

(51) International Patent Classification:
G06F 13/00 (2006.01)

(21) International Application Number:

PCT/JP2010/052570

(22) International Filing Date:

15 February 2010 (15.02.2010)

(25) Filing Language:

English

(26) Publication Language:

English

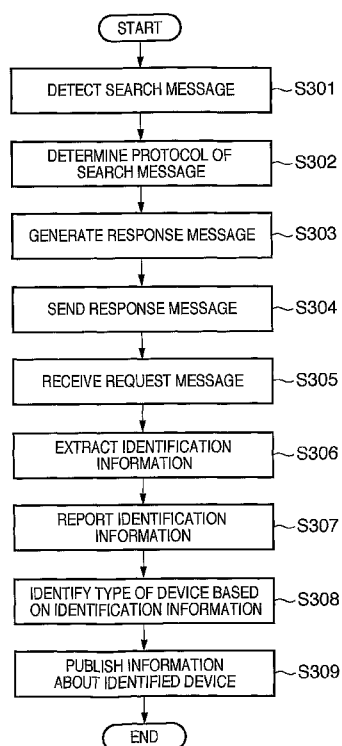
(71) Applicant (for all designated States except US): **Telefon-
aktiebolaget L M Ericsson (publ)** [SE/SE]; SE-164 83,
Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **YASUKAWA,
Kenta** [JP/JP]; 3-7-7-102, Doshida, Nerima-ku, Tokyo,
1790076 (JP). **SUGIMOTO, Shinta** [JP/JP];
13-17-2013, Nakamaruko, Kawasaki-shi, Kanagawa,
2110012 (JP). **GERDES, Martin** [DE/DE]; Retzstr. 31,
52156, Monschau-Rohren (DE).(74) Agent: **OHTSUKA, Yasunori**; 7th FL., KIOICHO
PARK BLDG., 3-6, KIOICHO, CHIYODA-KU, Tokyo,
1020094 (JP).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, 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,

[Continued on next page]

(54) Title: NETWORK NODE FOR DETECTING A COMMUNICATION DEVICE

FIG. 3

(57) Abstract: There is provided a network node for detecting a communication device (stealth device) in a local network and identifying a type of the detected communication device. According to the embodiments of the present invention, the network node 200 detects a search message sent out by a stealth device, and sends a response message to the stealth device as if the network node 200 were a target node to be searched for. The network node 200 then receives a request message from the stealth device, and extracts, from the request message, identification information (e.g., a User-Agent header) that corresponds to a type of the stealth device. The identifying unit 208, which may be located inside or outside the network node 200, identifies the type of the stealth device based on the extracted identification information.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

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

Declarations under Rule 4.17:

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

- 1 -

DESCRIPTION

NETWORK NODE FOR DETECTING A COMMUNICATION DEVICE

TECHNICAL FIELD

[0001] The present invention generally relates to a network node for detecting a communication device in a local network and identifying the type of the detected communication device, and a control method therefor.

BACKGROUND

[0002] Currently, communication devices are known that are capable of communicating with each other thereby forming a local network. An example of such a communication device is a personal computer (PC) that is equipped with a network interface card and a mobile phone that is equipped with an IEEE 802.11a/b/g-compliant communication module. Configurations are also known whereby the local network is connected to a wide area network (WAN) via a gateway. In this case, the communication devices in the local network can communicate with external servers via the WAN and receive various services therefrom. An example of such a service is a video streaming service; a communication device such as a PC and a mobile phone receives video

data from a video server, and renders the video data on a display.

[0003] These days, the number of service providers that provide local networks with their services is increasing. As a result, the burden for a user of communication devices in a local network to choose their desired services is also increasing. One solution to reduce the burden of a user is to make service providers propose, to a local network, only services that fit with the local network. For example, if a local network does not include a digital audio player, service providers should not propose audio services to that local network.

[0004] In order to implement such a solution effectively, it is necessary for service providers to know the capabilities of communication devices in a local network. Service providers can know the capabilities of communication devices that are configured to announce their existence and capabilities to the other communication devices and service providers. An example of such a communication device that announces its existence and capabilities is DLNA® Digital Media Server (DMS). However, all communication devices in a local network do not necessarily announce their existence and capabilities explicitly. An example of a communication device (hereinafter referred to as "stealth device") that does not announce its

- 3 -

existence and capabilities is a DLNA® Digital Media Player (DMP). The DLNA® DMP searches for and controls a DLNA® Digital Media Server (DMS) to obtain and playback media, but is not designed to be controlled by other communication devices. Other than DLNA® DMPs, communication devices that are not controlled by other communication devices are likely designed not to announce their existence and capabilities, because their existence and capabilities are not essential to the other communication devices under conventional usage.

