Title: PERSONAL DIGITAL SERVER™ (PDS™)

Abstract: Personal digital server ("PDS") is a unique computer application for the storage, updating, management and sharing of all types of digital media files, including audio, video, images and documents, irrespective of their format. PDS provides users with a single location to store and access, both locally and remotely, all of their digital media. It also provides the user total control of the overall management of these assets.
PERSONAL DIGITAL SERVER℠ (PDS℠)

This application claims priority of provisional application Serial No. 60/344,066 filed December 28, 2001, the disclosure of which is hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates to telecommunications, and in particular to management, distribution and sharing of digital media files.

BACKGROUND INFORMATION

With the advances of computer information systems, individuals and businesses around the world have collected a wide variety of content on their computers, including music files, digital photographs and various types of documents including word processing documents and spreadsheets. One of the primary needs of computer users is the ability to share such content with other users because of affinity, friendship, and business relationships. Although there are other computer systems that allow sharing of content, there does not currently exist a comprehensive system to manage a wide variety of content from initial organization through sharing. Moreover, none of the existing systems ensure satisfactory digital rights management and are thus increasingly prone to legal challenges.

SUMMARY OF THE INVENTION

The present invention is a unique computer application ("PDS") for the storage, updating, management and sharing of
all types of digital media files, including audio, video, images and documents, irrespective of their format. PDS provides users with a single location to store and access all of their digital media. It also provides the user total control of the overall management of these assets. This level of user control is unparalleled in the marketplace today.

PDS enables a content owner (an "Owner") to share his or her digital media catalog with a limited group (a "Peer Group") of permitted users ("Peers") over a peer-to-peer network that requires only limited interaction with a central server. The sharing of Owner’s audio and video files is limited to streaming them to one Peer (or another pre-set limited number of Peers) at a time and, optionally, without an opportunity for the Peer to download, permanently store or make copies of the files, and is thus copyright-friendly. PDS makes digital content accessible from any Internet-enabled electronic device, e.g., desktop and portable computers, PDA and web-enabled cellular telephones. PDS allows each Owner to monitor and control the use of his or her digital catalog, including the ability to see which Peers are accessing particular files and to cancel their access at any time. The system also allows an Owner to expose or grant access to files on Owner’s computer without having to move files to a special place and without exposing any of the characteristics of the folder or directory structure of Owner’s computer. This
access method is keyed to the visitor's email address and enables secure trusted communications without exposing passwords or requiring a complex setup.

PDS users will also benefit from a proprietary User Interface designed specifically for the new ways in which personal digital media can be managed via the storage server. In addition to its core technology, PDS may include the following "add-on" features:

- **Music**: organizer, playback (by multiple simultaneous users via any Internet enabled device), play lists, detailed artist/album information, recommendations, downloads, purchase, CD creation & management of portable MP3 players.

- **Photos**: organizer, storage for thousands of photos, display with zoom, printing (to low-cost photo quality printers), auto-upload from digital cameras.

- **Internet Radio**: organizer, access to thousands of stations, time based recording and playback, download to portable players.

- **Home Video**: organizer, storage of home videos, playback (by multiple simultaneous user via any Internet enabled device).

- **Books**: organizer, storage for hundreds of audio or eBooks, playback (by multiple simultaneous users via any Internet enabled device), download to portable players.

- **Document Library**: organizer, storage for thousands of files, upload, download, auto PC backup.
Third-Party Delivery: music downloads, photo processing, documents.

PDS' core technology utilizes several components that can be categorized as follows: (1) authentication and authorization of Peers, (2) "real-time" detection and sorting of a Peer's digital files, (3) indexing of digital files and exchange of such indices among the Peer Group, (4) searching for auxiliary content, (5) remote access to digital content, (6) restricting access to copyrighted media, (7) intelligent bandwidth management and (8) information system and architecture for a peer-to-peer network. Each of these components is detailed below.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a flow diagram of the authentication and authorization processes;

Figure 2 is a flow diagram of the index update and exchange processes;

Figure 3 is a flow diagram of the global content distribution process;

Figure 4 is a flow diagram of the search algorithm;

Figure 5 is a flow diagram of the file lending process;

Figure 6 is a flow diagram of the bandwidth allocation algorithm; and

Figure 7 is an illustration of the PDS system architecture.

