

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
10 August 2006 (10.08.2006)

PCT

(10) International Publication Number
WO 2006/083171 A1

- (51) International Patent Classification:
H04N 7/15 (2006.01) *H04L 12/18* (2006.01)
- (21) International Application Number:
PCT/NO2006/000038
- (22) International Filing Date: 27 January 2006 (27.01.2006)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
20050625 4 February 2005 (04.02.2005) NO
- (71) Applicant (for all designated States except US): **TAND-
BERG TELECOM AS** [NO/NO]; Philip Pedersens vei 22,
N-1366 Lysaker (NO).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **STAURNES, Jarl,
Ove** [NO/NO]; Asbjørn Klosters vei 11, N-1472 Fjell-
hamar (NO). **GJØDUM, Nicolai** [NO/NO]; Oscarsgt. 54,
N-0258 Oslo (NO).
- (74) Agent: **OSLO PATENTKONTOR AS**; P.O. Box 7007M,
N-0306 Oslo (NO).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,

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

Declaration under Rule 4.17:

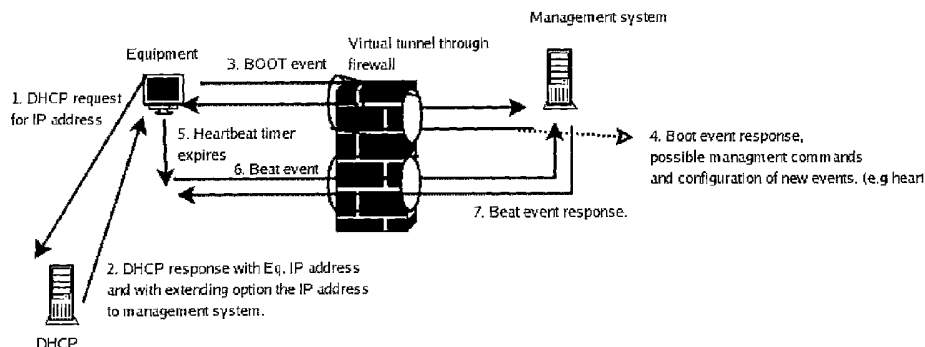
- as to applicant's entitlement to apply for and be granted a
patent (Rule 4.17(ii))

Published:

- with international search report
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments

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

(54) Title: METHOD OF MONITORING AND CONFIGURING



(57) Abstract: The present invention discloses a method for managing and monitoring communication devices in a firewall/NAT protected network from a Management system outside the firewall/NAT protected network by periodically and at predefined events opening an http connection and transmitting a request from the respective communication devices to the Management system through a firewall/NAT installation protecting the network, and when receiving said request in the management system, transmitting instructions and data to the communication devices from the management system in a http response through said http connection.

METHOD FOR MONITORING AND CONFIGURATION

Technical field

The present invention relates to monitoring, configuration and administrating IP terminals behind Firewalls and NAT traversing nodes.

5 Background art

Conventional conferencing systems comprise a number of end-points communicating real-time video, audio and/or data streams over and between various networks such as WAN, LAN and circuit switched networks.

10 A number of conference systems residing at different sites may participate in the same conference, most often, through one or more MCU's (Multipoint Control Unit) performing i.a. switching functions to allow the audiovisual terminals to intercommunicate properly.

15 As videoconferencing involves various recourses and equipment simultaneously interoperating at different localizations and capabilities, there is a need for the possibility to manage the resources involved both for scheduled and ad hoc conferences.

Conferencing systems are therefore often provided with a management tool. The management tool may i.a. include a resource scheduler, a monitor module and a routing module.

20 As early conferencing equipment was ISDN based, it has now started migrating to IP based terminals and infrastructure. IP-based equipment is often connected to a Local Area Network (LAN), which is protected by Firewalls and NAT installations. This introduces a new problem in connecting between Management systems and the associated nodes and equipment. The
25 Management system might as well be operating from outside the LAN, meaning that communication towards the managed nodes and endpoints has to force through Firewalls and NAT's. This is a problem due to a most often strict policy for what is allowed to pass through a firewall. Conventionally, all communication sessions through a firewall has to be initiated from inside. This means that all
30 requests initiated from a management system to a device located inside a LAN

would be rejected by the firewall. In addition, the management system would not know the terminating IP address of the device as the NAT installation hides the actual addresses of the devices.

Thus, the equipments may be able to transmit their reports out to the
5 administration tool if the firewall is configured to let these reports out, but the administrator would have difficulties configuring and otherwise administrating the equipments, as it is prevented from requesting devices behind the firewall.

Allowing the reports out through the firewall may cause other information leaking out that was not intended to.

