



(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2017/031317

(22) International Filing Date:
05 May 2017 (05.05.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/148,880 06 May 2016 (06.05.2016) US

(71) Applicant: GLOBAL TEL*LINK CORP. [US/US];
12021 Sunset Hills Road, Suite 100, Reston, Virginia 20190 (US).

(72) Inventor: HODGE, Stephen L.; 12184 FM 428, Aubry, Texas 76227 (US).

(74) Agent: SPECHT, Michael D. et al.; STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C, 1100 New York Avenue, NW, Washington, District of Columbia 20005 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: CONTROLLED ENVIRONMENT MEDIA AND COMMUNICATION SYSTEM

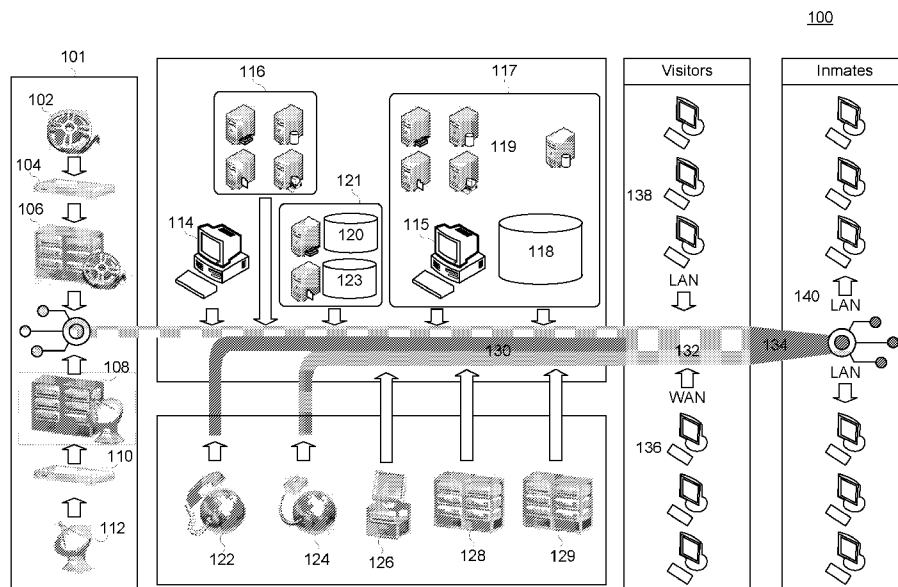


FIG. 1

(57) Abstract: The Controlled Environment Media And Communication System delivers communications services to residents of controlled facilities using a common network architecture. Some of the communications capabilities of the Controlled Environment Media And Communication System include media distribution, video visitation, intra-facility messaging, and other such communications services.



Published:

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

CONTROLLED ENVIRONMENT MEDIA AND COMMUNICATION SYSTEM

BACKGROUND

Field

[0001] The disclosure relates to methods and systems for delivery of multimedia content and other communications services in secured facilities.

Background

[0002] American prisons house millions of individuals in controlled environments all over the country. The rights of these prisoners are largely restricted for a number of reasons, such as for their safety and the safety of others, the prevention of additional crimes, as well as simple punishment for crimes committed. However, these prisoners are still entitled to a number of amenities that vary depending on the nature of their crimes. Such amenities may include phone calls, commissary purchases, access to libraries, digital media streaming, as well as others.

BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

[0003] Embodiments are described with reference to the accompanying drawings. In the drawings, like reference numbers indicate identical or functionally similar elements. Additionally, the left most digit(s) of a reference number identifies the drawing in which the reference number first appears.

[0004] Fig. 1 is an overview of a controlled environment media and communication system according to an embodiment;

[0005] Fig. 2 is an illustration of an access kiosk according to an embodiment;

[0006] Fig. 3 is an illustration of an access kiosk according to an embodiment;

[0007] Fig. 4 is an illustration of an access kiosk according to an embodiment.

DETAILED DESCRIPTION

[0008] The following Detailed Description refers to accompanying drawings to illustrate exemplary embodiments consistent with the disclosure. References in the

Detailed Description to "one exemplary embodiment," "an exemplary embodiment," "an example exemplary embodiment," etc., indicate that the exemplary embodiment described may include a particular feature, structure, or characteristic, but every exemplary embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same exemplary embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an exemplary embodiment, it is within the knowledge of those skilled in the relevant art(s) to affect such feature, structure, or characteristic in connection with other exemplary embodiments whether or not explicitly described.

[0009] The exemplary embodiments described herein are provided for illustrative purposes, and are not limiting. Other exemplary embodiments are possible, and modifications may be made to the exemplary embodiments within the spirit and scope of the disclosure. Therefore, the Detailed Description is not meant to limit the invention. Rather, the scope of the invention is defined only in accordance with the following claims and their equivalents.

[0010] Embodiments may be implemented in hardware (e.g., circuits), firmware, software, or any combination thereof. Embodiments may also be implemented as instructions stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may include read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), and others. Further, firmware, software, routines, instructions may be described herein as performing certain actions. However, it should be appreciated that such descriptions are merely for convenience and that such actions in fact results from computing devices, processors, controllers, or other devices executing the firmware, software, routines, instructions, etc. Further, any of the implementation variations may be carried out by a general purpose computer, as described below.

[0011] For purposes of this discussion, any reference to the term "module" shall be understood to include at least one of software, firmware, and hardware (such as one

or more circuit, microchip, or device, or any combination thereof), and any combination thereof. In addition, it will be understood that each module may include one, or more than one, component within an actual device, and each component that forms a part of the described module may function either cooperatively or independently of any other component forming a part of the module. Conversely, multiple modules described herein may represent a single component within an actual device. Further, components within a module may be in a single device or distributed among multiple devices in a wired or wireless manner.

[0012] The following Detailed Description of the exemplary embodiments will so fully reveal the general nature of the invention that others can, by applying knowledge of those skilled in relevant art(s), readily modify and/or adapt for various applications such exemplary embodiments, without undue experimentation, without departing from the spirit and scope of the disclosure. Therefore, such adaptations and modifications are intended to be within the meaning and plurality of equivalents of the exemplary embodiments based upon the teaching and guidance presented herein. It is to be understood that the phraseology or terminology herein is for the purpose of description and not of limitation, such that the terminology or phraseology of the present specification is to be interpreted by those skilled in relevant art(s) in light of the teachings herein.

[0013] As discussed above, secured facilities endeavor to provide residents with an ever-growing capability for communication and entertainment. The Controlled Environment Media And Communication System IP-based platform offers significant advantages, including the ability to integrate television, local / network video / audio content, with other IP-based services like our offender messaging service, VOIP based voice telephone calling, VoIP or WebRTC based video conferencing, or future IP enhanced services as the jurisdictions needs dictate. The IP-based Controlled Environment Media And Communication System will be discussed in more detail below.

Network Architecture Overview

[0014] The Controlled Environment Media And Communication System 100 enables various communications services for residents of a controlled environment. In an embodiment, the controlled environment is a correctional institution such as a prison

facility and the residents are inmates or otherwise incarcerated in the correctional institution. In other embodiments, the controlled environment may be any type of facility with a need to control and monitor content consumption such as a hospital, a dormitory, a mental health institution, a hotel, or other such facilities.

[0015] These types of controlled environments have unique requirements for communications and media distribution that are not present in other, non-controlled environments. First is the need to monitor and control access to communications pathways. Second, the authorities providing media to a controlled environment have a strong interest in censoring the types and subject matter of media content and communications sessions involving residents of the secured facility. Third, a controlled environment communication system operated by a controlled environment jurisdiction or authority must be cost efficient and have the capabilities to recover costs from residents for access to services. Finally, secured facilities have an incentive to provide communications services that are desirable to use and meet the needs of a large resident population. There may be other additional unique concerns and/or requirements in controlled environments that are not discussed here.

[0016] In a prison, the jurisdiction operating the prison has a strong interest in controlling the consumption and exposure to media and other content. For example, extremely violent media and content is not appropriate for a violent offender. In another example, some media content is associated with particular social movements or gang activity and may be deemed not appropriate for prisoner consumption. Even in the case of appropriate content, prison authorities may control access to media and content, for example as a reward for good behavior. In these ways, conventional media and communication systems do not address the unique needs and requirements of a system designed for controlled environments.