(a) Simplicity - Using E-mail Addresses to Verify User Authorization. PDS includes a very simple e-mail address based system for an Owner to authorize others to access Owner’s media. To provide access to a given user (a “Guest”), the Owner simply enters the Guest’s email address. PDS then sends an e-mail “Invitation” to the Guest. If the Guest has never registered with the PDS central server, the Guest is directed to set up a PDS master account on the PDS central server by submitting a valid e-mail address and a password of their own creation. This registration only needs to occur once, and the Guest is then enabled, though not authorized, to access any PDS-networked/enabled device.

(b) Security - Using GUID at the Peer-to-Peer Level. When the Guest tries to access the Owner’s PDS to which the Guest had been invited, the Owner’s PDS requests a global unique identifier (“GUID”) that applies only to transactions between this particular pair of users (i.e., the Owner and the Guest). This GUID is used in place of the Guest’s password, so that the Owner’s PDS never needs to see or store the Guest’s password. If the Owner’s PDS is not supplied with the correct GUID from the Guest, it issues a challenge and requests that the PDS central server authenticate the Guest. This initiates a process illustrated in FIG. 1, whereby the
PDS central server authenticates the Guest and generates a new "GUID" which is then supplied to both the Owner's PDS and the Guest. The Guest is now authorized to access the Owner's PDS. Thus, for example, if a user (the "Requesting User") wishes to listen to a song stored by a Peer (the "Providing User"), the Requesting User's computer (or another access device) needs to transmit the correct e-mail addresses and the corresponding GUID. This method avoids sharing passwords among users of the system, thus providing privacy to the Requesting User and also eliminating the occurrence of "cascading" breaches (where an intruder who breaks into the hard drive of one user can steal the passwords of all of such user's Peers and therefore defeat the security on each successive degree of separation). The GUID-based authentication system (as opposed to password-exchange alternatives) also helps prevent a Requesting User from caching or downloading streamed audio and video files, thereby making PDS copyright-friendly. It additionally allows a Guest to create his or her own password that works across an unlimited number of unconnected devices without ever passing the Guest's password to those devices.

(c) Fault Tolerance and Scale - Limited Need for a Central Server. GUID-based authentication substantially reduces the burden on the PDS central server. The central server needs to be involved only the first time the Requesting User's access device contacts the Providing User. All
subsequent communications or transactions can occur on a direct Peer-to-Peer basis by using the GUID. This vastly improves the fault tolerance and scalability of the PDS network, as new users and devices can be added without exerting significant additional strain on the central server.

2. **File Detection.** After installing the software, the PDS file detection algorithm scans all of the user’s drives and directories with the exception of system and temporary directories, detects and identifies media files and organizes them by type, regardless of the application that created, updated or stored them. This operation takes several minutes, as opposed to the half-hour or more required by the existing algorithms. The reason it is quicker is that it initially identifies metadata by parsing the filename, instead of reading the imbedded tags within the MP3, WMA and associated files. Filenames can be parsed effectively, because many storage applications utilize standardized nomenclature. For example, the names of audio files typically include the artist, album and track titles, and the file type. Existing file detection algorithms look at the filename to detect the file type, but identify the media content itself by searching for imbedded tags within the file. PDS, on the other hand, looks at the filename to detect both the file type and identify the media content. Only if the filename does not
contain the metadata, PDS would look for "embedded" tags within the file.

While a user's PDS is running, the algorithm intermittently scans the hard drive whenever the user's computer is idle, i.e., is not performing other, memory consuming functions. During the initial data collection, the algorithm compiles a table of directories where it finds media files. At each subsequent scan, the algorithm looks at these directories first, and when a file changes in a directory, that directory is automatically rescanned, and the listing of its contents is updated. This "background" scanning is incremental, i.e., it only detects files that have been added to the user's computer since the previous scan, and therefore takes mere seconds. Another distinguishing feature of this algorithm is that it searches locations where new files might be stored in the decreasing order of likelihood: it first looks at the most logical place other applications store media files, then proceeds to look in the least likely places. This methodology conserves search time and the operating memory of the user's computer.

