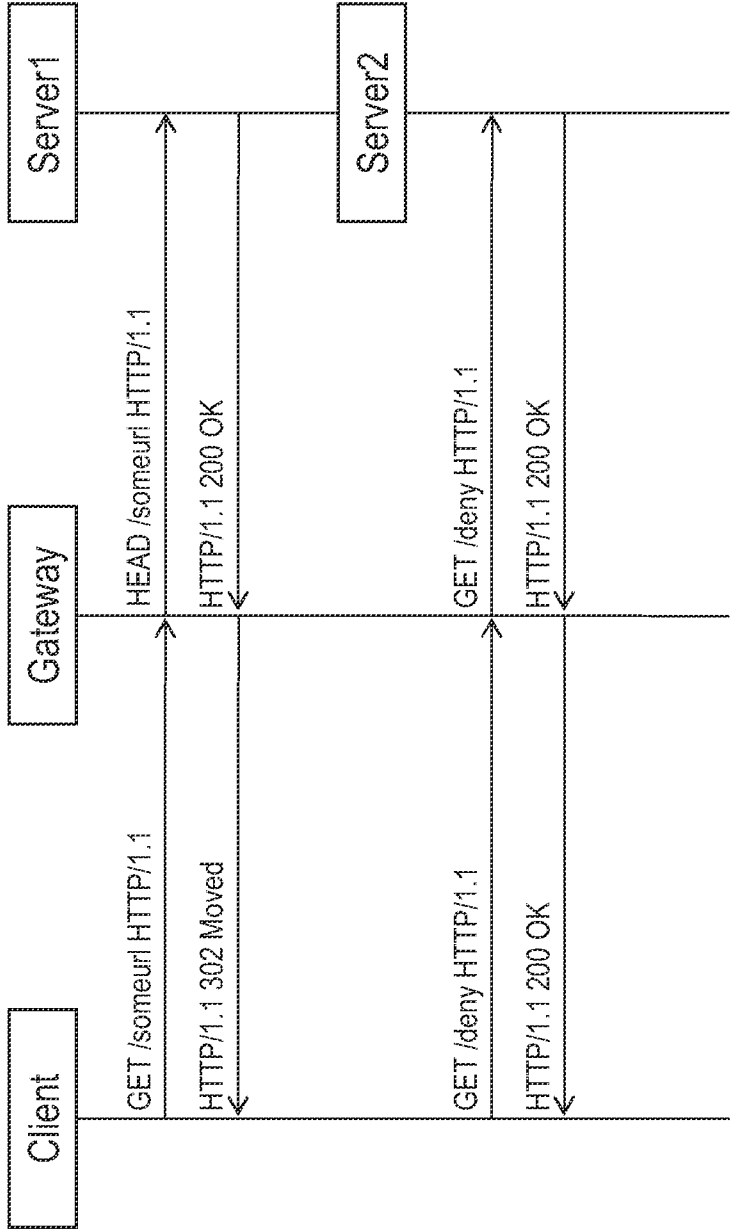
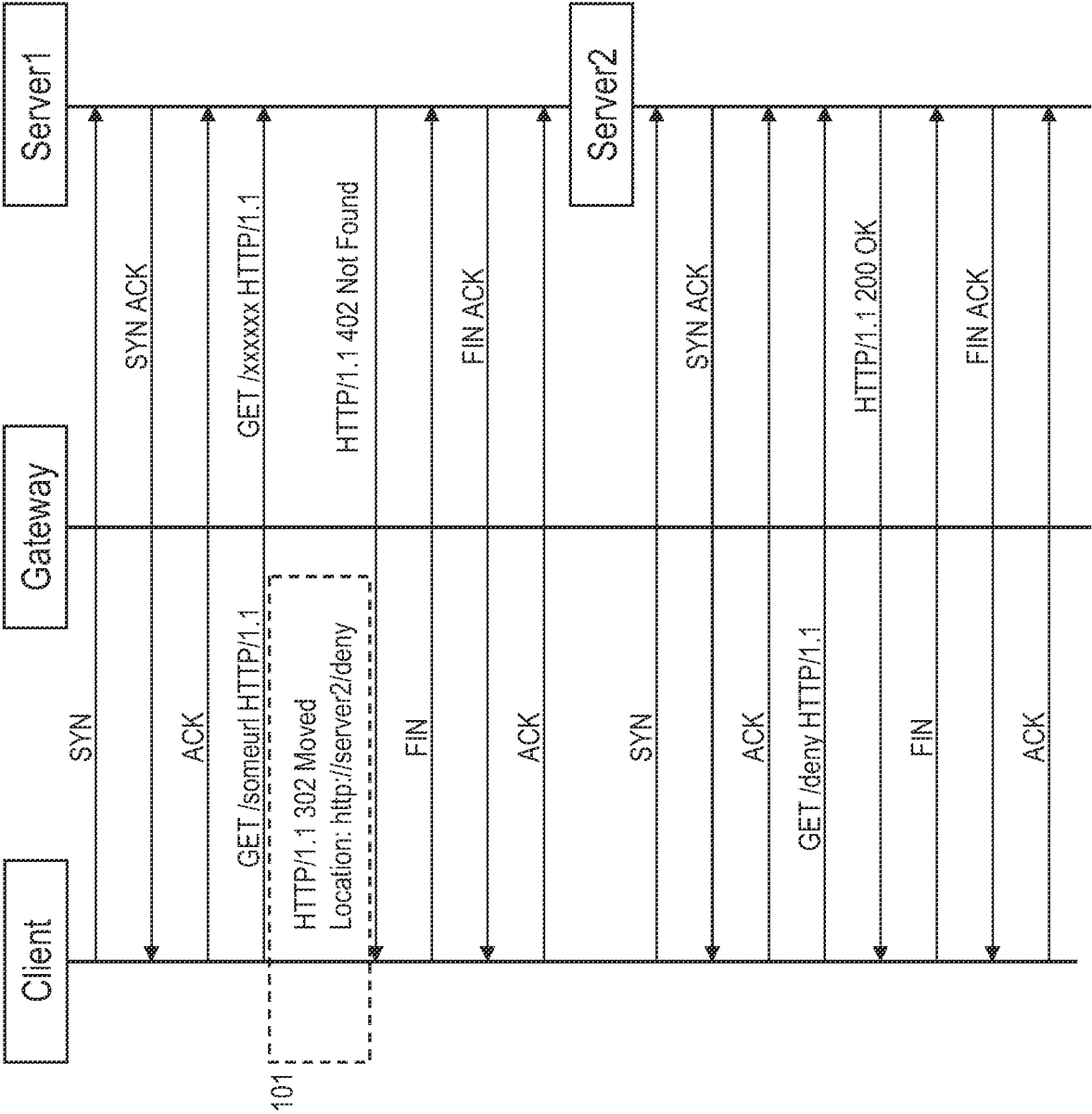