10 Most IP equipment of prior art uses SNMP (Simple Network Management Protocol) for monitoring purposes. The equipment sends a trap to the management system when something happens using a UDP/IP packet to a specific port. The management system might then probe the equipment using another specified port. For this to work through a firewall, the SNMP ports must
15 be opened. This poses a very high security risk because mostly all IP equipment has SNMP, and thus the entire network would be exposed to the outside. Also the security mechanisms of SNMP is rather weak and malicious parties might intercept the messages and pretend to be the management system and issue the same administrator commands as the management
20 system and alter the equipments configurations.

Another problem is that SNMP uses a specific port for the management system to access the equipments, thus if the management system is outside the firewall and NAT is in use, only one of the equipment on the inside could be accessed as the firewall could only map one port to one address on the inside. A way to
25 work around this is to make a tunnel through the firewall and a specific utility on the inside (proxy) that would redirect the connection to the equipment. However, this would require some special extension in the management system and quite a lot of configurations.

Disclosure of the invention

30 It is an object of the present invention to provide a method avoiding the above described problems.

The features defined in the independent claims enclosed characterise this method. The present invention discloses a method for managing and monitoring communication devices in a firewall/NAT protected network from a Management system outside the firewall/NAT protected network by periodically and at
5 predefined events opening an http connection and transmitting a request from the respective communication devices to the Management system through a firewall/NAT installation protecting the network, and when receiving said request in the management system, transmitting instructions and data to the communication devices from the management system in a http response
10 through said http connection.

Brief description of the drawings

In order to make the invention more readily understandable, the discussion that follows will be supported by the accompanying drawing,

Figure 1 is a block diagram showing the data flow between an endpoint and a
15 management system according to one embodiment of the present invention.

Best mode for carrying out the invention

In the following, the present invention will be discussed by describing a preferred embodiment, and supported by the accompanying drawings. However, people skilled in the art will realize other applications and
20 modifications within the scope of the invention as defined in the enclosed independent claims.

As already mentioned in the background section, firewalls allow establishment of communication sessions initiated from inside the protected area, but not in the opposite direction e.g. from the public Internet into the protected area.
25 Particularly, most firewalls have HTTP (port 80) and HTTPS (port 443) open from the inside to the outside of the firewall. When a TCP connection then is established from the inside to a verified area on the outside (server, node, terminal etc.), the verified area can transfer information back to the originating system. This possibility is utilised in the present invention for managing IP
30 equipment behind firewalls/NAT installations relative to the management system.

According to the invention, the inside equipment periodically sends data in an initiating request, allowing the management system to send configuration or other administration command in the response. By selecting proper initiating request intervals and/or defining proper initiating events, a system on the inside
5 of a firewall can be configured, monitored and administrated from the outside without compromising with security. Preferably, the secure protocol HTTP/S is used as the transport mechanism. HTTP/S is a protocol standardized by IETF designed to send individual messages securely through the Internet. The only configuration that is required when deploying new equipment is setting the IP
10 address of the administration tool on the equipment. However, by using an extension to DHCP (Dynamic Host Configuration Protocol), the administration tool address can be configured in the DHCP server once and then all equipments will automatically be configured when they are connected to the network.

15 In a preferred embodiment of the invention, an event scheme defines when the equipment behind the firewall sends request posting an event with certain information (different types depending on the situation) or simply a repeating request, and then the management system in response will issue configuration and other types of commands for managing the equipment. The request is
20 preferably a SOAP request, which is a request according to the Simple Object Access Protocol compatible with http for exchanging information in an Internet environment.

For the event scheme to be activated, the equipment has to retrieve the address of the management system. This is preferably provided automatically in
25 that the equipment is configured to utilise DHCP for obtaining its IP address configuration. When the equipment is turned on, a query is sent to a DHCP server. The DHCP server then responds with a packet containing the IP configuration and other optional settings. By extending the DHCP packet using a free option, the equipment can then receive the IP address of the
30 management system.

Further, when the equipment connects to the network, it first checks if it has received an IP address to the management system from DHCP. If so, the address is used in conjunction with a stored service path (configurable, e.g. "/public/externalmanager.asmx") to make a URL which it then try to establish an
35 HTTP or HTTPS connection to the management system.

Alternatively, if no management system address is received from DHCP, or DHCP is not in use, a (pre-configured) stored address to the management system is then used.

5 After the URL has been created and the HTTP/S (TCP connection) has been established, a SOAP request is generated. By using SOAP the service mechanism (SOAP + WSDL == web services) can very easily be implemented in a management system, as it is an existing standard.

