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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/102454 A1

(51) International Patent Classification:
*G06F 21/00* (2006.01)

(21) International Application Number:
PCT/US2006/010474

(22) International Filing Date: 20 March 2006 (20.03.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/085,761 21 March 2005 (21.03.2005) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 11/085,761 (CON)
Filed on 21 March 2005 (21.03.2005)

(71) **Applicant** *(for all designated States except US)*: **MARVELL WORLD TRADE LTD.** [BB/BB]; L'horizon, Gunsite Road, Brittons Hill, St. Michael, BB14027 (BB).

(72) **Inventor; and**

(75) **Inventor/Applicant** *(for US only)*: **SUTARDJA, Sehat** [US/US]; 27330 Elena Road, Los Altos Hills, California 94022 (US).

(74) **Agents: WIGGINS, Michael D.** et al.; HARNESS, DICKEY & PIERCE, P.L.C., P.O. Box 828, Bloomfield Hills, MI 48303 (US).

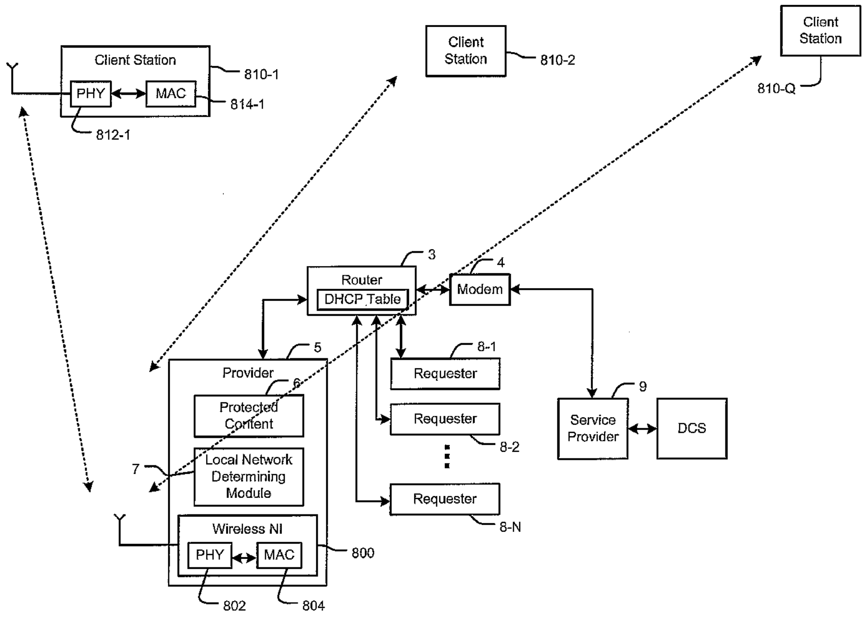
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, 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, 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).

**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*

*[Continued on next page]*

(54) **Title:** NETWORK SYSTEM FOR DISTRIBUTING PROTECTED CONTENT



(57) **Abstract:** A system for distributing content in a network comprises memory that stores content. A provider network device communicates with the memory and wirelessly communicates with a requester network device that requests a copy of the content. The provider network device determines a local/remote status of the requester network device, transmits a key request to the requester network device when the requester network device has a local status, receives a key from the requester network device, encrypts the content with the key and transmits the encrypted content to the requester network device.

WO 2006/102454 A1

# NETWORK SYSTEM FOR DISTRIBUTING PROTECTED CONTENT

## FIELD OF THE INVENTION

**[0001]** The present invention relates to networks, and more particularly to network systems that allow secure distribution of protected content.

## BACKGROUND OF THE INVENTION

**[0002]** Consumers often purchase video content on digital versatile discs (DVDs). A DVD player may be used to output the video content to a television (TV) or other video monitor. Some DVD players may include a carousel for allowing selection and play of one of a plurality of DVDs. In some situations, a consumer may want to view the DVD content on a first TV in one room of the consumer's home when the DVD player is located and connected to a second TV in another room. As a result, the DVD player needs to be disconnected from the second TV, moved to the room with the first TV and reconnected to the first TV. Alternately, if the consumer has a second DVD player, the consumer moves the DVD to the other player.

**[0003]** One possible solution to this problem involves copying the DVD content onto another DVD. DVD players typically include only one DVD player, which makes copying DVDs difficult. To copy the DVD, the user must copy the DVD contents to a hard drive system. Typically, copy protection schemes such as digital rights management (DRM) prevent such copying despite the fact that some copying may be allowed under the copyright laws. This is due, in part, to the fact that the data is decrypted and/or decoded by the DVD player and is therefore in an unprotected form when it is output to other devices. This solution also requires an additional DVD player.

## SUMMARY OF THE INVENTION

**[0004]** A system for distributing content in a network comprises memory that stores content. A provider network device communicates with the memory and wirelessly communicates with a requester network device that requests a copy of the content. The provider network device determines a local/remote status of the requester network device, transmits a key request to the requester network device when the requester network device has a local status, receives a key from the requester network device, encrypts the content with the key and transmits the encrypted content to the requester network device.

**[0005]** The provider network device at least one of receives and determines at least one of a signal quality estimate, a data rate estimate, a distance estimate and a direction estimate for a link and determines the local/remote status based on the at least one of the signal quality estimate, the data rate estimate, the distance estimate and the direction estimate.

**[0006]** In other features, the provider network device includes a digital versatile disc (DVD) system. The requester network device includes a hard disk drive (HDD) system. The provider network device includes a local network determining module that determines the local/remote status of the requester network device.

**[0007]** In other features, the HDD system comprises nonvolatile HDD memory that stores data in a nonvolatile manner and that includes a user accessible section and a hidden section. A hard disk drive control (HDD) module communicates with the HDD nonvolatile memory, selectively requests and receives content from the provider network device and stores the requested content in the hidden section of the nonvolatile HDD memory.

**[0008]** In other features, after sending the request to the provider network device, the HDD control module receives a key request and transmits a key to the provider network device in response to the key request. The requested content received by the HDD system from the provider network device is encrypted using the key. The HDD control module decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory. The HDD control module makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the nonvolatile HDD memory. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage.

**[0009]** In other features, the DVD system comprises nonvolatile memory that stores content. A DVD control module communicates with the nonvolatile memory and selectively receives requests for content from the requester network device. The DVD control module requests a key from the requester network device before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The DVD system encrypts the requested content before sending the requested content to the HDD system. The DVD control module includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies a number of allowable uses. The usage data specifies a duration of allowable usage.

**[0010]** The provider network device communicates with a wireless network interface including a physical layer device and a medium access control device. At least one of the physical layer device and the medium access control device generates the at least one of the signal quality estimate, the distance estimate, the direction estimate and the data rate estimate. The wireless network interface is associated with an access point.

**[0011]** A system for distributing content in a network comprises storing means for storing content. Provider network means communicates with the storing means and wirelessly communicates with a wireless requester network means that requests a copy of the content. The provider network means determines a local/remote status of the requester network means, sends a key request to the requester network means when the requester network means has a local status and receives a key from the requester network means, encrypts the content with the key and sends the encrypted content to the requester network means.

**[0012]** In other features, the provider network means at least one of receives and determines at least one of a signal quality estimate, a data rate estimate, a distance estimate and a direction estimate for a link and determines the local/remote status based on the at least one of the signal quality estimate, the data rate estimate, the distance estimate and the direction estimate. The provider network means includes a digital versatile disc (DVD) system. The requester network means includes a hard disk drive (HDD) system. The provider network means includes local network determining means for determining the local/remote status of the requester network means.

**[0013]** In still other features, the HDD system comprises nonvolatile HDD memory means for storing data in a nonvolatile manner and that includes a user accessible section and a hidden section. Hard disk drive control (HDD) means communicates with the HDD nonvolatile memory means, selectively requests and receives content from the provider network means and stores the requested content in the hidden section of the nonvolatile HDD memory means.

**[0014]** In other features, after sending the request to the provider network means, the HDD control means receives a key request and transmits a key to the provider network means in response to the key request. The requested content received by the HDD system from the provider network means is encrypted using the key. The HDD control means decrypts the requested content. The requested content includes usage data that is also written to the hidden portion of the nonvolatile HDD memory means and wherein the HDD control means makes the requested content unavailable when the usage data indicates allowable use is over. The HDD system deletes the requested content from the nonvolatile HDD memory means. The usage data specifies a predetermined number of allowable uses. The usage data specifies a duration of allowable usage.

**[0015]** In other features, the DVD system comprises nonvolatile memory means for storing content, and DVD control means that communicates with the nonvolatile memory means, for selectively receiving requests for content from the requester network means. The DVD control means requests a key from the requester network means before sending the requested content and determines an amount of time that is required to receive the key from the HDD system after sending the key request to the HDD system. The DVD control means encrypts the requested content before sending the requested content to the HDD system. The DVD control means includes usage data in the requested content that is transmitted to the HDD system. The usage data specifies at least one of a number of allowable uses and a duration of allowable usage.

**[0016]** In other features, wireless network interface means communicates with the provider network means for providing a wireless interface and includes physical layer means for providing a physical layer interface, and medium access control means for providing an interface between the physical layer means and a host. At least one of the physical layer means and the medium access control means generates the at least one of the signal quality estimate, the distance estimate, the direction estimate and the data rate estimate. The wireless network interface is associated with an access point.

**[0017]** Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0018]** The present invention will become more fully understood from the detailed description and the accompanying drawings, wherein:

**[0019]** FIG. 1 is a functional block diagram of a provider network device that provides protected digital content to one or more requester network devices in a local network;

**[0020]** FIG. 2 is a functional block diagram of a first exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

**[0021]** FIG. 3 is a functional block diagram of a second exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

**[0022]** FIG. 4 is a functional block diagram of a third exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

**[0023]** FIG. 5 is a functional block diagram of a fourth exemplary networked DVD and HDD system according to the present invention that communicates with a modem;

**[0024]** FIG. 6 is a functional block diagram of an exemplary requester network device including a HDD system;

**[0025]** FIG. 7A is a functional block diagram of an exemplary provider network device including a DVD system with read-only operation;

**[0026]** FIG. 7B is a functional block diagram of an exemplary provider network device including a DVD system with read-write operation;

**[0027]** FIG. 7C is a functional block diagram of a provider or requester network device that includes a combined DVD/HDD system;

**[0028]** FIG. 8 illustrates user accessible and hidden sections of nonvolatile memory of the HDD of FIG. 6;

**[0029]** FIGs. 9A-9D are flowcharts illustrating security steps performed by the provider and/or requester network devices;

**[0030]** FIG. 10 is a flowchart illustrating steps of a method for allowing playback of a copy protected file from the requester network device N times;

**[0031]** FIG. 11 is a flowchart illustrating steps of a method for limiting the amount of time that a copy protected file stored on the requester network device can be played;

**[0032]** FIG. 12A is a functional block diagram of a network including a media server that serves protected content from a provider to a requester;

**[0033]** FIG. 12B is a functional block diagram of a network including a media server that serves protected content from a DVD system to a HDD system;

**[0034]** FIG. 13 illustrates the media server in an exemplary network configuration;

**[0035]** FIG. 14 is a flowchart illustrating steps performed by the media server according to the present invention;

**[0036]** FIG. 15 is a functional block diagram of a provider network device that determines a local/remote status of a wireless network device such as a client station;

**[0037]** FIGs. 16A-16E are functional block diagrams of a physical layer device of a wireless network device such as an access point or wireless network interface;

**[0038]** FIG. 17 is a functional block diagram of a provider network device that includes a wireless network interface;

**[0039]** FIG. 18A is a functional block diagram of a requester wireless network device that communicates with a provider network device via one or more repeaters;

**[0040]** FIG. 18B is a flowchart illustrating steps of an exemplary method for identifying whether a requesting wireless network device is communicating via one or more repeaters; and

**[0041]** FIG. 19 is a flowchart illustrating steps performed by a requester network device for selectively removing restrictions.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

**[0042]** The following description of the preferred embodiment(s) is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses. As used herein, the term module or device refers to an application specific integrated circuit (ASIC), an electronic circuit, a processor (shared, dedicated, or group) and memory that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable components that provide the described functionality. For purposes of clarity, the same reference numbers will be used in the drawings to identify similar elements.

**[0043]** Referring now to FIG. 1, a local network 2 includes a router 3, a modem 4, and a provider network device 5, which selectively provides protected content 6 to one or more local requester network devices as will be described below. The provider network device 5 is a network compatible device that includes a local network determining module 7. One or more requester network devices 8-1, 8-2, ... and 8-N (collectively referred to as requesters 8) selectively request copies of the protected content 6. As can be appreciated, while the router 3 and wire line connections are shown, other network configurations will be apparent to skilled artisans including but not limited to wireless Access Points (AP), ad-hoc network connection configurations, and/or wireless network configurations. While the provider network device 5 is shown to include memory such as nonvolatile memory for the protected content 6, the protected content 6 may be stored internally and/or externally from the provider network device 5.

**[0044]** The modem 4 is connected to a broadband service provider 9, which provides video content, digital content, a broadband connection to a distributed communications system (DCS) 10, and/or other network services. The service provider 9 may provide broadband access using wired or wireless connections, coaxial cable, digital subscriber line (DSL), satellite and/or any other connection system or method.

**[0045]** The DCS 10 is connected by one or more servers 11-1, 11-2, ..., and 11-M to network devices 12-11, 12-12, ..., 12-1P, 12-21, 12-22, ..., 12-2P, ..., and 12-M1, 12-M2, ..., 12-MP (collectively referred to as network devices 12). The local network determining module 7 selectively determines whether the requester network device has a local or remote status when the requester network device requests a copy of the protected content 6. This approach increases security by preventing access to the protected content by remote network devices.

**[0046]** There are many different ways for the local network determining module 7 to determine the local/remote status of a requester network device. For example in some implementations, the provider network device 5 determines local/remote status by determining the amount of time that is required to receive a response from the requester network device. If the response time is less than a predetermined period, then the requester network device is determined to have a local status. If not, the requester network device has a remote status and the copy of the protected content is denied. The amount of time that is required to send and receive data via the service provider 9, DCS 10 and servers 11 to the remote network devices 12 is significantly greater than the amount of timer required by a local requester network device to respond. In other words, the predetermined period is set greater than the response time required by local requester network devices and less than the response time required by remote requester network devices.

**[0047]** In other implementations, the provider network device checks a dynamic host configuration protocol (DHCP) table in a DHCP server to determine medium access control (MAC) addresses of local network devices. If the requester network device matches a local MAC address in the table, then the requester network device has a local status and the copy of the protected content can be sent. If not, the requester network device has a remote status and the copy of the protected content is not sent.

**[0048]** In still other implementations, the provider network device 5 may send a message to the router 3 to temporarily block external ports of the router 3 or modem 4 to the service provider 9 (and DCS 10). After blocking the external ports, the provider network device 5 determines whether the requester network device is still able to communicate (which will be true if the requester network device has a local status). If the provider network device can communicate with the requester networkrequester network device, the provider network device sends the copy protected content. As can be appreciated by skilled artisans, one or more of these approaches may be combined and/or other approaches may be used to determine the local/remote status of the requester network device.

**[0049]** While portions of the following description employ a DVD system and/or a combined DVD/HDD system as the provider network device and another network device including a combined DVD/HDD system and/or a HDD system as the requester network device, skilled artisans will appreciate that other provider and/or requester network devices may be used. Skilled artisans will also appreciate that all of the implementations that are described below in conjunction with DVD and HDD systems can be implemented with any other suitable network devices.

**[0050]** Referring now to FIG. 2, a functional block diagram of a first exemplary networked DVD and HDD system is shown. A local network 13 includes a modem 14 that communicates over medium 16 with a service provider 18. The service provider 18 provides a connection to a distributed communications system (DCS) 22 such as the Internet, LAN, WAN, or other distributed network and/or provides other network services such as video content, telephone services and the like. The modem 14 can be connected to a router 28, which connects multiple network devices 30-1, 30-2, ..., and 30-N (collectively network devices 30) to the modem 14. One of the network devices 30-1 is connected to a hard disk drive (HDD) system 34, which may be connected to a television or monitor 38. The television or monitor 38 may also be connected to the medium 16 either directly or through a set top box (not shown) and receive content from the service provider 18.

**[0051]** The local network 13 may include an access point (AP) 40 that communicates with the router 28 and one or more wireless stations 42-1, 42-2, ..., and 42-N (collectively wireless stations 42). While the AP 40 is shown connected to the router 28, the AP and router functions may be combined in a single device. Alternately, a combined AP/router may be directly connected to the modem 14. Still other types of network configurations and connections will be apparent to skilled artisans.

