



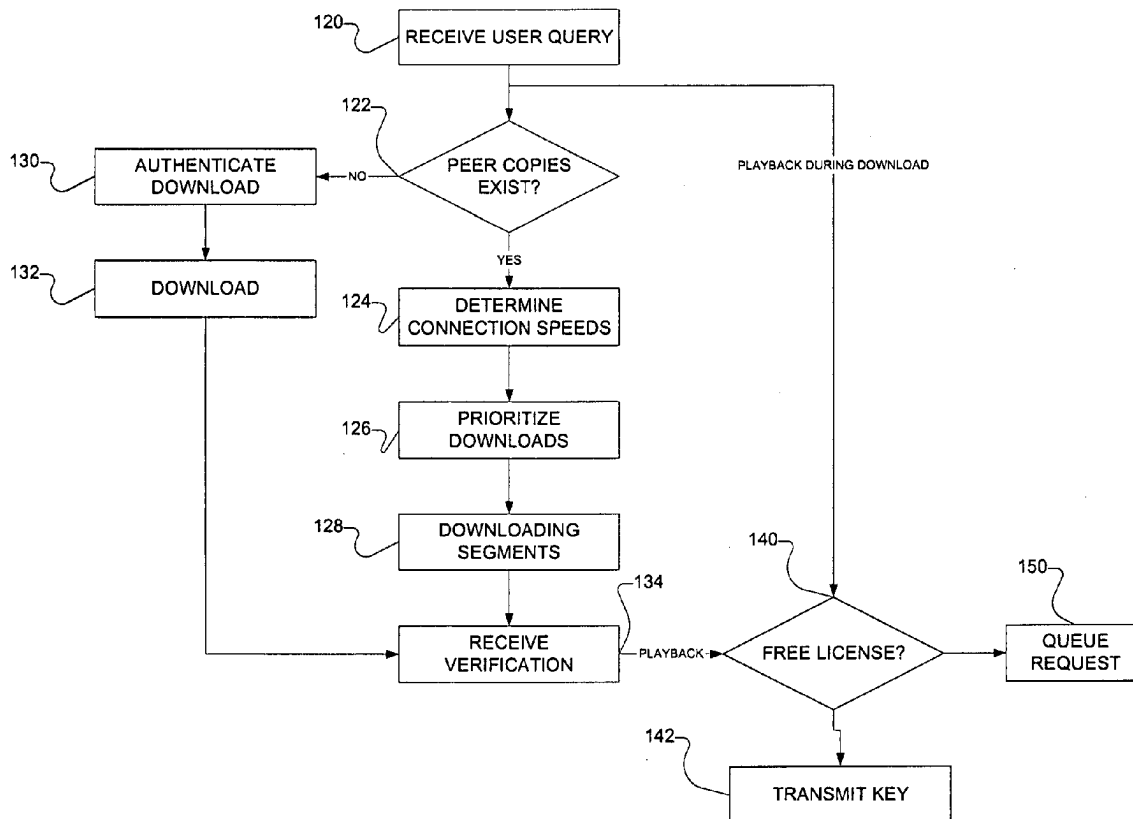
US 20060064386A1

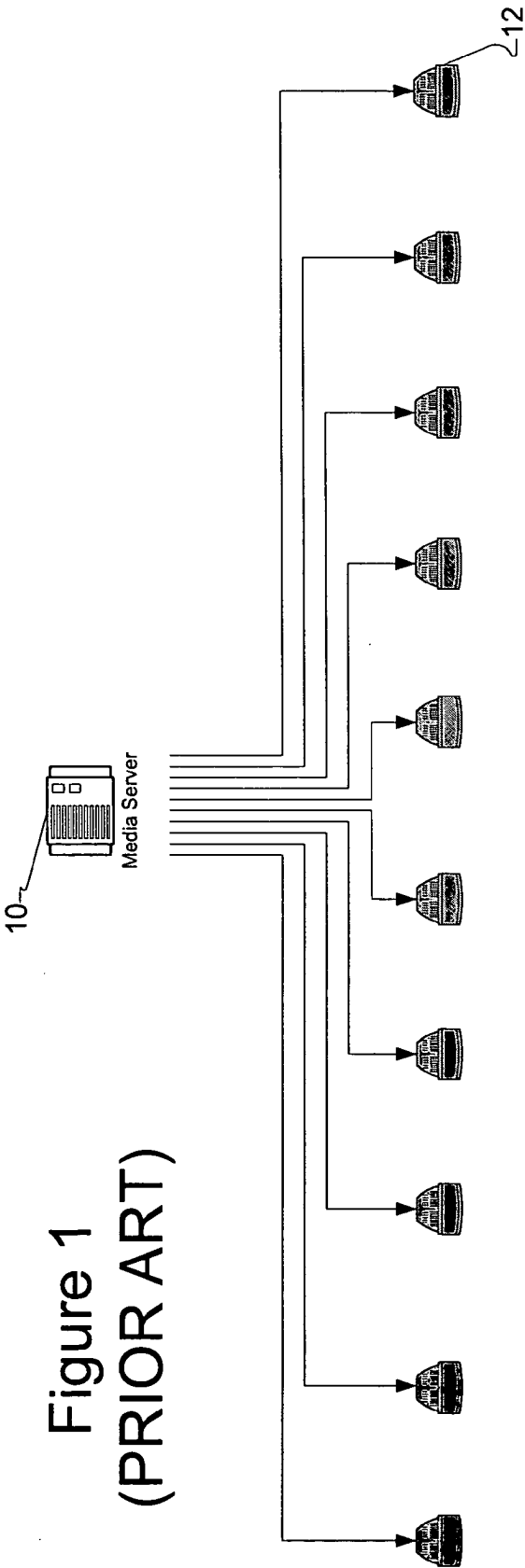
(19) **United States**(12) **Patent Application Publication**  
**Marking**(10) **Pub. No.: US 2006/0064386 A1**(43) **Pub. Date: Mar. 23, 2006**(54) **MEDIA ON DEMAND VIA PEERING**(52) **U.S. Cl. .... 705/59**(76) **Inventor: Aaron Marking, Portland, OR (US)**