3. **Index Updates and Exchange; Content Distribution.**

After PDS scans a user's hard drive for digital media content, it organizes the new content by file type and creates or updates an index of the content. The user's PDS then sends a copy of the updated index to each of its other Peer Group
members, utilizing the GUID authentication algorithm described in paragraph 1 above. This operation is performed intermittently and upon detection of new content, throughout the period of time the user is logged on the PDS network. The advantage of such index exchange is that Peers are not required to search the entirety of each other’s hard drives to find a particular file — instead, they search each other’s indices which are continuously updated. This again conserves time and operating memory. Importantly, neither the users’ digital media content nor their indices are copied onto the central server, which makes the network much more scalable and less prone to be overloaded and malfunction. The updates are user specific, so that the Peers only receive indexes that list content they are authorized to access. Additionally, the distributed indexes allow users to review the index of content stored even on those devices which are not turned on. FIG. 2 illustrates an index update and exchange algorithm according to the present invention.

The technology involved in index exchange also enables (but does not require) distribution of content from the PDS central server. Thus, it is very easy and convenient to send software upgrades, promotional messages and media files to the users of the network. FIG. 3 illustrates a variation of the index-exchange algorithm that enables such network-wide content distribution.
4. Searching for Auxiliary Content. The central server may contain certain information of general interest about particular media files stored on a user's hard drive, for example, a database of music titles, cover art and artists' biographies. A user requesting a particular title from a Peer might want to access and download such information. The PDS content search algorithm is unique in that it will begin searching for the requested information at the less likely source, i.e., on the Peers' hard drives, and will turn to the most likely source - the central server - only if none of the active Peers have the information. This method significantly reduces search time and the overloading of the central server. FIG. 4 illustrates an algorithm for this search function. - This new method of programming - moving from less reliable sources of information to the most reliable source - can be applied in many applications where network-wide speed and conservation of resources is more important than immediate reliability.

Remote File Access. There are currently two general types of remote-access applications that allow users' to access their own (and each other's) files across various Internet-enabled devices, neither of which matches the remote-access capabilities of PDS. The first type includes applications which depend on replicating the home computer's graphical desktop environment on the remote-access device. This method does not work well for access devices which either are not
built for a graphical desktop environment or use a "smarter screen resolution, such as PDA and cell phones. It also requires a high-speed Internet connection and does not work well in a multi-user setting, due to its limited ability to control access at the file level. The second type of remote-access applications, such as access based on the FTP protocol or facilitated by a web-server, depends on the ability of the remote device to browse the home computer's file directories. It is prohibitively complex to integrate the functions of authorization of users and files into applications of this type. It also poses issues in that the users must know what the content is named and where the content is located on the host. Instead, PDS' remote access feature utilizes a method of publishing a view of the content (formatted in XML if relevant to include) that is user specific (only the content that specific user is authorized to see) and able to include enhanced meta data (logically organized and containing descriptions/labels more meaningful than simply file names). This view is able to be easily formatted to any device as it requires neither the replication of the desktop environment, nor the browsing of file directories. This enables PDS users to access and or share their own media files (e.g., listen to music and view videos) remotely in a contextually relevant, simple and reliable manner regardless of the type of access device.

6. **Restricted File Access.** PDS ensures copyright-friendly music and video file sharing by (a) preventing the recipient of streamed audio and video files from saving,
copying, caching or downloading them and (b) blocking others from accessing the file while it is being streamed. This approach electronically replicates the lending of copyrighted works in the physical world of books, tapes and CDs. There currently does not exist a system for peer-to-peer sharing of digital media, which limits the sharing of media to a one-on-one experience, such that, for example, a single song from a CD is played to only one person (or another pre-set number of simultaneous users) at any one time. PDS creates a vehicle for the sharing of music (and/or video) with reasonable limitations on the User, whereby music is not spread unintentionally or intentionally beyond the single play of one song for one user (or another pre-set number of simultaneous users) at a time. The PDS system further limits the sharing of music (and/or video) to closely-related users, such as friends or business associates.

Other systems that are capable of preventing access to a content stream do so by authorizing access to particular groups of content, with the number of simultaneous users limited only by the resources of the system’s central server, not by software design as in the case of PDS. Additionally, these other systems do not block access to the underlying media file itself; the file may thus be used by several applications at the same time, creating a possibility of copyright infringement. PDS is more protective of copyright
owners in that it blocks the streamed file from being accessed by any other user or application. The PDS approach also allows for treating different types of media files differently, i.e., access need not be restricted for personal photographs and documents, where copyright infringement is unlikely. In addition, each Owner can customize levels of access to such Owner’s digital catalog using several parameters, e.g., identity of a Peer, file type and individual file name. The Owner can also limit the length of time a Peer can access a file, as well as specify the type of access the Peer is granted, e.g. playing, viewing or borrowing. The Owner can terminate or change the level of a Peer’s access at any time. Finally, the system can be used for streaming real-time content, as well as sharing downloaded content utilizing Digital Rights Management techniques. Below is the technical description of the PDS file-access restriction method:

File “borrowing” can be implemented by streaming or by having the Requesting User make a copy of the file. Streaming has the advantage of allowing the Requesting User to immediately render the file via the stream. Streaming requires that the Requesting User have an Internet connection to the Owner’s PDS device for the duration of the streaming. Copying, on the other hand, has the advantage of allowing the Requesting User to render the file at a later time without being connected to the Owner’s PDS device. The examples below
outline the methods of streaming and copying by one Peer at a time; however, the PDS software is configurable to limit the streaming and copying to two or any other number of Peers at a time.

A. Method for Peer-to-Peer File "Borrowing" via Streaming:

1. The PDS software running on a Requesting User's access device maintains an index of all media files. The index also contains metadata for each media file, including information about who currently has borrowed the file, when they borrowed the file, and for how long they borrowed the file.

2. When the Requesting User attempts to stream a media file, the system first determines (by reading the metadata about the file from the index) if the file is already "borrowed" by another Peer. If so, it rejects the request. Otherwise, it will update the metadata for the file in the index, lock the file from use by other applications and allow the Requesting User access to the stream.

3. The stream is encrypted in a way which will only allow it be "rendered" by the Requesting User while being streamed from the Owner's PDS device. This prohibits the Requesting User from making a "copy" of the stream for later playback or viewing.
B. Method for Peer-to-Peer File “Borrowing” via Copying the File:

1. The PDS software running on a Requesting User’s access device maintains an index of all media files. The index also contains metadata for each media file including information about who currently has borrowed the file, when they borrowed the file, and for how long they borrowed the file.

2. When the Requesting User attempts to copy a media file, the system first determines (by reading the metadata about the file from the index) if the file is already “borrowed” by another Peer. If so, it rejects the request. Otherwise, it will update the metadata for the file in the index to reflect that the Requesting User has borrowed the file and lock the file from use by other applications.

3. The system encrypts the file, adding encrypted metadata to the beginning of the file marking who the Owner is, who the Requesting User is, and when the “borrowing” will expire. A copy of the encrypted file is then transferred to the Requesting User’s machine.

4. The software will restrict the Owner of the file from rendering the file in any way until the expiration date and time of the “borrowing” has been reached.
5. The software will only allow the Requesting User to render the file up until the time the expiration has been reached.

FIG. 5 illustrates an exemplary flow of events among three peers, showing restricted access to media files according the present invention.

7. Bandwidth Management. PDS utilizes a novel approach to bandwidth management by monitoring and streaming from a Providing User’s PDS device and restricting access when that device is at or near the peak of its overall bandwidth capacity. This provides a better user experience, reduces the delay in file access and facilitates more even allocation of Peer Group resources. The system also allows for reserving a “guaranteed” amount of bandwidth (and thus a “guaranteed” level of access) for certain users or groups of users. FIG. 6 illustrates a bandwidth management algorithm according to the present invention.

8. An Information System and Architecture for a Peer-to-Peer Network. Most computer network systems on the Global Computer Network rely on a central node or “super node” for the co-ordination, organization and management of their related users and the sharing of information and content. There currently does not exist a system for peer-to-peer access and the sharing of content among users, which does not rely on the continuous use of a central device. The PDS
peer-to-peer network described herein only relies on the central server for initial setup, fail over, and addition and authorization of new users and devices. An exemplary peer-to-peer network is schematically illustrated in FIG. 7. The system’s design provides for the direct secure communication among the networked devices without the involvement of a central server. Each PDS device contains the required information that allows it to directly communicate with and update all of the other PDS devices within its Peer Group. This self-reliance of individual nodes provides the system with:

- Ability to directly and securely request and implement peer-to-peer content sharing and transfer
- A scalable system not limited by amount of content or number of devices in the network
- Ability to securely request information from Peers regarding another Peer without accessing a central server and without disclosing the Peer’s password.
- Ability to self-configure and maintain network connections without the involvement of a central server.
What is claimed:

1. A system for sharing content between a plurality of computer users, comprising:
   a central server for initial authorization of said users to participate in said plurality;
   at least one first computer, wherein said content is stored; and
   at least one second computer, designated as the guest, wherein communication between said first computer and said guest is authorized by a global unique identifier.