**[0052]** The network device 30-2 communicates with the router 28 and with a DVD player or a combined DVD/HDD player 44 (both referred to hereinafter as "DVD player 44") such as the one shown and described in U.S. Patent Application Serial No. 11/039,288, filed January 19, 2005, which is hereby incorporated by reference in its entirety. The DVD player 44, in turn, may communicate with a television or monitor 46, which may be connected to the medium 16 or to a set top box 50. The service provider 18 provides broadband access to the DCS 22, video content and/or other services. One or more other servers 54-1 and 54-2, (collectively servers 54) provide an interface for network devices 60, computers 62, personal digital assistants (PDAs), etc. to the DCS 22.

**[0053]** In some implementations, the user of the television or monitor 38 may desire access to DVD content associated with the DVD player 44. Initially, the HDD 34 may request a list of available content from the DVD player. The DVD sends a list of available content. The HDD 34 sends a message to the DVD player 44 via the network requesting a copy of content selected from the list. The DVD system determines whether the HDD system has a local status. If the HDD system or other requester network device has local status, the content file is sent. If the HDD system or other requester network device has a remote status, the request is denied. The local/remote status determination can be made based upon response time, MAC addresses in the DHCP table, external port disconnection and corresponding dialogue, and/or other suitable methods.

**[0054]** In some implementations, the DVD 44 responds by requesting a key from the HDD 34. The DVD 44 begins a timer that determines the amount of time that is required by the HDD 34 to respond. The HDD 34 sends the requested key to the DVD 44. The DVD 44 determines whether the HDD 34 responded within a predetermined amount of time.

**[0055]** If the HDD 34 responds within the predetermined amount of time, the DVD 44 scrambles the selected content with the key and sends the scrambled content over the network to the HDD 34. The HDD 34 descrambles the content with the key and allows replay of the content at the television or monitor 38. As can be appreciated, the key exchange can also occur earlier when the HDD initially requests the list of available content.

**[0056]** The HDD 34 may also receive usage data from the DVD player that constrains use. For example, the usage data may allow N replays and/or replay for a predetermined period. After the allowed usage period is over as specified in the usage data, the HDD 34 makes the video content unavailable. For example, the HDD may delete the video content.

**[0057]** In some implementations, the HDD 34 includes a user accessible section and a hidden section. The video content from the DVD 44 is stored in the hidden section of the DVD 44. The key that is provided by the HDD 34 may be part of a public/private key encryption system and/or other suitable data encryption. Alternately other forms of key-based scrambling can be performed.

**[0058]** If the DVD player is a single DVD player, the DVD sends a list of content available on the DVD in the DVD player. If the DVD player includes a carousel, the DVD player sends a list of DVD content available from DVDs in the carousel. If the DVD player is a combined DVD/HDD player, the DVD/HDD player sends a list of DVD content available on the DVD or DVDs in the player along with DVD content stored on the associated HDD.

**[0059]** Referring now to FIGs. 3-5, various exemplary configurations of the present invention are shown. In these implementations, the provider network device includes a DVD system and/or a combined DVD/HDD system and the requester network device includes a HDD system and/or a combined DVD/HDD system. In FIG. 3, the HDD 34 is connected to the network by the station 42-1, which wirelessly communicates with the AP 40. The DVD 44 and television 46 are connected by the network device 30-2 and medium 16 to the router 28. In FIG. 4, the HDD 34 is connected by the network device 30-1 and medium 16 to the router 28. The DVD 44 is connected to the network by the station 42-2, which wirelessly communicates with the AP 40. In FIG. 5, the HDD 34 and DVD 44 are connected by one or more stations 42-1 and/or 42-2 to the network. Various other network configurations will be apparent to skilled artisans.

**[0060]** Referring now to FIG. 6, an exemplary requester network device includes a HDD system 110 with a HDD PCB 114. A buffer 118 stores read, write and/or volatile control data that is associated the control of the HDD system 110. The buffer 118 usually employs volatile memory having low latency. For example, SDRAM or other types of low latency memory may be used. Nonvolatile memory 119 such as flash memory may also be provided to store critical data such as nonvolatile control code.

**[0061]** A processor 122 arranged on the HDD PCB 114 performs data and/or control processing that is related to the operation of the HDD system 110. A hard disk control module (HDC) 126 communicates with an input/output interface 124 and with a spindle/voice coil motor (VCM) driver or module 130 and/or a read/write channel module 134. The HDC 126 coordinates control of the spindle/VCM driver 130, the read/write channel module 134 and the processor 122 and data input/output with a host 135 via the interface 124.

**[0062]** During write operations, the read/write channel module 134 encodes the data to be written onto a read/write device 159. The read/write channel module 134 processes the write signal for reliability and may apply, for example, error correction coding (ECC), run length limited coding (RLL), and the like. During read operations, the read/write channel module 134 converts an analog read signal output of the read/write device 159 to a digital read signal. The converted signal is then detected and decoded by known techniques to recover the data that was written on the HDD.

**[0063]** A hard disk drive assembly (HDDA) 150 includes one or more hard drive platters 152 that include magnetic coatings that store magnetic fields. The platters 152 are rotated by a spindle motor that is schematically shown at 154. Generally the spindle motor 154 rotates the hard drive platter 152 at a controlled speed during the read/write operations. One or more read/write arms 158 move relative to the platters 152 to read and/or write data to/from the hard drive platters 152. The spindle/VCM driver 130 controls the spindle motor 154, which rotates the platter 152. The spindle/VCM driver 130 also generates control signals that position the read/write arm 158, for example using a voice coil actuator, a stepper motor or any other suitable actuator.

**[0064]** The read/write device 159 is located near a distal end of the read/write arm 158. The read/write device 159 includes a write element such as an inductor that generates a magnetic field. The read/write device 159 also includes a read element (such as a magneto-resistive (MR) element) that senses the magnetic field on the platter 152. The HDDA 150 includes a preamp circuit 160 that amplifies the analog read/write signals. When reading data, the preamp circuit 160 amplifies low level signals from the read element and outputs the amplified signal to the read/write channel module 134. While writing data, a write current is generated that flows through the write element of the read/write device 159. The write current is switched to produce a magnetic field having a positive or negative polarity. The positive or negative polarity is stored by the hard drive platter 152 and is used to represent data.

**[0065]** Referring now to FIGs. 7A and 7B, an exemplary provider network device includes a DVD system 210. A DVD PCB 214 includes a buffer 218 that stores read data, write data and/or volatile control code that is associated the control of the DVD system 210. The buffer 218 may employ volatile memory such as SDRAM or other types of low latency memory. Nonvolatile memory 219 such as flash memory can also be used for critical data such as data relating to DVD write formats and/or other nonvolatile control code. A processor 222 arranged on the DVD PCB 214 performs data and/or control processing that is related to the operation of the DVD system 210. The processor 222 also performs decoding of copy protection and/or compression/decompression as needed. A DVD control module 226 communicates with an input/output interface 224 and with a spindle/feed motor (FM) driver 230 and/or a read/write channel module 234. The DVD control module 226 coordinates control of the spindle/FM driver, the read/write channel module 234 and the processor 222 and data input/output via the interface 224.

**[0066]** During write operations, the read/write channel module 234 encodes the data to be written by an optical read/write (ORW) or optical read only (OR) device 259 to the DVD platter. The read/write channel module 234 processes the signals for reliability and may apply, for example, ECC, RLL, and the like. During read operations, the read/write channel module 234 converts an analog output of the ORW or OR device 259 to a digital signal. The converted signal is then detected and decoded by known techniques to recover the data that was written on the DVD.

**[0067]** A DVD assembly (DVDA) 250 includes a DVD platter 252 that stores data optically. The platter 252 is rotated by a spindle motor that is schematically shown at 254. The spindle motor 254 rotates the DVD platter 252 at a controlled and/or variable speed during the read/write operations. The ORW or OR device 259 moves relative to the DVD platter 252 to read and/or write data to/from the DVD platter 252. The ORW or OR device 259 typically includes a laser and an optical sensor.

**[0068]** For DVD read/write and DVD read only systems, the laser is directed at tracks on the DVD that contain lands and pits during read operations. The optical sensor senses reflections caused by the lands/pits. In some DVD read/write (RW) applications, a laser may also be used to heat a die layer on the DVD platter during write operations. If the die is heated to one temperature, the die is transparent and represents one binary digital value. If the die is heated to another temperature, the die is opaque and represents the other binary digital value. Other techniques for writing DVDs may be employed.

**[0069]** The spindle/FM driver 230 controls the spindle motor 254, which controllably rotates the DVD platter 252. The spindle/FM driver 230 also generates control signals that position the feed motor 258, for example using a voice coil actuator, a stepper motor or any other suitable actuator. The feed motor 258 typically moves the ORW or OR device 259 radially relative to the DVD platter 252. A laser driver 261 generates a laser drive signal based on an output of the read/write channel module 234. The DVDA 250 includes a preamp circuit 260 that amplifies analog read signals. When reading data, the preamp circuit 260 amplifies low level signals from the ORW or OR device and outputs the amplified signal to the read/write channel module device 234.

**[0070]** The DVD system 210 further includes a codec module 240 that encodes and/or decodes video such as any of the MPEG formats. Audio and/or video digital signal processors and/or modules 242 and 244, respectively, perform audio and/or video signal processing, respectively.

**[0071]** As with the HDD system 110, portions of the DVD system 210 may be implemented by one or more integrated circuits (IC) or chips. For example, the processor 222 and the DVD control module 226 may be implemented by a single chip. The spindle/FM driver 230 and/or the read/write channel module 234 may also be implemented by the same chip as the processor 222, the DVD control module 226 and/or by additional chips. Most of the DVD system 210 other than the DVDA 250 may also be implemented as a SOC.

**[0072]** Referring now to FIG. 7C, a simplified functional block diagram of an exemplary combined DVD/HDD system 280 according to some implementations of the present invention is shown. The combined DVD/HDD system can be used as a provider or requester network device. The combined DVD/HDD system 280 includes a combined system control module 284 that communicates with nonvolatile memory 290 and volatile memory 292, which stored data for both DVD and HDD operation. The system control module 284 communicates via an interface 294 with an interface 296 of a host 298. In some implementations, the interfaces 294 and 296 are serial ATA interfaces, Fiber Channels (FC), serial attached small computer system interfaces (SAS), or other suitable interfaces.

**[0073]** The combined DVD/HDD system controls both DVD and HDD systems. The DVD/HDD system reduces overall system cost and provides improved functionality and performance. Cost is reduced through the use of a single DRAM and flash memory for both the DVD and HDD data storage. A single power supply and a reduced number of external connections are required, which further reduces cost.

**[0074]** In addition, the unified DVD/HDD system allows copy protected content to be copied bit-by-bit to directly to the HDD. In other words, the copy protected content can be copied without decrypting the copy protection scheme or digital rights management (DRM) and without requiring significant operating system involvement. Conventional separate DVD and HDD systems require the DVD to decode/decrypt the DRM or other copy protection prior to output. The DRM or other copy protection may or may not allow subsequent copying to the HDD. By combining the systems, additional functionality is provided due to the built-in security of the copy protection or DRM scheme since the DRM or copy protection remains intact. For example, single DVD drive copy operations are supported without removal of the copy protection or DRM. Additionally, the HDD can operate as a virtual DVD changer. Still other variations of the combined DVD/HDD system are shown and described in U.S. Patent Application Serial No. 11/039,288, filed on January 19, 2005.

**[0075]** Referring now to FIG. 8, partitioning of the nonvolatile memory 300 of the HDD into user accessible and hidden areas according to some implementations is shown. The nonvolatile memory 300 of the HDD is allocated into a first portion 304 that is user accessible and a second portion 308 that is not user accessible (or hidden). The second hidden portion 308 is used in one or more of the following ways according to some implementations of the invention. The hidden portion 308 is used to store the contents of a DVD that is to be copied. In addition, the hidden portion 308 of the HDD is used to provide a virtual DVD carousel. In other words, multiple DVDs may be copied to the HDD and played back at a later date.

**[0076]** Referring now to FIG. 9A, steps performed by the network devices are shown. Control begins in step 350. In step 352, control determines whether the provider network device receives a request for a copy of protected content. If not, control returns to step 352. If step 352 is true, control determines whether the requester network device is located on the local network in step 354.

If step 354 is false, control denies the request and returns to step 352. If step 354 is true, the provider network device sends a copy of the protected content to the requester network device.

**[0077]** The provider network device determines whether the requester network device is on the local network in any suitable fashion. For example, a response time of the requester network device can be compared to a predetermined threshold. In other implementations, the provider network device can temporarily request that the external ports of the router or modem be blocked so that the provider network device can confirm the local/remote status of the requester network device before the file sent. In other implementations, a local server can be queried to determine the local network devices. Still other methods for determining local/remote status may be used.

**[0078]** Referring now to FIG. 9B, steps for determining local/remote status by temporarily blocking an external port are shown. Control begins with step 360. In step 362, control determines whether the provider network device receives a request for a copy protected file. If step 362 is false, control returns to step 362. If step 362 is true, control continues with step 364 where the provider network device requests the external ports of the router or modem to be blocked. In step 368, the provider network device determines whether the requester network device has a local status. For example, the provider network device may send a message to the requester network device and wait for a response. If step 368 is false, the provider network device denies the request and control returns to step 362. If step 368 is true, the provider network device sends a copy of the file to the requester network device in step 370. The provider network device unblocks the external connection or port of the router or modem in step 374.

**[0079]** Referring now to FIG. 9C, steps for consulting a local server (such as a DHCP server) to determine the local/remote status are shown. Control begins with step 380. In step 382, control determines whether the provider network device receives a request for a copy protected file. If step 382 is false, control returns to step 382. If step 382 is true, control continues with step 384 where the provider network device queries the server for identification of local network devices. The identification can include MAC addresses although other identification types can be used. In step 386, the provider network device determines whether the requester network device has a local status. If step 386 is false, the provider network device denies the request and control returns to step 382. If step 386 is true, the provider network device sends a copy of the file to the requester network device in step 388.

**[0080]** Referring now to FIG. 9D, steps performed by the network system are shown generally at 400. In step 402, control begins. In step 404, the provider network device determines whether a requester network device requests a copy of the content. If not, control returns to step 404. Otherwise control continues with step 408 and the provider network device requests a key from the requester network device. In step 412, the provider network device starts a timer.

**[0081]** In step 416, the provider network device determines whether the key is received. If the key is not received and (in some implementations) the predetermined period has not been exceeded, control continues with step 416. Otherwise, control continues with step 420 and the provider network device stops the timer. In step 422, control determines whether the timer is less than a predetermined period.

**[0082]** In some implementations, the predetermined period is less than or equal to the amount of time that a packet would require to travel one or two hops. By limiting the response time, additional security is provided. The amount of time that would be required for a computer or other device outside of the home network to respond will exceed the predetermined period. In other words, a packet containing a key from a computer such as computer 62 or other network device such as network device 60 that is connected outside of the home network will exceed one or two hops. This is due to the time required to pass through the modem and the service provider.

**[0083]** If step 422 is false, control returns to step 404. If step 422 is true, the provider network device encrypts or scrambles the content with the key and sends the encrypted or scrambled content over the network to the requesting device in step 426 and control continues with step 404.

**[0084]** Referring now to FIG. 10, steps of a method for allowing playback of a copy protected file from the requester network device N times are shown. Control begins with step 600. In step 602, control determines whether copy protected files have been stored on the requester network device. If not, control returns to step 602. It step 602 is true, control sets N=1 for the file in step 604. In step 606, control determines whether the copy protected file stored on requester network device has been played. If step 606 is false, control returns to step 606. If step 606 is true, control increments N in step 610. In step 614, control determines whether N = $N_{max}$. If step 614 is false, control returns to step 606. If step 614 is true, control deletes or otherwise makes the copy protected file unavailable from the requester network device in step 618 and control returns to step 602.

**[0085]** Referring now to FIG. 11, steps of a method for limiting the amount of time that a copy protected file stored on the requester network device can be played are shown. Control begins with step 640. In step 644, control determines whether the copy protected file has been stored on the requester network device. If step 644 is false, control returns to step 644. Otherwise, control continues with step 646 and sets a timer. In step 648, control determines whether the timer is up. If step 648 is false, control returns to step 648. If step 648 is true, control deletes the copy protected file from the requester network device in step 652 and control continues with step 644. While a timer is described, any usage measurement and/or comparison may be performed. For example, a date and/or time stamp may be used and compared to current data and/or time. Still other usage data types will be apparent to skilled artisans.