Correspondence Address:

**MARGER JOHNSON & MCCOLLOM, P.C.**  
**210 SW MORRISON STREET, SUITE 400**  
**PORTLAND, OR 97204 (US)**(21) **Appl. No.: 10/945,623**(22) **Filed: Sep. 20, 2004****Publication Classification**(51) **Int. Cl.**  
**G06F 17/60 (2006.01)**(57) **ABSTRACT**

A non-autonomous peer network includes a network of media devices, each device having a storage for storing media content, a processor, a communications port to allow the processor to interact with the network, and a media port to allow the processor to deliver the media content to a user. The network also has a media module to authenticate each device to allow it to receive content and control download of media to a requesting one of the devices, wherein control includes an ability to direct other devices to transfer media content to the requesting device.





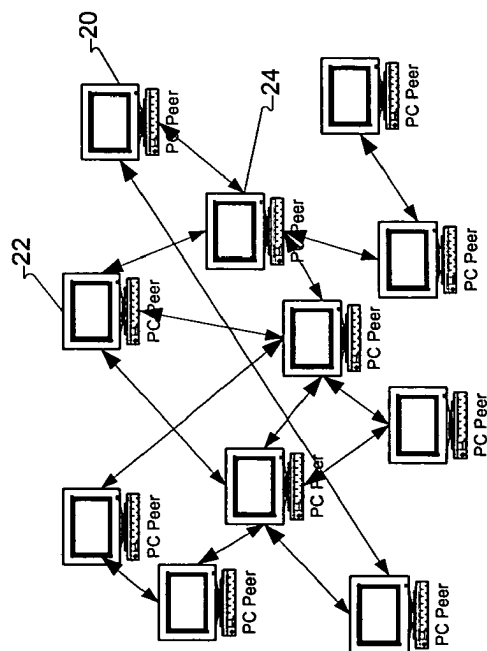


Figure 2  
(PRIOR ART)

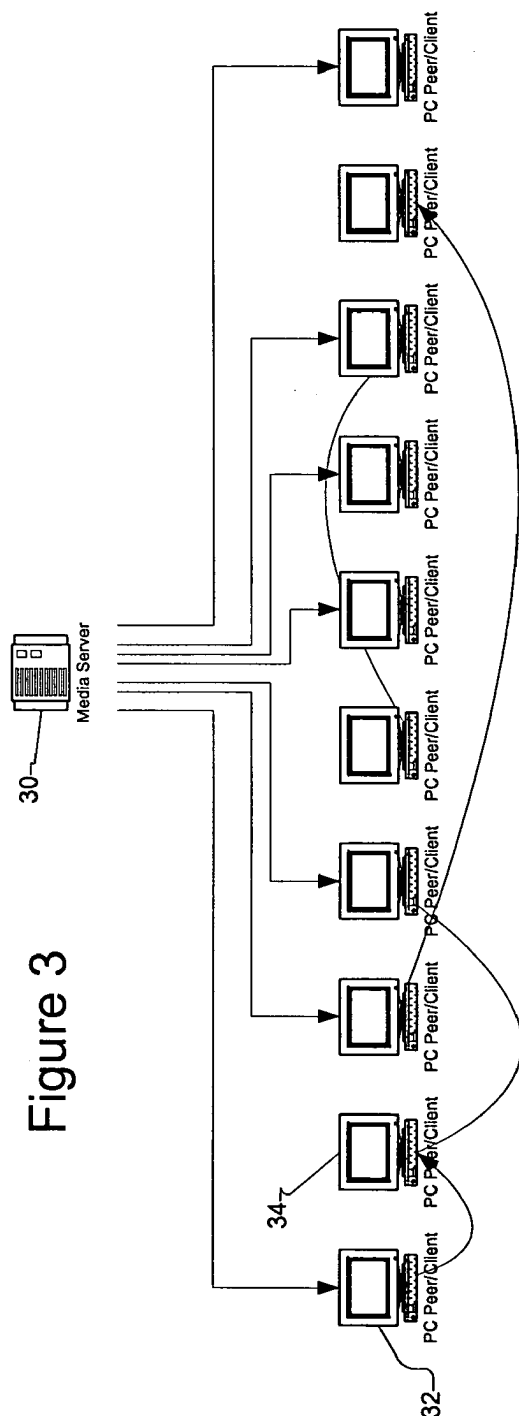
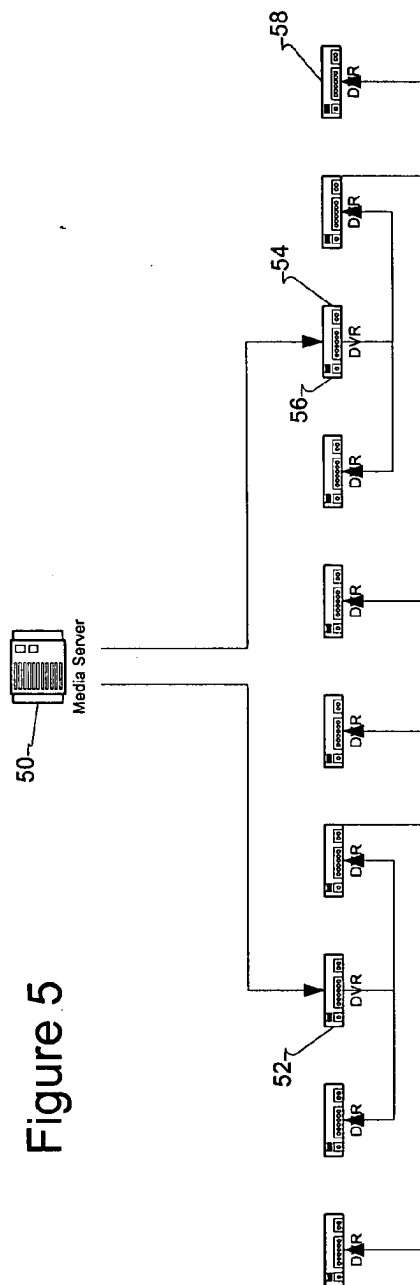
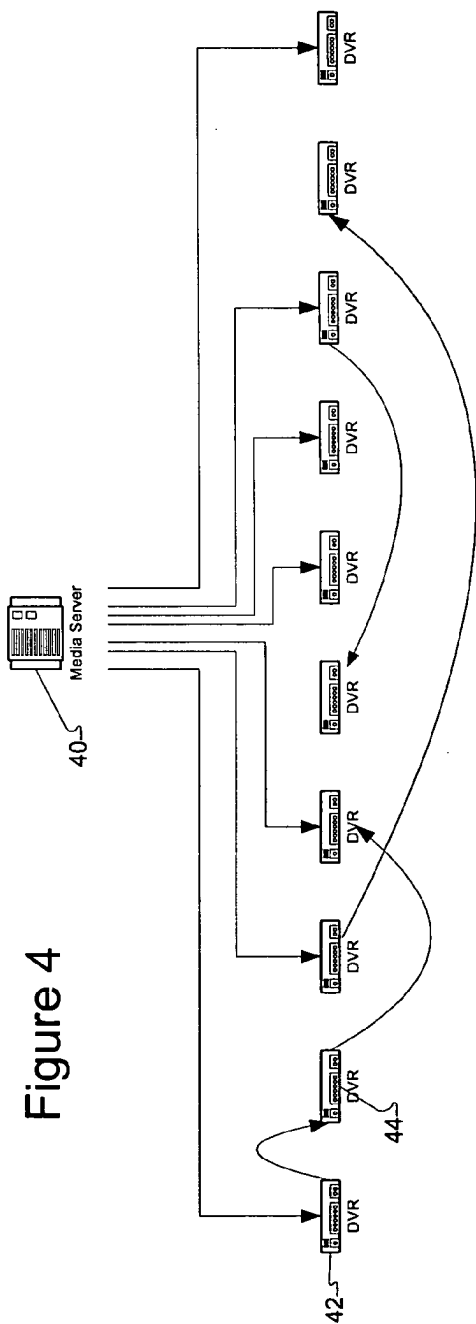