[0005] US 2008/0235358 A1 and US 6094681 A discloses techniques for detecting the existence of stealth devices by capturing messages sent out by the stealth devices. However, although the techniques disclosed in these patent documents enable the detection of stealth devices, the techniques do not enable the identification of the type of the detected stealth devices. In the end, according to the conventional art, it is not possible for service providers to know the capabilities of stealth devices in a local network.

SUMMARY

[0006] The present invention is intended to address the above-described problem, and it is a feature thereof to introduce a technology that enables

- 4 -

the detection of communication devices in a local network and identification of the type of the detected communication devices.

[0007] According to the first aspect of the present invention, there is provided a network node for detecting a communication device in a local network and identifying a type of the detected communication device, comprising:

- a detecting unit that detects a search message sent out by a communication device in the local network, the search message including an indicator of a target node to be searched for;

- a generating unit that generates a response message upon detection of the search message, the response message including a network address at which the communication device can access the network node and an indicator of the target node;

- a sending unit that sends the response message to the communication device as a response to the search message;

- a receiving unit that receives a request message addressed to the network address from the communication device, the request message including identification information which corresponds to a type of the communication device;

- an extracting unit that extracts the identification information from the request message;

and

a reporting unit that reports the identification information to an identifying unit that identifies the type of the communication device based on the identification information.

[0008] According to the second aspect of the present invention, there is provided a method for controlling a network node for detecting a communication device in a local network and identifying a type of the detected communication device, comprising:

a detecting step of detecting a search message sent out by a communication device in the local network, the search message including an indicator of a target node to be searched for;

a generating step of generating a response message upon detection of the search message, the response message including a network address at which the communication device can access the network node and an indicator of the target node;

a sending step of sending the response message to the communication device as a response to the search message;

a receiving step of receiving a request message addressed to the network address from the communication device, the request message including identification information which corresponds to a type of the

communication device;

an extracting step of extracting the identification information from the request message; and

a reporting step of reporting the identification information to an identifying unit that identifies the type of the communication device based on the identification information.

[0009] The main advantage of the present invention is that it is possible to detect a communication device in a local network and identify the type of the detected communication device even if the communication device is a stealth device.

[0010] Further features of the present invention will become apparent from the following description of exemplary embodiments with reference to the attached drawings, in which like reference characters designate the same or similar parts throughout the figures thereof.

BRIEF DESCRIPTION OF DRAWINGS

[0011] Fig. 1 is an overview of a local network 100 according to an exemplary embodiment of the present invention;

[0012] Fig. 2 is a functional block diagram of a network node 200 according to the exemplary embodiment of the present invention; and

- 7 -

[0013] Fig. 3 is a flowchart illustrating a procedure whereby the network node 200 detects a stealth device and identifies a type of the detected stealth device according to the exemplary embodiment of the present invention.

DETAILED DESCRIPTION

[0014] Fig. 1 is an overview of a local network 100 according to an exemplary embodiment of the present invention. The local network 100 is, for example, a local area network (LAN), a personal area network (PAN), or the like. As shown in Fig. 1, the local network 100 includes several communication devices such as a personal computer (PC) 101, digital camera 102, and a digital media player (DMP) 103. The local network 100 also includes a gateway 104, and the local network 100 is connected to a wide area network (WAN) 110 such as the Internet via the gateway 104. Accordingly, the communication devices in the local network 100 can receive various services via the gateway 104 from external servers such as a video server 120 and a game server 130 that are connected to the WAN 110.

[0015] Some of the communication devices in the local area network 100 are "stealth devices" that do not announce their existence and capabilities to the other communication devices and the external servers. In the present embodiment, it is assumed that the DMP

103 is a stealth device. In order to enable the detection of the stealth device (e.g., the DMP 103) in the local network 100 and identification of the type of the detected stealth device, the present embodiment provides a network node 200.

[0016] Typically, the network node 200 is implemented in the gateway 104 as illustrated in Fig. 1. However, the implementation is not limited to the illustration of Fig. 1; for example, the network node 200 may be implemented in a dedicated communication device that is included in the local network 100 (see the dashed box 200').

[0017] Fig. 2 is a functional block diagram of the network node 200 according to the exemplary embodiment of the present invention. It should be noted that the functionality of each block in the network node 200 may be implemented using dedicated hardware, using software executed by a processor (not shown), or a combination thereof.

[0018] The network node 200 comprises a detecting unit 201, a determining unit 202, a generating unit 203, a sending unit 204, a receiving unit 205, an extracting unit 206, and a reporting unit 207. The network node 200 may also comprise an identifying unit 208 and a database 209. However, the identifying unit 208 and the database 209 may be located outside the network node 200; for example, they may be located in a server

(not shown) that is connected to the WAN 110. The operations of respective units will be described later with reference to the flowchart shown in Fig. 3.

