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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2004 (29.01.2004)

PCT

(10) International Publication Number
WO 2004/010659 A1

(51) International Patent Classification[7]: H04L 12/56, 29/06, H04Q 7/22

(21) International Application Number: PCT/FI2003/000577

(22) International Filing Date: 22 July 2003 (22.07.2003)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
20021407 24 July 2002 (24.07.2002) FI

(71) Applicant *(for all designated States except US)*: **TYCHO TECHNOLOGIES OY** [FI/FI]; P.O. Box 661, FIN-00101 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PIPONIUS, Toni** [FI/FI]; c/o Tycho Technologies Oy, P.O. Box 661, FIN-00101 Helsinki (FI).

(74) Agent: **PAPULA OY**; P.O. Box 981, FIN-00101 Helsinki (FI).

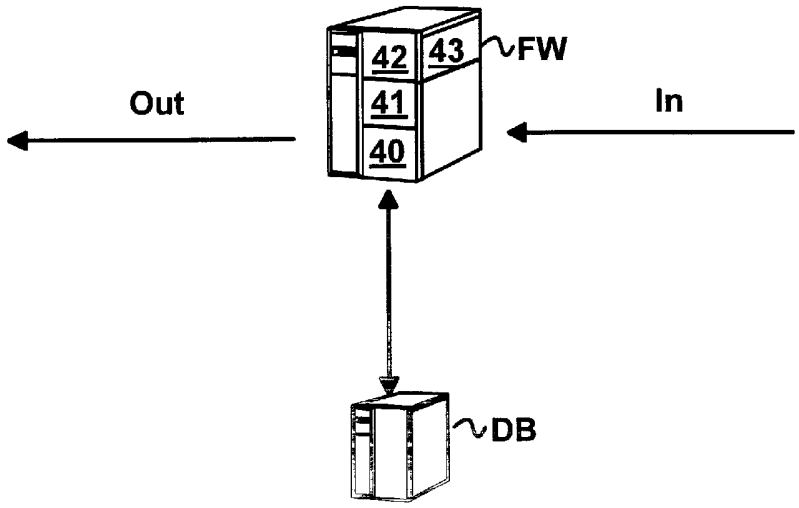
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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.

(54) **Title:** METHOD AND SYSTEM FOR FILTERING PACKETS BASED ON SOURCE- AND DESTINATION ADDRESSES



(57) **Abstract:** The invention relates to filtering of telecommunication in the network, in which the devices connected to the network have device-specific filtering rules. A firewall component (FW) is arranged in the telecommunication network in such a manner that all the telecommunication goes through the firewall component (FW). The firewall component (FW) is connected to a database server (DB), to which the filtering rules are saved. It is possible to connect several firewall components (FW) to the same database. The firewall component (FW) retrieves from the database (DE) the sender's and the recipient's filtering rules based on unique identification information. In addition, from the database (DE) it is possible to retrieve the filtering rules of the service provider or additional filtering rules, e.g. group-specific rules. Each rule is handled separately, and in case the telecommunication is in accordance with all the rules, it is transmitted further.

WO 2004/010659 A1

METHOD AND SYSTEM FOR FILTERING PACKETS BASED ON SOURCE- AND DESTINATION ADDRESSES

FIELD OF THE INVENTION

The invention relates to telecommunication technique. In particular, the invention relates to a method and system for filtering telecommunication in a telecommunication network.

BACKGROUND OF THE INVENTION

As the amount of telecommunication explosively increases, the filtering of non-desired telecommunication has become a necessity. In conventional telecommunication networks, telecommunication is filtered by means of firewalls and blocking lists of routers. A firewall can be implemented either purely as a software application or as a hardware specifically designed for filtering.

Typically, a firewall is used to filter incoming traffic, but the filtering of outgoing traffic is also possible. This is advantageous e.g. in situations in which one wishes to make sure that it is not possible to transfer information e.g. by means of back gate programs. The firewall is arranged in the network to be protected in such a manner that all the traffic going from the network into the outside world goes through the same firewall. In case there are other possible routes to the network, they must be protected with corresponding firewalls because the level of protection of the network is determined based on the weakest link.

Telecommunication can be filtered based on various principles. Typically, the filtering regards, however, the filtering of certain protocols and addresses. In most cases, the firewall is configured such that it is possible to connect to the network only to certain server devices, and the rest of the network is invisible to the outside world. The access may also be determined in such a manner that some de-

vices can be connected only from determined addresses. With the present systems, various different variations are possible.

The actual filtering is based on rules. The maintainer of the firewall system creates a number of rules which are gone through in a certain order. In the rules it is e.g. possible to describe to what addresses the traffic is allowed or from what addresses the traffic is automatically rejected. The set of rules applies to the whole network, and making exceptions is possible by adding new rules. To clarify the set of rules, the rules may consist of sub rules. For example, each allowed address need not have to have its own rule, instead in the set of rules, one rule is created to which a set of sub rules or addresses are saved from which the incoming traffic is allowed.

The problem with the prior-art list of rules is their big size. In case there are thousands of devices included in the network to be protected, the list of rules may grow remarkably big. The firewall must, however, check the whole list for each incoming packet. If the packet is rejected, it is possible to stop going through the list as the rejecting rule is realized. Correspondingly, as concerns the allowed traffic, the list is gone through up to the accepting rule. This adds to the power requirements of the firewall and adds to the risk of error.