**[0086]** Referring now to FIG. 12A, a media server 700 can be used to serve protected content from a provider 702 to a requester 704. While a router is shown connecting the media server 700, the provider 702 and the requester 704, other network configurations and connections may be used such as but not limited to ad-hoc network modes, peer to peer modes, and other approaches. In some implementations, the media server includes a local/remote status determining module 701, as previously described above. The media server 700 provides a list of available content to the requester 704. The requester 704 requests content. The media server 700 confirms that the requester is on the local network in any of the ways described above. If the requester 704 is on the local network, the media server 700 requests the content from the provider 702. The provider 702 sends the content directly to the requester 704 or to the the media server 700, which sends the content to the requester 704.

**[0087]** Referring now to FIGs. 12B and 13, the media server 700 serves protected content from a DVD system 710 to a HDD system 712. The DVD system 710 and the HDD system 712 can be implemented as described in the embodiments set forth above. In FIG. 13, the media server 700 can be implemented in a network as shown. Other network configurations such as those described herein as well as other network configurations are contemplated. The media server can be connected to the network in a wired or wireless manner.

**[0088]** Referring now to FIG. 14, a flowchart illustrating steps performed by the media server according to the present invention are shown. Control begins in step 720. In step 722, control determines whether the server receives a request for a copy of a protected file from the requester. If false, control returns to step 722. If true, the media server determines whether the requester has a local status. The local status of the requester may be determined in any of the ways described above. If true, the server requests the file from the provider and sends the file to the requester. Alternately, the provider may send the file directly to the requester.

**[0089]** Referring now to FIG. 15, a provider network device 5 determines a local/remote status of a wireless network device that is requesting protected content. The provider network device 5 may communicate with an access point 800 via the router 3. The access point 800 may include a physical layer (PHY) device 802, which provides an interface with the wireless medium, and a medium access control (MAC) device 804, which provides an interface between the physical layer device 802 and a host device.

**[0090]** The physical layer device 802 may determine at least one of a link speed of a link with a client station, a signal quality of a link with the client station, a link distance to the client station and/or a link direction to the client station. The wireless access point 800 includes an antenna system 805 that may include one or more antennas. For example, the antenna system may be a multiple-in, multiple out (MIMO) antenna system. If multiple antennas are used, the physical layer device 802 may selectively determine a direction that the client station is located with respect to the access point 800 and forward the direction information to the provider network device 5. The physical layer device 802 may determine the direction based on triangulation techniques and/or using other approaches.

**[0091]** For example, the wireless network device may include a client station 810-1. The client station 810-1 includes a physical layer (PHY) device 812-1, which provides an interface with the wireless medium. The client station 810-1 also includes a medium access control (MAC) device 814-1, which provides an interface between the physical layer device 812-1 and a host such as a laptop, personal digital assistant and/or any other suitable device. Additional client stations 812-2 and 812-3 (collectively client stations 812) also may establish wireless links with the wireless access point 800. The wireless access point 800 may also determines link speed, signal quality, link distance and/or link direction with the client stations 812-2 and 812-3 when they request access to protected content.

**[0092]** The wireless access point 800 may selectively transmit the link speed, signal quality, link distance and/or link direction for the corresponding client stations 810 to the local network determining module 7. The local network determining module 7 compares the link speed, signal quality, link distance and/or link direction with a predetermined threshold and/or adaptive threshold and makes a decision as to whether the particular client station 810 is local or remote. If the client station 810 is local, the protected content may be sent to the client station 810 as described above. If the client station 810 is remote, the protected content is not sent to the client station 810 and/or further verification steps may be performed.

**[0093]** The link speed and/or signal quality of the link between the wireless access point 800 and the client station 810 tends to decrease as a function of a distance between the wireless access point 800 and the client station 810. Therefore, when the client station 810 requests access to protected content (requester networkrequester network device), the provider network device can evaluate whether the client station is local or remote. Thus, the provider network device 5 can limit fraudulent requests for the protected content. While the exemplary embodiment shown in FIG. 15 relates to an infrastructure mode wireless network, an ad-hoc mode wireless network can also be used.

**[0094]** Referring now to FIG. 17, the provider network device 5 can include a wireless network interface 850, which includes a physical layer device 852 and a medium access control (MAC) device 854. The wireless network interface 850 can operate as an access point/router in an infrastructure mode, as a client station in an ad-hoc configuration, and/or in any other suitable network configuration.

**[0095]** FIGs. 16A-16E are functional block diagrams of exemplary physical layer devices for wireless network devices such as an access point or wireless network interface. The physical layer device 802 may include a link rate determining module 820 as shown in FIG. 16A. The link rate determining module 820 determines the link rate that data is transmitted by the client station 810 to the access point 800 and forwards the link rate information to the provider network device 5. The physical layer device 802 may include a link signal quality determining module 830 as can be seen in FIG. 16B that estimates the signal quality of the link and forwards the signal quality information to the provider network device. Signal quality can be estimated based on a received signal strength indicator (RSSI), bit or packet error rates and/or other suitable criteria.

**[0096]** In FIG. 16C, the physical layer device 802 may include a link direction determining module 840. The link direction determining module 840 may use triangulation (for example using multiple antennas) and/or other techniques to determine a direction that the client station is located relative to the physical layer device 802. The physical layer device 802 forwards the link direction information to the local network determining module 7. For example, the access point may be located adjacent to an outer wall of a building. If a client station 810 is located in a direction that would be inside of the building, then additional speed, distance and/or signal quality determinations can be made to determine whether the client station is local or remote. However, if the client station 810 is located in a direction that would be outside of the building, the client station 810 can be classified as remote without further analysis. The link direction, link distance, link signal quality and/or link data rate estimates can also be estimated in the medium access control (MAC) device of the access point, network interface and/or in the provider network device.

**[0097]** In FIG. 16D, the physical layer device 802 may include a link distance determining module 850 that estimates a distance to the client station 810. The distance may be estimated based on the amount of time required to send and/or receive data between the access point 800 and client station 810.

**[0098]** In FIG. 16E, the physical layer device may generate 802 two or more of the link direction, link speed, link distance and link signal quality estimates. The provider network device may determine a local/remote status based on two or more of the estimates.

**[0099]** Referring now to FIGs. 18A and 18B, the provider network device may determine the local/remote status of a requesting wireless network device by determining whether the signal from the requesting wireless network device was received via a repeater and/or more than R repeaters, where R is an integer greater than one. The use of one or more repeaters may be an indication that the requesting wireless network device does not have a local status.

**[00100]** In FIG. 18A, a requester wireless network device 900 communicates with a provider network device 910 via one or more repeaters 902-1, ..., and 902-R, where R is an integer greater than 0. In this exemplary implementation, the provider network device 910 communicates with the requesting wireless network device 900 in an infrastructure mode via an access point 904 and a router 906. However, an ad-hoc mode may also be used. The provider network device 910 determines whether the requester network device is communicating via one or more repeaters and/or the number of repeaters that are being used. The provider network device 910 determines a local/remote status of the requester network device based on the repeater determination.

[00101] For example, some provider network devices may determine that the requester network device is remote if any repeaters are used. In other exemplary networks, the provider network device may determine the requester network device is remote if more than R repeaters are used, where R is greater than one. The provider network device 910 may sense whether repeaters are used using any suitable method. For example. The provider network device may use a time required for acknowledgement (ACK) from the requester network device as one criterion.

[00102] In FIG. 18B, is a flowchart illustrating steps of an exemplary method for identifying whether a requesting wireless network device is communicating via one or more repeaters. Control begins with step 920. In step 924, control determines whether the local or remote status of a requester network device needs to be determined. If true, control continues with step 926 and starts a timer.

[00103] In step 928, control sends a message to a requester network device. In step 930, control determines whether an acknowledgment (ACK) has been received from the requester network device. If not, control determines whether the timer is less than a maximum threshold $T_{thmax}$ in step 934. If true, control returns to step 930. It step 930 is true, control stops the timer in step 940. In step 942, control determines whether the timer is less than a second threshold $T_{th}$. If true, control continues with step 944 and sets the status equal to local for the requester network device. It step 942 is false or step 934 is false, control continues with step 946 and sets the status of the requester network device equal to remote. Control ends in step 950.

[00104] Referring now to FIG. 19, steps of the method for operating the requester network device are shown. The requester network device may initially request access to content that may be rented by a provider network device. When the restrictions relating to the content expire at the requester network device, the requester network device may request access to the content again. If the provider network device grants access M times, where M is an integer greater than or equal to 2, it may be fair to assume that the provider network

device now has ownership of the content and unlimited access by the requester network device may be acceptable.

**[00105]** Control begins with step 960. In step 964, control determines whether the requester network device has received content with restrictions. If step 964 is true, control continues with step 966 and stores the restrictions. Control sets a counter N=1. In step 970, control applies the restrictions. In step 974, control determines whether the restrictions have expired. If false, control returns to step 974. Otherwise, control continues with step 978 and determines whether the user requests the same content again. If not, control returns to step 978. It step 978 is true, control determines whether the requester network device receives approval. If true, control increments N in step 986. In step 990, control determines whether N is greater than or equal to M, where M is an integer greater than or equal to 2. If step 990 is false, control returns to step 970 continues to apply the restrictions. In step 990 is true, control continues with step 994 and removes the restrictions for the content.

**[00106]** Those skilled in the art can now appreciate from the foregoing description that the broad teachings of the present invention can be implemented in a variety of forms. Therefore, while this invention has been described in connection with particular examples thereof, the true scope of the invention should not be so limited since other modifications will become apparent to the skilled practitioner upon a study of the drawings, the specification and the following claims.

## CLAIMS

What is claimed is:

1. A system for distributing content in a network, comprising:

memory that stores content;

a provider network device that communicates with said memory and wirelessly communicates with a requester network device that requests a copy of said content,

wherein said provider network device determines a local/remote status of said requester network device, transmits a key request to said requester network device when said requester network device has a local status and receives a key from said requester network device, encrypts said content with said key and transmits said encrypted content to said requester network device.

2. The system of Claim 1 wherein said provider network device at least one of receives and determines at least one of a signal quality estimate, a data rate estimate, a distance estimate and a direction estimate for a link and determines said local/remote status based on said at least one of said signal quality estimate, said data rate estimate, said distance estimate and said direction estimate.

3. The system of Claim 1 wherein said provider network device includes a digital versatile disc (DVD) system.

4. The system of Claim 1 further comprising said requester network device wherein said requester network device includes a hard disk drive (HDD) system.

5. The system of Claim 4 wherein said HDD system comprises:

nonvolatile HDD memory that stores data in a nonvolatile manner and that includes a user accessible section and a hidden section; and a hard disk drive control (HDD) module that communicates with said HDD nonvolatile memory, that selectively requests and receives content from said provider network device and that stores said requested content in said hidden section of said nonvolatile HDD memory.

6. The system of Claim 5 wherein after sending said request to said provider network device, said HDD control module receives a key request and transmits a key to said provider network device in response to said key request, wherein said requested content received by said HDD system from said provider network device is encrypted using said key.

7. The system of Claim 6 wherein said HDD control module decrypts said requested content.

8. The system of Claim 5 wherein said requested content includes usage data that is also written to said hidden portion of said nonvolatile HDD memory and wherein said HDD control module makes said requested content unavailable when said usage data indicates allowable use is over.

9. The system of Claim 8 wherein said HDD system deletes said requested content from said nonvolatile HDD memory.

10. The system of Claim 8 wherein said usage data specifies a predetermined number of allowable uses.

11. The system of Claims 8 wherein said usage data specifies a duration of allowable usage.

12. The system of Claim 3 wherein said DVD system comprises:

nonvolatile memory that stores content; and a DVD control module that communicates with said nonvolatile memory, and that selectively receives requests for content from said requester network device.

13. The system of Claim 12 wherein said DVD control module determines an amount of time that is required to receive said key from said HDD system after sending said key request to the HDD system.

14. The system of Claim 13 wherein said DVD system sends said requested content to said HDD system if said key is received within a predetermined period.

15. The system of Claim 14 wherein said DVD system encrypts said requested content before sending said requested content to the HDD system.

16. The system of Claim 15 wherein said DVD control module includes usage data in said requested content that is transmitted to the HDD system.

17. The system of Claim 16 wherein said usage data specifies a number of allowable uses.

18. The system of Claim 16 wherein said usage data specifies a duration of allowable usage.

19. The system of Claim 2 further comprising a wireless network interface including a physical layer device and a medium access control device, and wherein at least one of said physical layer device and said medium access control device generates said at least one of said signal quality estimate, said distance estimate, said direction estimate and said data rate estimate.

20. The system of Claim 19 wherein said wireless network interface is associated with an access point.

21. A method for distributing content in a network, comprising:

storing content in memory of a provider network device;

wirelessly communicating with a wireless requester network device that requests a copy of said content;

determining a local/remote status of said requester network device;

transmitting a key request to said requester network device when said requester network device has a local status;

receiving a key from said requester network device;

encrypting said content with said key; and

transmitting said encrypted content to said requester network device.

22. The method of Claim 21 further comprising:

at least one of receiving and determining at least one of a signal quality estimate, a data rate estimate, a distance estimate and a direction estimate for a link; and

determining said local/remote status based on said at least one of said signal quality estimate, said data rate estimate, said distance estimate and said direction estimate.

23. The method of Claim 21 wherein said provider network device includes a digital versatile disc (DVD) system.

24. The method of Claim 21 wherein said requester network device includes a hard disk drive (HDD) system.

25. The method of Claim 24 further comprising:

storing data in a nonvolatile manner in nonvolatile HDD memory that includes a user accessible section and a hidden section;

selectively requesting and receiving content from said provider network device; and storing said requested content in said hidden section of said nonvolatile HDD memory.

26. The method of Claim 25 further comprising:

receiving a key request and transmitting a key to said provider network device in response to said key request after sending said request to said provider network device; and

encrypting said requested content received by said HDD system from said provider network device is using said key.

27. The method of Claim 26 further comprising decrypting said requested content using said key.

28. The method of Claim 25 further comprising:

including usage data with said content that is also written to said hidden portion of said nonvolatile HDD memory; and

making said requested content unavailable when said usage data indicates allowable use is over.

29. The method of Claim 28 further comprising deleting said requested content from said nonvolatile HDD memory.

30. The method of Claim 28 wherein said usage data specifies a predetermined number of allowable uses.

31. The method of Claims 28 wherein said usage data specifies a duration of allowable usage.

32. The method of Claim 23 further comprising:

storing content in nonvolatile memory of said DVD system; and

receiving requests for said content from said requester network device.

33. The method of Claim 32 further comprising determining an amount of time that is required to receive said key from said HDD system after sending said key request to the HDD system.

34. The method of Claim 33 further comprising sending said requested content to said HDD system if said key is received within a predetermined period.

35. The method of Claim 34 further comprising encrypting said requested content before sending said requested content to the HDD system.

36. The method of Claim 35 further comprising including usage data in said requested content that is transmitted to the HDD system.

37. The method of Claim 36 wherein said usage data specifies a number of allowable uses.

38. The method of Claim 36 wherein said usage data specifies a duration of allowable usage.

39. The method of Claim 21 further comprising:

determining whether a signal received from said requester network device has been transmitted via R repeaters, where R is an integer greater than or equal to one; and

determining said local/remote status based on whether said signal has been transmitted via said R repeaters.

40. The method of Claim 21 further comprising:

monitoring a number of times that said requester network device receives first content with restrictions; and selectively removing said restrictions for said first content when said number of times exceeds M times, where M is an integer greater than one.

41. The system of Claim 1 wherein said provider network device determines whether a signal received from said requester network device has been transmitted via R repeaters and determines said local/remote status based on whether said signal has been transmitted via said R repeaters, where R is an integer greater than or equal to one.

42. The system of Claim 4 wherein said requester network device monitors a number of times that said requester network device receives first content with restrictions and that removes said restrictions when said number of times exceeds M times, where M is an integer greater than one.