[0017] The Controlled Environment Media And Communication System 100 illustrated in FIG. 1 addresses these unique requirements and constraints imposed by the secured facility environment and further supports additional capabilities built on the network capabilities. Central to the Controlled Environment Media And Communication System 100 is Core Network 130. Core Network 130 connects all systems and services in Controlled Environment Media And Communication System 100. Core Network 130 is any suitable data networking system for transmitting data. In an embodiment, Core Network 130 is an Ethernet based network operating over

twisted-pair type wires or coaxial-type wires. Core Network 130 comprises network switching capabilities, networking cabling, and network interfaces for all connected terminals and services. In an embodiment, Core Network 130 is a fiber-optic based network including fiber-optic cables, fiber-optic switches, and other fiber-optic type networking equipment. In another embodiment, Core Network 130 is a wireless radio frequency based network such as Wi-Fi™. In some embodiments, Core Network 130 comprises network segments of disparate technologies, such that some elements of Core Network 130 operate on different networking technology than other components. For example, Core Network 130 may include an Ethernet-based wired segment and a Wi-Fi™-based wireless segment that inter-operate to provide data connectivity and services.

[0018] There are several different levels of network access in a secured facility, just like there are several different levels of physical access in a secured facility. For example, in a prison secured facility, prison inmates are physically secured within one section of the facility. Another section of the facility may be physically accessible to prison staff and visitors, and finally members of the public may interact with the prison on the outer-most level of physical security, such as a mailman delivering mail. The same analogy holds true for network access within a secured facility.

[0019] The Core Network 130 contains subsections, or sub-parts that are segmented from one-another for security purposes. Core Network 130 may use networking technologies such as Virtual LAN (“VLAN”), network firewalls, Network Address Translation (“NAT”), or other network partitioning or segmenting techniques to create these subsections. Only network traffic approved by the jurisdiction operating the Core Network 130 is allowed to traverse network segments by using these techniques. In addition, network segments are physically separated from each other such that an unsecured network is not available in a secured physical location. For example, access to the outermost, least secured network layer is not available to inmates in their cells. Rather, devices in physically secured areas of the facility, such as a prison cell, are only exposed to the appropriate network segment for that secured area.

[0020] The most secured network segment is Access Network 134. Access Network 134 is the network segment that is available to the most secured locations in the

secured facility. For example, Access Network 134 is the network available to inmates in prison cells in a prison secured facility. Next is Edge Network 132. Edge Network 132 is an intermediate network segment available to semi-secured areas of the secured facility such as areas for visitors. Next, Core Network 130 is available to the least-restrictive areas and facilities in the network. Finally, Core Network 130 is connected to one or more external networks, some of which may be a public network. In an embodiment, one external network is the Internet. In other embodiments, Core Network 130 can also interface with public networks other than the Internet as well.

[0021] The Controlled Environment Media And Communication System 100 includes Authentication Subsystem 129 which authenticates users on the network. In an embodiment, Authentication Subsystem 129 implements the Lightweight Directory Access Protocol (LDAP), providing integration capability with most currently existing authentication systems.

[0022] In an embodiment, Core Network 130 includes Class of Service ("CoS") administration features. The Core Network 130's Class of Service engine analyzes parameters of data packets to determine the types of payloads contained in the packets. Based on these identifiers, the Core Network 130 can implement Quality of service ("QoS") rules to shape traffic on the Core Network. For example, Core Network 130 may prioritize real-time video communications over simple file transfers to maintain a high quality of video. These features become even more important to the functioning of Core Network 130 when multiple services utilize the network such as media distribution, video visitation, and voice services.

User Interface Hardware And Software

[0023] Users interact with the Controlled Environment Media And Communication System 100 through a range of interfaces. In an embodiment, a kiosk format is used. One kiosk type is an inmate, or in-pod kiosk that is designed to be deployed in a controlled environment accessible to inmates or offenders. The Inmate Kiosk 200 includes computing resources and a range of input and output devices to facilitate communication with inmates. Inmate Kiosk 200 includes a CPU. The CPU includes a processor, storage, and memory for executing instructions to communicate with the Controlled Environment Media And Communication System 100. In an embodiment,

the CPU runs a standard operating system such as Microsoft Windows™. In another embodiment, the CPU runs a customized operating system. In an embodiment, the CPU executes instructions stored on storage local to the CPU, for example a hard drive or solid state drive. In an alternative embodiment, the CPU executes instructions stored on a network, for example by booting via PXE to load an operation system stored remotely. In an embodiment, Inmate Kiosk 200 communicates with Access Network 134.

[0024] For example, Inmate Kiosk 200 includes Input Devices 202 and 204. Input Device 202 is a keyboard. Input Device 204 is a trackball type input device. In alternative embodiments, other input devices may be substituted for those pictured, including mouse type input devices, touchscreen type input devices, touchpad type input devices, or the like. In an embodiment, Inmate Kiosk 200 also includes authorization input devices, such as Magnetic Card Reader 206. In alternative embodiments, Inmate Kiosk 200 includes any other kind of authorization input device, such as but not limited to biometric devices, a fingerprint reader, an iris scanner, a facial recognition camera, or an RFID reader. In an embodiment, Inmate Kiosk 200 includes Camera 208 for video communications, administrative supervision, or other uses. In an embodiment, Camera 208 is a three dimensional camera. In an embodiment, Inmate Kiosk 200 also includes Microphone Jack Input Connector 210. Monitor 212 is an LCD-type monitor, although any visual display can be used in alternative embodiments. Inmate Kiosk 200 also includes Speaker 216. Inmate Kiosk 200 includes Handset 214, including a microphone and speaker. In an embodiment, Inmate Kiosk 200 is compatible with functionality to enable communications to and from persons with hearing or speech difficulties. For example, Inmate Kiosk 200 may include support for standard TTY and TDD devices and protocols.

[0025] Inmate Kiosk 200 is housed in a hardened enclosure designed to withstand physical abuse and resist ingress or damage to the computing components inside. For example, Inmate Kiosk 200 can be enclosed in a primary stainless steel enclosure 218 of a thick gauge. In addition, Monitor 212 is enclosed behind a protective covering, for example quarter-inch thick security glass. Input Devices 202-208 are similarly designed to be resistant to physical abuse or vandalism. Any openings on Kiosk 200 are able to be locked closed so that only authorized access is permitted. In

some embodiments, Inmate Kiosk 200 includes a powered ventilation system to provide adequate ventilation for computing and networking components contained therein. For example, Inmate Kiosk 200 includes a vandalism-resistant fan opening to allow airflow to within the chassis.

[0026] In an embodiment, Inmate Kiosk 200 is designed to be accessible to all persons, including disabled persons in compliance with any applicable standard for accessibility to disabled persons. In an embodiment, Inmate Kiosk 200 is designed to be mounted on a wall. In an alternative embodiment, Inmate Kiosk 200 is designed to be pedestal mounted.

[0027] In an embodiment, inmates interact with the system through a tablet form-factor computer housed in a secure housing. Tablet Computer 302 includes a Touchscreen 304, Microphone 306, Speaker 310, and Audio Jack 308. Tablet Computer 302 is housed in a secure housing 312. In other embodiment, Tablet Computer 302 is not housed in a secure housing. In some embodiments, Tablet Computer 302 also includes a Camera 314. In an embodiment, Tablet Computer 302 operates similar or substantially the same software as Inmate Kiosk 200 such that all available services that are available on the Inmate Kiosk 200 are also available on Tablet Computer 302. Some examples below are illustrated in terms of Inmate Kiosk 200, but it is to be understood that Tablet Computer 302 could take the place of Inmate Kiosk 200 for any embodiment described herein.

[0028] Another kiosk type is a kiosk designed for use by visitors, or other non-inmate individuals. In an embodiment, the Visitor Kiosk 138 is deployed in common or visitation areas of a secured facility. In an embodiment, the Visitor Kiosk 138 is substantially similar to the Inmate Kiosk 200. In another embodiment, the Visitor Kiosk 138 is not required to be as vandalism-resistant as the Inmate Kiosk 200, and is not built to the same vandalism-resistant specification as the Inmate Kiosk 200. One key differentiator between Inmate Kiosk 200 and Visitor Kiosk 138 is that Visitor Kiosk 138 is connected to Edge Network 132, and Inmate Kiosk 200 is connected to Access Network 134. Similar to the Inmate Kiosk 200, Visitor Kiosk 138 may be embodied in different form factors, including a tablet computer.