A conventional firewall is not suitable for filtering wireless terminal devices, since the firewall is arranged in between the company intranet and the public network. When using a wireless terminal device the user first connects to the public network and proceeds via it to the protected network of the company behind the firewall. In that case, the wireless terminal device is left without the protection of the firewall, so that it must have a firewall application of its own. However, firewalls of this kind are

quite heavy applications, especially for wireless terminal devices. A prior-art solution is to place another firewall in the premises of the provider of the wireless data transfer service, but this makes it difficult to answer to the individual needs of the client, especially in situations in which the clients wish to change the settings of their firewalls frequently.

Reference publication WO 02/23831 discloses a system in which there is a specific access node arranged in the wireless telecommunication network. In the case of a GPRS (General Packet Radio Service) network, the access node is preferably placed in the GGSN component (Gateway GPRS Support Node). In the system according to the reference publication, the filtering is started based on a separate filtering request. The filtering request is transmitted to the access node each time serving. In case there is no request for filtering, the client's terminal device is left without protection. The changes and the filtering request are made by means of a separate program arranged in the terminal device, so there must be capacity in the terminal device for running the program.

Also addresses to be dynamically allocated create a problem for a conventional firewall in the wireless environment. In the network of the company's own, the addresses to be dynamically allocated are allocated from a certain space. In case the connection to the public network is to be made from outside the company information network, the address may be any as such. In that case, the rules of the firewall must be changed in real time.

OBJECTIVE OF THE INVENTION

The objective of the invention is to eliminate the disadvantages referred to above, or at least

significantly to alleviate them. One specific objective of the invention is to disclose a new type of filtering method and system of telecommunication specifically for filtering the telecommunication of mobile devices.

SUMMARY OF THE INVENTION

The present invention relates to a new type of firewall solution that is particularly advantageous when using wireless terminal devices that move within the public network. The addresses of the terminal devices can be allocated dynamically, and they need not be allocated from a protected network or from an otherwise restricted address space.

The system according to the invention includes at least two terminal devices, a firewall component and a telecommunication system. The telecommunication system may be e.g. a conventional mobile communication network in which the data traffic is transmitted by means of packet switching. The telecommunication may also be transmitted to another public network, such as the Internet.

In the system according to the invention, the firewall is placed in the telecommunication system such that all the traffic goes through the firewall. Advantageously, the firewall is arranged to retrieve the rules from a database which is common to all the firewall components of the telecommunication network. Since the terminal devices may be disposed in the same cell, the firewall component must be arranged such that also the internal traffic of the cell gets filtered. Typically, in a telecommunication network, the telecommunication goes through the component that is aware of the location of the terminal device. The firewall component of the invention is advantageous to arrange in conjunction with the component that is

aware of the location of the terminal device. In case the terminal devices are located in the same cell, the telecommunication can be filtered directly without directing the traffic to a separate firewall component.

In the system according to the invention, the telecommunication is filtered step by step for each terminal device specifically. Arranged in the firewall component, for each terminal device specifically, is a collection of rules which the client can freely modify. When a packet is sent from the client's terminal device, the firewall component first checks the firewall settings of the terminal's own. In case the transmission of the packet in question is not allowed, the packet is immediately rejected. In case the packet is allowed, it is forwarded further. In the next phase it is advantageous to filter the telecommunication using the rules of the service provider. These rules are used to check whether it is at all possible to transmit the transferred telecommunication. This phase is not obligatory. In case the telecommunication is in accordance with the rules of the service provider, the collection of rules of the recipient is loaded. In case the rules of the recipient allow the reception of the telecommunication, the packets are transmitted to their destination. The order of the filtering rules is not important from the point of view of the application, instead they may be arranged as desired.

The present invention improves the information security of terminal devices. The invention is particularly advantageous because by means of the system according to the invention the client can customize his or her own firewall application without changing the terminal device or acquiring a separate firewall application in his or her terminal device. As concerns the telecommunication network, the invention is advantageous because by means of it is possible to eliminate unnecessary telecommunication. By means of

the system according to the invention it is possible to check the authenticity and permissibility of the packets in time. This arrangement allows one to save band for allowed useful traffic. Furthermore, the system according to the invention is advantageous for controlling a big number of devices. The filtering rules allocated for each terminal device specifically can be retrieved from the database by means of a unique identifier of the terminal device. If as the identifier, e.g. the IMSI number of the terminal device is used, then the terminal's telecommunication address, typically the IP address, need not be fixed but can be dynamically allocated from anywhere from the address space.

LIST OF FIGURES

In the following, the invention will be described in detail by means of its embodiments, in which

Fig. 1 shows one embodiment of the firewall system according to the invention, and

Fig. 2 shows the system as shown in Fig. 2 in more detail, and

Fig. 3 shows a functional block diagram of the system according to Fig. 1, and

Fig. 4 shows a firewall component according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The system as shown in Fig. 1 comprises two telecommunication networks 12 and 13 independent of each other. Connected to the telecommunication network 12 are terminal devices MTE and DTE1. Connected to the telecommunication network 13 is a terminal device DTE2. The present invention does not limit the number

of terminal devices connected to the telecommunication networks, instead there may be several of them within the telecommunication network's own restrictions. The networks are connected to each other by means of a firewall component FW, which filters the traffic between the networks. The telecommunication in Fig. 1 is illustrated by means of two connections. Connection 11 represents the internal traffic of the telecommunication network 12, and connection 10 represents the traffic between the telecommunication networks.

The telecommunication connection 10 represents a typical connection from a mobile terminal device DTE1 to a server or to the second terminal device DTE2. The mobile terminal device may be connected to the information network e.g. by means of a mobile station or a wireless local area network. In Fig. 1, the terminal device DTE1 utilising the telecommunication connection 10 establishes a connection via the first telecommunication network 12. Since the traffic is directed to the second telecommunication network 13, it is directed through the firewall component FW. The firewall component FW filters based on predetermined rules. The filtered message is forwarded to the destination DTE2.