2. The system of claim 1, wherein said global unique identifier is created by said central server.

3. The system of claim 2, wherein said central server distributes said global unique identifier to said first and second computers.

4. The system of claim 1, further comprising a password used by said second computer to access a computer network, wherein said global unique identifier is different from said password.

5. The system of claim 1, wherein said global unique identifier is unique to communications between said first and second computers.

6. The system of claim 1, further comprising an email address for each computer user, wherein said communication is identified using said second computer user’s email address and said global unique identifier.
7. A method for a new computer user to access content contained within the computer of the owner of said content, comprising the steps of:
   a. registering said new computer user with a central server;
   b. attempting a first access to said owner's computer;
   c. receiving from said central server in response to said first attempted access, a global unique identifier, said identifier sent to said owner's computer and said new user's computer;
   d. accessing successfully said content from said owner's computer, using said global unique identifier to authorize said access.

8. The method of claim 7, wherein said central server receives a communication from said owner's computer to allow said new user to access said content.

9. The method of claim 7, wherein said new user registers with said central server by transmitting its email address and a password.

10. The method of claim 7, wherein said owner's computer notifies said central server of said first attempted access by transmitting said email address of said new user to said central server before receiving said global unique identifier therefrom.

11. The method of claim 10, wherein said central server verifies said email address of said new user's computer before distributing said global unique identifier to said new user and said owner.
12. A method wherein a computer user, designated as the owner of content, can allow a new computer user to access said content, comprising:
   a. sending a first communication to said new computer user offering access to said content;
   b. sending a second communication to a central server, said server responsible for maintaining a database of authorized users, notifying said server of said offer to said new user;
   c. rejecting a first attempt from said new user to access said content;
   d. notifying said central server of said rejection;
   e. receiving a global unique identifier to be used for all authorized accesses by said new user to said owner from said central server, wherein said central server generates said global unique identifier in response to said notification; and
   f. allowing access to said new user only when said access is accompanied by said global unique identifier.

13. The method of claim 12, wherein said second communication to said central server and said notification of said rejection to said central server comprise the email address of said new user.

14. A method for a central server to authorize communication between a computer user, designated as the owner of content and a new computer user, attempting to access said content, comprising:
a. receiving a first communication from said owner, authorizing said new user to access said content;
b. recording said authorization in an internal database;
c. receiving a second communication from said owner, notifying said central server that said new user has attempted access to said owner’s content;
d. Scanning said database for said new user’s authorization; and

e. Communicating a global unique identifier to said existing member and said new user if said new user is authorized within said database.

15. The method of claim 14, wherein said first and second communications contain the email address of said new user.

16. The method of claim 14, further comprising the step of receiving a communication from said new user, which registers said new user with said central server before said communication of said global unique identifier is permitted.

17. An efficient method of searching a computer file system for files comprising predetermined content, comprising:

a. scanning the directories within said file system to identify files having predetermined files types;
b. checking the filenames of said identified files to insure that said filename contains metadata, said
metadata comprising a description of said content;
and

c. using embedded tags within said file to obtain said
metadata, only if said metadata was not present in
said filename.

18. The method of claim 17 wherein said predetermined
content is media.

19. The method of claim 17, wherein said files are
stored in a list.

20. The method of claim 17, wherein a list of
directories wherein said files are located is generated
by and stored within said computer during said search.

21. An efficient way of updating a list of files in a
computer file system, said computer having created a list
of directories wherein said files are located,
comprising:

a. first checking said list of directories for
   alterations since last said check;

b. rescanning said directory if said alterations are
   found; and

c. updating said list of files with results from said
   rescan;

22. The method of claim 21, wherein the order that said
directories are checked is based on the likelihood of
finding said files in said directory, whereby the
directory with the highest said likelihood is checked
first.
23. A method for a first computer user, designated as the owner of content, to notify a plurality of computer users of the availability of said content available for sharing, each of said plurality having authorization to access a subset of the said content, comprising:
   a. creating an index of said content;
   b. updating said index whenever new content is created;
   and
   c. communicating said updated index to said plurality.
24. The method of claim 23, wherein said communication is authorized by a global unique identifier.
25. The method of claim 23, wherein said communicated updated index to each of said plurality contains the subset of said content that each has said authorization to access.
26. A method for a first computer user to determine the newest content available for sharing on a second computer, wherein said first computer contains an index of said content available on said second computer as of a defined date and time whereby said first computer requests an updated index of said newest content created since said defined date and time.
27. A method of distributing content from a central server to a plurality of computer users, comprising:
   a. sending said content from said central server to a first computer of said plurality of computers;
b. sending, from said central server to said first computer, a list of users from said plurality authorized to access said content; and

c. sending said content from said first computer to each user of said plurality identified on said list.