10 The first SOAP request sent from the equipment to the administration tool defines a "Boot" event. This is a special registration event that is used to signal to the administration tool that the equipment is just connected to the network (or booted up).

In the top heading of a SOAP request associated with a "Boot" event is an identification element including information about the equipment for the management system to uniquely identify it.

15 On response to the "Boot" event SOAP request, the management system sends a set of parameters to be used by the equipment for the succeeding communication with the management system, e.g. defining requests intervals and event schemes. Below are a few examples of parameters depicted.

20 ***HeartBeatInterval*** - A number defining the frequency of heartbeat events, i.e. periodical SOAP request, in seconds.

25 ***FilesToDownload*** - A group parameter containing a **SoftwareUpgrade** parameter informing the equipment to download new software. The parameter contains the address and authorization key. Further, a set of **FileToDownload** parameters simply mapping a network address file to a local file path to which the equipment should download.

Management - This parameter element is the key to managing. All event responses have this. A set of sub elements is used to separate the different types of administration commands. Examples of such commands are **Command**, **Configuration** and **Directory** is in use.

Expressions - Group element holding several Expression definitions e.g. defining different events.

Whenever a heartbeat frequency is defined as a result of a previous event response, a timer is started with the number of seconds specified between each
5 "heartbeat". When it expires, an event is sent to the management system as a "Beat" event type.

The response from the management system contains the same parameters as the Boot event.

Whenever an Expressions element is returned in a previous event response,
10 each of the Expression elements are registered in the change machinery. When a change in the system satisfies one of the registered expressions, an event is sent to the Management system as an Expression event type. Within the event request, the expression that triggered the event is passed as a parameter to the management system. The response from the management system is the same
15 parameters as for the Boot event. However, any HeartBeat or Expressions elements will override previous defined events.

By referring to figure 1, an example of data flow between a videoconference terminal behind a firewall and a management system is discussed.

The terminal sends a DHCP request for retrieval of its own IP address
20 configuration (1). The DHCP server returns information, with extension to supply management system IP address (2).

After receiving the information from the DHCP server, the terminal sends a BOOT event to the management system using the IP address that was
25 retrieved or pre-configured in the previous steps (3). The event is sent over an HTTP connection, and by doing so, a virtual tunnel is made through the firewall so that a two-way communication with the management system is established.

Thereafter, the management system sends a (HTTP) response through the tunnel (4) where it may instruct the equipment to issue new events in the future (a timed event, or when changes occur matching an expression). Along with
30 these instructions, the management system may issue other administration commands, e.g. configurations or control commands.

If the management system requested a heartbeat event, a timer in the equipment was created as specified (5).

When the heart beat timer expires, the equipment sends a new event (BEAT) to the management system (6). Again, opening a new HTTP connection and thus
5 creating a new communication tunnel.

Finally, the Management system responds with possible new instructions (7).

The usage of the present invention is particularly advantageous when deploying equipment in larger numbers that require initial configuration. The mechanism can be implemented as a part of a solution to ease this process. By having a
10 configuration server with the initial configuration for the equipment stored, this server can return configuration data and instruct the equipment to download files or upgrade firmware, even when the equipment is behind a NAT firewall/router. This allows an administrator to be able to roll out new equipment without configuring it on beforehand. The only step necessary is to register the
15 equipment with the configuration server if it is not configured to give configuration data to any system connecting to it. The equipment would typically use DHCP to locate the configuration server.

Another possibility that opens is a more flexible mechanism for pro-active notifications for the administrator. By implementing a mechanism on the
20 configuration server that would send e-mails based on events from the equipment, the administrator could configure feedback expressions that would supply him with notifications of his own choice. The configuration server could also send e-mails when a heartbeat event has not been received, to inform that a unit is offline.

Further, by using the heartbeat frequency in a dynamic manner, the
25 configuration server is allowed to schedule contact with the equipment at any time in the future upon receiving the next request. E.g. if the standard heartbeat interval is 5 minutes, and the configuration server would like to issue a command on the equipment in 13 minutes, the configuration server could set it
30 to 3 minutes on the request before the command should be executed. At the time the command is to be executed on the equipment, the equipment would contact the configuration server with the heartbeat request, get the command in the response, and the heartbeat interval would be set back to 5 minutes.

The disadvantage of using the event scheme for issuing administration commands is that the Management system can not at any time send these commands but have to wait for the next event. By carefully selecting the expressions and heart beat interval, this would not be a big issue in practice.

5 However, by keeping the tunnel up (in fact, this is the default behaviour of HTTP 1.1) and extending the HTTP protocol so that requests can be issued from both sides (like RTSP, real time streaming protocol). The management system could send a new form of request for issuing management commands.