The telecommunication connection 11 represents a connection in which the mobile terminal devices communicate directly with each other. In the telecommunication connection 11 both of the terminal devices MTE and DTE1 communicate with each other via the telecommunication network 12. Since the terminal devices are located in the area of the same network, a firewall arranged at the point of interconnection traffic of two telecommunication networks does not protect the connections. Due to this, the telecommunication connection 11 must be circulated via the firewall component FW.

Fig. 2 shows the system of Fig. 1 in more detail. In the example of Fig. 2, the first telecommunication network is a mobile communication network provided with the GPRS facility (General Packet Radio Service) that includes base stations BTS1 and BTS2 (Base Transceiver Station). Connected to the base station BTS1 is one terminal device TE1, and connected to the base station BTS2 are the terminal devices TE2 and TE3. The present invention does not restrict the number of base stations or the number of terminal devices connected to them. In the system as shown in the figure, the cell-specific components of the base station BTS1 include base station controller BSC1, serving GPRS support node SGSN1 and gateway GPRS support node GGSN1. The corresponding components of the base station BTS2 are BSC2, SGSN2 and GGSN2. A GPRS core network 20 is arranged in between the service nodes and gateway nodes. In Fig. 2 also the firewall component of the telecommunication system is arranged for each cell specifically. The firewall components FW1 and FW2 are components of the first telecommunication system, and they are connected to the common database of rules DB. The embodiment according to the invention uses advantageously the database of rules, but if necessary, the rules may also be downloaded from the terminal device as the terminal device connects to the network. The firewall components are connected to the second telecommunication network 21, which may be e.g. the Internet. The terminal device TE4 of Fig. 2 is located in the local area network separated from the internet by means of a firewall FW3. The firewall FW3 is typically a conventional firewall solution, but if necessary, also it can be connected to the database of rules DB.

In Fig. 2, substantial from the point of view of the invention is the placing of the firewall component. The GPRS traffic is routed such that the trans-

mitted and received packets always go through the gateway GGSN. In case the terminal devices are located in the area of the same cell, such as TE2 and TE3, the gateway directly routes the traffic back to where it came from. Since the firewall component must be arranged in the telecommunication network such that all the packets go through the firewall, the firewall cannot be placed behind the gateway GGSN. If the firewall is placed behind the gateway, then all the packets must be routed also to the firewall. In Fig. 2, the firewall components FW1 and FW2 have been depicted as being located in front of the gateways GGSN1 and GGSN2. In the most preferred implementation mode, the firewall component is arranged in conjunction with the gateway. In that case, all the packets go through the firewall component.

Fig. 3 illustrates the operation of one embodiment of the filtering system according to the invention. The operation of the embodiment starts with the receiving of a packet, step 31. When the address has been received, it is checked whether the address belongs to a wireless terminal device, step 32. In case the terminal device is wireless, the identifier corresponding to the address is retrieved, step 33. As the identifier of the address, e.g. the IMSI code of the mobile station or some other corresponding unique identifier saved to the SIM card can be used. The relationship between the address and the identifier can be saved to a cache memory for a prescribed time. The information can be saved e.g. when the user logs into the network or out of the network. The piece of identification information corresponding to the piece of address information can be retrieved from an external database or from a network component. In the case of a GPRS system, the external network component is a GGSN. It must be noted that when necessary, by means of the piece of identification information it is also possi-

ble to retrieve the necessary IP address when retrieving or handling the rules, since the relationship between the address and the identifier is two-way. When the terminal device has been identified, the filtering rules of the transmitting terminal device are retrieved, step 34. Since the filtering rules are retrieved based on the user's identifier, the IP address of the terminal device need not be fixed. In case the terminal device has no separate address, default rules can be used, or the traffic can be transmitted without filtering. The firewall component interprets the filtering rules and checks whether the packet is in accordance with the rules, step 35. In case the packet is against the rules, it is rejected, step 36.

If the packet is in accordance with the rules of the sender, the default rules of the service are retrieved, step 37. Using these rules the service provider can determine what services can be used in the network. Additional services can be activated with an additional charge, in which case the user's information has an effect on the service rules to be loaded. The client can also order an unlimited service in which no service rules are loaded. When the rules have been loaded, it is checked whether the packet is in accordance with the service rules, step 38. In case the packet is against the rules, it is rejected, step 39.

As the last filtering step, the packet is filtered based on the destination address. If the service rules are fulfilled, the destination address of the packet is retrieved, step 310. When the address has been received, it is checked whether the address belongs to a wireless terminal device, step 311. In case the terminal device is wireless, the identifier corresponding to the address is retrieved, step 312. When the terminal device has been identified, the filtering rules of the transmitting terminal device are

retrieved, step 313. The firewall component interprets the filtering rules and checks whether the packet is in accordance with the rules, step 314. In case the packet is against the rules, it is rejected, step 315. In case the packet is allowed, it is transmitted to the recipient, step 316.

It must be noted that the firewall application according to the invention can also be configured in some other manner. The telecommunication can be filtered in a firewall also in such a manner that the firewall application first retrieves all the rules and then interpreters them all in a row. The filtering described above can be arranged to be assigned to the first firewall, but the task can also be divided between the firewall of both the transmitting and receiving cell. By means of a divided filtering the firewall also functions in situations in which the clients are located in the networks of different operators and the operators do not have a common database of rules.

It is possible to increase the number of filtering rules and levels of filtering, if necessary. In that case, the traffic can be first filtered e.g. based on the unique rules of the sender and then based on the group-specific rules of the sender. In case both rules are fulfilled, one proceeds to the rules of the service provider. Correspondingly, the rules of the recipient can be divided into unique ones and group-specific ones.