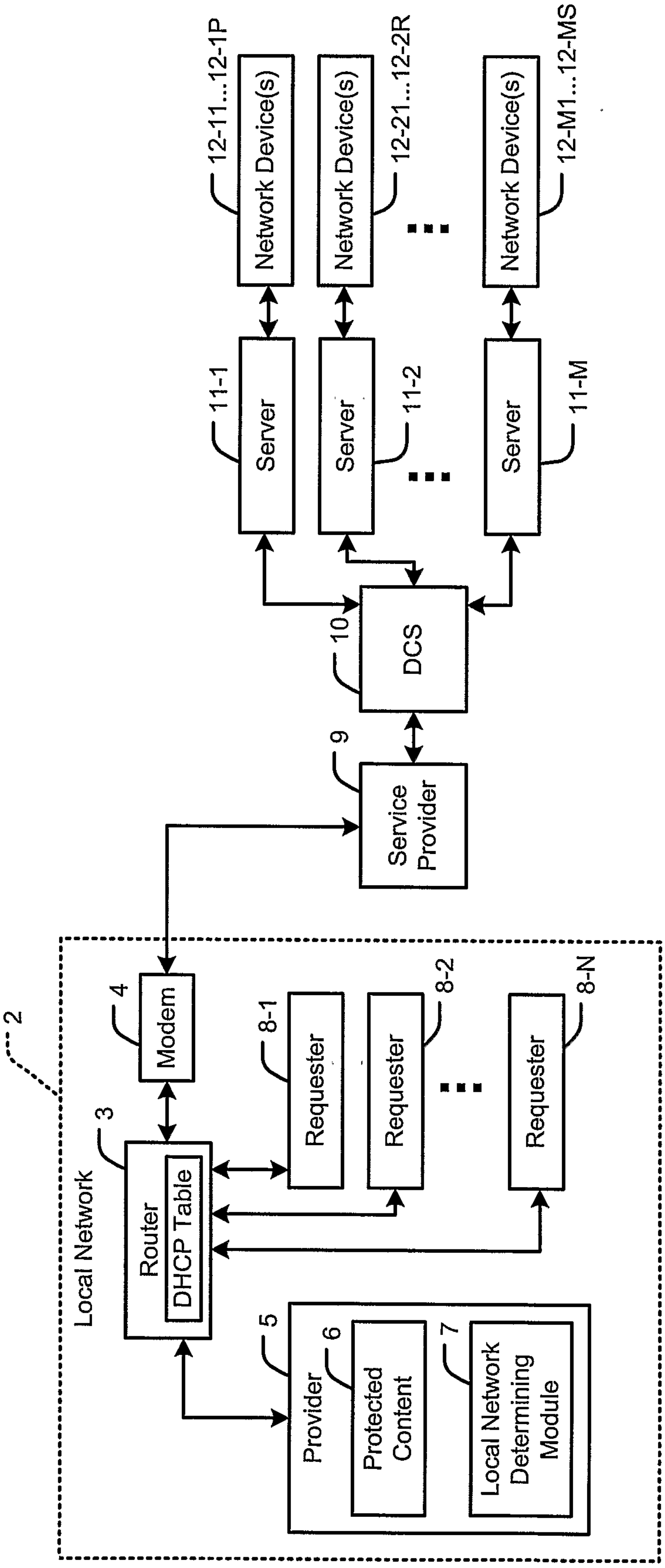

2
Local Network
3
Router
DHCP Table
4
Modem
5
Provider
6
Protected Content
7
Local Network Determining Module
8-1
Requester
8-2
Requester
8-N
Requester
9
Service Provider
10
DCS
11-1
Server
11-2
Server
11-M
Server
12-11...12-1P
Network Device(s)
12-21...12-2R
Network Device(s)
12-M1...12-MS
Network Device(s)

FIG. 1

FIG. 2

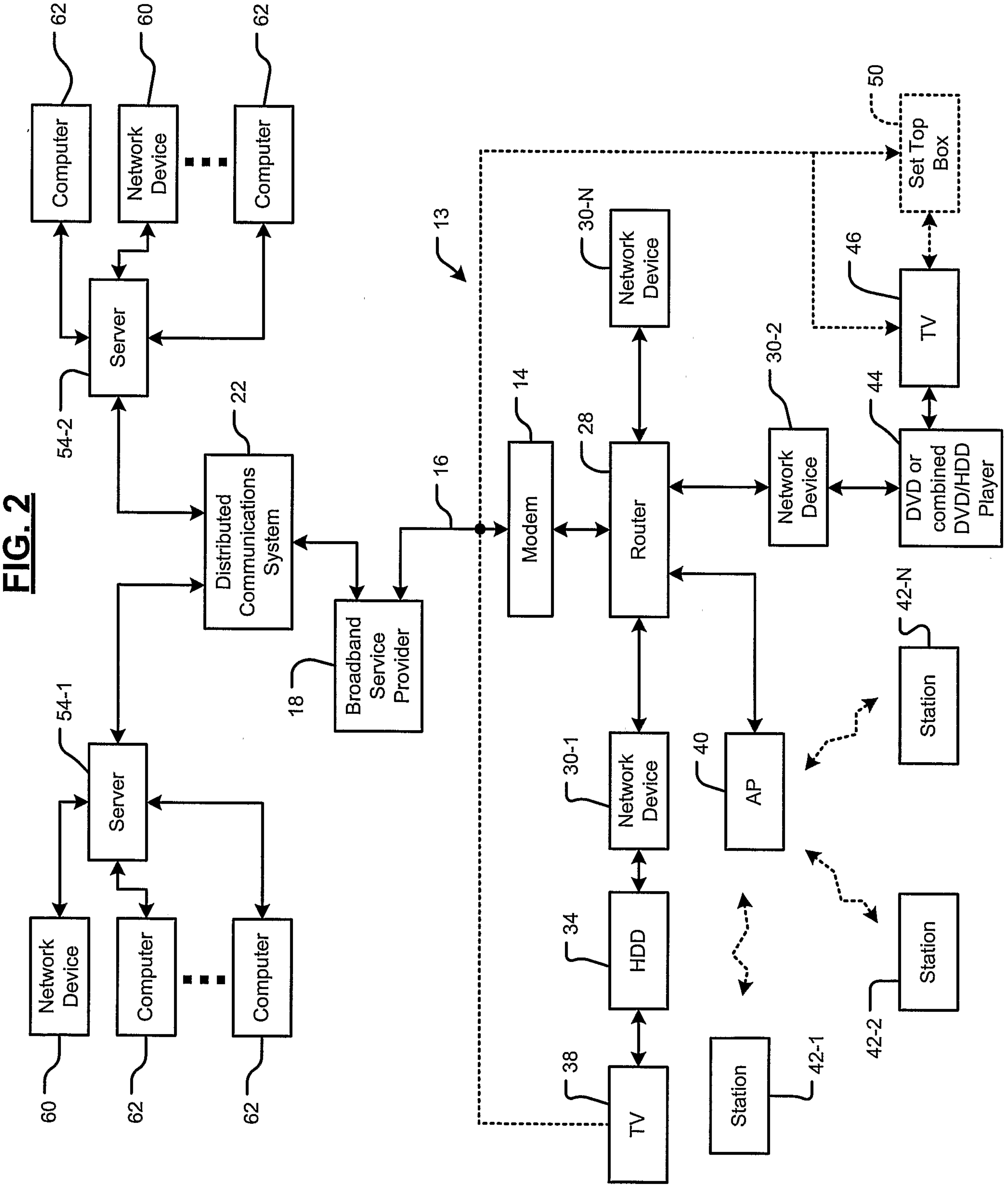

Computer
62
Network Device
60
Computer
62
Server
54-2
Distributed Communications System
22
16
Broadband Service Provider
18
Server
54-1
Network Device
60
Computer
62
Computer
62
13
Modem
14
Router
28
Network Device
30-N
Network Device
30-2
Network Device
30-1
AP
40
HDD
34
TV
38
Station
42-1
Station
42-2
Station
42-N
DVD or combined DVD/HDD Player
44
TV
46
Set Top Box
50

FIG. 3

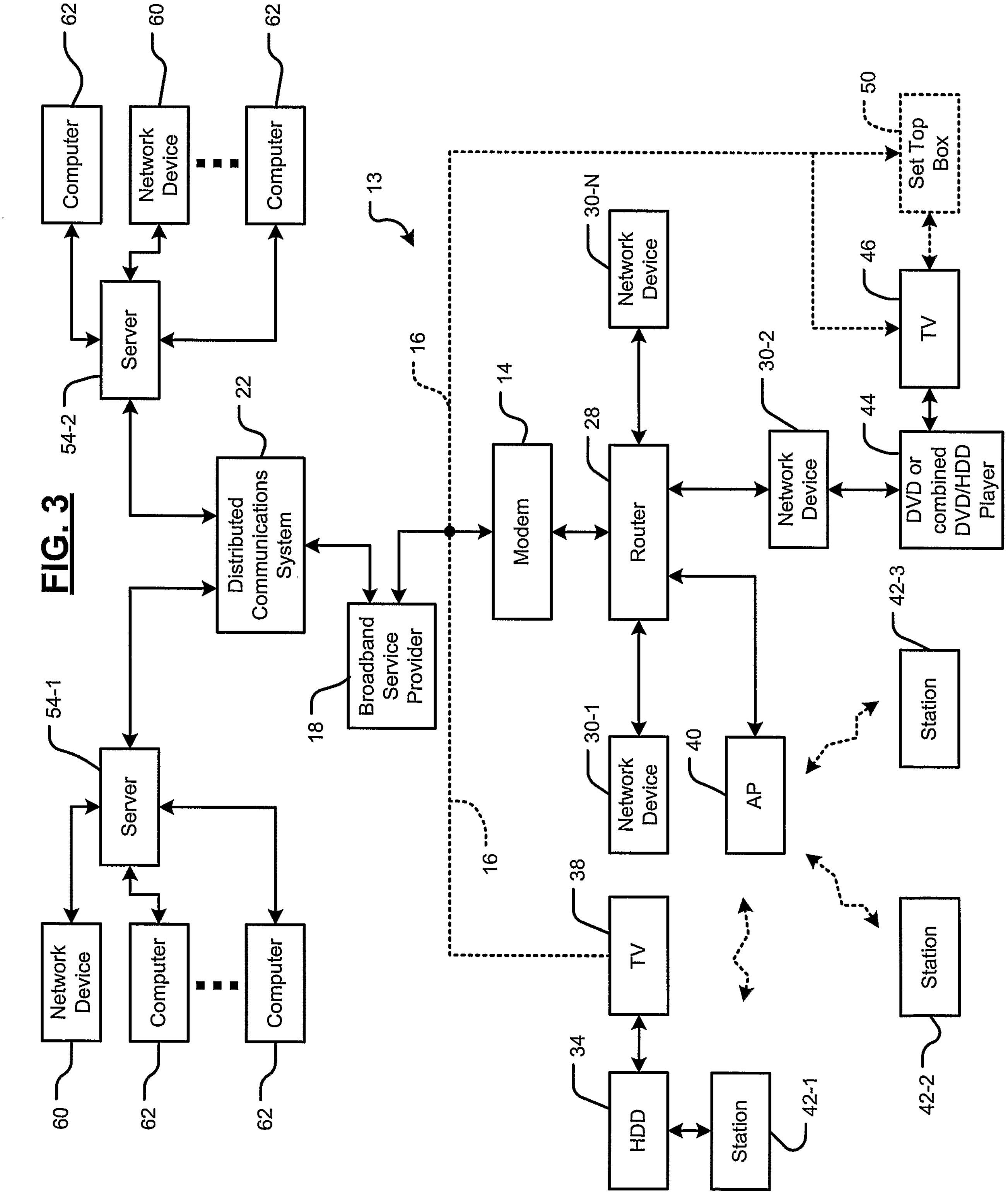

13
Computer
62
Network Device
60
Computer
62
Server
54-2
Distributed Communications System
22
Server
54-1
Network Device
60
Computer
62
Computer
62
Broadband Service Provider
18
16
16
Modem
14
Router
28
Network Device
30-N
Network Device
30-2
Network Device
30-1
AP
40
TV
38
HDD
34
Station
42-1
Station
42-2
Station
42-3
Set Top Box
50
TV
46
DVD or combined DVD/HDD Player
44

FIG. 4

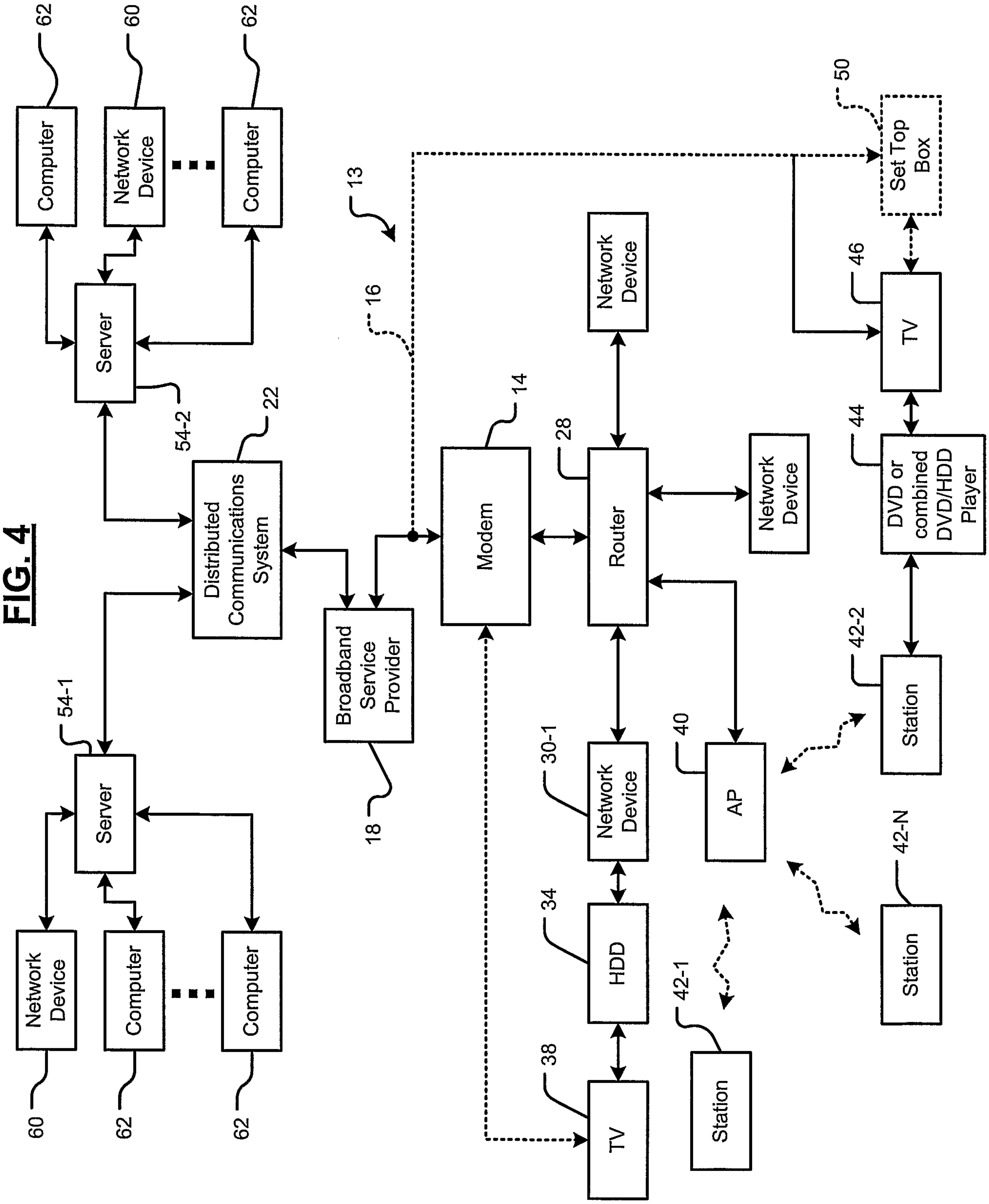
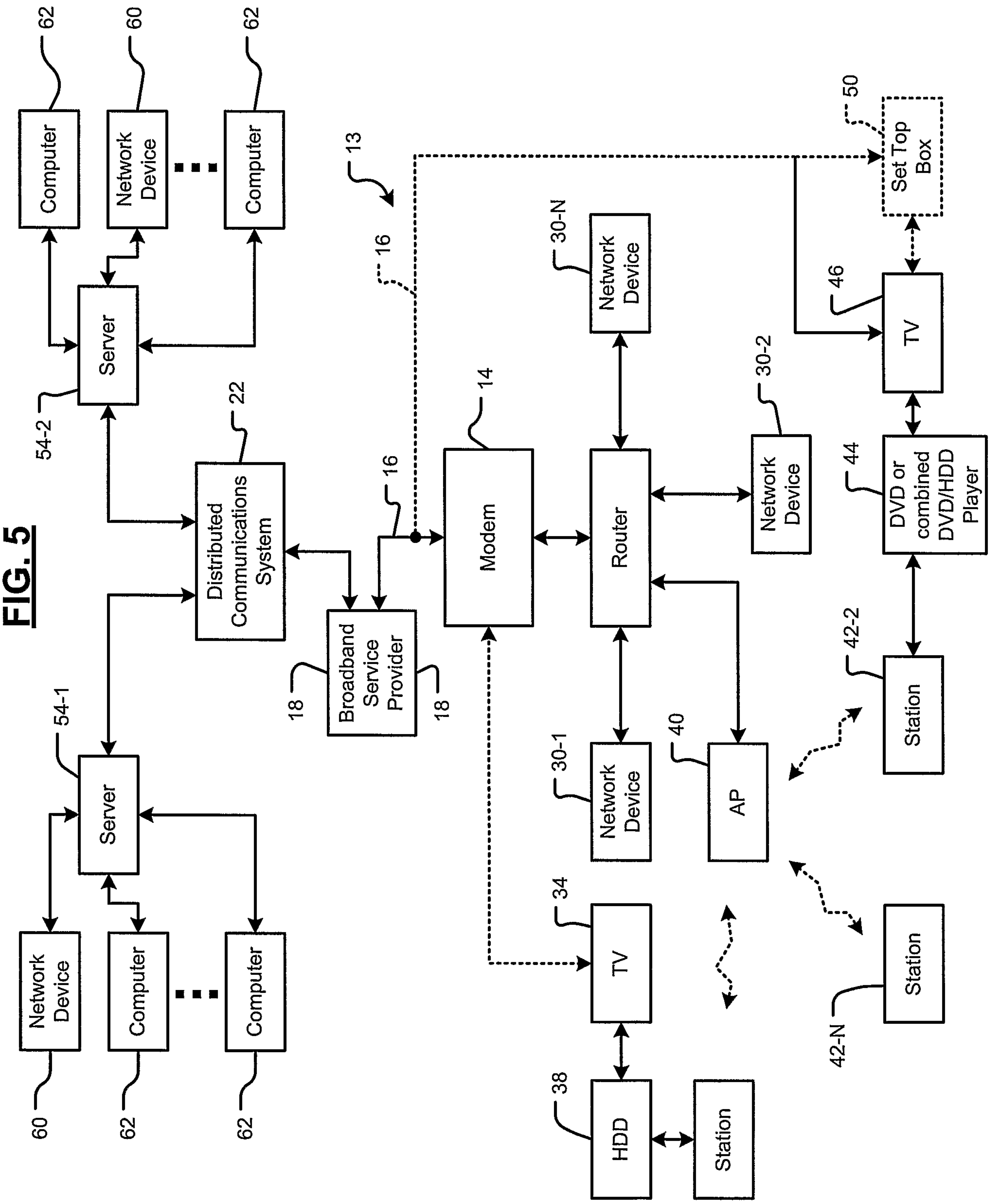