Figure 3



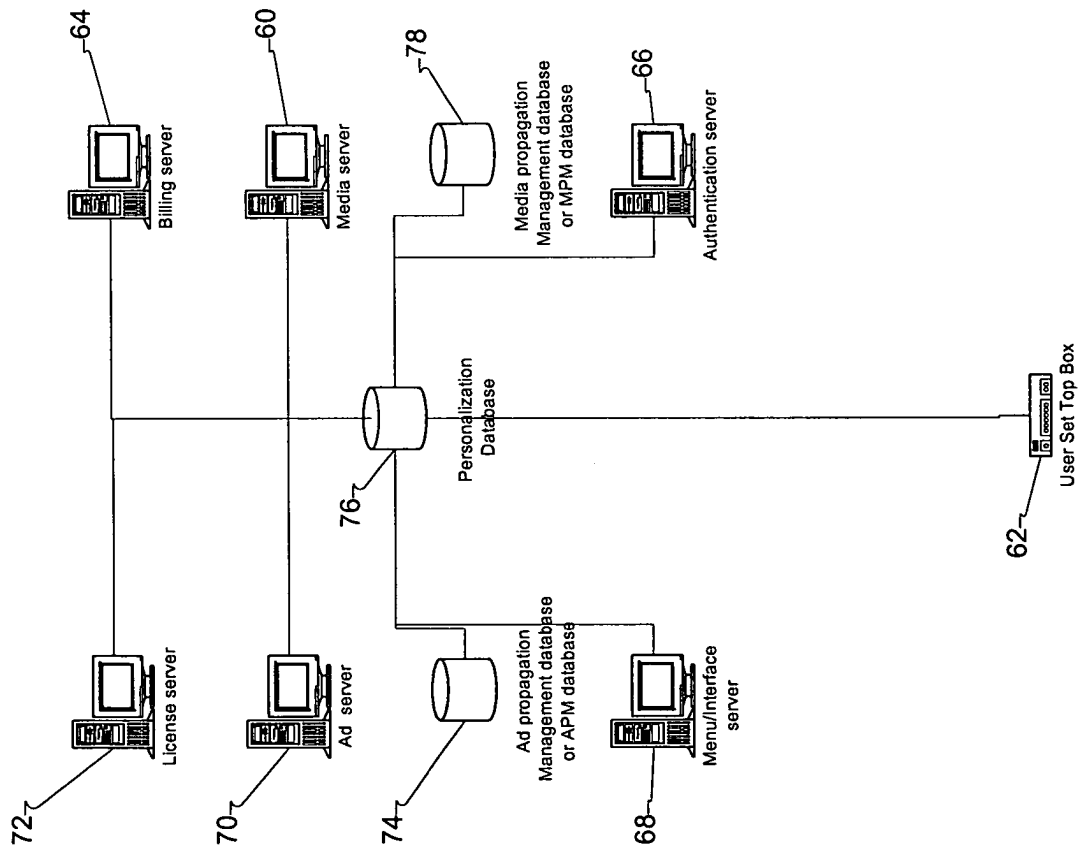


Figure 6

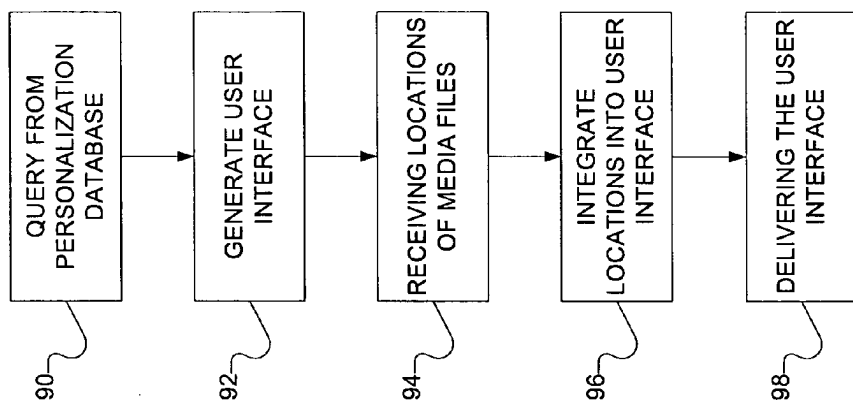


Figure 7

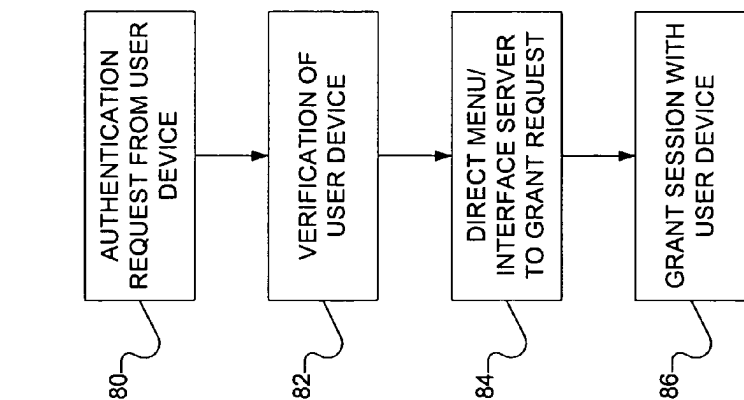


Figure 8

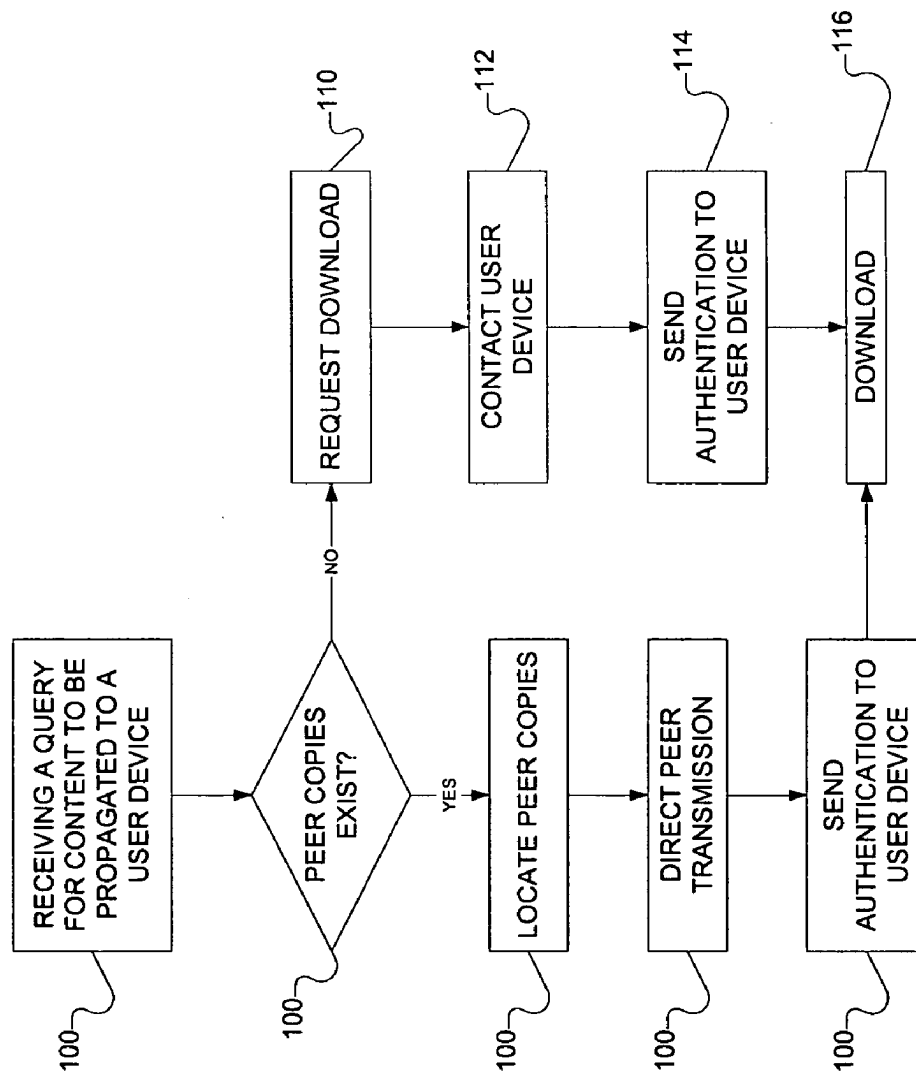
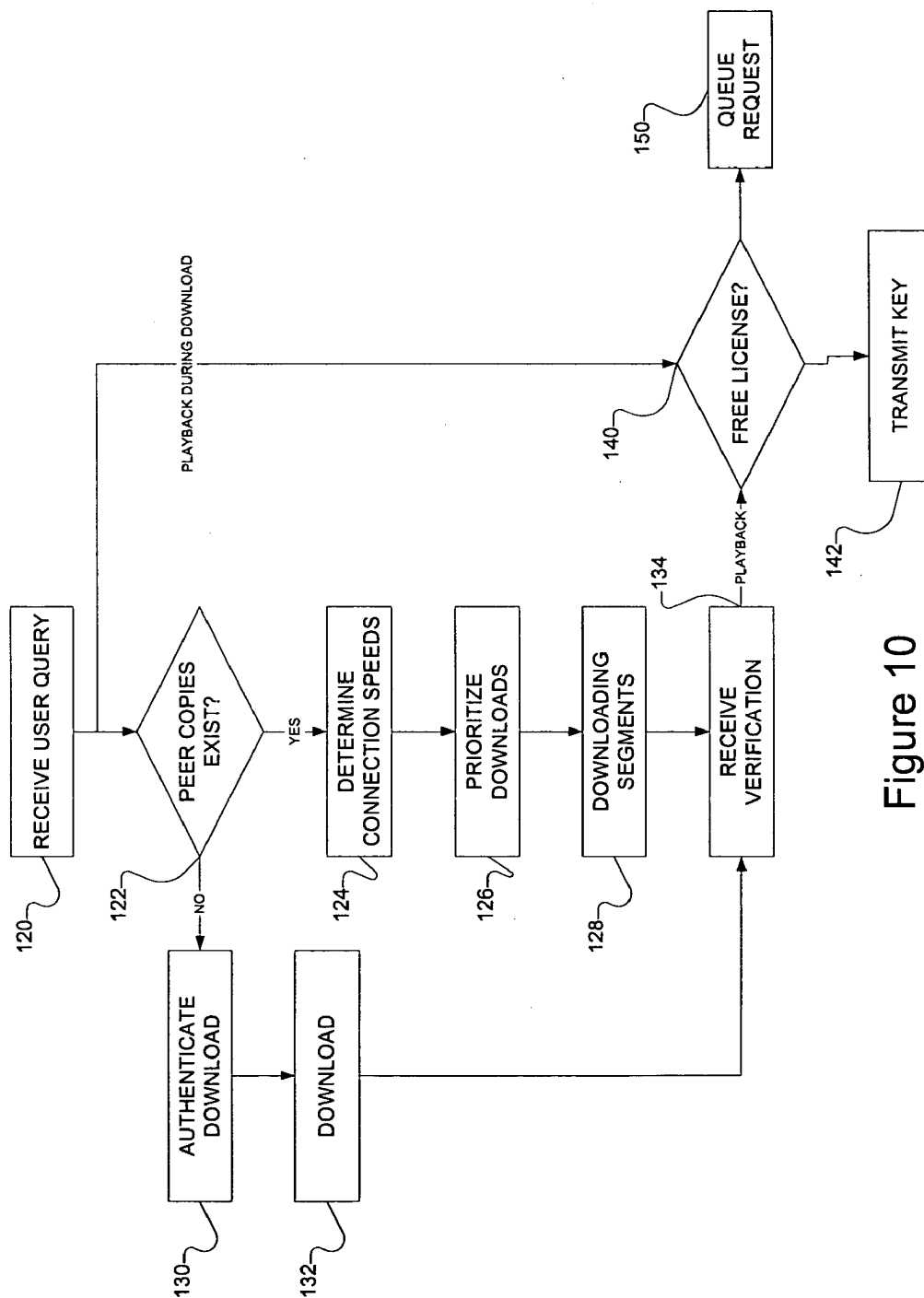


Figure 9



## MEDIA ON DEMAND VIA PEERING

### BACKGROUND

[0001] Delivery of media, such as video, music, and pictures, across networks can raise many issues. For example, sharing of digital files, such as music files, led to the situation that arose with Napster™. Owners of the content objected to having their properties being freely distributed with no payments being made to the owners.

[0002] Video on demand, such as through cable and satellite providers, may result in issues at the distribution, or head, end. The head end hardware must be extremely robust and the connectivity must be very high, as the content is delivered from one central location. This results in high start up costs, and continued operational costs.