28. A method for a first computer user, designated the requestor, to find content among a plurality of computer users and a central server responsible for authorizing said users to participate in said plurality, comprising:

a. requesting, from each of said plurality, said content, in decreasing order of likelihood that said user possesses said content, until said content is found; and

b. requesting said content from said central server only if said content is not available from said plurality.

29. The method of claim 28, whereby the requestor uses a first address to communicate with each of said plurality, wherein said requestor requests an updated address for each said user that said requestor is unable to establish communication with using said first address.

30. The method of claim 29, wherein said requestor requests said updated address from said users of said plurality that said requestor is able to communicate with.

31. The method of claim 29, wherein said requestor uses said updated address to request said content from said
previously unreachable user prior to requesting said content from said central server.

32. The method of claim 29, wherein said addresses are IP addresses.

33. A method to allow access to content on a computer remotely, using a remote access device, whereby an application on said computer reformats and packetizes said content before transmitting to said remote access device.

34. A method for electronically sharing content on a first computer among a plurality of computer users, whereby said first computer can allow said plurality to borrow said content, comprising:
   a. rejecting access to said content if said content is currently borrowed; and
   b. accepting said access if said content is not borrowed.

35. The method of claim 34, further comprising:
   a. maintaining an index of all said content contained on said computer; wherein said index comprises title of said content, and whether said content is currently borrowed;
   b. checking said list when one of said plurality attempts to access said content;
   c. rejecting said access if said index indicates said content is currently borrowed;
   d. accepting said access if said content is not borrowed; and
e. updating said index to denote said content is borrowed after accepting said access.

36. The method of claim 34, wherein said content is copyrighted.

37. The method of claim 34, wherein said first user determines a time period for which said content can be borrowed.

38. The method of claim 35, wherein said index further comprises the date that said content was borrowed.

39. The method of claim 35, wherein said index further comprises the date when said borrowing will expire.

40. The method of claim 34, whereby exactly one of said plurality can access said content at a time.

41. The method of claim 34, whereby said content become unusable to said borrower after the period of said borrowing has expired.

42. A method of encrypting a file so as to allow a first computer user to borrow said file from a second computer user such that said file is only usable by said first computer user from a predetermined time, by adding encrypted metadata denoting when said predetermined time expires.

43. The method of claim 42, wherein said second computer user is unable to use said file until said predetermined period expires.

44. The method of claim 42, wherein said metadata further comprises information denoting said first user as the borrower of said file.
45. The method of claim 42, wherein said metadata further comprises information denoting said second user as the owner of said file.

46. A method of allocating bandwidth among a plurality of computer users accessing content on a first computer comprising:
   a. gauging optimal bandwidth needed for accessing said content by one user of said plurality;
   b. allowing access to said content by said one user if overall available bandwidth exceeds said optimal bandwidth;
   c. reducing said overall available bandwidth by said optimal bandwidth if said access is allowed; and
   d. rejecting said access to said content if overall available bandwidth is less than said optimal bandwidth.

47. The method of claim 46, wherein said optimal bandwidth is determined by sending a test file from said first computer to said accessing user.

48. The method of claim 46, wherein a portion of said overall available bandwidth can be reserved, said portion only available for use by a group of preferred users, to guarantee access to said content by said group of preferred users.

49. A system for a plurality of computers to share content securely and directly with one another, comprising:
   a. a first computer,
b. a second computer, said second computer sharing said content with said first computer; and
c. a central server, said server responsible for creating a secure link between said first computer and said second computer.

50. The system of claim 49, further comprising a third computer, wherein said central server authorizes said third computer to participate in said plurality.