[0019] Fig. 3 is a flowchart illustrating a procedure whereby the network node 200 detects a stealth device and identifies a type of the detected stealth device. In Fig. 3, the DMP 103 is shown as an example of a stealth device. The DMP 103 is configured to send out a search message such as an SSDP Discovery message to the local network 100 when, for example, the DMP 103 joins the local network 100. Although the process of Fig. 3 slightly varies depending on the protocol of the search message, the generic process is described first, and protocol-specific processes are described later taking Bonjour® and UPnP™ as an example.

[0020] In step S301, the detecting unit 201 detects a search message sent out by a stealth device (e.g., the DMP 103). The search message includes an indicator of a target node to be searched for. At this moment, the detecting unit 201 does not know the protocol of the search message. The detecting unit 201 passes the detected search message to the determining unit 202.

[0021] In step S302, the determining unit 202 determines a protocol of the detected search message. For example, the determining unit 202 maintains the

following table. Although Bonjour® and UPnP™ are shown as an example, it is possible to design the network node 200 to support more protocols by making the table contain more entries.

Dest. IP address	Dest. port number	Protocol
224.0.0.251	5353	Bonjour
239.255.255.250	1900	UPnP

[0022] The determining unit 202 searches the table for the entry that matches the destination IP address and the destination port number of the search message. For example, if the destination IP address is 239.255.255.250 and the destination port number is 1900, the determining unit 202 determines that the protocol of the search message is UPnP™. The determining unit 202 passes the search message to the generating unit 203 together with the indicator of the determined protocol.

[0023] In some embodiments, the network node 200 may be designed for a single specific protocol (e.g., UPnP™). In this case, the determining unit 202 may be omitted, and the detecting unit 201 detects an SSDP Discovery message and passes the detected message to the generating unit 203.

[0024] In step S303, the generating unit 203

- 11 -

generates a response message to respond to the search message that was detected in step S301. The response message includes a network address (e.g., the combination of an IP address and a port number) at which the stealth device can access the network node 200. Moreover, by investigating the search message, the generating unit 203 identifies the target node that is searched for by the stealth device. The generating unit 203 then includes an indicator of the same target node in the response message such that the network node 200 operates as if it were the target node.

[0025] In step S304, the sending unit 204 sends the response message to the stealth device as a response to the search message. Since the response message includes the indicator of the target node, when the stealth device receives the response message, the stealth device recognizes that the network node 200, which functions as the target node, is found. Therefore, the stealth device generates a request message and sends it to the network address included in the response message. The request message includes identification information that corresponds to a type of the stealth device. An example of the identification information is a User-Agent header. For example, if the stealth device is a PlayStation® 3, the User-Agent header is "Mozilla/5.0 (PLAYSTATION 3; 2.00)". The request message (to be exact, the Layer 2

- 12 -

header of the packets that carries the request message) may also include a MAC address of the stealth device; the MAC address is unique information that distinguishes the stealth device, which has sent out the request message, from another communication device. It should be noted that the search message detected in step S301 includes the same MAC address. To be more general, all messages originating from the same stealth device include the same source MAC address. Accordingly, the network node 200 can determine whether or not respective messages originate from the same stealth device by comparing the source MAC addresses of the messages with each other.

[0026] In step S305, the receiving unit 205 receives the request message addressed to the network address of the network node 200 from the stealth device. The receiving unit 205 passes the request message to the extracting unit 206.

[0027] In step S306, the extracting unit 206 extracts the identification information (e.g., a User-Agent header) from the request message. The extracting unit 206 may also extract the MAC address from the request message.

[0028] In step S307, the reporting unit 207 reports the identification information to the identifying unit 208. The reporting unit 207 may also report the MAC address to the identifying unit 208 in

- 13 -

association with the identification information.

[0029] In step S308, the identifying unit 208 searches the database 209 for a type that is associated with the identification information. For example, the database 209 includes the following table.

Identification Information	Type of Device (Device Name)
User-Agent = "Mozilla/5.0 (PLAYSTATION 3; 2.00)"	PlayStation® 3
User-Agent = "XXX"	DMP AAA
User-Agent = "XXX"	DMP BBB
ID = "ZZZ"	DMP BBB
ID = "ZZZ"	DMP CCC

[0030] If a User-Agent header is "Mozilla/5.0 (PLAYSTATION 3; 2.00)", "PlayStation 3" is found in the table. In this case, the identifying unit 208 determines that the type of the stealth device is PlayStation® 3.