[0003] Other types of media distribution, such as rentals, present their own issues. Rental stores must track the outstanding rentals and charge fees for overdue rentals. This decreases consumer satisfaction. Other media distributors, such as NetFlix, may suffer from high costs due to low consumer turnover of the media. Every copy of a movie owned by NetFlix has a cost associated with it. As the users are flat fee users, when a user holds on to one copy of a title for a long time, the profit made from that copy decreases.

### BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Embodiments of the invention may be best understood by reading the disclosure with reference to the drawings, wherein:

[0005] FIG. 1 shows a prior art embodiment of a client/server network.

[0006] FIG. 2 shows a prior art embodiment of a peering network.

[0007] FIG. 3 shows an embodiment of a non-autonomous peer network.

[0008] FIG. 4 shows an alternative embodiment of a non-autonomous peer network.

[0009] FIG. 5 shows a method of propagating data throughout a peer network.

[0010] FIG. 6 shows an embodiment of a non-autonomous peer network having multiple components.

[0011] FIG. 7 shows an embodiment of a method to authenticate a user in a non-autonomous peer network.

[0012] FIG. 8 shows an embodiment of a method to personalize a user interface in a non-autonomous peer network.

[0013] FIG. 9 shows an embodiment of a method to perform personalization content delivery.

[0014] FIG. 10 shows an embodiment of a method to deliver licensed content to a user in a non-autonomous peer network.