In the system according to the invention, each user has got his or her own rules, which are divided into incoming and outgoing traffic. The users can freely modify these rules. In the database, the rules are indexed based on the user's address information or the address identifier. In this manner, the client's rules can be easily managed and quickly re-

trieved. The system according to the invention enables one to arrange unique rules for a big number of users.

Fig. 4 shows the firewall component FW according to the invention. The firewall component FW receives incoming traffic IN. In order to filter the telecommunication, the firewall is provided with means 40 for filtering the telecommunication based on the sender's filtering rules and means 41 for filtering the telecommunication based on the recipient's filtering rules. Further, the firewall FW is provided with means 42 for filtering the telecommunication based on the service provider's rules. Each filtering rule is handled separately. The number of filtering means can be added, if necessary. Additional rules of this kind can include e.g. group-specific rules. The rules can be saved to the firewall FW, or they can be retrieved from a separate database server DB. Since the filtering rules are handled based on the piece of unique identification information of the terminal device, the firewall can further comprise means 43 for establishing a connection between the address of the public network of the user, e.g. a dynamic IP address, and the unique identifier of the terminal device, e.g. an IMSI code.

The invention is not limited merely to the examples of its embodiments referred to above, instead many variations are possible within the scope of the inventive idea defined in the claims.

CLAIMS

1. A method for filtering packet-switched telecommunication between two terminal devices, in which there is a filtering component arranged in between the terminal devices, the method comprising the following steps:

receiving, by means of the filtering component, telecommunication from the transmitting terminal device; and

filtering the telecommunication based on the filtering rules; and

transmitting the telecommunication allowed by the rules to the receiving terminal device,

characterised in that the method further comprises the steps:

establishing a connection between the address of the public network of the user and the unique identifier of the terminal device, which unique identifier of the terminal device is a fixed feature of the terminal device, a feature of the subscription to be used in the terminal device, an identifier input by the user, or the like;

filtering the telecommunication in accordance with the filtering rules of the transmitting terminal device based on the unique identifier of the transmitting terminal device; and

filtering the telecommunication in accordance with the rules of the receiving terminal device based on the unique identifier of the receiving terminal device

2. The method according to claim 1, characterised in that the telecommunication is filtered in accordance with the rules of the service provider.

3. The method according to claim 1 or 2, characterised in that the filtering rules are group-specific.

4. The method according to claim 1, 2 or 3, characterised in that the source and destination addresses are retrieved from the packet to be filtered.

5. The method according to any one of the preceding claims 1-4, characterised in that the filtering rules are retrieved from a separate database based on the unique identifier of the user's terminal device.

6. The method according to any one of the preceding claims 1-5, characterised in that the address of the public network of the user is an IP address.

7. The method according to any one of the preceding claims 1-6, characterised in that the user's unique terminal device-specific identifier is an IMSI code.

8. The method according to any one of the preceding claims 1-8, characterised in that the traffic is filtered based on one or more additional filtering rules.

9. The method according to claim 8, characterised in that the additional filtering rule is a group-specific filtering rule of the sender.

10. The method according to claim 8, characterised in that the additional filtering rule is a group-specific filtering rule of the recipient.

11. The method according to any one of the preceding claims 1-10, characterised in that the rules of both the sender and the recipient are handled independently as groups of their own.

12. The method according to any one of the preceding claims 1-11, characterised in that the possible additional filtering rules and filtering rules of the service provider are handled independently as groups of their own.

13. The method according to any one of the preceding claims 1-12, c h a r a c t e r i s e d in that the telecommunication is filtered based on the most limiting filtering rules.

14. A firewall (FW) for filtering telecommunication, the firewall (FW) comprising:

means for filtering telecommunication;

means for filtering telecommunication based on filtering rules; and

means for transmitting allowed traffic further;

c h a r a c t e r i s e d in that the firewall further comprises:

means (43) for establishing a connection between the public address of the user and the unique identifier of the terminal device, the unique identifier of the terminal device being a fixed feature of the terminal device, a feature of the subscription being used in the terminal device, an identifier input by the user, or the like;

means (40) for filtering telecommunication in accordance with the sender's filtering rules based on the unique identifier of the sender's terminal device; and

means (41) for filtering telecommunication in accordance with the recipient's filtering rules based on the recipient's unique identifier.

15. The firewall (FW) according to claim 14, c h a r a c t e r i s e d in that the firewall further comprises means (42) for filtering the telecommunication based on service-specific filtering rules.

16. The firewall (FW) according to claim 14 or 15, c h a r a c t e r i s e d in that the firewall (FW) is arranged to retrieve the source and destination addresses from the packet to be filtered.

17. The firewall (FW) according to the any one of the preceding claims 14-16, c h a r a c t e r -

i s e d in that the firewall is arranged to retrieve the filtering rules from a separate database (DB) based on the unique identification information of the terminal devices.

18. The firewall (FW) according to any one of the preceding claims 14-17, c h a r a c t e r i s e d in that the firewall is arranged to handle the filtering rules of both the sender and the recipient independently as groups of their own.

19. The firewall (FW) according to any one of the preceding claims 14-18, c h a r a c t e r i s e d in that the address of the public network of the user is an IP address.

20. The firewall (FW) according to any one of the preceding claims 14-19, c h a r a c t e r i s e d in that the unique identifier of the user's terminal device is an IMSI code.

21. The firewall (FW) according to any one of the preceding claims 14-20, c h a r a c t e r i s e d in that the firewall is arranged to filter the telecommunication based on additional filtering rules.

22. The firewall (FW) according to any one of the preceding claims 14-21, c h a r a c t e r i s e d in that the additional filtering rule is a group-specific rule of the user.

