



US 20090070477A1

(19) **United States**

(12) **Patent Application Publication**
Baum et al.

(10) **Pub. No.: US 2009/0070477 A1**

(43) **Pub. Date: Mar. 12, 2009**

(54) **CONTROLLING DATA ROUTING AMONG NETWORKS**

(76) Inventors: **Marc Baum**, San Jose, CA (US);
Paul J. Dawes, Woodside, CA (US); **Chris DeCenzo**, Atherton, CA (US); **Gerry Gutt**, Tucson, AZ (US); **Reza Raji**, Menlo Park, CA (US); **Aaron Wood**, Boulder Creek, CA (US)

Correspondence Address:

COURTNEY STANIFORD & GREGORY LLP
P.O. BOX 9686
SAN JOSE, CA 95157 (US)

(21) Appl. No.: **12/198,060**

(22) Filed: **Aug. 25, 2008**

Related U.S. Application Data

- (63) Continuation-in-part of application No. 11/084,232, filed on Mar. 16, 2005, Continuation-in-part of application No. 11/761,718, filed on Jun. 12, 2007, Continuation-in-part of application No. 11/761,745, filed on Jun. 12, 2007, Continuation-in-part of application No. 12/019,554, filed on Jan. 24, 2008, Continuation-in-part of application No. 12/019,568, filed on Jan. 24, 2008, Continuation-in-part of application No. 12/189,757, filed on Aug. 11, 2008.
- (60) Provisional application No. 60/957,997, filed on Aug. 24, 2007, provisional application No. 60/968,005, filed on Aug. 24, 2007, provisional application No. 60/987,359, filed on Nov. 12, 2007, provisional application No. 60/987,366, filed on Nov. 12, 2007, provi-

sional application No. 61/019,162, filed on Jan. 4, 2008, provisional application No. 61/019,167, filed on Jan. 4, 2008, provisional application No. 61/023,489, filed on Jan. 25, 2008, provisional application No. 61/023,493, filed on Jan. 25, 2008, provisional application No. 61/023,496, filed on Jan. 25, 2008, provisional application No. 61/087,967, filed on Aug. 11, 2008.

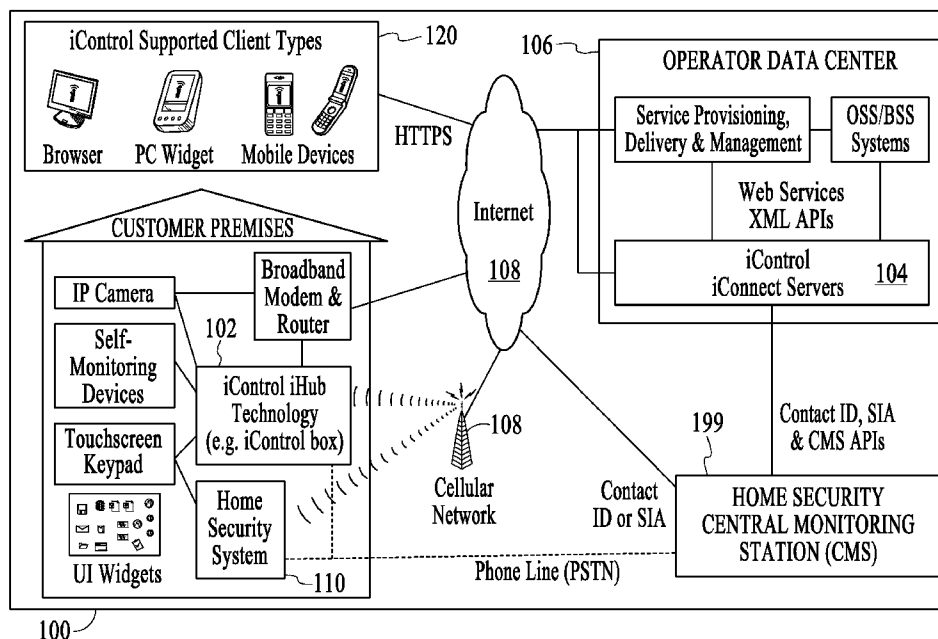
Publication Classification

(51) **Int. Cl.**
G06F 15/16 (2006.01)