### DETAILED DESCRIPTION OF THE EMBODIMENTS

[0015] FIG. 1 shows a traditional client/server type of media-on-demand network. A central server 10, which may be a regional server or local hub as well, delivers the content

to the requesting user such as 12. The distribution hardware must be very robust so as to not fail in the middle of media content delivery, and the connection between the requesting user device and the central server must remain stable. The distribution hardware must also be able to support multiple concurrent users. In order to ensure this reliability, the components are generally expensive. This results in high startup costs, scaling costs to expand the network, and high, continuing operational costs.

[0016] As an alternative, a peering network uses each user device as a miniature server. The term 'server' as used here does not necessarily mean a separate, dedicated device as is implied by the prior art. A server could be one device upon which multiple functions are running, and so will be referred to here as a module. A media module and a license module may both be processes running on the same device, although they may be referred to separately here, for ease of discussion. Each miniature module such as 20, 22 and 24, shares storage and bandwidth resources. This mitigates the head end bandwidth and scaling problems.

[0017] As seen by examples such as Napster™ and Kazaa™, the ability to abuse the rights of the content owners is also enabled. Media license owners have come to view these types of networks with suspicion. Indeed, the very distributed nature of peering PC-based networks that allows the fast delivery of content also may make it vulnerable to hacking. There is no centralized server to authenticate users and validate the media being exchanged. Piracy becomes commonplace and the quality of the media varies greatly.

[0018] FIG. 3 shows an example of a non-autonomous network. Non-autonomous, as used here, indicates a network that cannot function in the manner of a true peer-to-peer network. Participation in the network as a peer server, as well as access to the content available from peers and centralized storage, is done through a centralized authentication process. However, once a user device is validated, it can become a peer server. In addition, each transaction can be validated to further ensure that only verified devices can receive downloads.

[0019] While transactions are centrally validated and initiated, it must be understood that there is also a large measure of anonymity. No user knows from where the content is coming, or to where it is being sent. Users will only know that they are receiving verified downloads and possibly sending content to other users.

[0020] For example, once device 32 requests a download of content, and the device has been validated by the media module 30, the content is downloaded to 32. Further on in the operation of the network, if device 34 requests a download and is verified, device 34 may receive the download from peer 32, at least in part. As the device 32 may be local to device 34, the peer download may occur more quickly than the download from the media module 30. As will be discussed in more detail further, there may be several peers similar to 32 that are transmitting data to peer 34.

[0021] The devices of FIG. 3 are shown as being personal computers. In an alternative embodiment, shown in FIG. 4, the peer devices 42 and 44 could be television set top boxes. The set top boxes (STBs) may also include digital video recorders (DVRs), such as TiVO®, or RePlayTV™ boxes. A network already connects these devices, which may be the

Internet. Each device has its own network address, more than likely an Internet Protocol (IP) address and a connection to the Internet. This network also already has some centralized control, by the subscription management system within the media module system **40**. In addition, the devices could be one of many media devices, such as music players, video games, etc.

**[0022]** As mentioned previously one embodiment of the invention uses 'shotgun' downloading, where each media file desired by a user is divided into predefined segments, such as by time, and the segments are received from several different peers. In this manner, the bandwidth needed to download content in such a system is vastly reduced when compared to a traditional client/server download. For example, consider 10 users each desiring the same 10 Megabyte (MEG) download. This results in a requirement of 100 MEGs of bandwidth. Add on top of that an overhead value for transactional instructions. For ease of discussion, 100 kilobytes (100 K) will be assumed. The overall requirement is  $2 \times 100K \times 10$ , which equals 2 MEG, plus the 100 MEGs of data to be downloaded. The bandwidth necessary is therefore 102 MEG. The need for concurrent download capability such that each user is requesting their data at the same time places a large bandwidth load on the system.

**[0023]** In contrast, a shotgun download from peers that have previously received the file reduces the amount of bandwidth required. As can be seen in **FIG. 5**, the first two peers to receive the file, **52** and **54**, then act as servers to transmit it to other peers when requested, such as peers **56** and **58**. The same file can be downloaded 10 times but only require 20 MEGs of download bandwidth, plus  $3 \times 100K \times 10$ , for transactional instructions. The same download therefore only requires 23 MEGs of bandwidth. The ability to serve several different users concurrently with relatively low bandwidth is a large advantage of this approach.

**[0024]** The network diagrams of **FIGS. 4 and 5** are simplified for ease of discussion. The network may have several different types of modules and databases distributed throughout it. Examples of other possible components of the network are shown in **FIG. 6**. As discussed previously, the user of the term 'server' does not necessarily imply a device running server software. The server may be process running in parallel or series with other processes on the same device, as well as a logical layer in a database. Essentially, a server here is a functionality provided in whatever means the system designer desires and is used interchangeably with module.

**[0025]** Generally, the network has a media module **60** and a network of user media devices, such as set top box **62**. The set top box would have storage for storing media content, a processor, a communications port to allow the processor to interact with the network, which may include exchange of data with other boxes on the network, and a media port to allow the processor to deliver the media content, such as a speaker port or a display port. The media module would then be operable to authenticate each device to allow it to receive content and control download of media to a requesting one of the devices, such as **62**, wherein control includes an ability to direct other devices to transfer media content to the requesting device.

**[0026]** A license module **72** may exist in the network. It may maintain a database of decryption keys allowing the

devices to decode the content delivered in encrypted form. The license module may track title usage in real-time to ensure that each license for each title stays within its limits. For example, there may be five available licenses for a particular title, and the license module would ensure that only five versions of the file were in use at any given time. It may also track the payouts to license holders.

**[0027]** A billing module **64** may administrate user accounts, track usage and ensure users are billed for their usage of the titles. The billing module may also allow electronic payment, etc., for the user accounts. The billing module may also take information from the license module and ensure that license holders are appropriately paid.