[0029] In an embodiment, users interact with the Controlled Environment Media And Communication System 100 through a software client. The software client can be run on any client computing device, for example a smartphone, a laptop computer,

a desktop computer, or a tablet computer, for example. In an embodiment, the software client is executed on a smartphone such as Smartphone 400. The software client is fully configurable by the jurisdiction operating the Controlled Environment Media And Communication System 100. In an embodiment, the operations of Visitor Kiosk 138 are fully encompassed by the software client operating on a visitor's own hardware.

Media Distribution

[0030] Controlled Environment Media And Communication System 100 provides distribution of media to users through the various access points, including for example Inmate Kiosk 200 through Media Subsystem 101. The Media Subsystem 101 provides support for both real-time and on-demand media, including video and audio. Examples of real-time media include broadcast television, broadcast radio, cable television, satellite television (i.e., Ku, Ka, or C-band), satellite radio, and live internet streaming of video and/or audio. Examples of on-demand media include video-on-demand (VOD), audio-on-demand, movie downloads, music downloads, pay-per-view video (PPV), and other such asynchronous media distribution methods. The Controlled Environment Media And Communication System 100 makes available any combination of real-time and on-demand media as required by the jurisdiction operating the secured facility.

[0031] Asynchronous video content is sourced from Media Source #102. In an embodiment, Media Source 102 is a third party cloud media provider. In another embodiment, Media Source 102 is a media repository integral to Media Subsystem 101. Media from Media Source 102 is encoded by Media Encoder 104. In an embodiment, video content is encoded with MPEG-2, MPEG-4, H.264, or any other suitable video CODEC. Similarly, audio content is encoded with any suitable audio CODEC including but not limited to MP3, AAC, or other audio CODEC.

[0032] Next, the encoded media is made available to consumers from Media Acquisition Server 106. Media Acquisition Server 106 stores encoded media from Media Source 102 for future consumption. Media Acquisition Server 106 maintains a catalog of media that is available to consumers. The media catalog is available to consumers to select media from Media Acquisition Server 106.

- [0033]** In an embodiment, Media Source 102 stores video or movie content and Media Acquisition Server 106 provides video-on-demand (VOD) services to consumers. In an embodiment, Media Source 102 stores audio or music content and Media Acquisition Server 106 provides music-on-demand services to consumers. In other embodiments, both video and audio media formats are handled by the same system and both media types are made available to consumers.
- [0034]** Broadcast media content is sourced from Broadcast Media Source 112. In an embodiment, Broadcast Media Source 112 is a publicly broadcast media signal, such as broadcast television or radio. In an embodiment, Broadcast Media Source 112 is a privately broadcast medium such as a private internet stream, satellite television, or satellite radio broadcast. In an embodiment, Broadcast Media Source 112 is a television or radio broadcast internal to the secured facility or a network of secured facilities. For example, a secured facility can operate an informational television broadcast that is only available to residents of the secured facility.
- [0035]** Media from Broadcast Media Source 112 is encoded by Broadcast Media Encoder 110. In an embodiment, video content is encoded with MPEG-2, MPEG-4, H.264, or any other suitable video CODEC. Similarly, audio content is encoded with any suitable audio CODEC including but not limited to MP3, AAC, or other audio CODEC.
- [0036]** Next, the encoded Broadcast media is made available to consumers, such as the inmates, from Broadcast Media Acquisition Server 108. Broadcast Media Acquisition Server 108 buffers encoded media from Broadcast Media Source 112 for consumption. Broadcast Media Acquisition Server 108 maintains a guide of broadcast media that is available to consumers. For example, a television guide indicating the channels available and the media broadcast on those channels is made available by Broadcast Media Acquisition Server 108. The media guide is available to consumers to select broadcast media from Broadcast Media Acquisition Server 108.
- [0037]** Media from both Media Acquisition Server 106 and Broadcast Media Acquisition Server 108 is delivered via the Core Network 130 to user hardware such as Inmate Kiosk 200 for consumption. In an embodiment, a Media Distribution Cluster 116 is interposed between the acquisition servers and the consumers. Media Distribution Cluster 116 operates as a cache or buffer to distribute load and relieve

the acquisition servers. In an embodiment, Media Distribution Cluster 116 comprises individual servers that are disposed within closer physical proximity to the consumer such that overall network load is reduced.

[0038] In an embodiment, Core Network 130 supports multicast routing to reduce network load and increase bandwidth efficiency. Multicast routing enables Media Distribution Cluster 116 to send one stream of data to many clients such as Inmate Kiosk 200 at once, reducing the load on the network. In an embodiment, typical unicast networking is utilized where appropriate.

[0039] Media Subsystem 101 streams content to remote end users utilizing Unicast and Multicast TCP, UDP, or WebRTC connections depending on source content. Encoders 104 and 110 convert or transcode media from any source format to any consumption format necessary for end users. For example, some of the media formats used are MPEG-4, H.264, or VC-1 formats. In an embodiment, use of these formats enables distribution of standard-definition video ("SDTV") content with requirements of about 1 Mbps per stream and about 5 Mbps for high-definition video content ("HDTV").

[0040] In an embodiment, Encoders 104 and 110 are software based, and in another embodiment Encoders 104 and 110 are hardware-based. In another embodiment, a combination of both software and hardware are used to encode media in Encoders 144 and 110. In an embodiment, using advanced video compression and multicast routing, Media Subsystem 101 can achieve a virtually unlimited number of channels to a virtually unlimited number of users on the network. In an embodiment, over 1000 simultaneous channels is achievable.

[0041] Media Subsystem 101 can be administered either on premise or remotely. In an embodiment, the Media Subsystem 101 includes a remote administration module that enables content provision and management of Media Subsystem 101 from a remote location. All content distributed by Media Subsystem 101 is controlled by the system administrator utilizing a proprietary Class of Service administration.

[0042] In an embodiment, Media Subsystem 101 is designed to be fault tolerant. It is important that Media Subsystem 101 remain operational even in the event of an emergency to broadcast emergency messages. Thus, the Media Subsystem 101 can include redundant systems including redundant Media Acquisition Server 106, Broadcast Media Acquisition Server 108, Media Distribution Cluster 116, and all

other components of Media Subsystem 101. Media Subsystem 101 includes automatic failover means to automatically remove inaccessible or otherwise unresponsive components out of the network and continue to provide services to the secured facility.

Video Visitation

[0043] One aspect of the Controlled Environment Media And Communication System 100 is video visitation provided by Video Visitation Subsystem 117. Video visitation is the process of a bi-directional or unidirectional video communication between an inmate and a visitor such as family, friends, clergy, or the like. In an embodiment, Video Visitation Subsystem 117 enables video visitation through Inmate Kiosk 200 illustrated in FIG. 2. The Video Visitation Subsystem 117 makes use of Camera 208 in the Inmate Kiosk 200 and similar cameras in other hardware used to access the Controlled Environment Media And Communication System 100. In an embodiment, video visitation is supported between users on smartphones , tablet computers, inmate kiosks, and Visitor Kiosks 138. Other forms of video visitation include educational video visitation where an inmate can participate in a classroom via video feed.

[0044] The Video Visitation Subsystem 117 utilizes the Core Network 130 to route video visitation traffic between inmate kiosks and visitor kiosks. Local real-time video visitation can be broadcast using similar multicast techniques to reduce network traffic. For example, in an embodiment, an on premise classroom is broadcast throughout the secured facility using multicast routing to a plurality of inmate kiosks and inmate devices, delivering educational experiences to large amounts of inmates simultaneously while not significantly increasing network load. In an embodiment video transport uses IGMP version 2 for connecting to a multicast stream and the Real Time Streaming Protocol (RTSP) to deliver video content. Video content may be compressed with any known video compression codec, including but not limited to H.264, H.265, WebM, MPEG-4, MPEG-2, or the like. Likewise, video streams originating from the inmate hardware, including Inmate Kiosk 200 or Tablet Computer 302 are compressed using similar video coding techniques. In an embodiment, video compression and decompression is assisted in the Inmate Kiosk 200 by a graphical processing unit (GPU) co-processor.