[0031] In step S309, the identifying unit 208 publishes information about the identified stealth device to the WAN 110. For example, if the stealth device is a PlayStation® 3, the identifying unit 208 publishes, to the WAN 110, information indicating that a PlayStation® 3 is included in the local network 100.

- 14 -

Accordingly, it is possible for the external servers (e.g., the video server 120 and the game server 130) to propose, to the local network 100, services that fit with a PlayStation® 3.

[0032] In some embodiments, the identifying unit 208 may retrieve the capabilities of the identified stealth device (e.g., a PlayStation® 3) from the database 209, and publish the retrieved capabilities to the WAN 110. In this case, it is not necessary for the external servers to have knowledge about the capabilities of various types of communication devices in advance, because the capabilities are published when the type of the communication device is identified.

[0033] As shown in the above table, some identification information items (e.g., User-Agent = "XXX") may be associated with two or more types of communication devices. In this case, those two or more types of communication devices are candidates for the type of the stealth device. Accordingly, the identifying unit 208 chooses one of the candidates in accordance with the following procedure.

[0034] The identifying unit 208 stores the candidates (e.g., "DMP AAA" and "DMP BBB") in a memory (not shown) in association with the MAC address which has been reported in step S307 in association with the identification information. The identifying unit 208 then waits for another (the second) identification

- 15 -

information associated with the same MAC address. When the stealth device, which previously sent the request message including the User-Agent header "XXX" to the network node 200, sends another request message including the second identification information, the second identification information is reported to the identifying unit 208 in association with the same MAC address in the same way as described with reference to steps S305-S307. It is assumed that the second identification information is ID = "ZZZ", although the type of the second identification information varies depending on the type of the request message. The identifying unit 208 then searches the database 209 for a type which is associated with the second identification information ID = "ZZZ". In this example, "DMP BBB" and "DMP CCC" are found. Since "DMP BBB" was previously stored in the memory in association with the MAC address, the identifying unit 208 determines that not "DMP CCC" but "DMP BBB" is the type of the stealth device. In other words, the identifying unit 208 searches the database 209 for a type that is associated with both the first identification information reported in association with a MAC address and the second identification information reported in association with the same MAC address. In this example, one (i.e., "DMP BBB") of the candidates is identified by use of the first and second identification information. However,

- 16 -

in the case that two or more candidates still remain, the same process is repeated for the subsequent (i.e., the third, fourth, fifth, and so on) identification information until one of the candidates is identified.

[0035] Hereinafter, processes unique to specific protocols are described.

[0036] If the stealth device is equipped with a UPnP™ control point and sends out an SSDP Discovery message to the local network 100, the search message detected by the detecting unit 201 in step S301 is, for example, as follows.

M-SEARCH * HTTP/1.1

S: uuid:ijklmnop-7dec-11d0-a765-00a0c91e6bf6

Host: 239.255.255.250:1900

Man: "ssdp:discover"

ST: ge:fridge

MX: 3

[0037] In step S302, the determining unit 202 checks the Layer 3 header of the packets that carries the search message, and found that the destination IP address is 239.255.255.250 and the destination port number is 1900. Accordingly, the determining unit 202 determines that the protocol of the search message is

- 17 -

UPnP™.

[0038] In step S303, because the protocol of the search message is UPnP™, the generating unit 203 looks for the search target (ST) in the search message. In the above example, "ge:fridge" is found, and the generating unit 203 determines that an indicator of the target node to be searched is "ge:fridge". Accordingly, the generating unit 203 generates a response message as follows.

```
-----  
HTTP/1.1 200 OK  
S: uuid:ijklmnop-7dec-11d0-a765-00a0c91e6bf6  
Ext:  
Cache-Control: no-cache="Ext", max-age = 5000  
ST: ge:fridge  
USN: uuid:abcdefgh-7dec-11d0-a765-00a0c91e6bf6  
Location: http://192.168.1.100:40000  
-----
```

[0039] This response message allows the network node 200 to mimic a UPnP™ device named "ge:fridge" as shown in the ST header. The network node 200 listens to a request message at the network address of "192.168.1.100:40000" (the IP address is 192.168.1.100 and the port number is 40000) as shown in the Location header.

- 18 -

[0040] Upon reception of the response message, the stealth device sends an HTTP GET request addressed to "192.168.1.100:40000". The HTTP GET request includes a User-Agent header, and the Layer 2 header of the packets which carries the HTTP GET request includes the MAC address of the stealth device. Accordingly, in step S206, the extracting unit 206 can extract the User-Agent header as identification information of the stealth device, and also extract the MAC address as the unique information of the stealth device. Upon reception of the HTTP GET request, the network node 200 may send an SSDP BYE message to the stealth device so as to remove the network node 200 from the list of discovered devices maintained by the stealth device.