23. The firewall (FW) according to any one of the preceding claims 14–22, c h a r a c t e r i s e d in that the firewall is arranged to handle the service-specific filtering rules and additional filtering rules independently as groups of their own.

24. The firewall (FW) according to any one of the preceding claims 14–23, c h a r a c t e r i s e d in that the firewall is arranged to filter the telecommunication based on the most limiting filtering rules.

25. A system for filtering telecommunication, the system comprising at least:

a transmitting terminal device (DTE1), and

a firewall device (FW);

a receiving terminal device (DTE2); and

a telecommunication network for connecting the aforementioned devices;

characterised in that the firewall further comprises:

means (43) for establishing a connection between the user's public address and the unique identifier of the terminal device, the unique identifier of the terminal device being a fixed feature of the terminal device, a feature of the subscription being used in the terminal device, an identifier input by the user, or the like;

means (40) for filtering telecommunication in accordance with the sender's filtering rules; and

means (41) for filtering telecommunication in accordance with the recipient's filtering rules.

26. The system according to claim 25, characterised in that the firewall (FW) further comprises means (42) for filtering the telecommunication based on service-specific filtering rules.

27. The system according to claim 25 or 26, characterised in that the firewall (FW) is arranged to retrieve the filtering rules from a separate database (DB) based on the unique identification information of the terminal devices.

28. The system according to claim 25, 26 or 27, characterised in that the firewall (FW) is arranged to retrieve the source and destination addresses from the packet to be filtered.

29. The system according to any one of the preceding claims 25–28, characterised in that the firewall (FW) is arranged to handle the filtering rules of both the sender and the recipient independently as groups of their own.

30. The system according to any one of the preceding claims 25–29, characterised in that the address of the public network of the user is an IP address.

31. The system according to any one of the preceding claims 25–30, characterised in that the unique identifier of the user's terminal device is an IMSI code.

32. The system according to any one of the preceding claims 25–31, characterised in that the firewall (FW) is arranged to filter the telecommunication based on additional filtering rules.

33. The system according to any one of the preceding claims 25–32, characterised in that the additional filtering rule is a group-specific rule of the user.

34. The system according to any one of the preceding claims 25–33, characterised in that the firewall (FW) is arranged to handle the service-specific filtering rules and additional filtering rules independently as groups of their own.

35. The system according to any one of the preceding claims 25–34, characterised in that the firewall (FW) is arranged to filter the telecommunication based on the most limiting filtering rules.