- [0045] A feature of the Video Visitation Subsystem 117 is the Video Visitation Investigative Unit 115. The Investigative Unit 115 performs real-time monitoring and storage of video visitations sessions for real-time and future review and analysis. Investigative Unit 115 allows investigators to view time-shifted video visitation feeds and pause, rewind, and fast-forward through video visitation sessions to efficiently and accurately analyze the content of the video visitation session. An investigative administrator is presented with the option to monitor any current video visitation feeds or to play archived video visitation sessions stored in Video Visitation Database 118.
- [0046] Video visitation session properly flagged as being confidential, such as a meeting between an attorney and a client, will not be made available to investigative workstations and is not recorded into Video Visitation Database 118. In an embodiment, sessions marked as confidential can be identified through one or more criteria such as a scheduling identifier, a specified remote contact, or a specified local access point such as a specific kiosk within the facility.
- [0047] Authorized users will have to ability to monitor visitation/encounter sessions in process. Although the inmate and called party are notified during the session setup that the session is recorded and subject to monitoring, actual live monitoring of a session are completely transparent to the parties.
- [0048] Investigators using Video Visitation Investigative Unit 115 are able to perform monitoring of live sessions. In an embodiment, the Investigator is able to select whether to see every visitation/encounter kiosk or just the ones with active sessions. The user interface displays information regarding the location of the kiosk stations and the identity of the offender and the visiting party. To start live monitoring, the session, the user clicks an icon in a graphical user interface. This opens a new window displaying the both end's video sessions and the session audio, which is played over workstation speakers or headphones if desired. If the administration users determine that the session is inappropriate, they will be able to cut off the session and/or make notes to the session (such as a case number) that can be searched for and reviewed later.
- [0049] While live monitoring (or pulling historical recordings), each users is able to add notes (see the user interface view below) to the session recording file.

Investigators are able to select a specific portion of the recorded session to save as a separate file and add notes related to their findings.

[0050] At a later time, investigator users using Investigative Unit 115 are able to retrieve video visitation session recordings. In an embodiment, investigators with appropriate account privileges are able to retrieve session recordings by utilizing a graphical user interface. In the graphical user interface are multiple options for searching of session records including “quick searches” keyed on offender, visiting party, kiosk ID, or date/time bands. Ad-hoc queries on more complex criteria are also be able to be defined. Once the search is conducted and session records are displayed, the records can be ordered on the basis of any of the session record fields by selecting the field name on a display header bar.

[0051] Session recordings are available for playback at the user’s discretion. Clicking an icon on the record will open a new window displaying the both end’s video sessions and the session audio, which will be played over workstation speakers or headphones if desired. The window provides tools for control of the playback. While listening to or viewing a recording, the user may add notes to the session recording file. The user will also be able to select a pertinent portion of the recorded session, save it as a separate file, add notes related to his/her findings and archive the recorded conversation on a DVD.

[0052] In addition to recording capabilities, the Video Visitation Subsystem 117 provides a full array of administrative capabilities, including the ability to initiate and terminate individual or multiple sessions, as well as an audio barge-in feature if desired for visitation warnings of unacceptable behavior or language. This barge in-feature can be invoked from live session monitoring as described above. In conjunction with existing jurisdiction scheduling databases, the Video Visitation Subsystem 117 is capable of auto-initiating and terminating sessions per the scheduled time. Time limit warnings will be made available to all system users for them to be aware of impending session termination.

[0053] A Video Visitation Scheduling System 119 enables inmates and/or visitors to schedule a video visitation session. The Scheduling System 119 also optionally alerts investigative administrators to the scheduled video visitation so that the investigator can supervise the video visitation session. The Video Visitation Subsystem 117 allows the jurisdiction to control and or approve online scheduling. In addition, the

authentication requirements, offender classification/designation, STG, or other jurisdiction may be designated by the jurisdiction from a Jail Management data feed or entry of the data into the system database. The Video Visitation Subsystem 117 also provides for the online scheduling of video visitation which would allow approved visitors to schedule visits according to jurisdiction visiting regulations.

[0054] In an embodiment, Video Visitation Subsystem 117 is compatible with industry standards such as H.320. H.320 is an umbrella recommendation by the ITU-T for running Multimedia (Audio/Video/Data) over ISDN based networks. Video Visitation Subsystem 117 can utilize bandwidth saving MPEG-4, H.264, or VC-1 formats for internal communication between Inmate Kiosk 200 and Visitor Kiosk 138, for example. For video visitation with a remote video visitation user, Video Visitation Subsystem 117 can use H.320 standards, for example. An example of a H.320 video visitation session is a minimum resolutions of 352x288 pixels at 30 frames per second with minimum bandwidth requirements up to 1.544Mbps per session as per H.320 standards. In an embodiment, Video Visitation Subsystem 117 utilizes WebRTC standards to communicate with remote video visitation participants. Other such standards, formats, and processes as known in the video communication arts can also be implemented as protocols in Video Visitation Subsystem 117.

Intra-Facility Communication

[0055] In addition to media services and video visitation services, Controlled Environment Media And Communication System 100 enables communication between controlled environment residents and the jurisdiction operating the controlled facility via Intra-Facility Communication Subsystem 121. One form of communication is a complaint or request, commonly referred to as a 'kite' in the correctional industry. A kite is a written request, complaint, or other communication from an inmate to facility staff and administrators. Examples of kites are requests to see a doctor, a question posed to a counselor, or other communications to facility staff.

[0056] The Inmate Kiosk 200 supports input and sending of a kite message. In an embodiment, a kite message includes an inmate's name, an identifying number associated with the inmate, the date the kite message is entered, the department the

message is to be routed to, and the individual staff member the message is directed to. In other embodiments, a kite message contains only a subset of these fields. The inmate is able to input the data for a kite message via the Inmate Kiosk 200 using any combination of input devices attached to or integral to Inmate Kiosk 200 such as a keyboard and mouse. In other embodiments where the inmates use a tablet computer to access the Controlled Environment Media And Communication System 100, the inmate inputs data for a kite message via a touchscreen. In an embodiment, some of the fields are presented as a drop-down menu in which the inmate entering in data can select a data value. For example, the department field may be a dropdown type input field with the options “Health,” “Services,” “Canteen,” “Unit Manager,” etc. Selecting the appropriate entry routes the kite message to the associated department within the secured facility. In an embodiment, the inmate is also allowed to flag a kite message with a priority indicator. Priority indicators include but are not limited to low priority, normal priority, high priority, or emergency priority. By indicating the appropriate level of priority, facility staff are able to service all inmate and resident needs more efficiently. After entering in data for all necessary fields, the inmate submits the kite message from the Inmate Kiosk by hitting a “send” button or the equivalent graphical user interface element.

[0057] The graphical user interface for generating kite messages also includes a frequently asked questions section where simple or oft-encountered kite requests can be addressed without the need to submit a kite request message. The purpose of the frequently asked questions format is to provide answers quickly and efficiently. The frequently asked questions can also be directed to the kite message submission process as well, such as information regarding who will process the kite message and when to expect a response.

[0058] Once a kite message is generated and submitted from an inmate by, for example, an Inmate Kiosk 200, the message is sent to the Intra-Facility Communication Subsystem 121. Received kite messages are stored in Kite Message Database 120. In an embodiment, Kite Message Database 120 is a relational database, for example an SQL database. In another embodiment, Kite Message Database 120 is a non-relational document store.

[0059] Intra-Facility Communication Subsystem 121 then validates the kite message upon receipt. One validation step is to flag kite messages containing certain

keywords and phrases. For example, keywords related to gangs, drugs, profanity, sexually explicit words, and other such topics are filtered and flagged for review by an appropriate administrator. The keywords and phrases are stored in Censorship Database 123. Censorship Database 123 can be updated at any time to include new words or phrases to search new incoming messages for. In addition, a search function allows administrators to search previously submitted kite messages in Kite Message Database 120 for keywords and phrases in the Censorship Database 123. An alert message can also be set to inform system administrators when a kite message containing certain keywords or phrases is submitted.

[0060] Another validation step is to disallow repetitive, duplicative, or otherwise abusive requests. In one embodiment, this filtering step is a rate-limiting step wherein inmates are disallowed from sending more than a set number of kite messages in a given time period. The rate-limiter can apply to all messages sent by an inmate, or can be specific to each recipient. For example, the rate limiter can be set to disallow more than 1 kite message to be sent to any given recipient each day. This prevents abuse of the Intra-Facility Communication Subsystem 121. Another validation step is to reject identical or substantially similar kite messages. Intra-Facility Communication Subsystem 121 searches the Kite Message Database 120 for similar or substantially similar messages submitted by the same inmate to the same recipient and disallows duplicates. This is also a mechanism by which inmates can be prevented from overwhelming the Intra-Facility Communication Subsystem 121. Any other appropriate algorithm or limitation can be set on the submission of kite messages by inmates to maintain a useful system that is not able to be abused. In an embodiment, the rate limitations are dynamically set on an individual basis so that repeat kite message abusers are subject to stricter limitations. In an embodiment, rather than simply disallowing repetitive or duplicative messages, the Intra-Facility Communication Subsystem 121 can flag such messages and inmates for disciplinary action by the facility staff.