10 The problem with this is that either of the equipment, firewall or administrator server can at any time close the tunnel if the link is inactive for a period of time. Therefore this approach will not guaranty more control for the management system.

The event model though will always reconnect the tunnel if necessary and are therefore guaranteed to work as defined.

15 One of the advantages of the present invention is that there is no need for configuring the firewall. Also, by using the DHCP extensions, the only configuration needed is to install the IP address for management system on the DHCP server once. Then all new equipment will automatically connect. Without the DHCP extension in use, all new equipment must be configured with this one
20 IP address for the administration tool. For other specialized administration protocols, the firewall must be configured to allow this new protocol through.

Further, by using the HTTPS protocol, a secure connection is made both ways so no eavesdrop or insertion of malicious commands can happen.

25 Another advantage is that there is no need to make new software for the equipment for generating new events as it is when using SNMP. In SNMP, a new trap handler must be created in the equipment if new reports are needed. With the event scheme using expressions, the management system can define the event as specific or general as convenient. All that is needed are a specification of the XML documents on the equipment and an XPath query
30 machinery than can trigger on changes on the equipment.

Since the model is using HTTP and HTTP is a well-known protocol that is in extensible use, all firewall will be supported. Also, they are normally pre-

configured to allow HTTP traffic out of the firewall thus a deployment of equipment and administration tools can be done without involving the firewall.

WAN	Wide Area Network
LAN	Local Area Network
MCU	Multipoint Control Unit
ISDN	Integrated Services Digital Network
IP	Internet Protocol
NAT	Network Address Translation
SNMP	Simple Network Management Protocol
UDP/IP	User Datagram Protocol/Internet Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
TCP	Transmission Control Protocol
IETF	Internet Engineering Task Force
DHCP	Dynamic Host Configuration Protocol
SOAP	Simple Object Access Protocol
URL	Uniform Resource Locator
RTSP	Real Time Streaming Protocol

Claims

1. A method for managing and monitoring communication devices in a firewall/NAT protected network from a Management system outside the firewall/NAT protected network,
5 characterized in the following steps:
periodically and at predefined events opening an http connection and transmitting a request from the respective communication devices to the Management system through a firewall/NAT installation protecting the network,
10 when receiving said request in the management system, transmitting instructions and data to the communication devices from the management system in a http response through said http connection.
2. A method according to claim 1,
characterized in that when one of the communication devices for the first time
15 is connected to the network:
opening an initial http connection and transmitting a BOOT request through said firewall/NAT installation from said communication device, when receiving said BOOT request in the management system, transmitting configuration data and parameters to said communication
20 device from the management system at least defining time intervals between periodical requests and events triggering event requests to be transmitted from said device.
3. A method according to claim 2,
characterized in the following step prior to the step of opening an initial http
25 connection:
transmitting from said communication device a DHCP request to a DHCP server,
transmitting from the DHCP server to the communication device a DHCP response at least including an IP address of the Management system.
- 30 4. A method according to one of the preceding claims,
characterized in that said requests are defined according to the Simple Object Access Protocol.

5. A method according to one of the preceding claims,
characterized in that the http connection is a http/s connection.

6. A method according to one of the preceding claims,
characterized in that said instructions and data at least include one of the
5 following:
new time intervals between periodical requests to be transmitted from
respective devices to the management system overriding any existing
ones,
definitions of new events initiating event requests to be transmitted from
10 respective devices to the management system,
command for initiation of download of new software from the
management system to respective devices,
command for instructing the respective communication devices to
transmit status information to the management system.

15 7. A method according to one of the preceding claims,
characterized in that the communication devices are IP based conference
endpoints and/or equipment.