51. The system of claim 49, wherein said first and second computer share said content after said creation of secure link directly without involvement of said central server.
Step 1. Authorization

A. User Sam@PDS.com authorizes Fred@Client.com by entering the email address in the authorize function in his PDS
B. User Sam@PDS.com's PDS sends Fred's authorization to the central server, which registers the relationship
C. User Sam@PDS.com's PDS emails Fred@Client.com to let him know of the authorization and provides instructions

Step 2. Registration

D. Fred@Client.com receives the email, optionally downloads and installs the PDS software and registers his email and personal password with the server

Step 3. Initial Access

E. User Fred@Client.com attempts to log in to Sam@PDS.com passing his email and a default GUID
F. User Sam@PDS.com's rejects the default GUID and sends an identification challenge to the central server
G. User Sam@PDS.com's notifies Fred@Client.com of the challenge. Fred@Client.com waits for new GUID from the Central Server
H. Central Server generates a new GUID specific to this pair of users
I. Central Server sends the new GUID to the two user's machines
J. Upon receipt of the new GUID, Fred@Client.com retries access

Step 4. Authorized Access

K. User Fred@Client.com attempts to log in to Sam@PDS.com, passing his email and the GUID associated with Sam@PDS.com
L. User Sam@PDS.com's PDS verifies the email and GUID and provides access

FIG. 1
A. User Sam@PDS.com detects a change in its index (this could occur at numerous points when the application is running).
B. User Sam@PDS.com's PDS sends the index changes to each of the PDSs that have access to it. This change list only contains changes that pertain to content that the specific PDS is authorized to access. The IP address of each of the destination PDSs is determined by first checking to see if the last known IP is still valid and, if not, then by following the process described in Section 4.

C. Fred@Client.com checks with Sam@PDS.com to see if there has been any index updates since a supplied date and time.
D. Sam@PDS.com processes the request and sends back changes, if any.

FIG. 2
Step 1. Content Push

A. The central server sends a piece of content (program update, media files, etc.) to a given PDS. Attached is a distribution list of other PDSs that the given PDS has an authorized relationship with.

B. User Sam@PDS.com detects the new file.

C. User Sam@PDS.com's PDS sends the file to each of the PDS on the distribution list. The IP address of each of the destination PDSs is determined by first checking to see if the last known IP is still valid and, if not, then by following the process described in Section 4.

FIG. 3
Step 1. Find most likely Peer

Central Server

A. Sam@PDS.com
B. Fred@Client.com

A. User Sam@PDS.com detects that it needs a file (album art, Bib, PDS IP address, etc.)
B. User Sam@PDS.com PDS checks the index of its Peer Group PDS’s content to see which is the most likely to have the needed content. (Likelihood is based on the similarity of the desired file to the PDS’s index, the size of the PDS’s index and/or the level of activity of the PDS’s index)

Step 2. Initial Test of Peers

Central Server

D. Sam@PDS.com
C. Peer Group PDS’s

C. User Sam@PDS.com’s PDS sends a content request to the most likely PDS to see if it has the needed content. The IP address of the PDS is determined by first checking to see if the last known IP is still valid.
D. If found, the content is returned to Sam@PDS.com. If not, Sam@PDS.com cycles through the potential PDS’s in its Peer Group. If the required content is still not found, goto step 3.

Step 3. 2nd Test of Peers

Central Server

F. Sam@PDS.com
E. Peer Group PDS’s

E. User Sam@PDS.com’s PDS sends a request to the Peer Group members for the last known IP address of any of the Peers that it has been unable to contact. Using the updated IP’s User Sam@PDS.com’s PDS sends a content request to the remaining PDS’s that it has been unable to contact to see if they have the needed content.
F. If found, the content is returned to Sam@PDS.com. If not, Sam@PDS.com cycles through the potential PDS’s in its Peer Group. If the requested content is still not found, goto step 4.

Step 4. Access Central Server

Central Server

G. Sam@PDS.com
H. Peer Group PDS’s

G. If the content is not found on any of the Peer Group PDSs, the PDS will contact the central server to get the needed content.
H. Central server returns the requested content.

FIG. 4
Step 1. User 1 accesses a file

Central Server

A. User Sam@PDS.com accesses a file (music, video, etc.) on Fred@Client.com's PDS.
B. Fred@Client.com locks the file (and any related files in its associated collection) and begins sending the file data to Sam@PDS.com. The lock can be for as long as the file is being accessed or for a given period of time.

Step 2a. User 2 tries to access the same file or collection

Central Server

D. User Jerry@music.com tries to access the same file (or any in the related collection) that Sam@User.com is currently using.
C. Fred@Client.com denies Jerry@music.com access.

Step 2b. PDS owner tries to access the same file or collection

Central Server

F.