[0061] Next, the kite message is routed to the appropriate department or individual for processing. A feature of the Intra-Facility Communication Subsystem 121 is that each message is tracked through its lifecycle, from creation, opening, reading, responding, taking action, and closing. These events are stored along with the original kite message in Kite Message Database 120. For example, when an

administrator first opens a new kite message, that administrator's identification and a timestamp is recorded along with the kite message to indicate that the message was read. Next, when a kite message is acted upon, for example an appointment with a doctor was scheduled, that action is also recorded along with identifiers and timestamps along with the kite message.

[0062] In an embodiment, facility staff who act on kite messages are required to electronically sign the kite message to document the interaction. System administrators can also register alerts to be generated at the occurrence of any event associated with a kite message. For example, a medical department head can set an alert for any kite message acted upon by any staff members of the medical unit. Staff members are able to forward a kite message to another staff member for further action.

[0063] Intra-Facility Communication Subsystem 121 enforces privacy and confidentiality of kite requests as set by the system administrator. Only those staff members and administrators authorized to view, edit, act on, or close kite messages are allowed to take such actions.

[0064] In an embodiment, any staff member that can act on a kite message can also add notes or annotations to the kite message for reference. These annotations are viewable only by the staff members and are for administrative purposes. For example, a note about an inmate's behavior, gang affiliation, or other information may be appropriate in certain situations. These annotations are also stored in Kite Message Database 120 along with the kite message. Notes and annotations may be in the form of text, images, or other records or data that is pertinent to the kite request.

[0065] Throughout the lifecycle of a kite message, inmate can view the status and any updates on their kite request through Inmate Kiosk 200. In an embodiment, the inmate is presented with a graphical representation of their kite messages and requests, who is addressing their kite message, and what action has been taken. Through this interface, inmates are able to cancel, amend, or append new information to a kite request to reflect changing circumstances. In this way, the Intra-Facility Communication Subsystem 121 enables a task-oriented two-way communications channel between inmates and facility staff. Staff members are also able to escalate a kite message request in the event that a higher authority is required to act on the kite message request.

- [0066]** Kite request messages may have an expiration data set by the inmate, a staff member, or automatically based on request type as defined by the jurisdiction operations the Intra-Facility Communication Subsystem 121. When an expiration date is reached the kite message is automatically closed by the Intra-Facility Communication Subsystem 121.
- [0067]** In an embodiment, Intra-Facility Communication Subsystem 121 can charge inmates for specific events associated with a kite message. For example, an institution can charge an inmate account for a medical visit or for a superfluous or duplicative request that burdens the administrative staff of the facility. If a staff member determines a charge should be levied upon the submitting inmate, that charge can be indicated in the Kite Message Database 120. In an embodiment, inmates are charged for repetitive or duplicative kite messages as detected in the validation described above. A separate billing and accounting process then makes sure the charge is properly paid and settled for the services or other functions performed.
- [0068]** Intra-Facility Communication Subsystem 121 also provides a robust investigation and analysis platform on which to examine kite messages stored in Kite Message Database 120. These analytics can provide valuable insight into the inner workings of a secured facility for facility administrators. For example, if a number of complaints are received about the same topic, facility administrators can address that topic. In this way, the kite system can act as a kind of suggestion box for facility administrators. In an embodiment, administrators are able to search past kite messages by key word, department, inmate, recipient, or any other data field or combination of data fields stored in Kite Message Database 120. Searches can be run one time, or stored to periodically generate reports for particular search queries. One example of a stored query is a query that outputs a list of similar kite messages received within a period of time from different inmates or residents. For example, if a number of inmates all submit kite messages identifying that there is a rodent infestation in the facility, administration will be notified immediately so that the problem can be rectified in a timely fashion.
- [0069]** In an embodiment, Intra-Facility Communication Subsystem 121 interfaces with a legacy system already in place at the secured facility. Several levels of interfacing with legacy systems are possible. First, the Intra-Facility Communication

Subsystem 121 can import archived data into Intra-Facility Communication Subsystem 121 for analysis and archiving. Second, Intra-Facility Communication Subsystem 121 can co-exist with an existing data entry system that is already in place, such that Intra-Facility Communication Subsystem 121 imports data from another source for processing and analysis. Third, Intra-Facility Communication Subsystem 121 can integrate with a legacy analysis and processing backend while using the Inmate Kiosk and other kite message input methods described herein. In any level of integration, the administration operating the secured facility is able to choose an optimal integration strategy to work with legacy systems.

[0070] Intra-Facility Communication Subsystem 121 includes a data export and import feature for integration with legacy systems and other system. In an embodiment, Intra-Facility Communication Subsystem 121 is able to export and import kite message data in standard data formats. For example, in an embodiment, Intra-Facility Communication Subsystem 121 can export and import kite messages in a comma separated value list for interfacing with any external system that can accept a comma separated list. Other formats may be used in other embodiments, such as but not limited to XML, JSON, HTML, database formats, spreadsheet formats, and the like.

Other Inmate Communications Services

[0071] In some embodiments, Controlled Environment Media And Communication System 100 facilitates other communications services to and from inmates and other secured-facility residents. One example of other communications services is Voice Service 122. Voice Service 122 enables bi-directional voice calling to and from the Inmate Kiosk 200 using VOIP protocols utilizing the same Core Network 130 as the other communications described herein.

[0072] Another example of other services are Data Services 124. Data Services 124 enable arbitrary data to be sent to and broadcast from the Inmate Kiosk 200. Examples of data that Data Services supports are news stories, news video clips, weather forecasts, live TV guides, video-on-demand directories, and other such data that is of interest to inmates within a secured facility.

[0073] The Controlled Environment Media And Communication System 100 also includes Emergency Alert System 126. Emergency Alert System 126 provides

jurisdiction system administrators with a barge-in capability of both video and/or audio which will override any and all current content consumption. For example, an inmate watching VOD or broadcast television content will be interrupted by Emergency Alert System 126 in the event of an emergency. Emergency Alert System 126 will then display the emergency alert message on the screen and also audibly announce the emergency. In an embodiment, Emergency Alert System 126 utilizes wake-on-Lan ("WoL") capabilities of client devices to activate non-active systems to broadcast the emergency message. The WoL capabilities can only be triggered by authorized administrative personnel.

Administrative Services

[0074] Administrative Workstation 114 has connectivity to Core Network 130. Administrative staff of the secured facility can operate Administrative Workstation 114 to manage all services offered on Core Network 130 within the facility. One function of Administrative Workstation 114 is to manage media content distribution. For example, different bundles of media content can be provided to users based on the needs of the secured facility and user preferences.

[0075] Administrative Workstation 114 also provides comprehensive real-time reporting capabilities which enable facility providers to manage their prison more effectively. One such report is a report of revenues, expenses, transactions, and other financial information and records associated with the provision of communications services described herein.

[0076] In an embodiment, the Administrative Workstation 114 offers real-time reporting of all media being consumed by inmates and other residents. This functionality is useful for facility providers who want to conduct inmate-metric analyses or evaluate the viewer demand for a particular channel, program, or content.

[0077] In an embodiment, the Administrative Workstation 114 offers interactive inmate surveys which enables content facility providers to collect information from inmates while they watch their favorite TV channels, program, or content. Survey questions can be defined in either closed-ended (multiple choice) or open-ended (no preset answer) formats. The survey functionality is attractive for service facility providers who want to conduct marketing research or measure results from advertising campaigns in real-time.