[0041] Next, the case of Bonjour® is described. If the stealth device is compliant with Bonjour®, it searches for a desired service by means of a multicast DNS query message. Accordingly, the search message detected by the detecting unit 201 in step S301 is, for example, as follows. It should be noted that, although the message below is described in a text format for the purpose of explanation, the actual multicast DNS query message is in binary format.

IP Src 10.0.1.2 Dst 224.0.0.251 UDP Src 5353 Port 5353
Queries:

- 19 -

```

_appletv._tcp.local: type PTR, class IN, "QU" question
_daap._tcp.local: type PTR, class IN, "QU" question
_touch-remote._tcp.local: type PTR, class IN, "QU"
question
_raop._tcp.local: type PTR, class IN, "QU" question
-----

```

[0042] In this example, Apple TV® is the target node to be searched for. Accordingly, the generating unit 203 generates the following response message (mDMS message) in order to mimic Apple TV®.

```

-----
IP Src 10.0.1.1 Dst 224.0.0.251 UDP Src 5353 Port 5353
Answers:

```

```

    appletv_raop._tcp.local: type PTR, class IN,
0017F2E27645@dummy.raop.tcp.local

```

Additional Records:

```

    dummy.local: type A, class IN, cache flush, addr
10.0.1.1

```

```

    dummy.local: type AAAA, class IN, cache flush, addr
fe80::217:f2ff:fee2:7645

```

```

    0017F2E27645@dummy.raop.tcp.local: type SRV, class IN,
cache flush, priority 0, weight 0, port 5000, target
dummy.local

```

```

    0017F2E27645@dummy.raop.tcp.local: type TXT, class IN,
cache flush

```

- 20 -

[0043] As similar to the case of UPnP™, upon reception of the response message, the stealth device sends a request message addressed to 10.0.1.1:5000. An example of the request message is as follows.

OPTIONS * RTSP/1.0

CSeq: 1

User-Agent: iTunes/9.0.3 (Windows; Microsoft Windows Vista Enterprise Edition Service Pack 1 (Build 6001)) AppleWebKit/531.21.8

Client-Instance: C8C3E3DD20D83FCB

DACP-ID: C8C3E3DD20D83FCB

Active-Remote: 797657571

Apple-Challenge: ovqAkP/UBi58koCpj4J8hA

[0044] The receiving unit 205 receives the request message described above. Accordingly, the extracting unit 206 can extract the User-Agent header as identification information of the stealth device, and also extract the MAC address as the unique information of the stealth device. Similar to the case of UPnP®, the network node 200 may send a "goodbye" message to the stealth device. Details of the process of sending

- 21 -

the "goodbye" message are found, for example, at <http://files.multicastdns.org/draft-cheshire-dnsext-multicastdns.txt> (in Section 11.2, it is noted that "a message with TTL=0" should be sent to indicate the recode is no longer valid).

[0045] As described above, according to the embodiments of the present invention, the network node 200 detects a search message sent out by a stealth device, and sends a response message to the stealth device as if the network node 200 were a target node to be searched for. The network node 200 then receives a request message from the stealth device, and extracts, from the request message, identification information (e.g., a User-Agent header) that corresponds to a type of the stealth device. The identifying unit 208, which may be located inside or outside the network node 200, identifies the type of the stealth device based on the extracted identification information.

[0046] Accordingly, it is possible to detect a communication device in a local network and identify the type of the detected communication device even if the communication device is a stealth device.

[0047] While the present invention has been described with reference to exemplary embodiments, it is to be understood that the invention is not limited to the disclosed exemplary embodiments. The scope of the following claims is to be accorded the broadest

interpretation so as to encompass all such
modifications and equivalent structures and functions.

CLAIMS

1. A network node (200) for detecting a communication device (103) in a local network (100) and identifying a type of the detected communication device, comprising:

a detecting unit (201) that detects a search message sent out by a communication device in the local network, the search message including an indicator of a target node to be searched for;

a generating unit (203) that generates a response message upon detection of the search message, the response message including a network address at which the communication device can access the network node and an indicator of the target node;

a sending unit (204) that sends the response message to the communication device as a response to the search message;

a receiving unit (205) that receives a request message addressed to the network address from the communication device, the request message including identification information which corresponds to a type of the communication device;

an extracting unit (206) that extracts the identification information from the request message;
and

a reporting unit (207) that reports the

- 24 -

identification information to an identifying unit (208) that identifies the type of the communication device based on the identification information.

2. The network node according to claim 1, further comprising the identifying unit, wherein the identifying unit is configured to identify the type of the communication device by searching a database (209) for a type which is associated with the identification information.