E. Jerry@music.com
G. Fred@Client.com

E. The owner of Fred@client.com tries to access the same file (or any in the related collection) that Sam@User.com is currently using.
F. The file(s) is locked so that Fred@Client.com is denied access.
G. The owner can optionally cancel/withdraw the access from Sam@PDS.com.

Step 3. User 1 finishes accessing the file

Central Server

H. User Sam@PDS.com finished accessing the file on Fred@Client.com
I. Fred@Client.com unlocks the file (and any related files in its associated collection).

FIG. 5
Step 1. User 1 connects to remote PDS

Step 2. User 2 tries to access the same PDS

A. User Sam@PDS.com accesses Fred@Client.com's PDS
B. Fred@Client.com sends Sam@PDS.com a test file to gauge available bandwidth
C. Fred@Client.com determines optimum bandwidth for this session

D. Jerry@Music.com accesses Fred@Client.com's PDS
E. Fred@Client.com sends Sam@PDS.com a test file to gauge available bandwidth
F. Fred@Client.com determines optimum bandwidth for this session

Step 3a. PDS owner tries to remotely access the PDS without reserve

Step 3b. PDS owner tries to remotely access the PDS with reserve

G. The owner of Fred@client.com remotely accesses Fred@Client.com's PDS
H. Fred@Client.com sends a test file to gauge available bandwidth
I. Fred@Client.com determines optimum bandwidth for this session and denies access
J. The owner can optionally cancel/withdraw the access from other users to gain access or additional bandwidth
K. The owner of Fred@client.com remotely accesses the Fred@Client.com PDS
L. Fred@Client.com has already reserved bandwidth for this user. Session begins.

FIG. 6
FIG. 7
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : HD4L 9/00
US CL : 713/171
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)
U.S. : 713/171

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 practicable, search terms used)
East

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5,748,735 A (GANESAN et al) 05 May 1998 (05.02.1998) Col. 8, line 15 - Col. 12, line 39</td>
<td>1-11, 14-16, 49-51</td>
</tr>
<tr>
<td>Y</td>
<td>Figs 3-5 Col. 6, line 5 - Col. 7, line 52 Col. 8, line 15 - Col. 12, line 39</td>
<td>12, 13</td>
</tr>
<tr>
<td>X,P</td>
<td>US 6,477,644 B1 (TURUNEN et al) 05 November 2002 (05.11.2002) Col. 1, line 10 - Col. 4, line 63</td>
<td>1-6, 49-51</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

Date of the actual completion of the international search
15 April 2003 (15.04.2003)

Date of mailing of the international search report
25 APR 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Gilberto Barron
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)
INTERNATIONAL SEARCH REPORT

Box I Observations where certain claims were found unserviceable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claim Nos.:
   because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claim Nos.:
   because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claim Nos.:
   because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. □ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. □ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. X No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 1-16, and 49-51

Remark on Protest □ The additional search fees were accompanied by the applicant’s protest.
□ No protest accompanied the payment of additional search fees.
BOX II. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

1. Claims 1-16, 49-51, drawn to a system for sharing content between a plurality of computer users.
2. Claims 17-20, drawn to a method of searching a computer file system for files.
3. Claims 21-22, drawn to an efficient way of updating a list of files in a computer file system.
4. Claims 23-26, drawn to a method to notify a plurality of computer users of the availability of content available for sharing.
5. Claims 27-32, drawn to a method of distributing content from a central server to a plurality of computer users.
6. Claim 33, drawn to a method to allow access to content on a computer remotely.
7. Claims 34-41, drawn to a method of electronically sharing content.
9. Claims 46-48, drawn to a method of allocating bandwidth. The inventions listed as Groups 1-9 do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group 1 has the special technical feature of authorizing a guest user by a global unique identifier that is created by the central server. Group 2 has the special technical feature of scanning directories within file systems to obtain metadata from files. Group 3 has the special technical feature of updating a list of files with the results of a rescanning operation. Group 4 has the special technical feature of communicating an updated index of content to a plurality of users. Group 5 has the special technical feature of sending to a first computer from a server a list of authorized users of content. Group 6 has the special technical feature of reformatting and packetizing content before transmitting to a remote access device. Group 7 has the special technical feature of rejecting or accepting access to content based on if the content is borrowed. Group 8 has the special technical feature of adding encrypted metadata to the content denoting when time limit expires. Group 9 has the special technical feature of gauging optimal bandwidth needed for accessing content by user.