Computer
Network Device
Computer
Server
Distributed Communications System
Server
Network Device
Computer
Computer
Broadband Service Provider
Modem
Router
Network Device
Network Device
Network Device
HDD
TV
AP
Station
Station
Station
DVD or combined DVD/HDD Player
TV
Set Top Box
62
60
62
54-2
22
54-1
60
62
62
18
13
16
14
28
30-1
34
38
40
42-1
42-2
42-N
44
46
50

FIG. 5


Computer
62
Network Device
60
Computer
62
Server
54-2
Distributed Communications System
22
13
16
Set Top Box
50
Network Device
30-N
TV
46
Modem
14
Router
Network Device
30-2
DVD or combined DVD/HDD Player
44
Broadband Service Provider
18
18
Server
54-1
Network Device
60
Computer
62
Computer
62
Network Device
30-1
AP
40
Station
42-2
TV
34
Station
42-N
HDD
38
Station

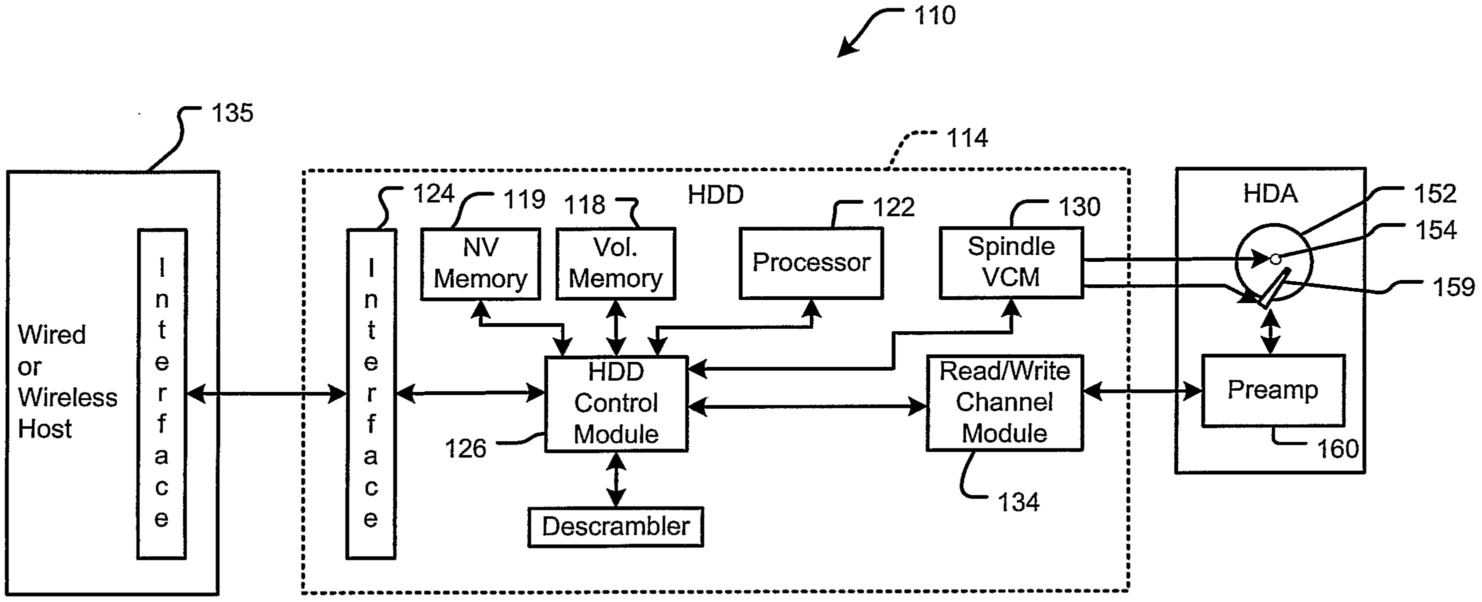

110
135
Wired
or
Wireless
Host
Interface
114
HDD
124
Interface
119
NV
Memory
118
Vol.
Memory
122
Processor
130
Spindle
VCM
HDD
Control
Module
126
Descrambler
Read/Write
Channel
Module
134
HDA
152
154
159
Preamp
160

FIG. 6

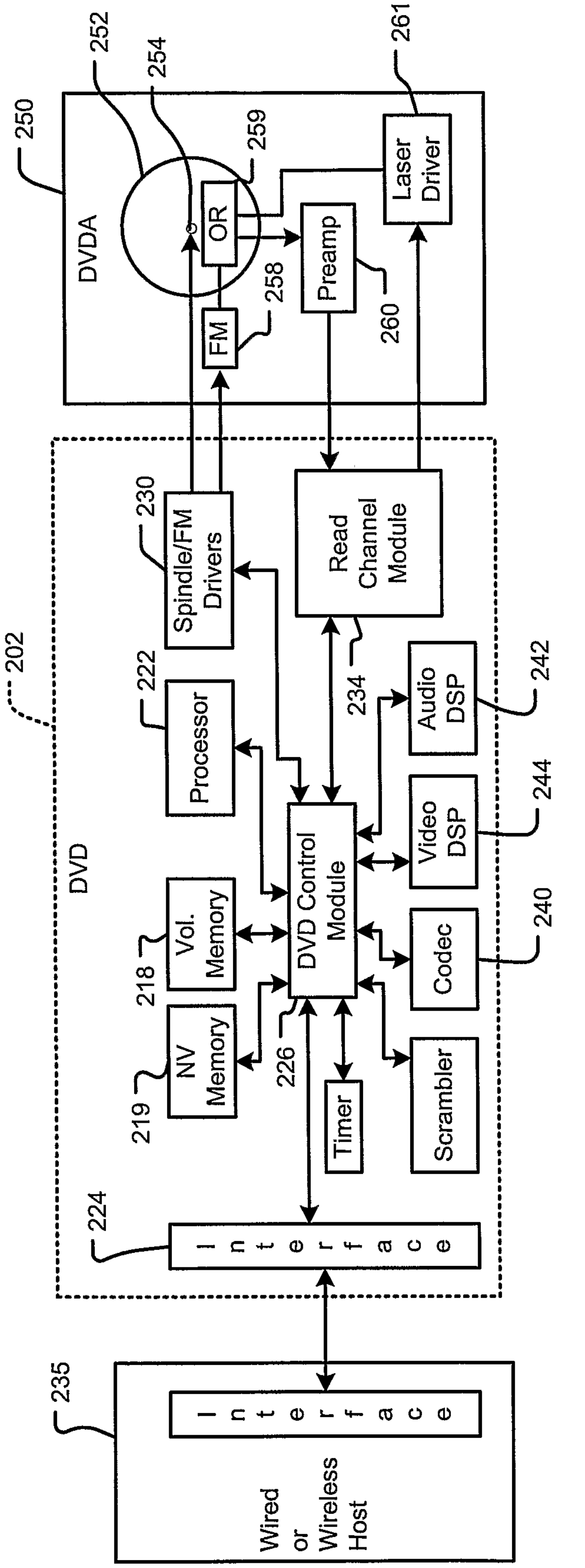

250
DVDA
252
254
259
OR
FM
258
Preamp
260
Laser Driver
261
202
DVD
230
Spindle/FM Drivers
Read Channel Module
234
222
Processor
218
Vol. Memory
219
NV Memory
DVD Control Module
226
Timer
Audio DSP
242
Video DSP
244
Codec
240
Scrambler
224
Interface
235
Interface
Wired or Wireless Host

FIG. 7A

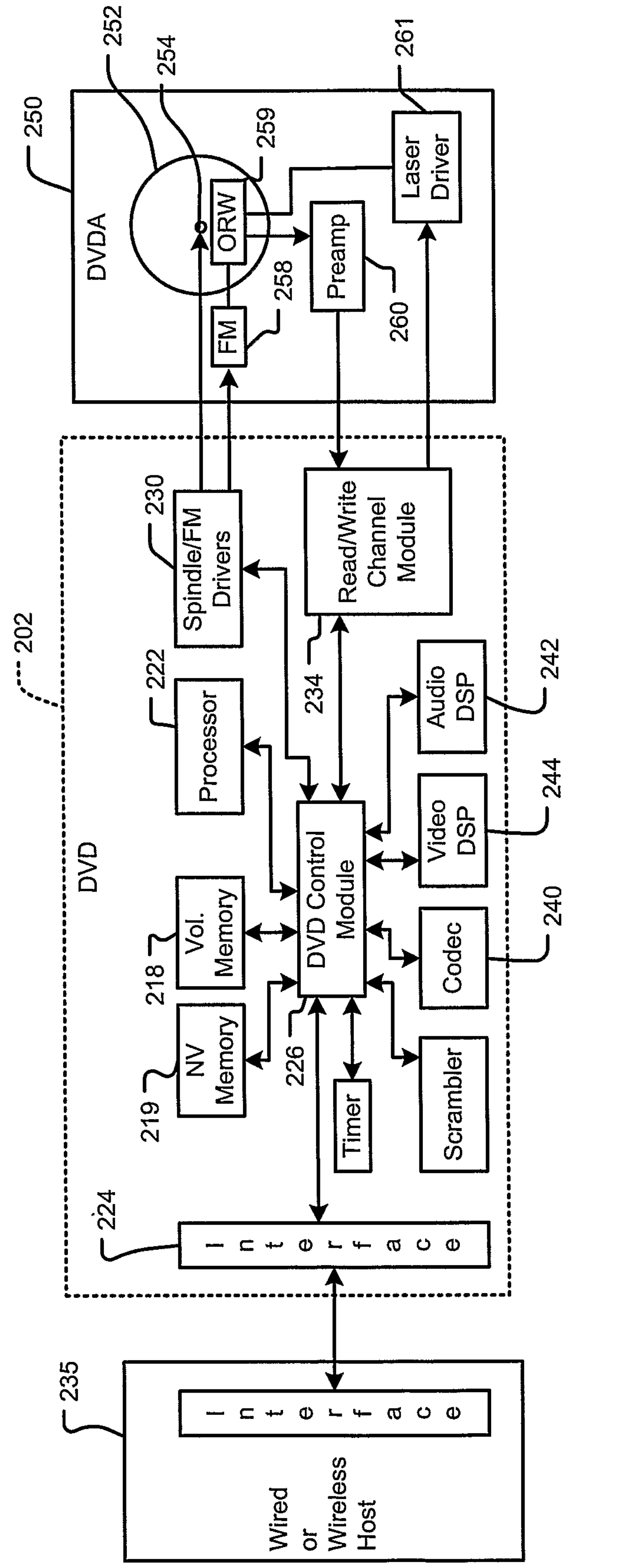

250
DVDA
252
254
259
ORW
258
FM
Preamp
260
261
Laser Driver
202
DVD
230
Spindle/FM Drivers
222
Processor
234
Read/Write Channel Module
242
Audio DSP
244
Video DSP
240
Codec
218
Vol. Memory
219
NV Memory
226
DVD Control Module
Timer
Scrambler
224
Interface
235
Interface
Wired or Wireless Host

FIG. 7B

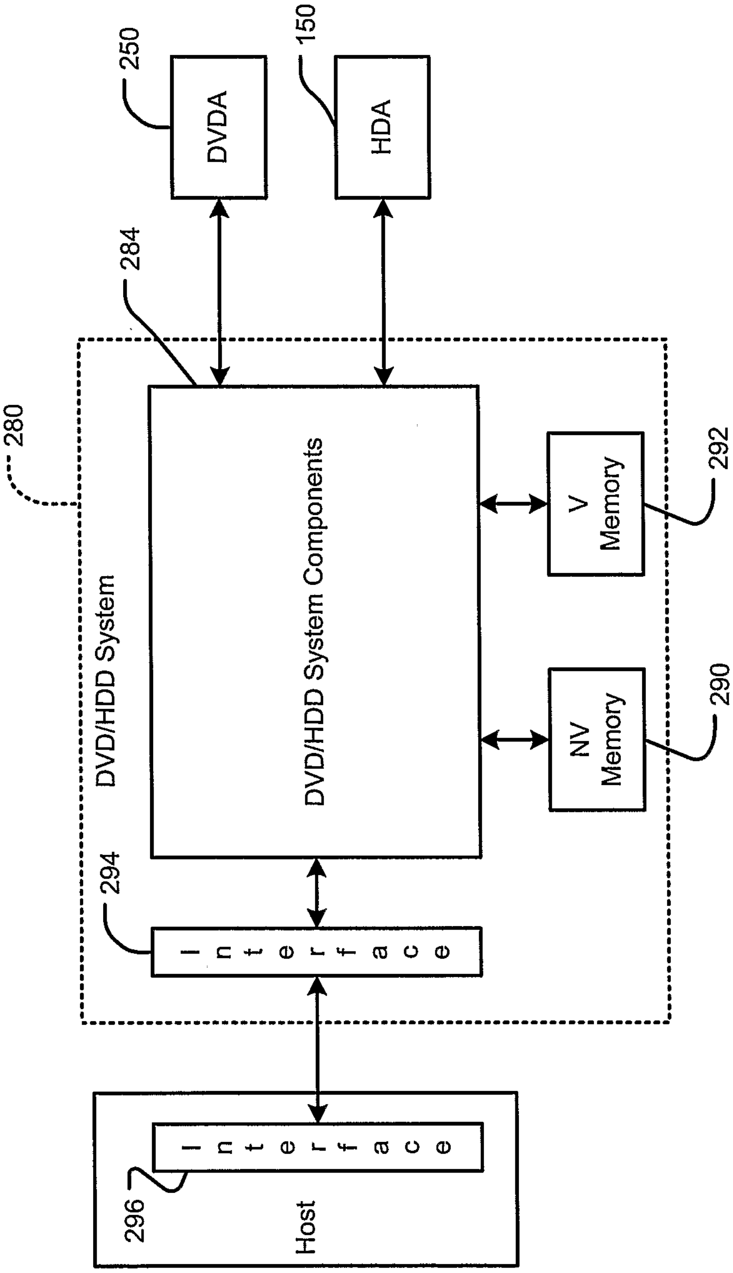

250
DVDA
150
HDA
284
280
DVD/HDD System
DVD/HDD System Components
V Memory
292
NV Memory
290
294
Interface
Interface
296
Host