3. The network node according to claim 2, wherein:
the request message further includes unique information which distinguishes the communication device from another communication device;

the extracting unit extracts, from the request message, the unique information in addition to the identification information;

the reporting unit reports, to the identifying unit, the unique information in association with the identifying information; and

the identifying unit is further configured to, if two or more types which are associated with the identification information is found by the searching, identify the type of the communication device by searching the database for a type which is associated with both the identification information and another

identification information reported by the reporting unit in association with the unique information.

4. The network node according to any one of claims 1-3, further comprising a determining unit (202) that determines a protocol of the search message by analyzing content of the search message,

wherein the generating unit generates a response message complying with the determined protocol as the response message to be sent by the sending unit.

5. A method for controlling a network node (200) for detecting a communication device (103) in a local network (100) and identifying a type of the detected communication device, comprising:

a detecting step (S301) of detecting a search message sent out by a communication device in the local network, the search message including an indicator of a target node to be searched for;

a generating step (S303) of generating a response message upon detection of the search message, the response message including a network address at which the communication device can access the network node and an indicator of the target node;

a sending step (304) of sending the response message to the communication device as a response to the search message;

- 26 -

a receiving step (S305) of receiving a request message addressed to the network address from the communication device, the request message including identification information which corresponds to a type of the communication device;

an extracting step (S306) of extracting the identification information from the request message;
and

a reporting step (S307) of reporting the identification information to an identifying unit (208) that identifies the type of the communication device based on the identification information.