- [0078]** In an embodiment, Administrative Workstation 114 provides system administrators with several cut-off/control mechanisms to control communications on the system. The cut-off allows the administrator to terminate individual kiosk services or all kiosk functions for individual, groups, or all kiosks simultaneously. In addition, administrators can take control of individual functions of the kiosk to support users or initiate investigative monitoring utilizing the hardware and software functions for example use the microphone and camera to monitor activity near the kiosk or use the speaker or display to instruct the inmate.
- [0079]** In an embodiment, more fine-grained controls are also available to system administrators via Administrative Workstation 114. For example, administrators can regulate access to the Media Subsystem 101 through a class of service ("COS") database. Users on interface endpoint such as Inmate Kiosk 200 can be grouped together by living unit, offender type, or individually. Each communication service offered by the Controlled Environment Media And Communication System 100 is controlled individually. For example, Media Subsystem 101 controls include fine-grained controls of which channels or media sources are available to a particular inmate, and the time of day those sources are available. Again, these controls can be applied individually or by any grouping of inmates.
- [0080]** In an embodiment, the Administrative Workstation 114 includes or duplicates all capabilities of Video Visitation Investigative Unit 115. Again, these capabilities are applicable to users on interface endpoint such as Inmate Kiosk 200 and can be grouped together by living unit, offender type, or individually.

Billing

- [0081]** Billing Subsystem 128 handles billing for media distribution, video visitation, and all other communication services offered by Controlled Environment Media And Communication System 100. In an embodiment, Billing Subsystem 128 is centralized and shared among all other subsystems and components of Controlled Environment Media And Communication System 100. In another embodiment, Billing Subsystem 128 comprises multiple components tailored to each other subsystem and unique to that subsystem. In all embodiments, Billing Subsystem 128 offers methods of billing residents, inmates, outside parties, and all other users of Controlled Environment Media And Communication System 100 for the

communication services rendered. For example, with respect to Media Subsystem 101, the Billing Subsystem 128 handles charging inmates and residents for delivery of media content. With respect to Video Visitation Subsystem 117, Billing Subsystem 128 charges residents, inmates, and/or outside parties appropriately for video visitation services.

[0082] In an embodiment, Billing Subsystem 128 performs real-time billing which reduces the risk of uncollectible accounts. To also reduce the chance of uncollectible accounts, Billing Subsystem 128 utilizes Authentication Subsystem 129 to authenticate users by any method available to Authentication Subsystem 129 such as biometric authentication, RFID authentication, Personal Identification Number entry, or multiples of the aforementioned.

[0083] In an embodiment, Billing Subsystem 128 supports both pre-paid and post-paid content billing, which provides extra flexibility for content facility providers. The pre-paid billing option reduces the risk of uncollectible accounts which enables facility providers to offer services on a global scale. The Billing Subsystem 128 bills all content requests in real-time to ensure that services are provided only to inmates with sufficient account balances.

[0084] In an embodiment, Billing Subsystem 128 charges a Debit Account. The resident can load funds onto the Debit Account in person, for example at a commissary, by electronic means, or by telephone. Funds can be added to the Debit Account from cash, bank accounts, or credit card accounts. Optionally, non-residents of the secured facility can be allowed to add funds to the resident's Debit Account as well.

[0085] As another form of payment, an Advance Pay Account can also be charged by Billing Subsystem 128. The Advance Pay Account can be funded by family and friends, and used for call fees associated with the resident. As with the Debit Account, the Billing Subsystem 128 can access the Advance Pay Account to determine that there are sufficient funds, when content is purchased.

[0086] In an embodiment, the Billing Subsystem 128 does not immediately deduct funds from an account, but accumulates usage over a billing cycle and forwards a bill to the resident at the end of the billing cycle. Parameters such as the length of the billing cycle, the total amount allowed to be billed during one billing cycle, and the

forms of payment that the bill can be paid in can be adjusted to suit the needs of a particular secured facility.

Operation

[0087] In operation, a user, such as an inmate, logs into the Controlled Environment Media And Communication System 100 through hardware and/or software such as the Inmate Kiosk 200. In an embodiment, the user is presented with a graphical user interface that prompts the user for authentication. In an embodiment, the authentication consists of a user identification and a password. In other embodiments, other authentication mechanisms can be used. For example, biometric, fingerprint, facial recognition, hand geometry, voice print, 3D facial recognition, radio frequency identification, or combinations or other such personal authentication means can be used.

[0088] In an embodiment, the user, such as an inmate, uses a graphical user interface and a menu system to select communications services to utilize or consume through the Inmate Kiosk 200. Channel selection will be accomplished by using the mouse to scroll and click a selection or the keyboard up/down arrows and enter key. Touch screen controls are available for hardware systems, such as tablets and smart portable devices. The inmate can also utilize the menu system to invoke the Video Visitation Subsystem 117 and the Intra-Facility Communication Subsystem 121 as well.

[0089] During use, the Inmate Kiosk 200 can optionally provide the user with the ability to minimize the picture of playing media to a smaller frame to allow multiple window viewing to the offender simultaneously while maintaining its aspect ratio. This allows offenders to perform functions such as offender email while viewing TV.

Conclusion

[0090] It is to be appreciated that the Detailed Description section, and not the Abstract section, is intended to be used to interpret the claims. The Abstract section may set forth one or more, but not all exemplary embodiments, and thus, is not intended to limit the disclosure and the appended claims in any way.

[0091] The invention has been described above with the aid of functional building blocks illustrating the implementation of specified functions and relationships thereof. The boundaries of these functional building blocks have been arbitrarily

defined herein for the convenience of the description. Alternate boundaries may be defined so long as the specified functions and relationships thereof are appropriately performed.

[0092] It will be apparent to those skilled in the relevant art(s) that various changes in form and detail can be made therein without departing from the spirit and scope of the disclosure. Thus, the invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A media distribution system for distributing media and facilitating video visitation within a secured facility, the media distribution system being available to a resident of the secured facility, the media distribution system comprising:
 - a media distribution server configured to receive media from a media source and make media available on a network;
 - a video visitation server configured to conduct video visitation sessions between a first video visitation endpoint and a second video visitation endpoint, at least one of the first and second video visitation endpoints having connectivity to the network; and
 - an access kiosk placed within a residential unit of a secured facility and accessible by the resident, the access kiosk configured to:
 - communicate with the video visitation server over the network to participate in video visitation sessions with one or more other video visitation endpoints; and
 - receive media from the media distribution server over the network and playback the media for consumption.
2. The system of claim 1, wherein the secured facility is a prison, the resident is an inmate of that prison, and the residential unit of a secured facility is a prison cell.
3. The system of claim 1, wherein the media source is a video-on-demand media source, and the media received from the media distribution server is video-on-demand media.
4. The system of claim 1, wherein the media source is a broadcast media source, and the media received from the media distribution server is broadcast media.
5. The system of claim 4, wherein the network supports multicast routing, the media distribution server utilizes multicast routing to route the broadcast media, and the access kiosk utilizes multicast routing to receive the broadcast media over the network.

6. The system of claim 1, wherein the access kiosk has access to the network only through a secured network segment, the secured network segment being limited to access only the network resources necessary for the access kiosk.
7. The system of claim 1, wherein the one or more other video visitation endpoints includes a second access kiosk, the second access kiosk placed within the secured facility and available to guests of the secured facility.
8. The system of claim 1, further comprising:
 - an intra-facility communications server with access to the network, the intra-facility communications server configured to route intra-facility communications on the network;
 - wherein the access kiosk is further configured to:
 - receive input indicative of an intra-facility message; and
 - transmit the intra-facility message to the an intra-facility communications server using the network.
9. The system of claim 1, further comprising:
 - a voice communications server with access to the network, the voice communications server configured to route voice communications on the network and one or more external networks;
 - wherein the access kiosk is further configured to place and receive voice calls over the network and one or more external networks utilizing the voice communications server.
10. An intra-facility communications system for sending and receiving messages within a secured facility, the system comprising:
 - a secured network, the secured network including first secured partition and a second secured partition;
 - an access terminal available to a resident of the secured facility, the access terminal configured to:
 - receive an intra-facility message from the resident;

transmit the intra-facility message using the first secured partition of the secured network;

a central intra-facility communications server, the central intra-facility communication server configured to:

receive the intra-facility message via the first secured partition of the secured network;

route the intra-facility message to its intended recipient using the second secured partition of the secured network.