FIG. 7C

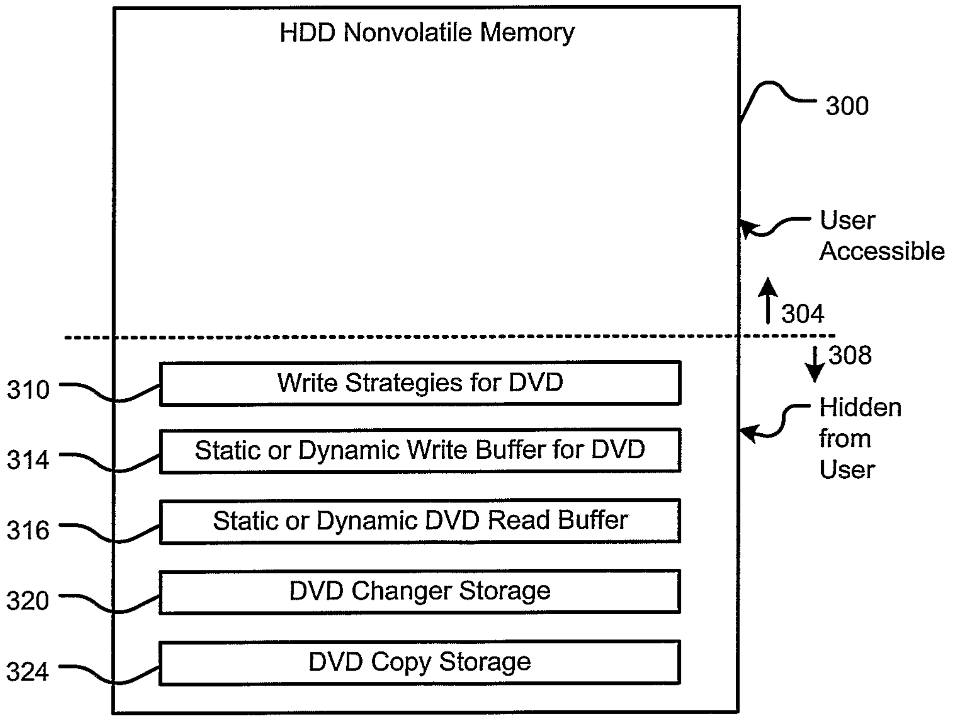

HDD Nonvolatile Memory
300
User Accessible
304
308
Hidden from User
310
Write Strategies for DVD
314
Static or Dynamic Write Buffer for DVD
316
Static or Dynamic DVD Read Buffer
320
DVD Changer Storage
324
DVD Copy Storage

FIG. 8

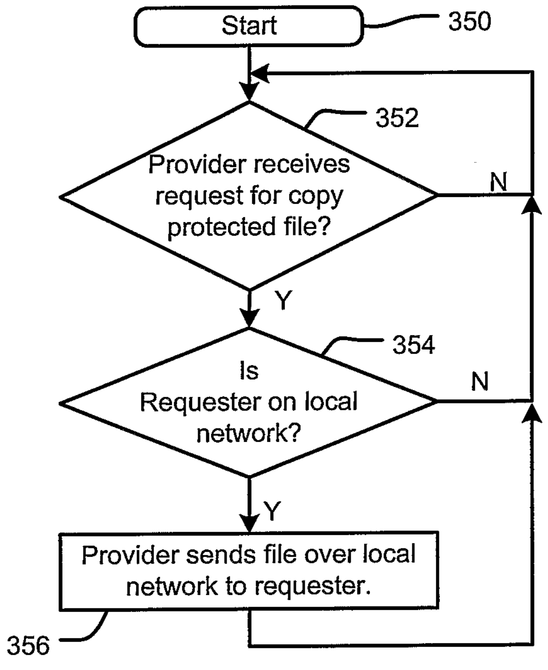

Start
350
352
Provider receives request for copy protected file?
N
Y
354
Is Requester on local network?
N
Y
Provider sends file over local network to requester.
356

FIG. 9A

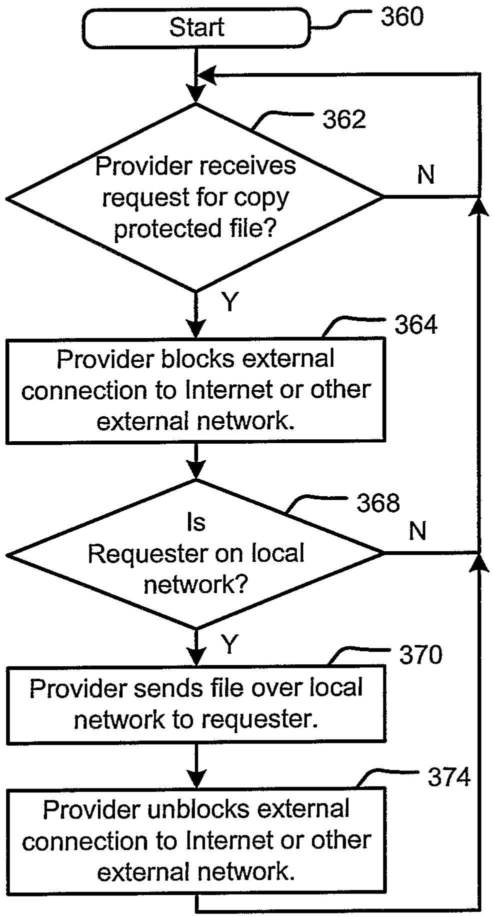

Start
360
362
Provider receives request for copy protected file?
N
Y
364
Provider blocks external connection to Internet or other external network.
368
Is Requester on local network?
N
Y
370
Provider sends file over local network to requester.
374
Provider unblocks external connection to Internet or other external network.

FIG. 9B

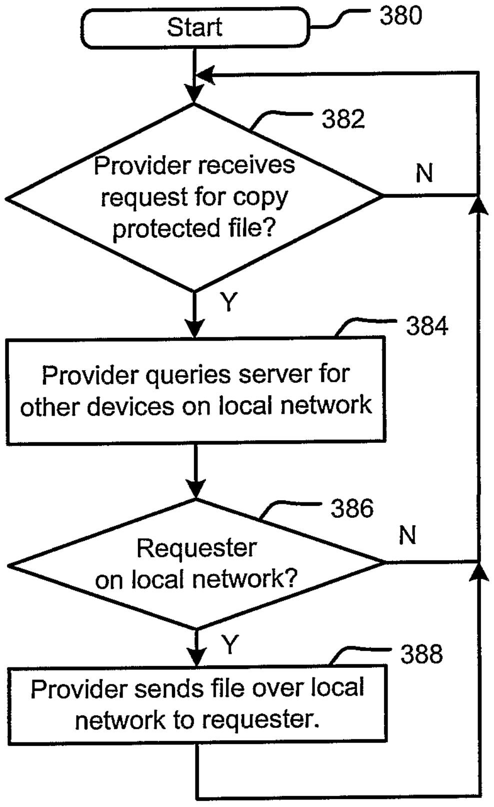

Start
380
382
Provider receives request for copy protected file?
N
Y
384
Provider queries server for other devices on local network
386
Requester on local network?
N
Y
388
Provider sends file over local network to requester.

FIG. 9C

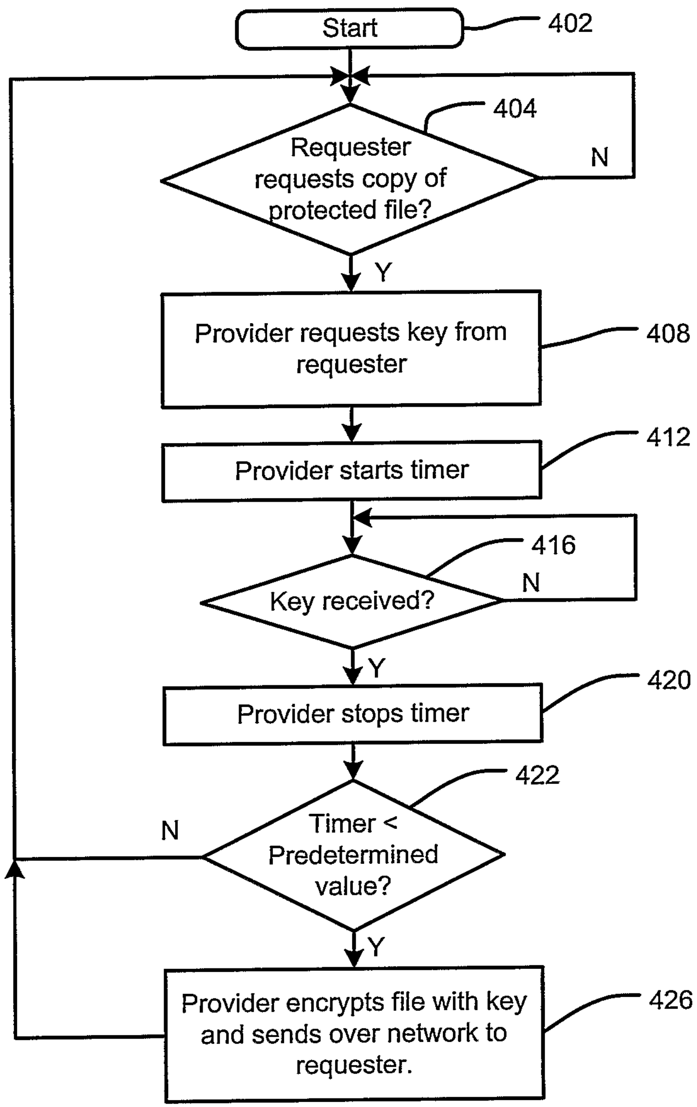

Start
402
404
Requester requests copy of protected file?
N
Y
Provider requests key from requester
408
Provider starts timer
412
416
Key received?
N
Y
Provider stops timer
420
422
Timer < Predetermined value?
N
Y
Provider encrypts file with key and sends over network to requester.
426

FIG. 9D

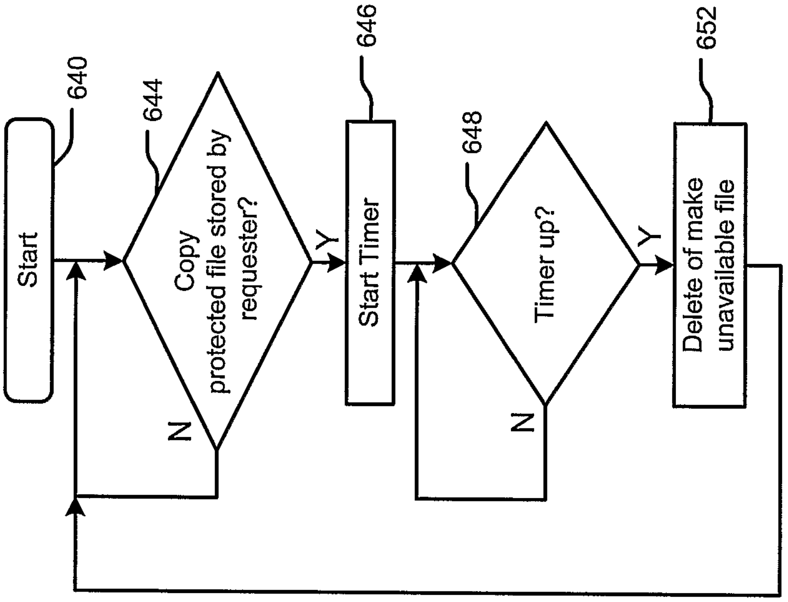

Start
640
Copy protected file stored by requester?
644
N
Y
Start Timer
646
Timer up?
648
N
Y
Delete of make unavailable file
652

FIG. 11

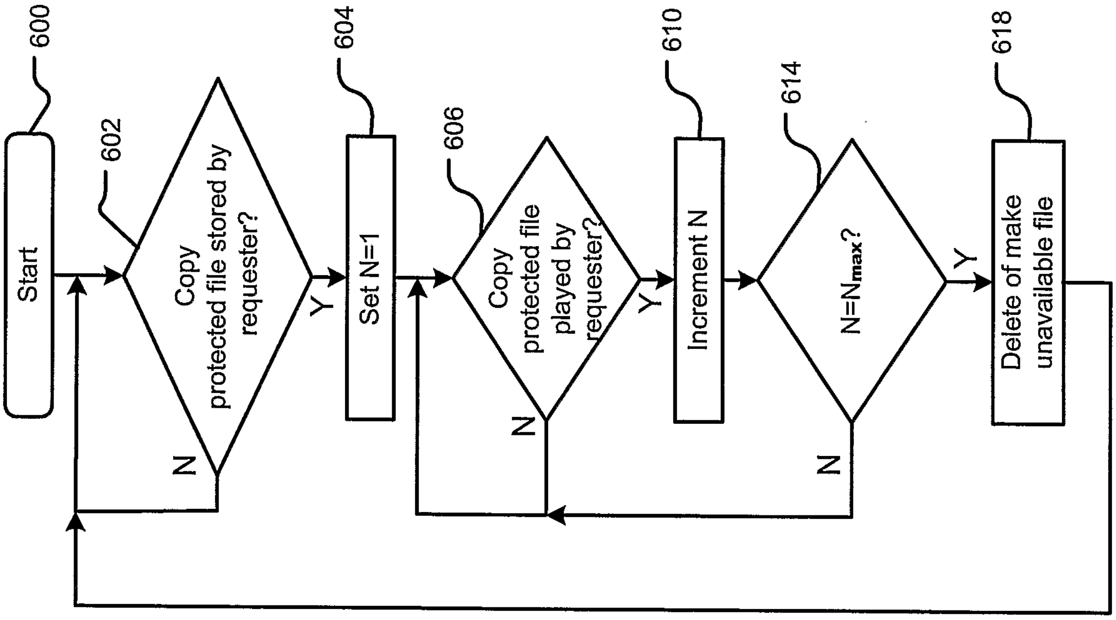
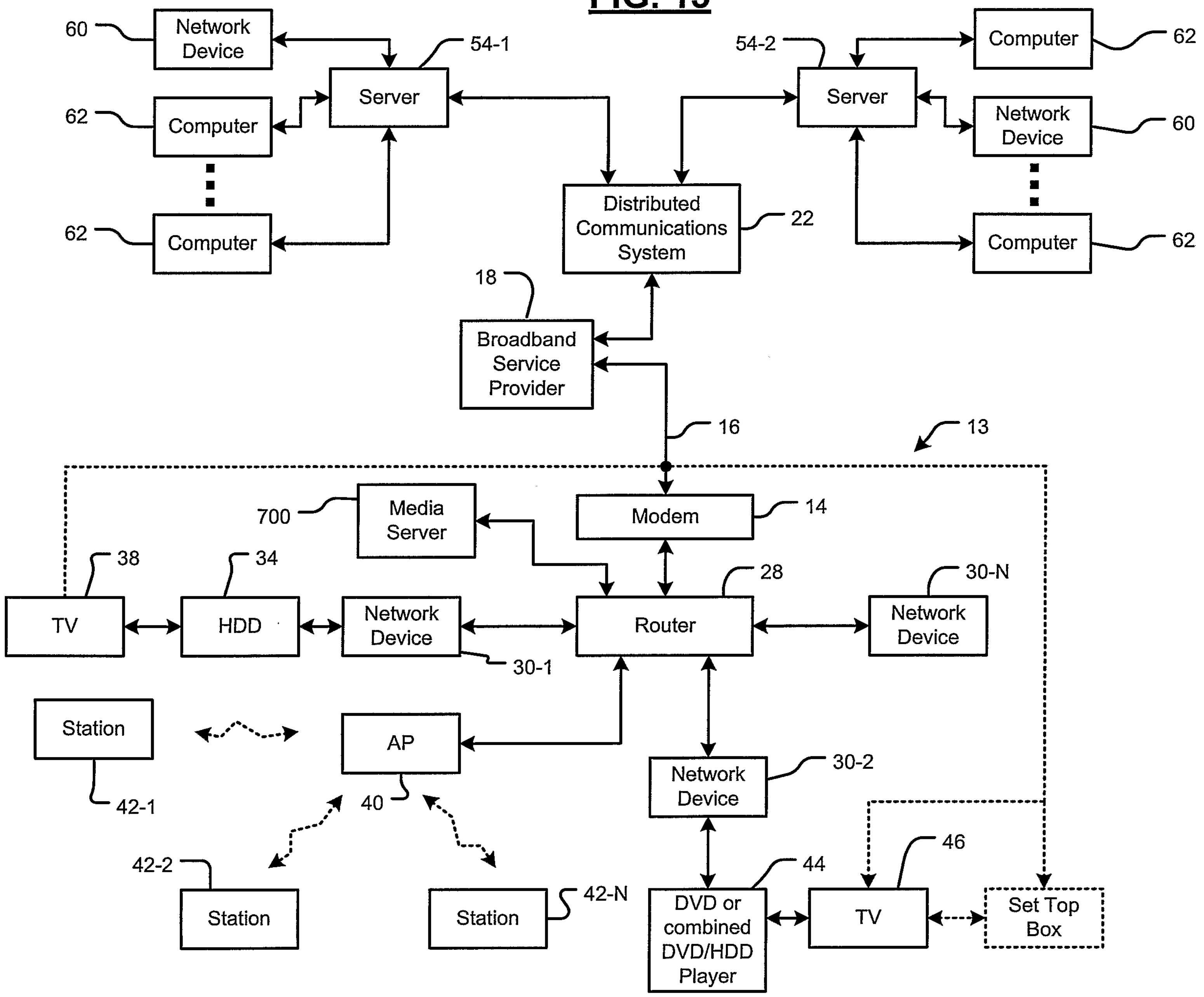