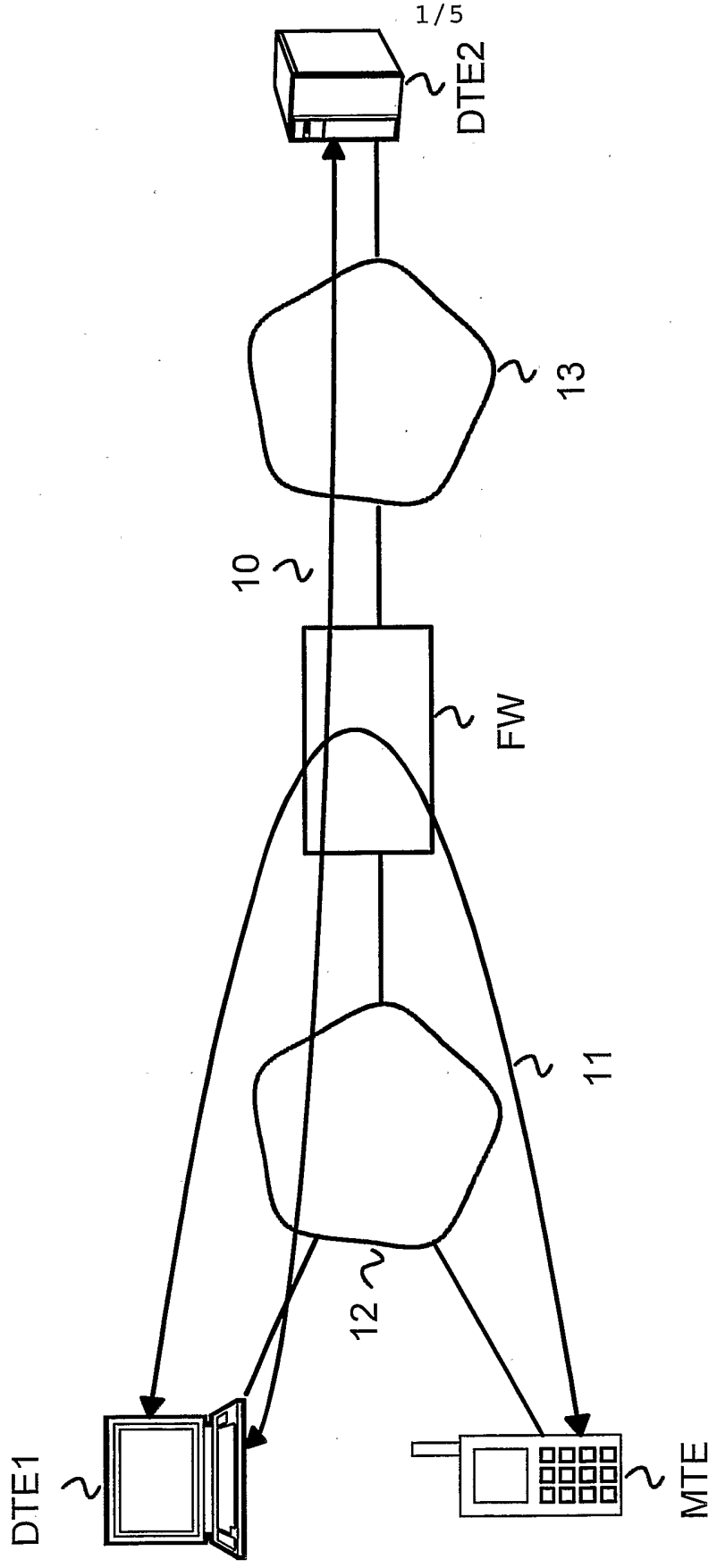


FIG 1

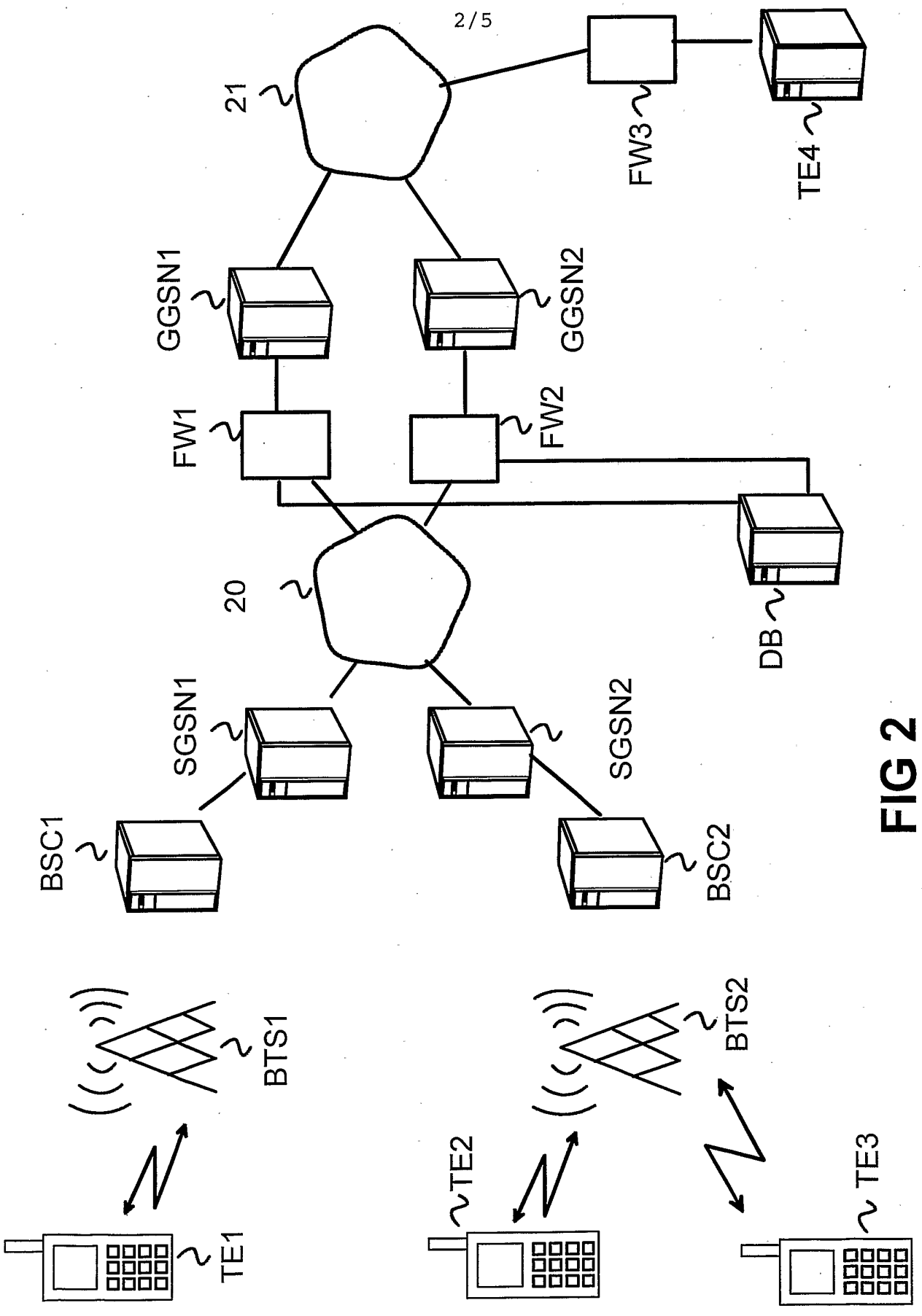

21
FW3
TE4
GGSN1
GGSN2
FW1
FW2
20
DB