11. The system of claim 10, wherein the secured facility is a prison and the residents of the secured facility are prison inmates, the first secured partition of the secured network is available to the prison inmates, and the second secured partition of the secured network is not available to prison inmates.
12. The system of claim 11, wherein access to the first secured network partition is available to prison inmates and access the second secured network partition is not available to prison inmates.
13. The system of claim 11, further comprising:
 - an authentication server with connectivity to the secured network;
 - wherein the prison inmates possess one class of authentication credentials which disallows access to the second secured partition of the secured network, and prison staff possess another class of authentication credentials which allows access to the second secured partition of the secured network.
14. The system of claim 11, wherein the access terminal is an inmate kiosk located within an inmate cell.
15. The system of claim 10, wherein the access terminal presents a list of options for intra-facility messages via a graphical user interface to the resident, the access terminal received input indicative of one of the list of options, and the intra-facility message includes the chosen option in the intra-facility message.

16. The system of claim 10, further comprising a media distribution server with access to the second secured partition of the secured network;
wherein the access terminal is further configured to receive media from the media distribution server and playback the media for consumption.
17. The system of claim 10, further comprising a video visitation server with access to the second secured partition of the secured network, the video visitation server configured to conduct video visitation sessions between the access terminal and a second video visitation endpoint;
wherein the access terminal is further configured to conduct video visitation sessions with one or more other video visitation endpoints by utilizing the video visitation server.
18. A method for emergency communications administration within a media distribution and communications system in a secured facility, the method comprising:
receiving an emergency signal from an administrative terminal, the emergency signal indicative of an emergency within the secured facility;
transmitting the emergency signal and a wake signal from the administrative terminal to a communications device that is in a standby state;
in response to receiving the emergency signal and the wake signal, waking the communications device from a standby state to an operational state and displaying an emergency notification on the media consumption device indicative of the received emergency signal.
19. The method of claim 18, wherein the secured facility is a prison, and the communications device is a media consumption device is in the possession or control of an inmate of the prison.
20. The method of claim 18, further comprising transmitting live sound and video from the media consumption device to the administrative terminal in response to receiving the emergency signal and the wake signal.