Start
600
Copy protected file stored by requester?
602
N
Y
Set N=1
604
Copy protected file played by requester?
606
N
Y
Increment N
610
N=Nmax?
614
N
Y
Delete of make unavailable file
618

FIG. 10

FIG. 13


60
Network Device
54-1
Server
54-2
Server
Computer
62
62
Computer
Network Device
60
62
Computer
Computer
62
Distributed Communications System
22
18
Broadband Service Provider
16
13
700
Media Server
Modem
14
38
34
28
30-N
TV
HDD
Network Device
Router
Network Device
30-1
Station
AP
42-1
Network Device
30-2
40
46
42-2
44
42-N
DVD or combined DVD/HDD Player
TV
Set Top Box
Station
Station

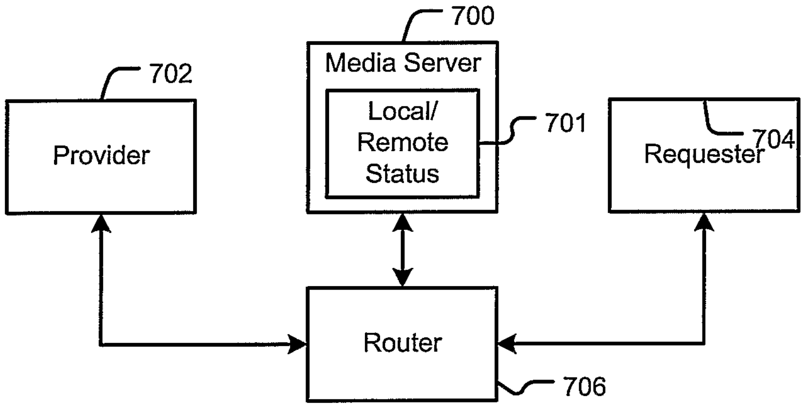


FIG. 12A

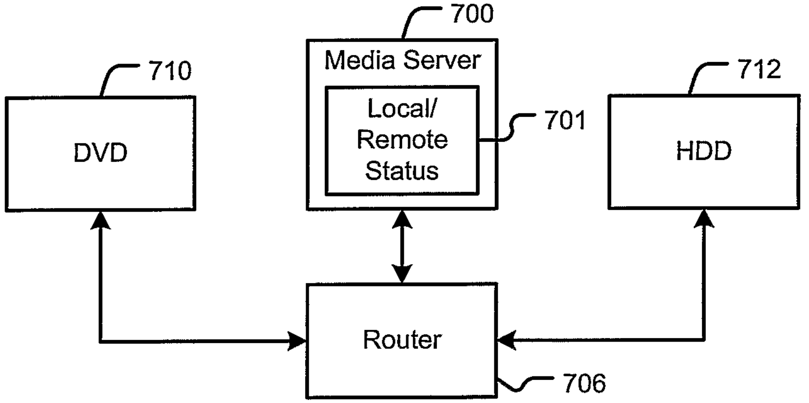


FIG. 12B

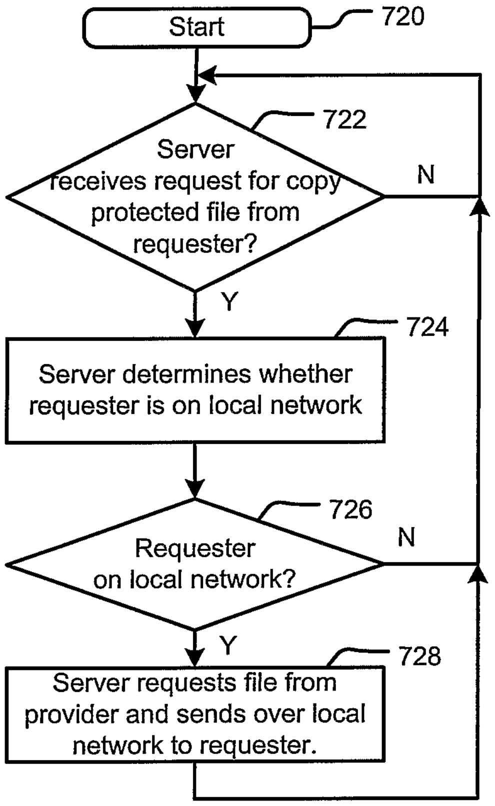

Start
720
Server
receives request for copy
protected file from
requester?
722
N
Y
Server determines whether
requester is on local network
724
Requester
on local network?
726
N
Y
Server requests file from
provider and sends over local
network to requester.
728

FIG. 14

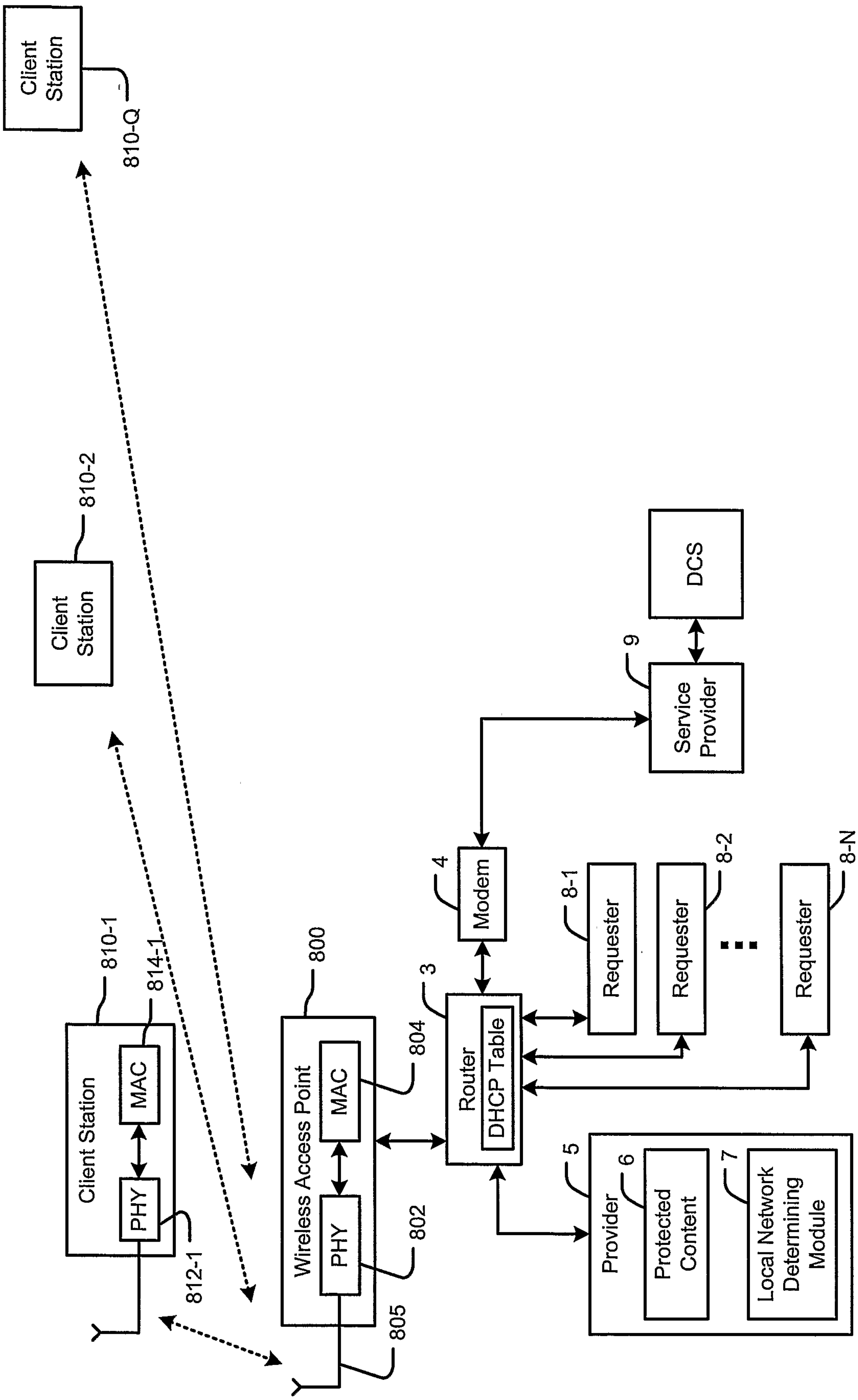
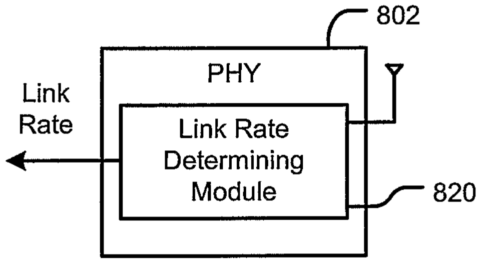
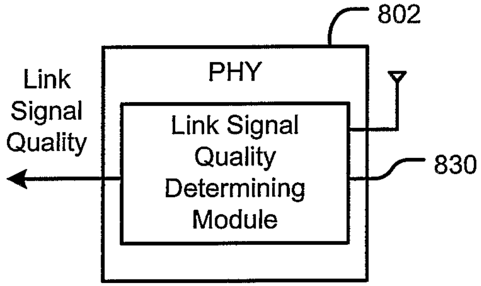

Client Station
810-Q
Client Station
810-2
Client Station
810-1
MAC
814-1
PHY
812-1
Wireless Access Point
800
MAC
804
PHY
802
805
Router
DHCP Table
3
Modem
4
Service Provider
9
DCS
Requester
8-1
Requester
8-2
Requester
8-N
Provider
5
Protected Content
6
Local Network Determining Module
7

FIG. 15

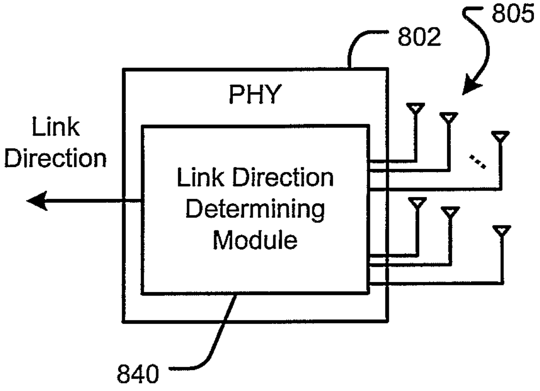
## FIG. 16A



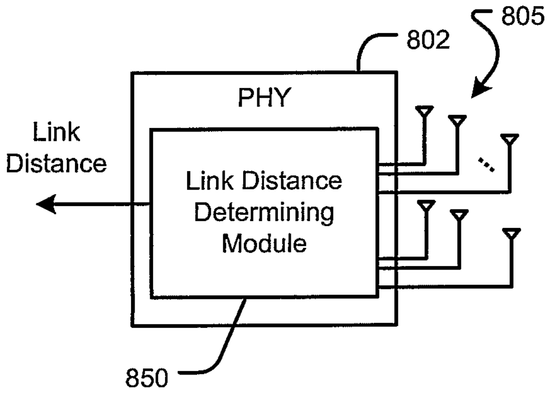
## FIG. 16B



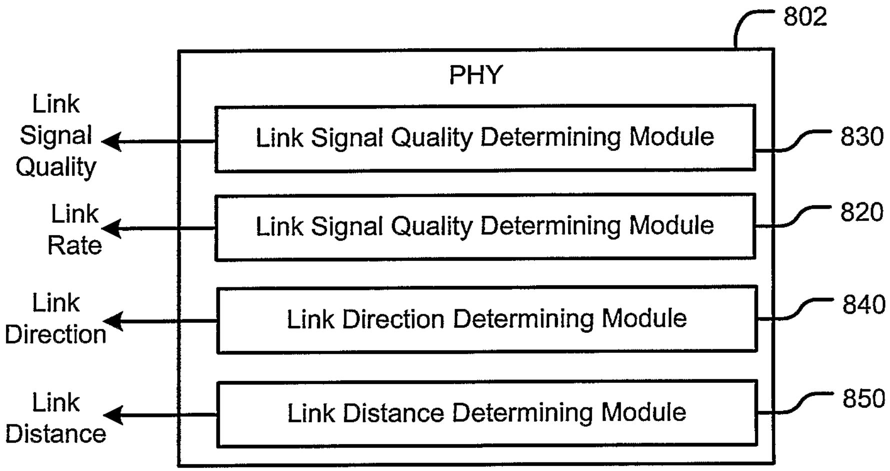
## FIG. 16C



## FIG. 16D



## FIG. 16E


802
PHY
Link Signal Quality
Link Signal Quality Determining Module
830
Link Rate
Link Signal Quality Determining Module
820
Link Direction
Link Direction Determining Module
840
Link Distance
Link Distance Determining Module
850

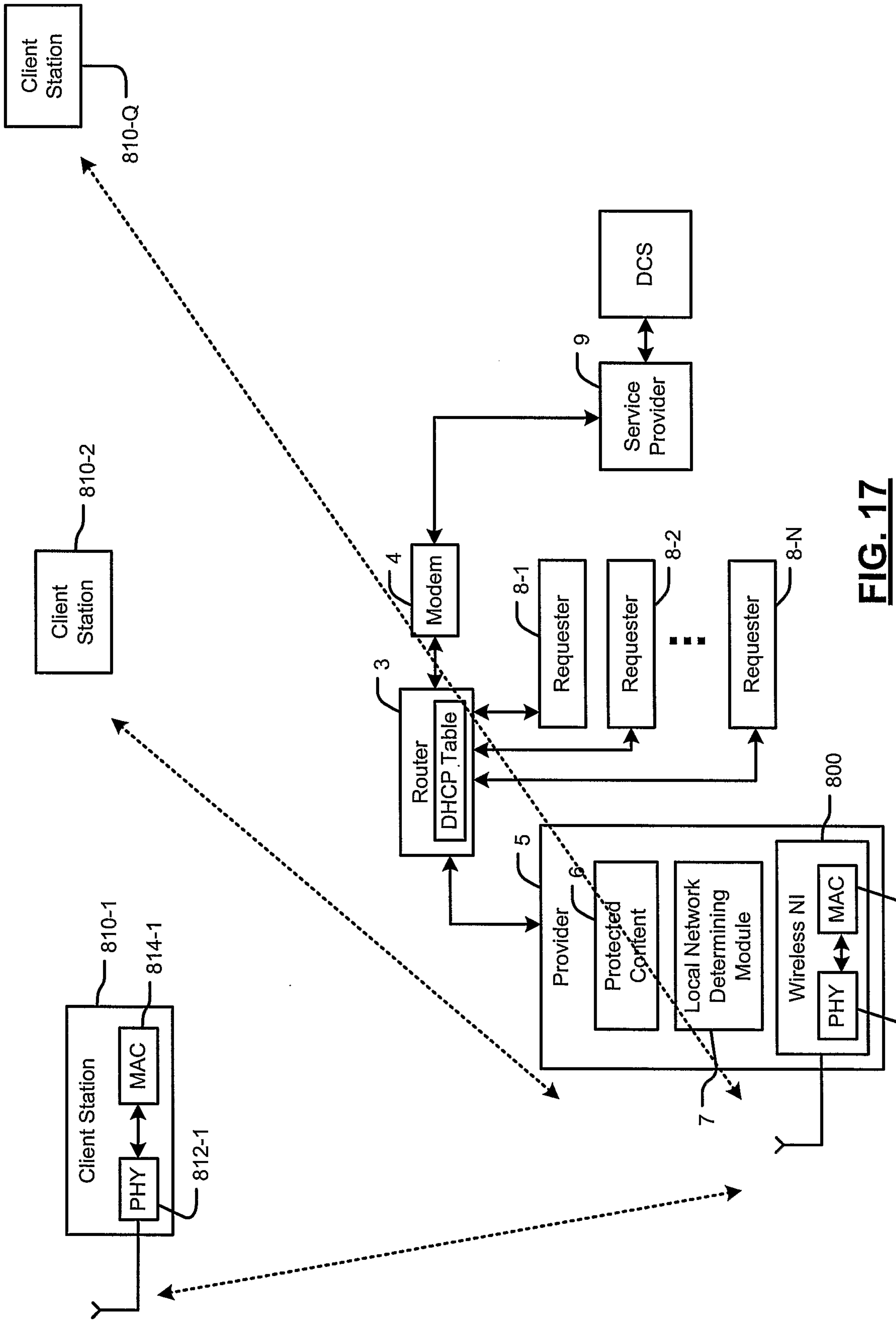

Client Station
810-Q
Client Station
810-2
Client Station
810-1
MAC
814-1
PHY
812-1
DCS
9
Service Provider
4
Modem
3
Router
DHCP Table
8-1
Requester
8-2
Requester
8-N
Requester
5
Provider
6
Protected Content
Local Network Determining Module
7
800
Wireless NI
MAC
804
PHY
802