FIG. 1

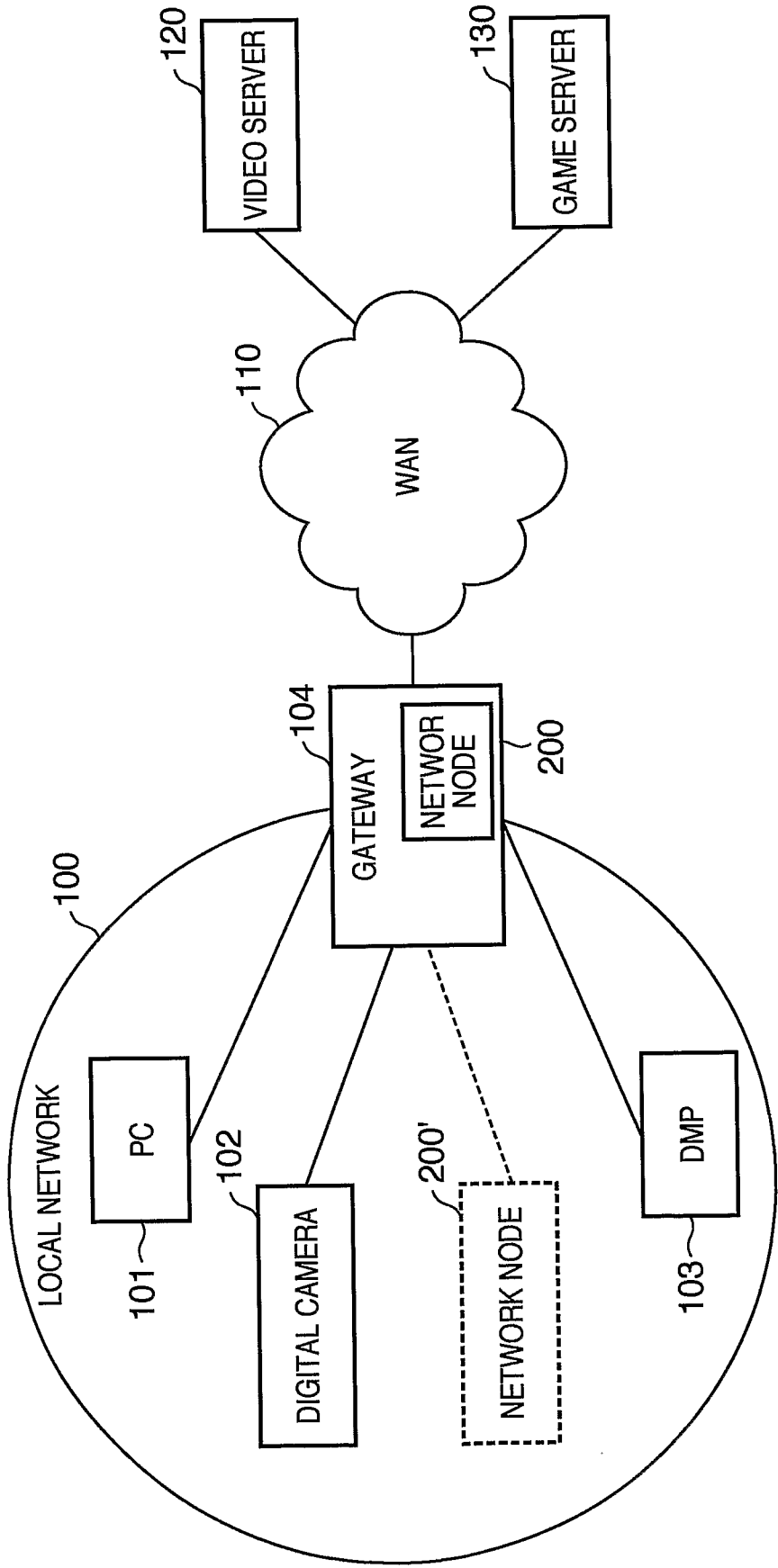


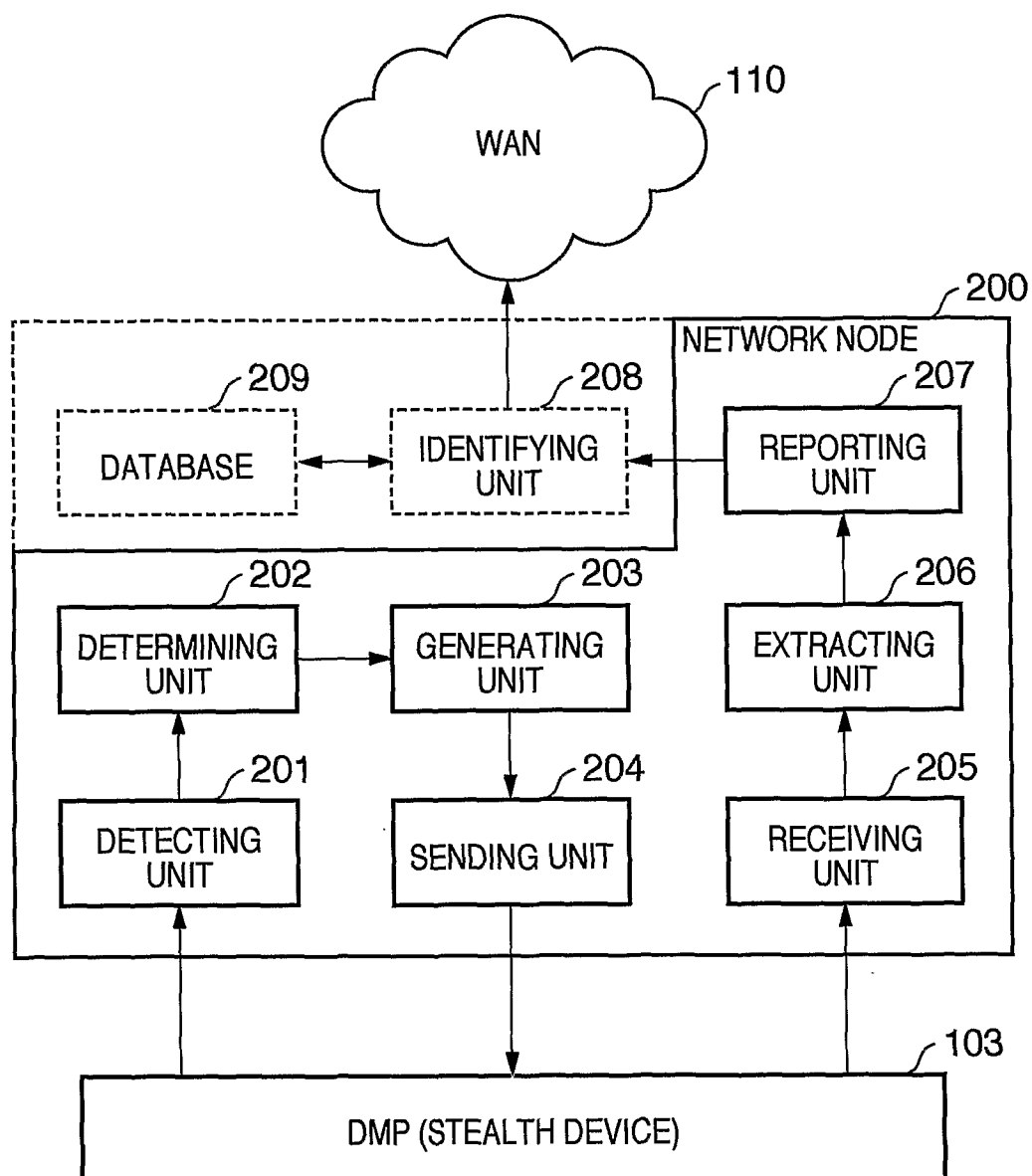
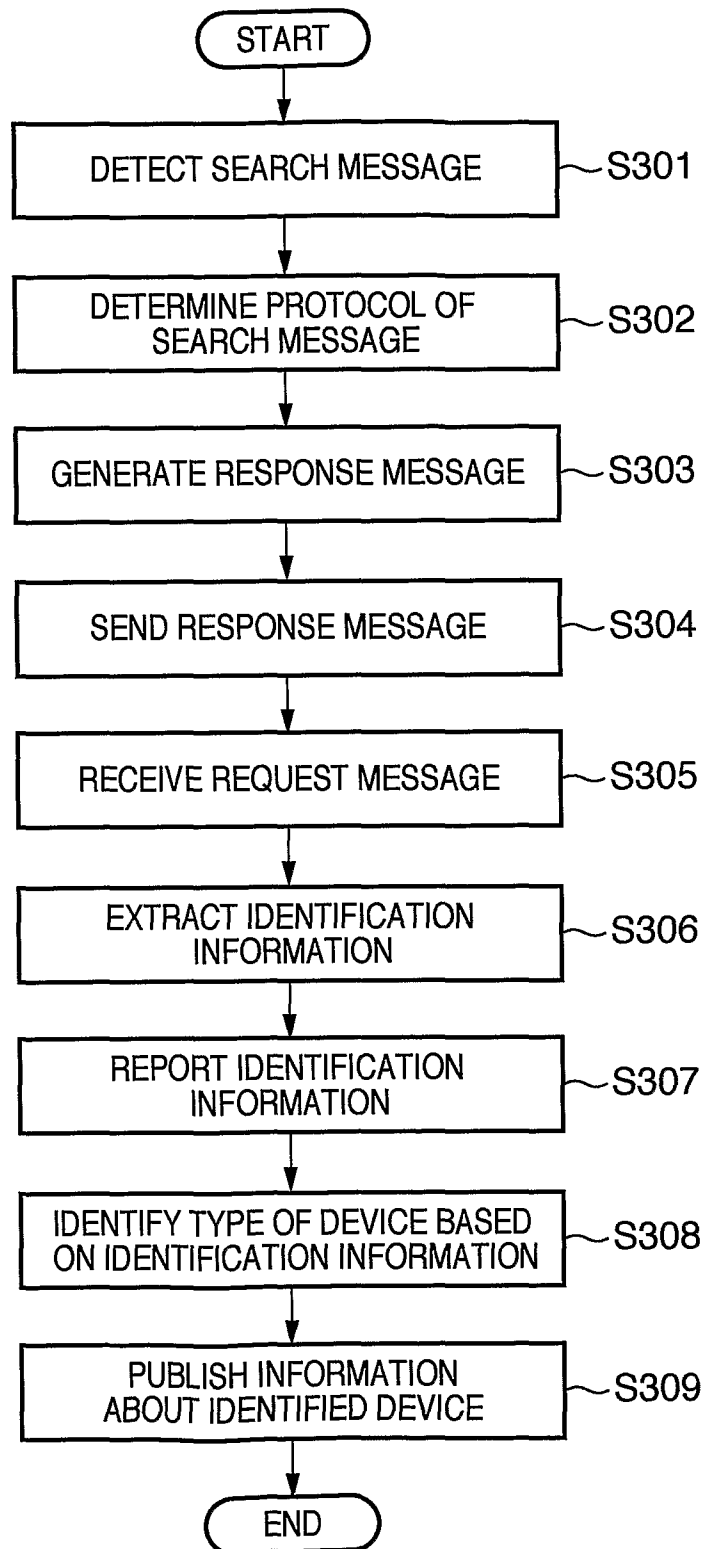
FIG. 2

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/052570

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06F13/00 (2006.01) i

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)

Int.Cl. G06F13/00

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2010
 Registered utility model specifications of Japan 1996-2010
 Published registered utility model applications of Japan 1994-2010

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008/0235358 A1 (Hirotaka MORIBE) 2008.09.25, par Nos[0093]-[0106], FIG.8 & JP 2008-236344 A	1-5
A	EP 1589691 A2 (MICROSOFT CORPORATION) 2005.10.26, par Nos[0025]-[0027], FIG.2 & JP 2005-310119 A & US 2005/0256973 A1 & DE 602005006654 D & KR 10-2006-0044411 A & CN 1691677 A & AT 395762 T	1-5



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

18.05.2010

Date of mailing of the international search report

25.05.2010

Name and mailing address of the ISA/JP

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan

Authorized officer

Tatsuya SUTO

Telephone No. +81-3-3581-1101 Ext. 3565

51

3051