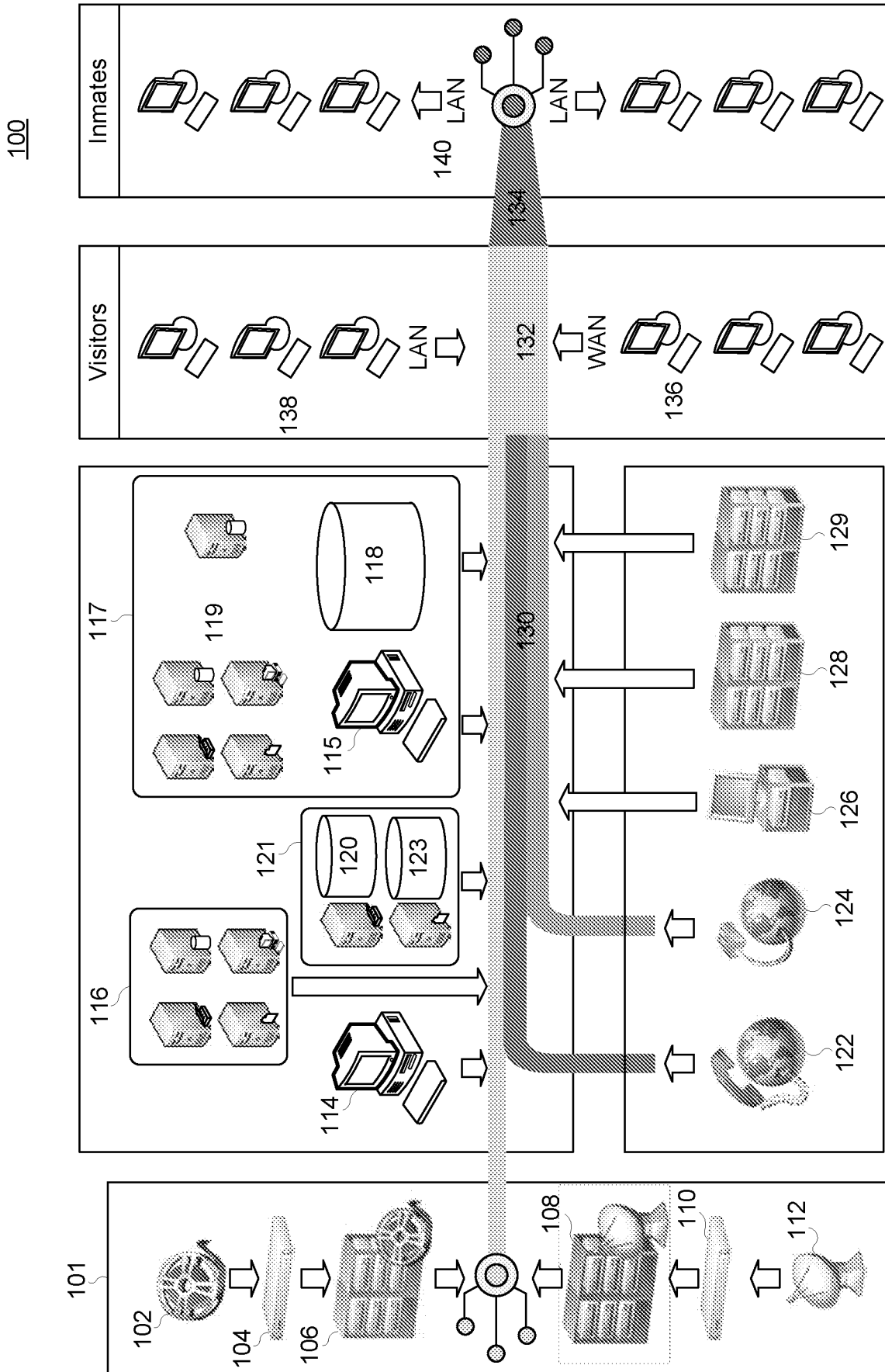


FIG. 1

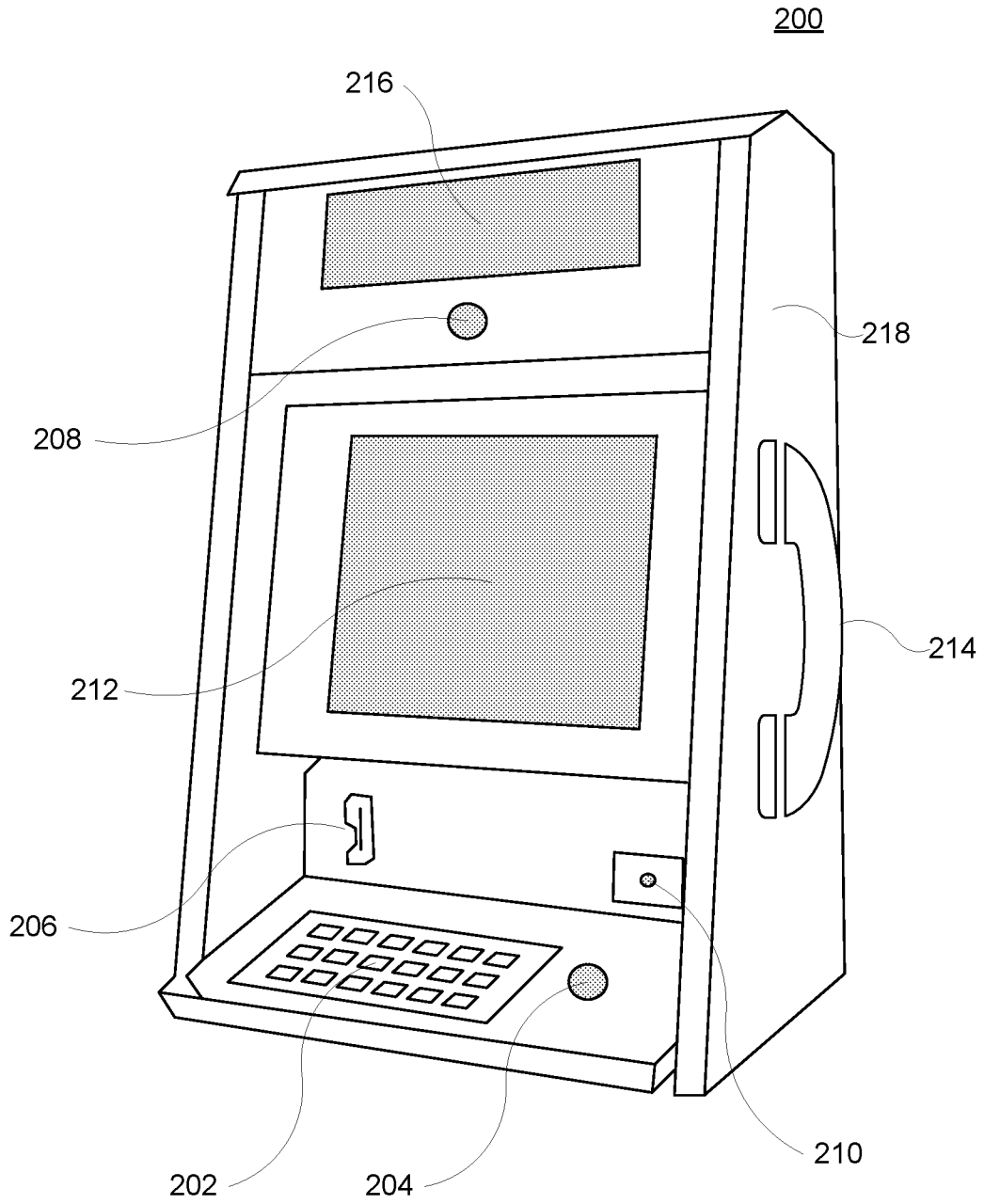


FIG. 2

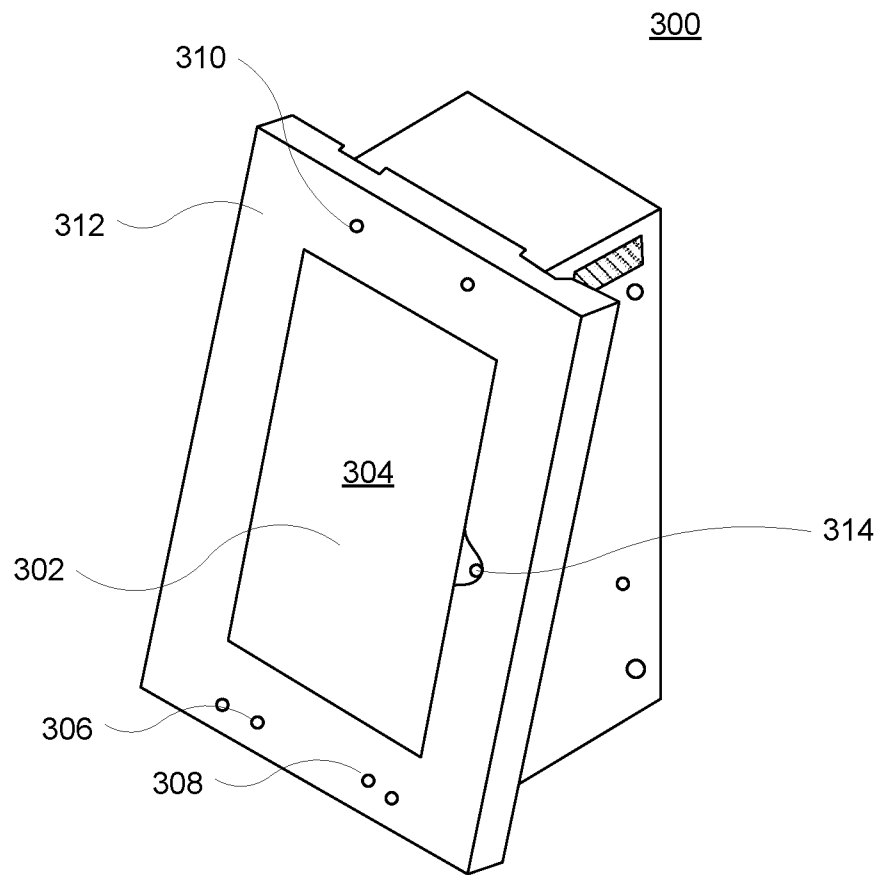


FIG. 3

400

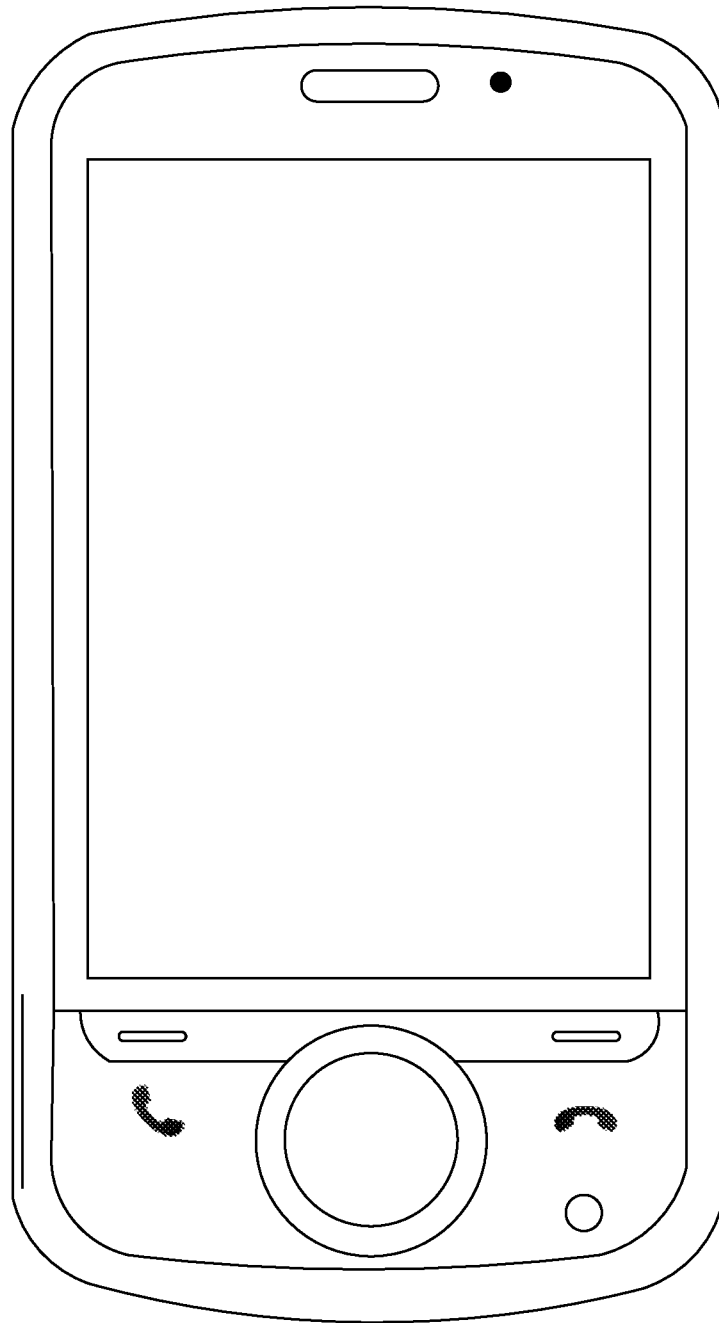


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 17/31317

A. CLASSIFICATION OF SUBJECT MATTER
 IPC(8) - G06F 15/16 (2017.01)
 CPC - H04L 29/08072, H04L 29/06, H04L 29/0809, H04L 29/06047, G06Q 30/02

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)

See Search History Document

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

See Search History Document

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

See Search History Document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2012/0262271 A1 (Torgersrud et al.) 18 October 2012 (18.10.2012), para. [0022], [0026], [0028], [0031], [0039]-[0041], [0043]-[0045], [0048], [0054], [0059]-[0062], [0064], [0068], [0070]-[0071], [0078], [0081]-[0084], and [0093]-[0094], and Figs. 1-2, 5, and 11, and claims 2, 4, and 28.	1, 6-13, 15-17 ----- 2-5, 14
Y	US 2004/0172652 A1 (Fisk et al.) 02 September 2004 (02.09.2004), para. [0051], [0079], [0100], [0153], and [0157], and claims 1 and 62.	2-5, 14
Y	US 2014/0253663 A1 (Edwards) 11 September 2014 (11.09.2014), para. [0021]-[0023], and [0036]-[0037], and Fig. 1.	18-20
Y	US 2013/0252575 A1 (Ewell, Jr. et al.) 26 September 2013 (26.09.2013), para. [0021], [0031], [0033], [0065], [0113], [0148], [0153], [0169], [0173], [0180], and [0199].	18-20

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	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 02 July 2017	Date of mailing of the international search report 02 AUG 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774