FIG. 17

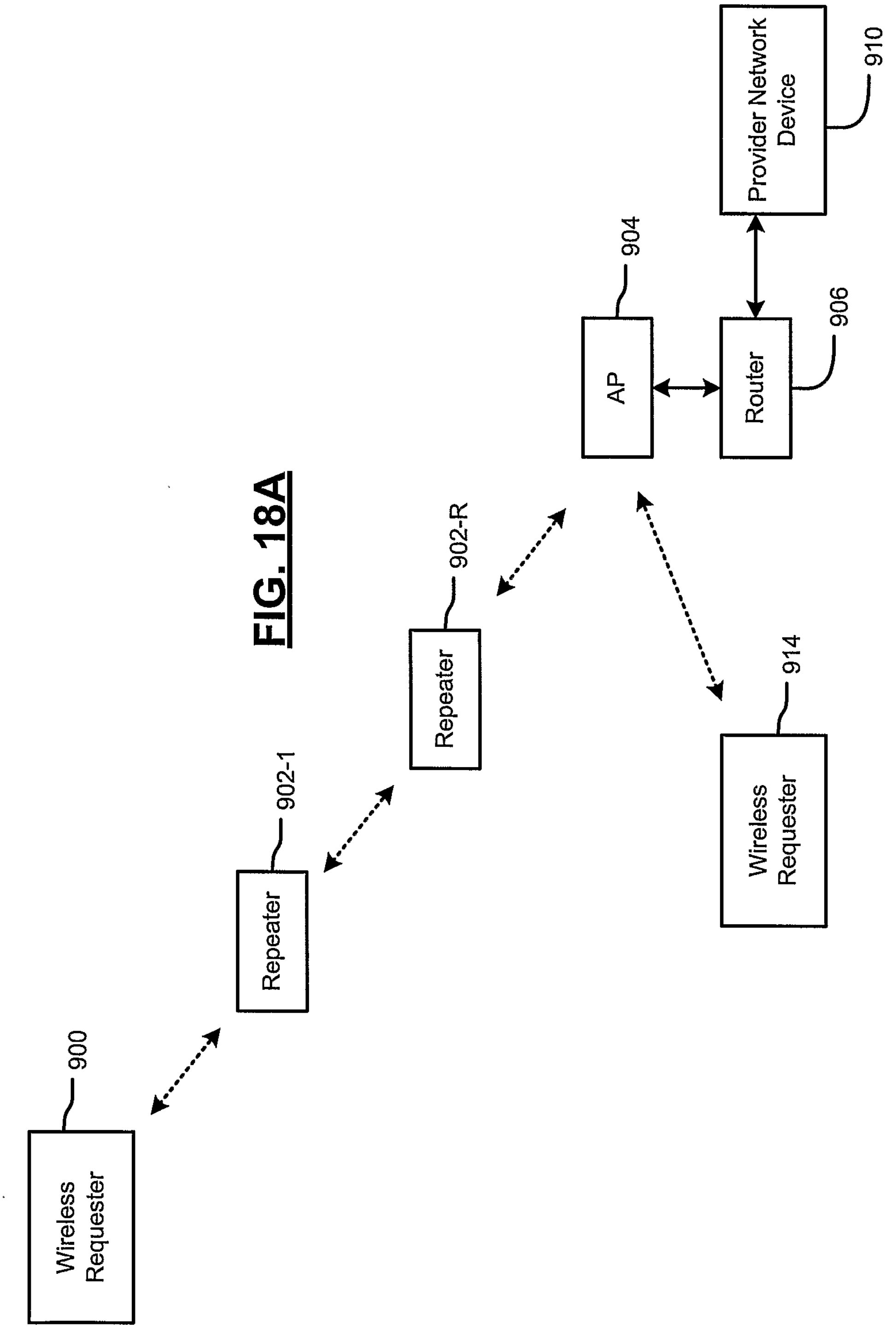

Wireless Requester
900
Repeater
902-1
Repeater
902-R
AP
904
Router
906
Provider Network Device
910
Wireless Requester
914

FIG. 18A

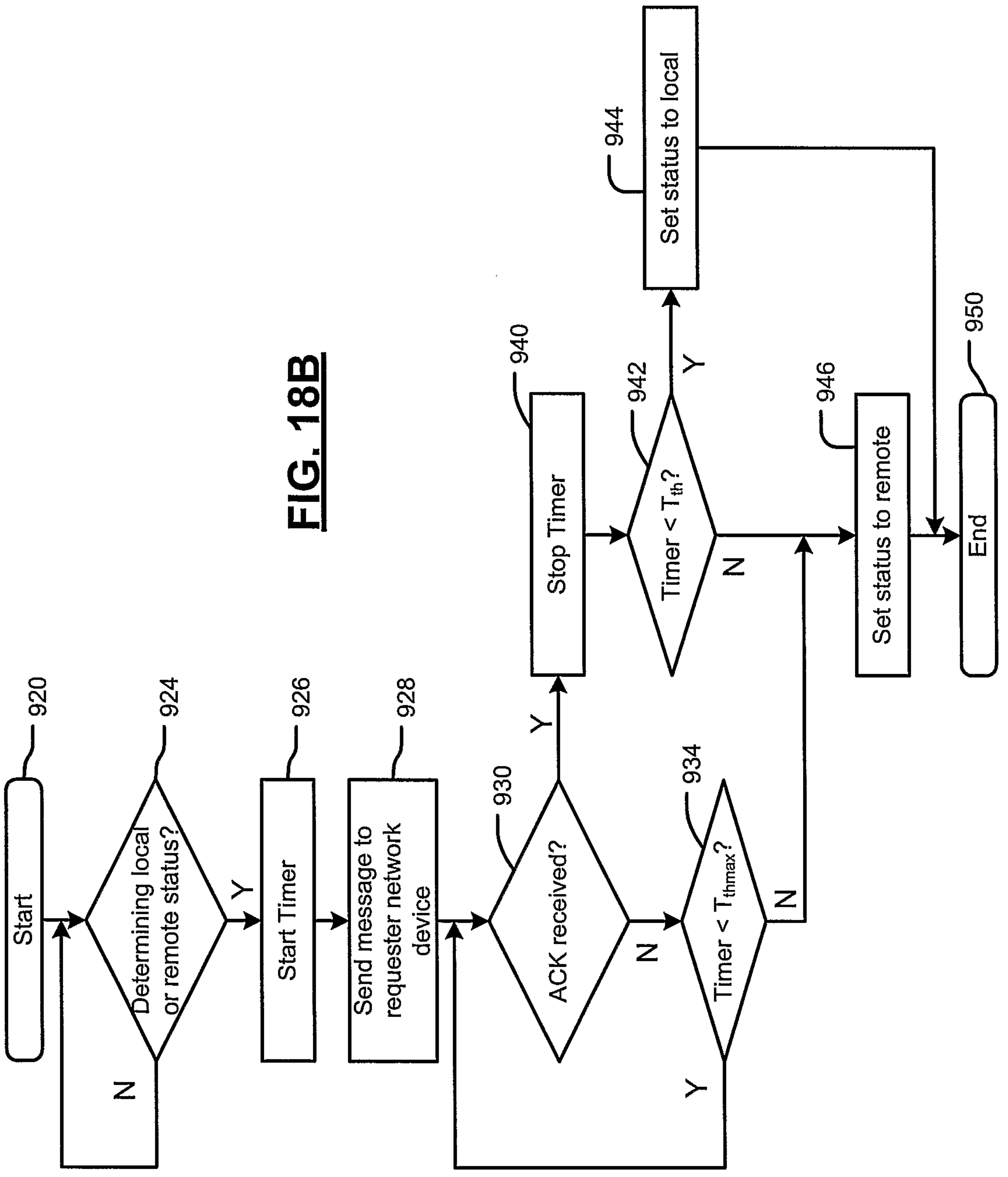

920
Start
924
Determining local or remote status?
N
Y
926
Start Timer
928
Send message to requester network device
930
ACK received?
N
Y
934
Timer < $T_{thmax}$?
Y
N
940
Stop Timer
942
Timer < $T_{th}$?
Y
N
944
Set status to local
946
Set status to remote
950
End

FIG. 18B

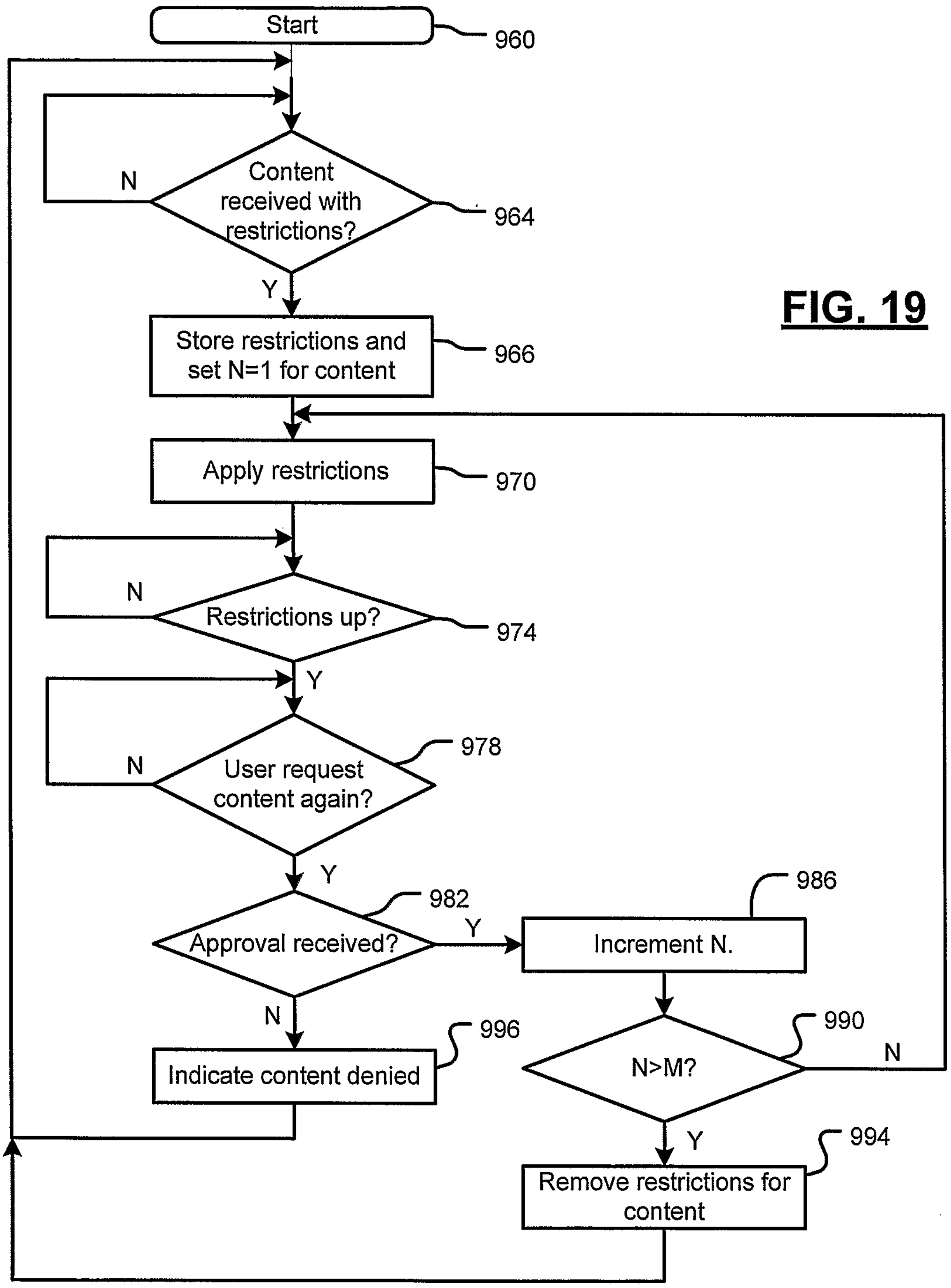

Start
960
Content received with restrictions?
964
N
Y
Store restrictions and set N=1 for content
966
Apply restrictions
970
Restrictions up?
974
N
Y
User request content again?
978
N
Y
Approval received?
982
Y
N
Increment N.
986
N>M?
990
N
Y
Indicate content denied
996
Remove restrictions for content
994

FIG. 19

# INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/010474

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

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)
G06F H04N H04L

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2004/213273 A1 (MA KENNETH)<br>28 October 2004 (2004-10-28)<br>abstract<br>paragraph [0003]<br>paragraph [0007]<br>paragraph [0011]<br>paragraphs [0041] - [0063]<br>----- | 1-42 |
| X | US 2004/117440 A1 (SINGER MITCH FREDRICK ET AL) 17 June 2004 (2004-06-17)<br>paragraph [0026] - paragraph [0028]<br>paragraph [0056]<br>paragraph [0073] - paragraph [0078]<br>paragraph [0094]<br>paragraph [0211]<br>-----<br>-/-- | 1-42 |

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

10 July 2006

Date of mailing of the international search report

17/07/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Alecu, M

International application No
PCT/US2006/010474

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2004/213408 A1 (KIM BYUNG JIN ET AL)<br>28 October 2004 (2004-10-28)<br>paragraph [0029]; figure 6<br>----- | 17,18,<br>37,38 |
| A | WO 03/075570 A (ADVANCED DIGITAL BROADCAST POLSKA SP. Z O.O; ADVANCED DIGITAL BROADCAS) 12 September 2003 (2003-09-12)<br>page 2, line 2 - line 5<br>----- | 2,19,22,<br>39 |
| A | EP 1 439 697 A (THOMSON LICENSING S.A)<br>21 July 2004 (2004-07-21)<br>paragraph [0013]<br>paragraph [0033]<br>----- | 13,14,<br>33,34 |
| A | US 2002/103964 A1 (IGARI FUBITO)<br>1 August 2002 (2002-08-01)<br>abstract<br>paragraph [0005] - paragraph [0009]<br>paragraph [0025] - paragraph [0027]<br>paragraph [0031] - paragraph [0051]<br>----- | 5-11,<br>25-31 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/010474

| Patent document cited in search report | | Publication date | Patent family member(s) | | | Publication date |
|---|---|---|---|---|---|---|
| US 2004213273 | A1 | 28-10-2004 | NONE | | | |
| US 2004117440 | A1 | 17-06-2004 | NONE | | | |
| US 2004213408 | A1 | 28-10-2004 | AU | 2004232281 | A1 | 04-11-2004 |
| | | | CA | 2523149 | A1 | 04-11-2004 |
| | | | EP | 1616324 | A1 | 18-01-2006 |
| | | | WO | 2004095438 | A1 | 04-11-2004 |
| WO 03075570 | A | 12-09-2003 | AU | 2003223148 | A1 | 16-09-2003 |
| | | | EP | 1481548 | A1 | 01-12-2004 |
| | | | US | 2005144248 | A1 | 30-06-2005 |
| EP 1439697 | A | 21-07-2004 | NONE | | | |
| US 2002103964 | A1 | 01-08-2002 | JP | 2002229859 | A | 16-08-2002 |
| | | | SG | 99385 | A1 | 27-10-2003 |