SGSN1
SGSN2
BSC1
BSC2
BTS1
BTS2
TE1
TE2
TE3

FIG 2

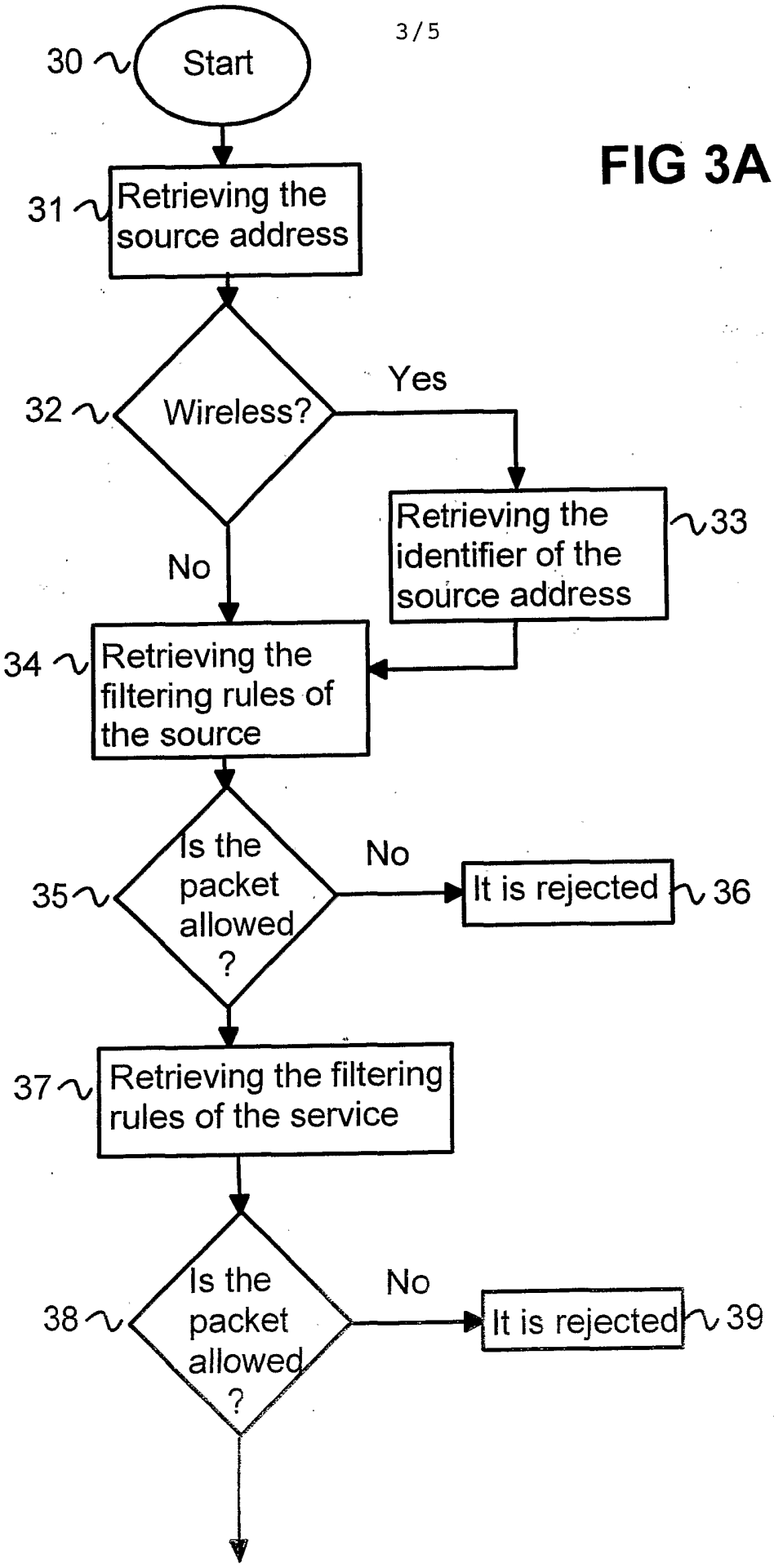
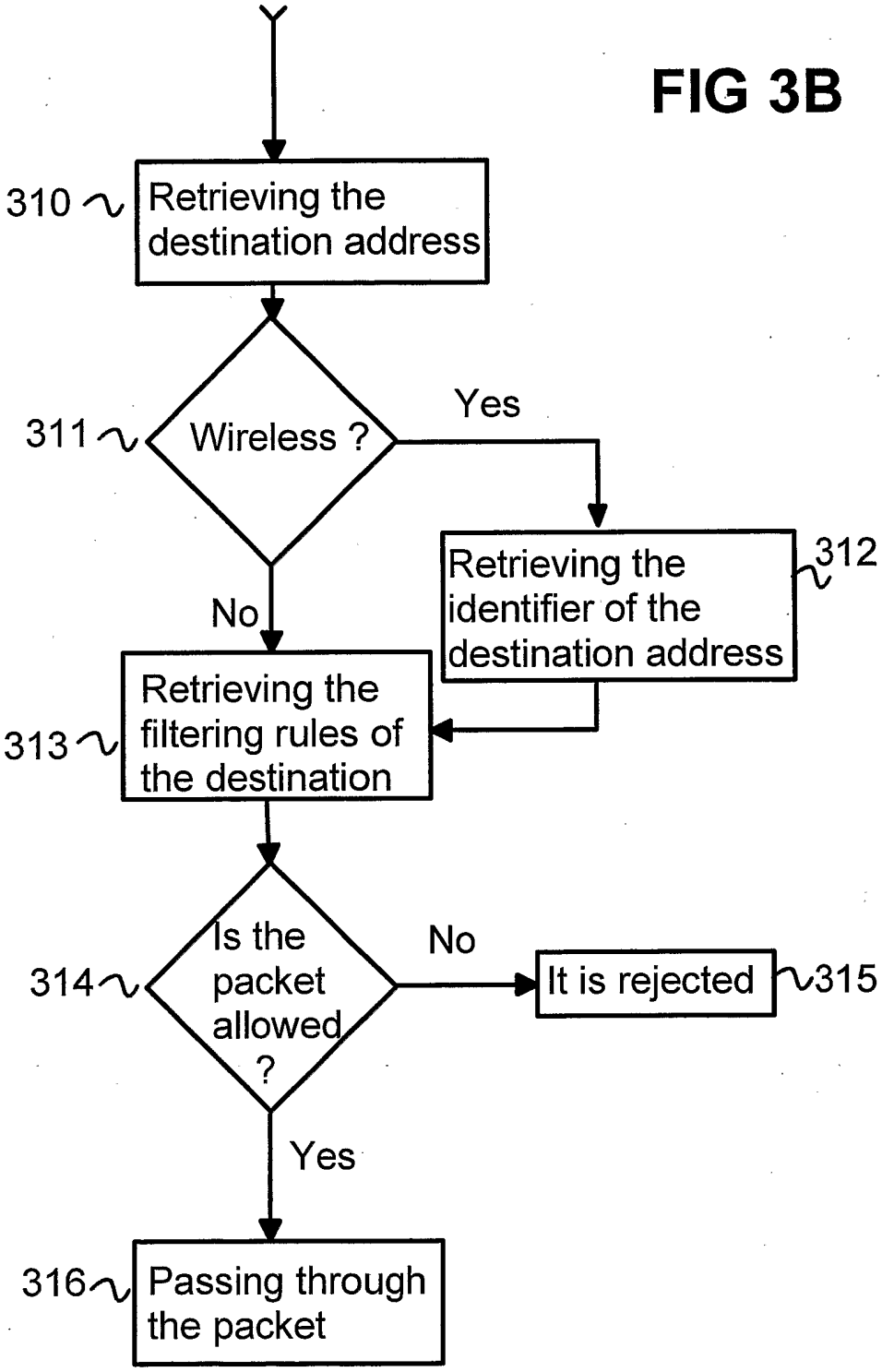