1/1

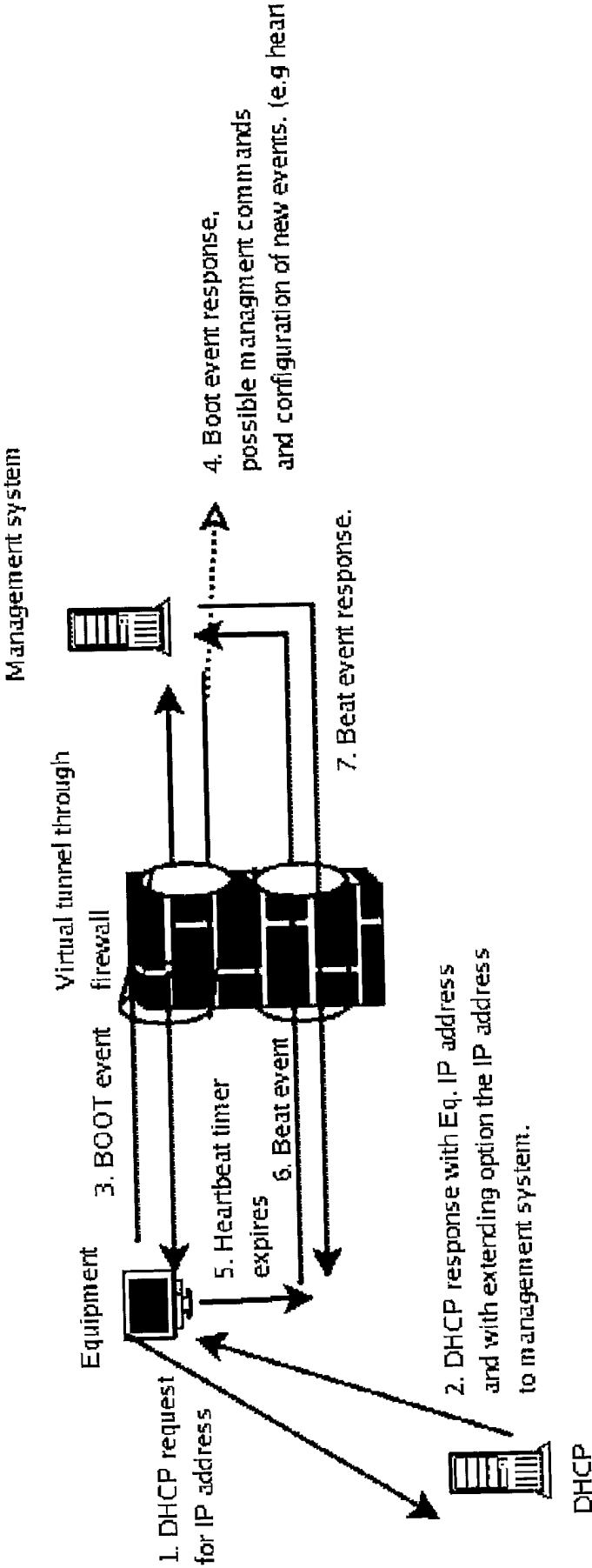


Fig 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO2006/000038

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04N, H04L, H04M

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, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1427211 A1 (NOVA CO., LTD), 9 June 2004 (09.06.2004), paragraphs 0050-0052; 0142-0146; abstract --	1,4-7
X	WO 0208856 A2 (BURSTBAND TECHNOLOGY CORPORATION), 31 January 2002 (31.01.2002), see the whole document --	1,4-7
X	US 20030125995 A1 (YAMATARI, M. ET AL), 3 July 2003 (03.07.2003), claims 1-9, abstract --	1,4-7

☒ 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

15 June 2006

Date of mailing of the international search report

19-06-2006

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

Henrik Andersson /LR

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/NO2006/000038

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2004053761 A1 (CHO, H-K.), 24 June 2004 (24.06.2004), page 9, line 23 - page 11, line 19, claim 1, abstract --	1,4-7
X	US 20020093948 A1 (DELTZ, G.A. ET AL), 18 July 2002 (18.07.2002), abstract --	1,4-7
A	EP 0717544 A2 (AT & T CORP.), 19 June 1996 (19.06.1996) -- -----	1-7

International patent classification (IPC)

H04N 7/15 (2006.01)*H04L 12/18* (2006.01)Download your patent documents at www.prv.se

The cited patent documents can be downloaded at www.prv.se by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **FYCLTBYZDO**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT
Information on patent family members

04/03/2006

International application No.

PCT/NO2006/000038

EP	1427211	A1	09/06/2004	CA	2450603 A	03/01/2003
				IL	159385 D	00/00/0000
				NZ	530306 A	24/03/2005
				US	20040205131 A	14/10/2004
				CN	1522537 A	18/08/2004
				JP	2003009105 A	10/01/2003
				WO	03001808 A	03/01/2003
WO	0208856	A2	31/01/2002	AU	7706401 A	05/02/2002
US	20030125995	A1	03/07/2003	GB	0229116 D	00/00/0000
				GB	2385171 A,B	13/08/2003
				JP	3634307 B	30/03/2005
				JP	2003199069 A	11/07/2003
WO	2004053761	A1	24/06/2004	AU	2003302836 A	30/06/2004
				KR	2003003193 A	09/01/2003
				US	20050222995 A	06/10/2005
US	20020093948	A1	18/07/2002	WO	02058418 A	25/07/2002
EP	0717544	A2	19/06/1996	CA	2160821 A	17/06/1996
				JP	8279808 A	22/10/1996