Fig.3



INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/067829

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 1 161 049 A (KAUFMANN OLIVER [DE]) 5 December 2001 (2001-12-05) paragraphs [0018] - [0023] paragraphs [0034] - [0037] paragraph [0043] -----	1-11, 14-18 12-13
X A	US 2008/306815 A1 (DYKES ROBERT ROSCOE [US] ET AL) 11 December 2008 (2008-12-11) paragraph [0020] paragraphs [0056] - [0063] paragraph [0072] paragraphs [0080] - [0082] paragraphs [0086] - [0090] ----- -/--	1-4, 10-11, 16-18 5-9, 12-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

& document member of the same patent family

Date of the actual completion of the international search

29 March 2010

Date of mailing of the international search report

07/04/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/067829

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2006/112174 A1 (L HEUREUX ISRAEL [US] ET AL) 25 May 2006 (2006-05-25) paragraphs [0046] - [0060] paragraphs [0068] - [0074] paragraph [0084] paragraph [0087] paragraphs [0110] - [0117] -----	1,6-11, 14-18 2-5, 12-13
X A	EP 1 755 314 A (THIRD BRIGADE INC [CA]) 21 February 2007 (2007-02-21) paragraphs [0014] - [0021] paragraphs [0027], [0028] page 6, lines 26-29 -----	1-3, 10-11, 16-18 4-9, 12-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/067829

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 1161049	A	05-12-2001	AT 211595 T	15-01-2002
			DE 69803369 D1	28-02-2002
			DE 69803369 T2	29-08-2002
			DK 0975128 T3	22-04-2002
			EP 0975128 A1	26-01-2000
			ES 2170985 T3	16-08-2002
			PT 975128 E	28-06-2002
			US 6453335 B1	17-09-2002
US 2008306815	A1	11-12-2008	AU 2008200565 A1	08-01-2009
			CA 2622187 A1	06-12-2008
			CN 101320369 A	10-12-2008
			EP 2015245 A1	14-01-2009
			JP 2008305381 A	18-12-2008
			KR 20080107248 A	10-12-2008
US 2006112174	A1	25-05-2006	US 2009327827 A1	31-12-2009
EP 1755314	A	21-02-2007	CA 2514039 A1	28-01-2007
			US 2007025374 A1	01-02-2007