30
Start
31
Retrieving the source address
32
Wireless?
Yes
No
33
Retrieving the identifier of the source address
34
Retrieving the filtering rules of the source
35
Is the packet allowed ?
No
It is rejected
36
37
Retrieving the filtering rules of the service
38
Is the packet allowed ?
No
It is rejected
39

FIG 3A

FIG 3B


310
Retrieving the destination address
311
Wireless ?
Yes
No
312
Retrieving the identifier of the destination address
313
Retrieving the filtering rules of the destination
314
Is the packet allowed ?
No
It is rejected
315
Yes
316
Passing through the packet

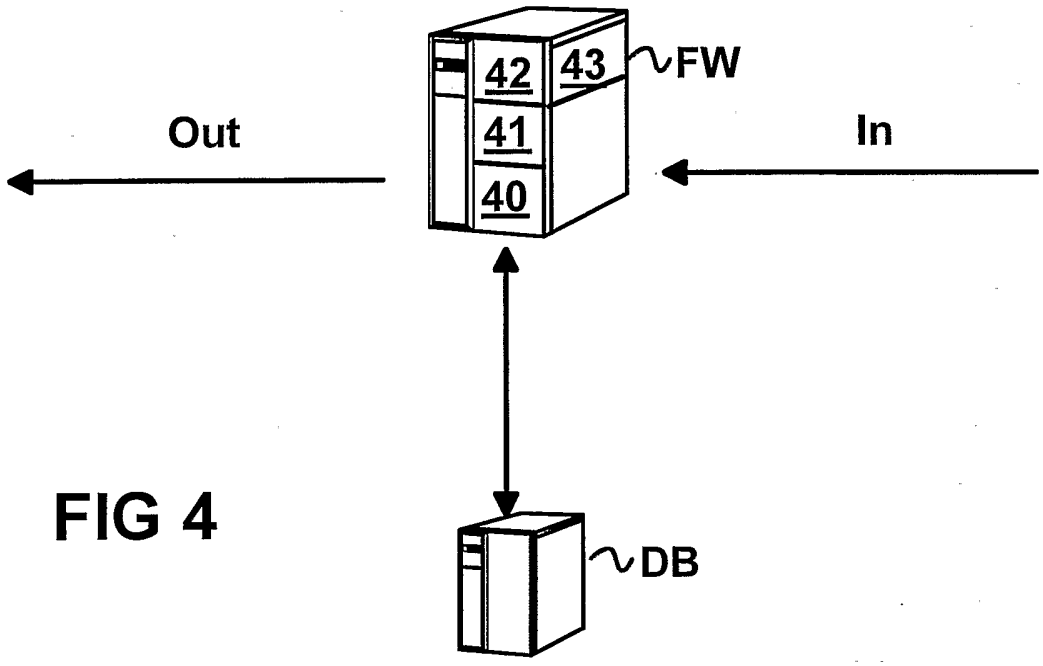


FIG 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 03/00577

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/56, H04L 29/06, H04Q 7/22
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)

IPC7: G06F, H04L, H04Q

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

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, 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.
Y	WO 9905828 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 4 February 1999 (04.02.99), page 9, line 9 - line 16; page 17, line 10 - line 15, claims 15,16, abstract --	1-35
Y	US 5951651 A (LAKSHMAN, T.V. ET AL), 14 Sept 1999 (14.09.99), column 1, line 44 - line 64, abstract --	1-35
A	EP 1119151 A2 (LUCENT TECHNOLOGIES INC), 25 July 2001 (25.07.01), page 2, line 5 - page 3, line 20, abstract -- --------	1-35

☐ 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 application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 Sept 2003	30-09-2003
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Ralf Boström /LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

26/07/03

International application No.
PCT/FI 03/00577

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9905828 A1	04/02/99	AU 739717 B	18/10/01
		AU 8369898 A	16/02/99
		BR 9810796 A	25/07/00
		CN 1271488 T	25/10/00
		EP 0997018 A	03/05/00
		NZ 502339 A	30/11/01
		AT 235455 T	15/04/03
		AU 740636 B	08/11/01
		AU 4321899 A	20/12/99
		CA 2332847 A	09/12/99
		DE 69906283 D	00/00/00
		DK 1084099 T	26/05/03
		EP 1084099 A,B	21/03/01
		SE 1084099 T3	
		JP 2002516893 T	11/06/02
		US 6040464 A	21/03/00
		WO 9962861 A	09/12/99
US 5951651 A	14/09/99	NONE	
EP 1119151 A2	25/07/01	CA 2328012 A	18/07/01
		JP 2001237895 A	31/08/01