**[0028]** An advertisement module **70** works in conjunction with an advertisement propagation management database to propagate advertisements and other paid media files such as sponsored events and movies to the user devices. The advertisement module may also be referred to as an advertisement propagation management module. Similarly, the media module **60** may be referred to as a media propagation management module operating in conjunction with the media propagation management database **78**.

**[0029]** The databases generally track locations, such as of the advertisement media or the content media, across the peered devices of the network. As mentioned above, the various modules may be layers within the databases.

**[0030]** The media module maintains encrypted copies of all of the titles. Early in a title life cycle, when not many devices have downloaded it, the media module will provide the copies of the media files as needed. Later in the life cycle, when enough copies have been propagated among the peers to allow peer downloads, the media module may maintain an archival copy.

**[0031]** There may also be a menu/interface module **68**, which produces the user interfaces provided at the user device to allow the user to navigate the available content. This may also allow other services, such as e-mail, account management, etc. The menu/interface module may receive personalization of the menus and selections from a personalization database **76**.

**[0032]** The personalization database **76** maintains a database record of user interface personalization data, selected preferences and usage history information. It may also allow multiple user profiles per customer account, such as for multiple users in a household. The user profiles may also allow parental controls, demographic targeting for advertisers and other tailored services. The personalization database may also provide information for billing, such as credit card selections, advertisement information for the advertisement module, etc.

**[0033]** The elements of the network may provide a peering network with all of its advantages, but there must also be some sort of protection in place for the rights holders. An authentication module **66** stores client account data and ensures that only authenticated devices are available as peers for other devices as well as for downloads from the media module. One of the first processes that will take place upon a user query for a title delivery is user authentication. An embodiment of this process is shown in flowchart form in **FIG. 7**, which may be better understood in conjunction with **FIG. 6**.

[0034] At 80, the authentication module receives a request from a user device, such as a set top box. At 82 the user device is verified. Verification may take many forms, but as the user device is a dedicated piece of hardware, a hardware solution may be most desirable, such as a hardware key, a smart card or a SIM card resident in the device.

[0035] At 84, the authentication module directs the menu/interface module to grant the user request and the menu/interface module initiates a secure session with the user device at 86. Generally, this process will take place for all transactions, as will be discussed in more detail further.

[0036] In FIG. 8, an embodiment of a method of providing a personalized interface to a user is shown in flowchart form. At 90, the menu/interface module receives a request from the personalization database. The user interface is generated and populated with information derived from the personalization database at 92. Media files related to the user preferences, etc., are located at 94 from the media propagation management module and the advertisement propagation management module in response to a request from the menu/interface module. These locations are then integrated into the user interface at 96 and delivered to the user at 98. The integration of the locations may be performed by the propagation management modules, either advertisement or media modules, both advertisement and media modules, or by the menu/interface module. These functions may be distributed throughout various physical devices, databases, and application, and any combinations thereof.

[0037] The personalization information for each user provides pinpoint demographic information. This may allow for a much higher level of content tailoring, both for media and advertising. This could be accomplished in the off hours, balancing the load on the network. An example of such a process is shown in flowchart form in FIG. 9.

[0038] At 100, the personalization database may query the propagation management modules to request content to be propagated to a user device. At 102, the propagation management modules determine if peer copies exist. If peer copies exist, the peer copies are located and peer transmission is directed and monitored by the propagation management modules at 106. In the meantime, authentication is sent to the user device at 108, to ensure that the user device will allow the peers access.

[0039] If no peer copies of the desired content exist at 102, a download from the appropriate media or advertisement propagation module is requested at 110. The user device is contacted at 112, and authentication sent at 114. In either case, the download, either from peers or the media module, occurs at 116. Once the data is downloaded, the user device may cache a local copy to have it available for other peers as needed.

[0040] Downloading media content, as opposed to advertising content that is assumed to be license free as its download is for the benefit of the license owners, may require a license verification. During a media download, shown in flowchart form in FIG. 10, no license may be required. When the user attempts playback.

[0041] At 120, a user query for requested content is received. At that point, two processes occur. First, the existence of any peer copies that can be used for downloading is determined at 122 and the existence of an available

license is determined at 140. Note that the term 'free license' does not imply free from costs, just that there is a license available to be put to use. If a license exists, a key is transmitted at 142 that allows the user device to decode the content when it is received, however it is received. If there is no license currently free to be given to the user device, the user request may be queued at 150 while the system waits for a license to become available, or other options may be presented to the user. Generally, the system will strive to ensure that enough licenses are available for multiple concurrent users. This may involve generation of licenses 'on-the-fly' by the license module, with the appropriate tracking for billing and accountability.

[0042] The license key may only be needed upon playback. It is possible, in this system, for the user device to begin playback during the download process. The playback device merely determines that it has enough content to begin playback that it will not 'run out' of content before more is downloaded. In this instance, the license transaction will occur for playback during download.

[0043] Alternatively, the license may not be required at a later time, when the user attempts playback. This is shown by the 'playback' path in FIG. 10. The user may store the content on the device for any period of time the user desires. The user device may be sending the content to other devices during this time. The license is only required when the content is to be played back.

[0044] Returning to the download process, the content may be downloaded from the media module if it is an initial download. If no peer copy exists at 122, the download is authenticated to the user device at 130 and the file downloaded at 132. Once the file is downloaded, the user device verifies it to the media propagation management module so the module is aware that the user device may become an available peer for future downloads.

[0045] If peer copies exist, the media propagation management module may then determine connection speeds between the various peers and the user device at 124. The segments of the file to be downloaded may then be prioritized to allow the highest priority segments to be downloaded across the fastest connection at 126. The segments are then downloaded at 128. The user device then verifies the download at 134. During the downloading process, the user device may perform an analysis of the properties of the downloaded data, such as the compression rate and download rate, to determine when the user can begin experiencing the content while the remaining portions of it are still be downloaded.

[0046] In this manner, the advantages of a peer network are employed in a non-autonomous manner, allowing management of and accounting for license rights to media content. The network is scalable with the addition of a few additional modules and the easy addition of more peers, has relatively low start up costs and continued operation costs.

[0047] Thus, although there has been described to this point a particular embodiment for a method and apparatus for media on demand through a peering network, it is not intended that such specific references be considered as limitations upon the scope of this invention except in-so-far as set forth in the following claims.

1. A non-autonomous peer network, comprising:  
 a network of user media devices, each device comprising:  
   a storage for storing media content;  
   a processor,  
   communications port to allow the processor to interact and exchange data with the network; and  
   a media port to allow the processor to deliver the media content to a user; and  
 a media module to:  
   authenticate each user media device to allow it to receive content; and  
   control download of media to a requesting one of the user media devices,  
 wherein control includes an ability to direct other authenticated user media devices to transfer media content to the requesting user media device, and to direct each user media device to receive content from other authenticated user media devices.

2. The network of claim 1, the media module further to inform the requesting device of addresses for source devices for the content.

3. The network of claim 1 further comprising a license module.

4. The network of claim 1 further comprising a billing module.

5. The network of claim 1 further comprising an advertisement module.

6. The network of claim 1 further comprising a menu/interface module.

7. The network of claim 1 further comprising an authentication module.

8. The network of claim 1 further comprising at least one database.

9. The network of claim 8, the at least one database including one selected from the group comprised of: a personalization database, a media propagation management database, and an advertisement propagation management database.

10. The network of claim 1, the network of media devices further comprising a network of television set top boxes.

11. The network of claim 10, the network of television set top boxes further comprising a network of digital video recorders.

12. A method of authenticating a user in a non-autonomous peer network, comprising:  
   receiving a request from a user media device;  
   verifying the user media devices; and  
   directing a menu/interface module to grant a session to the user media device making the user media device available as a non-autonomous peer to other authenticated user devices in the network such that the non-autonomous peer may be directed to exchange content with other authenticated user devices.

13. The method of claim 12 further comprising granting a secure session with the user media device.

14. The method of claim 12 receiving a request from a user media device further comprising receiving a request from a television set top box.

15. The method of claim 12 verifying the user media device further comprising authenticating the user media device using one selected from the group comprised of: a hardware key, a smart card, and a SIM card.

16. The method of claim 19, the method further comprising:

  receiving the query from a menu/interface module;

  generating a user interface for a user populated with information from a personalization database based upon data for the user;

  receiving media file locations for media files to be displayed on the user interface;

  integrating the media file locations into the user interface; and

  delivering the user interface to the menu/interface module.

17. The method of claim 16, the method further comprising delivering the user interface to the user.

18. The method of claim 16, receiving media file locations further comprising:

  querying propagation management modules to verify nearest locations of media files; and

  receiving the nearest locations.

19. A method of personalizing content for a user in a non-autonomous peer network, comprising:

  receiving a query for content to be propagated to a user media device;

  determining if peer copies exist of the content on other authenticated user media devices on the network;

  if peer copies exist, centrally authorizing other previously authenticated user media device to transfer the content from the other authenticated user media devices to the user device; and

  sending an authentication for the other previously authenticated user media devices to the user media device directing the user media device to allow transmission from the other user media devices.

20. The method of claim 19, receiving a query further comprising receiving a query at an advertisement propagation management module.

21. The method of claim 19, receiving a query further comprising receiving a query at a media propagation management module.

22. The method of claim 19 further comprising receiving content at a user media device and caching it in the user device.

23. The method of claim 19 further comprising downloading the content from a propagation management module, if no peer copies exist.

24. A method of granting a license for media content, comprising:

  receiving a user query from a user media device for a media file upon a user playback attempt;

  determining if a license is available for the media file;

  if a license is available, transmitting a key to the user media device upon the user playback attempt.

**25.** The method of claim 24 further comprising queuing the user query until a free license exists, if no free license exists.

**26.** The method of claim 24 further comprising generating a new license, if no free license exists.

**27.** A method of providing content to a user media device, comprising:

receiving a user query for a media file from a user media device at a media module;

determining if peer copies exist for the media file, wherein a peer copy is a copy residing on another user media device in the network;

if peer copies exist:

using the media module to determine connection speeds between the peers and the user media device;

prioritizing download segments of the media file based upon the connection speeds between the peers at the media module;

providing authorization from the media module for download of the segments of the media file from the peers; and

receiving verification of a complete download.

**28.** The method of claim 27, downloading the segments of the media file further comprising:

determining properties of the download; and

determining a time at which the user can begin to experience contents of the media file, based upon the properties of the download.

**29.** The method of claim 27 further comprising:

authenticating a download to a user media device if no peer copies exist;

downloading the media file from a media module to the user media device; and

receiving verification of the download from the user media device.

**30.** The method of claim 27 further comprising granting a license for the media file to the user media device.

**31.** The method of claim 30, granting license further comprising:

receiving a user query from a user media device for a media file;

determining if a free license exists for the media file; and

if a free license exists, transmitting a key to the user media device.

**32.** The method of claim 30 further comprising queuing the user query until a free license exists, if no free license exists.

**33.** The method of claim 19 further comprising encrypting each segment from each peer individually.

**34.** The method of claim 16 further comprising selecting advertisement content based upon demographics of the user stored in the personalization database and integrating the advertisement content into the user interface.

**35.** The method of claim 24 further comprising allowing the user to store the media file for any length of time the user desires.

\* \* \* \* \*