(52) **U.S. Cl.** **709/231; 709/238**

(57) **ABSTRACT**

An integrated security system integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network having remote connectivity and access. The integrated security system delivers remote premise monitoring and control functionality to conventional monitored premise protection and complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wirelessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices can be added, enabling users to remotely see live video or pictures and control home devices via a personal web portal or other client device. Camera management enables automatic configuration and management of cameras in the premise network. The camera management extends to remote control and monitoring from outside the firewall of the premise network to include routing of images or video from a streaming source device to a requesting client device.



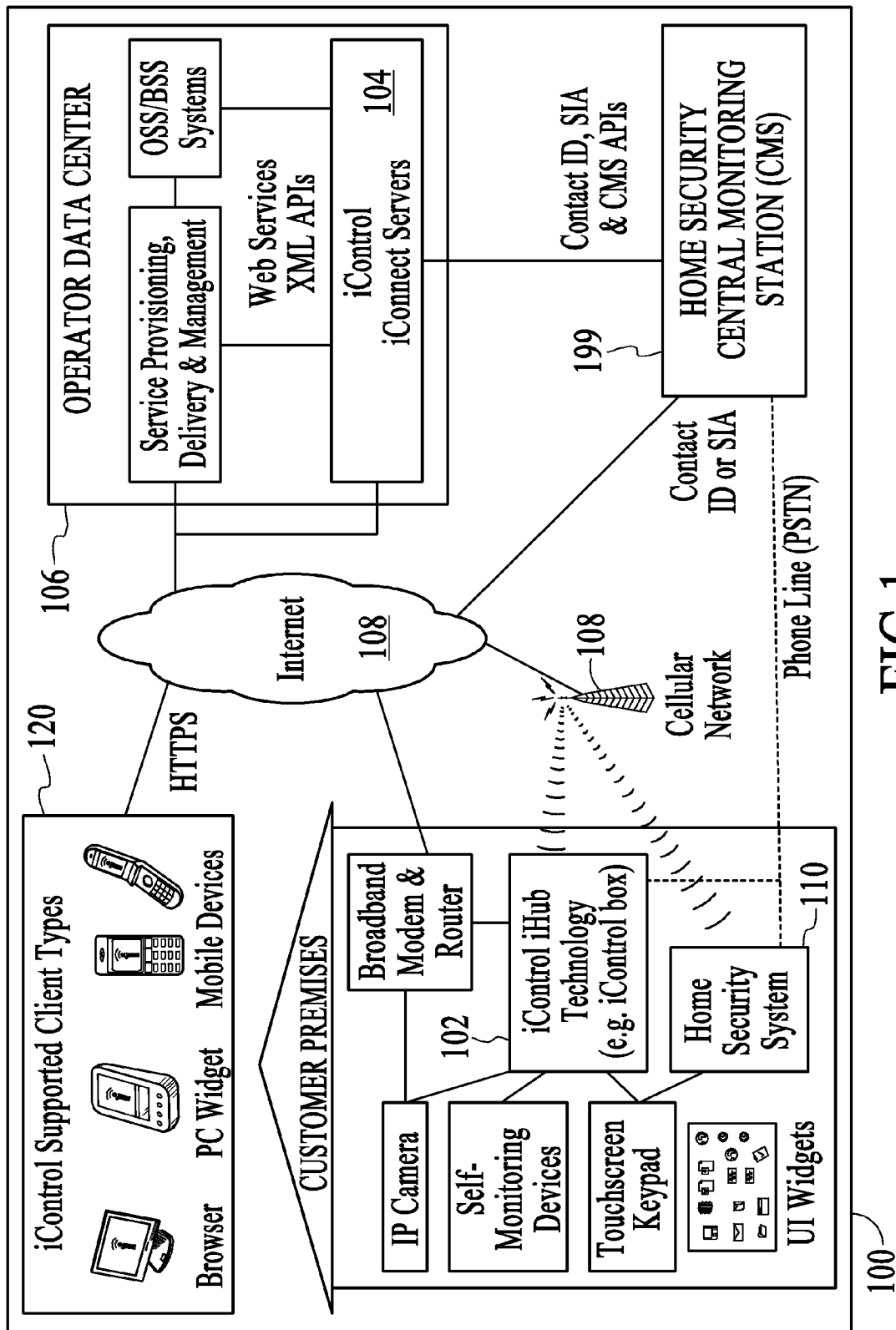


FIG. 1

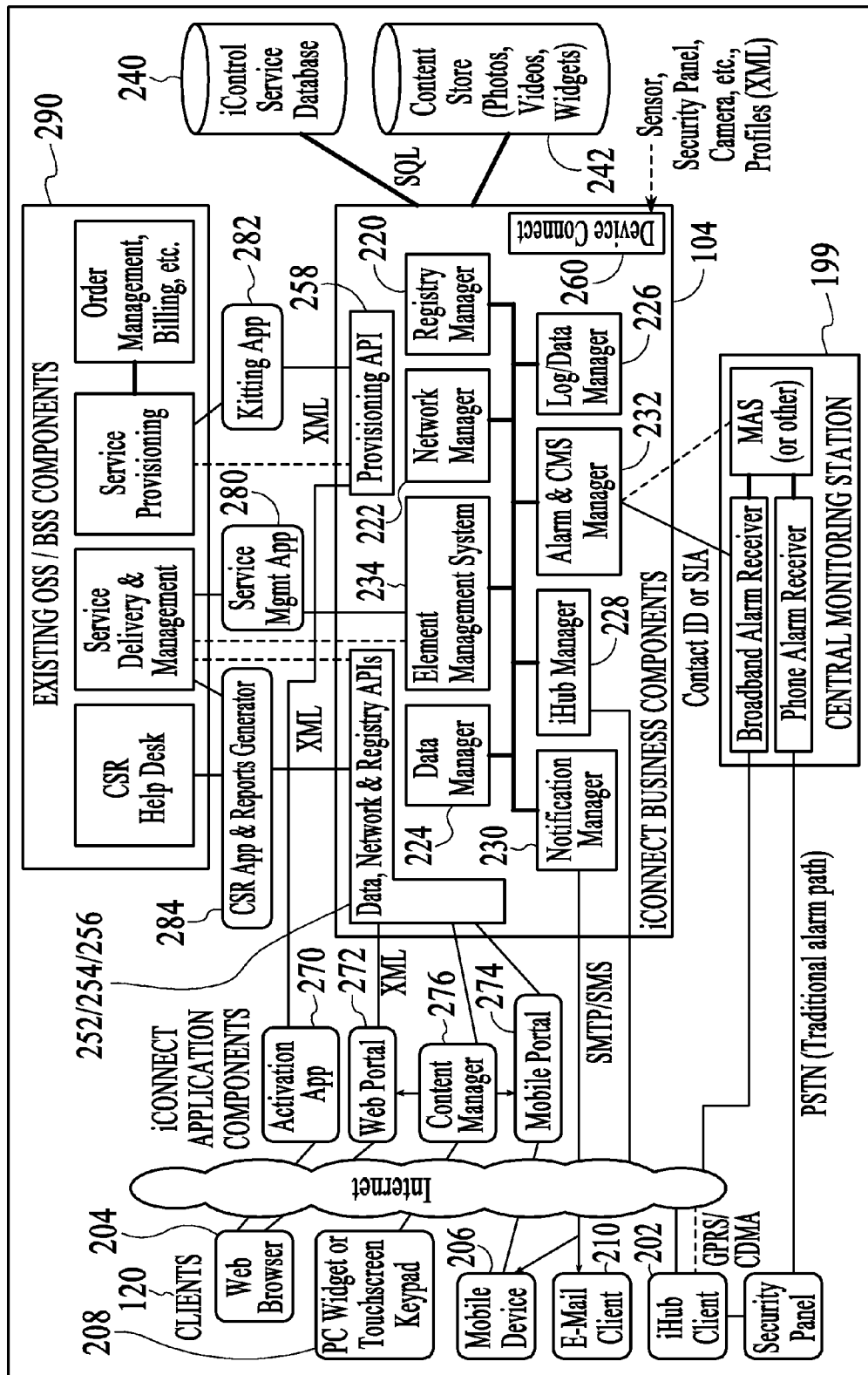


FIG. 2

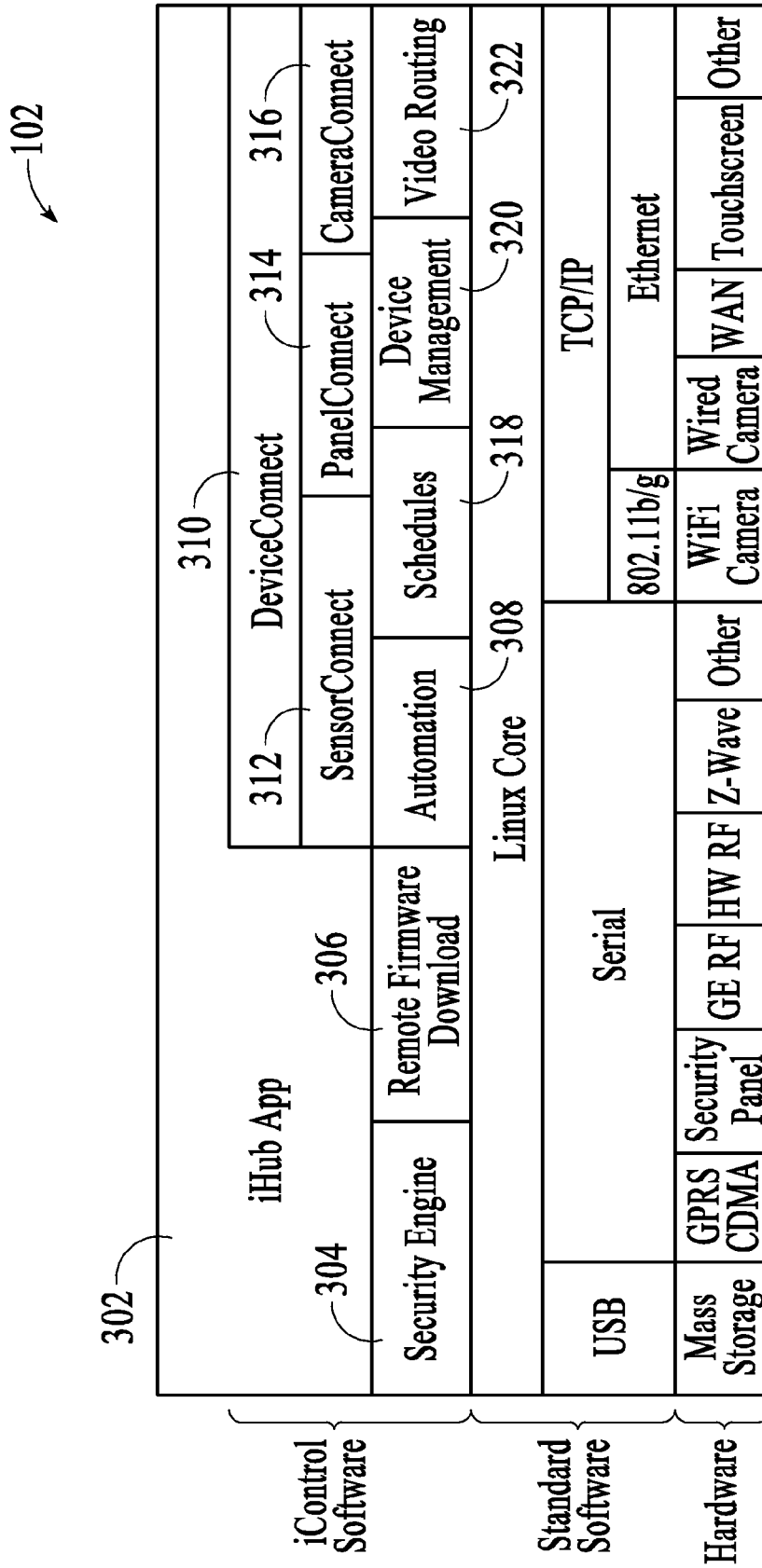


FIG.3

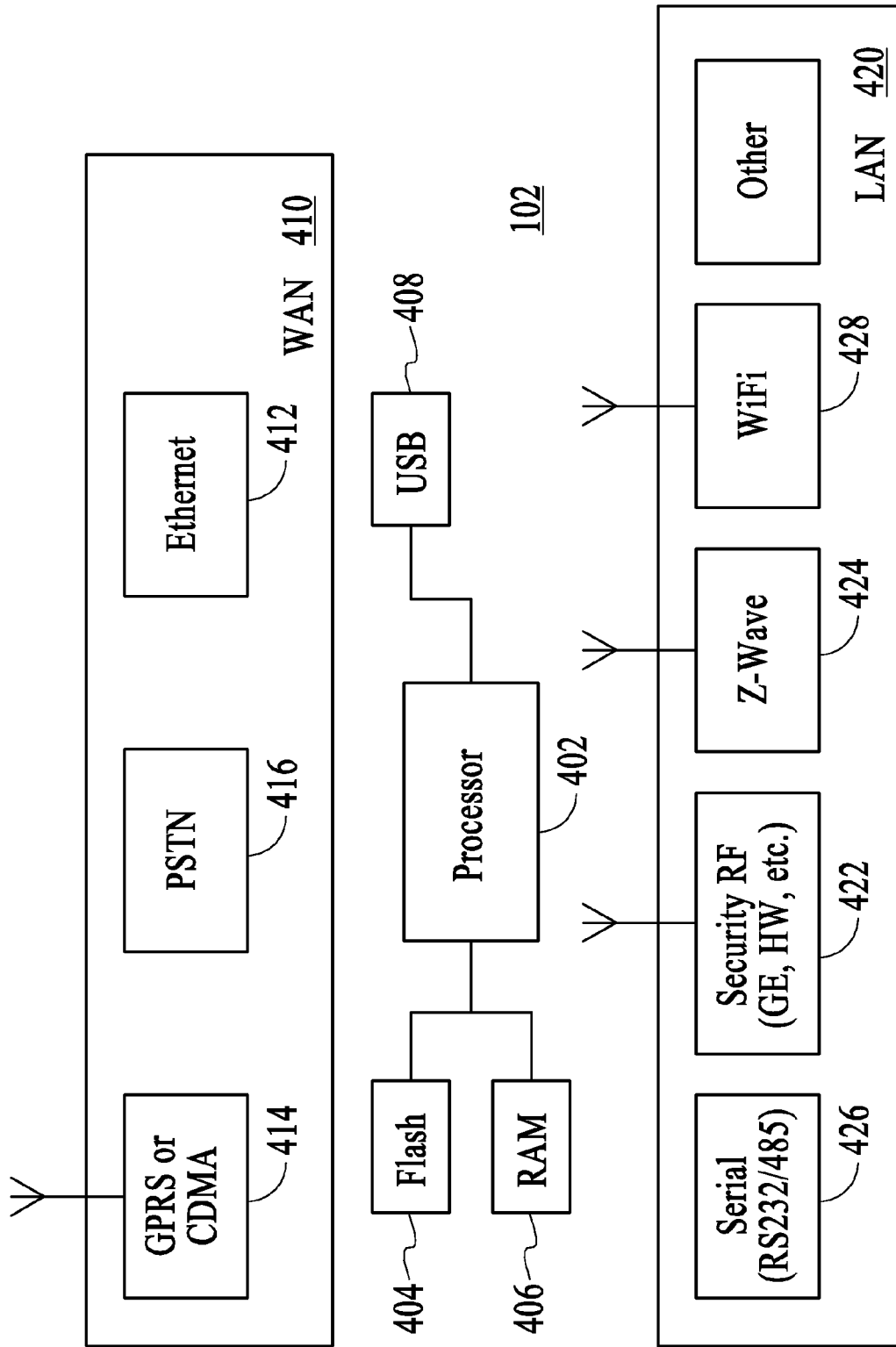
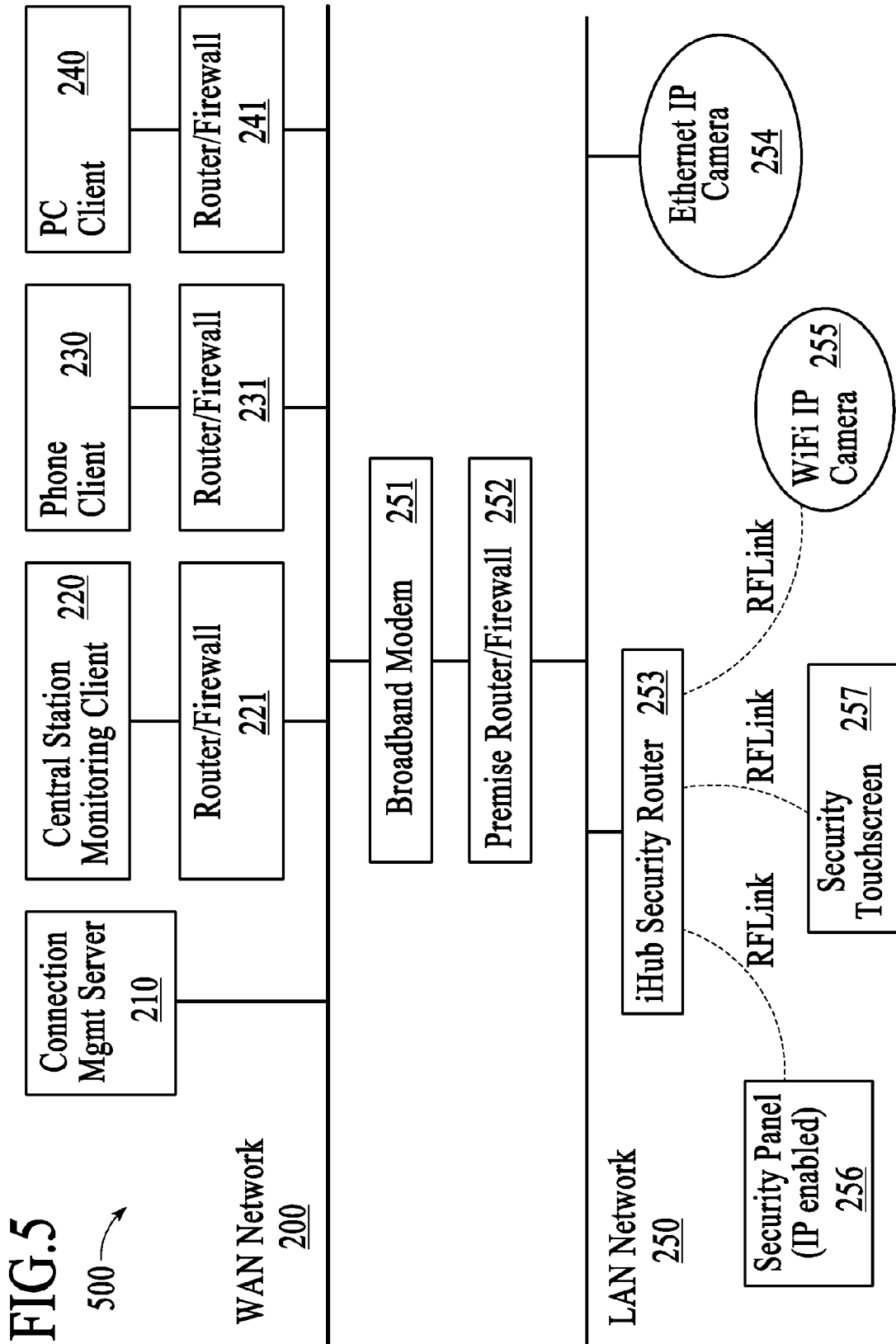
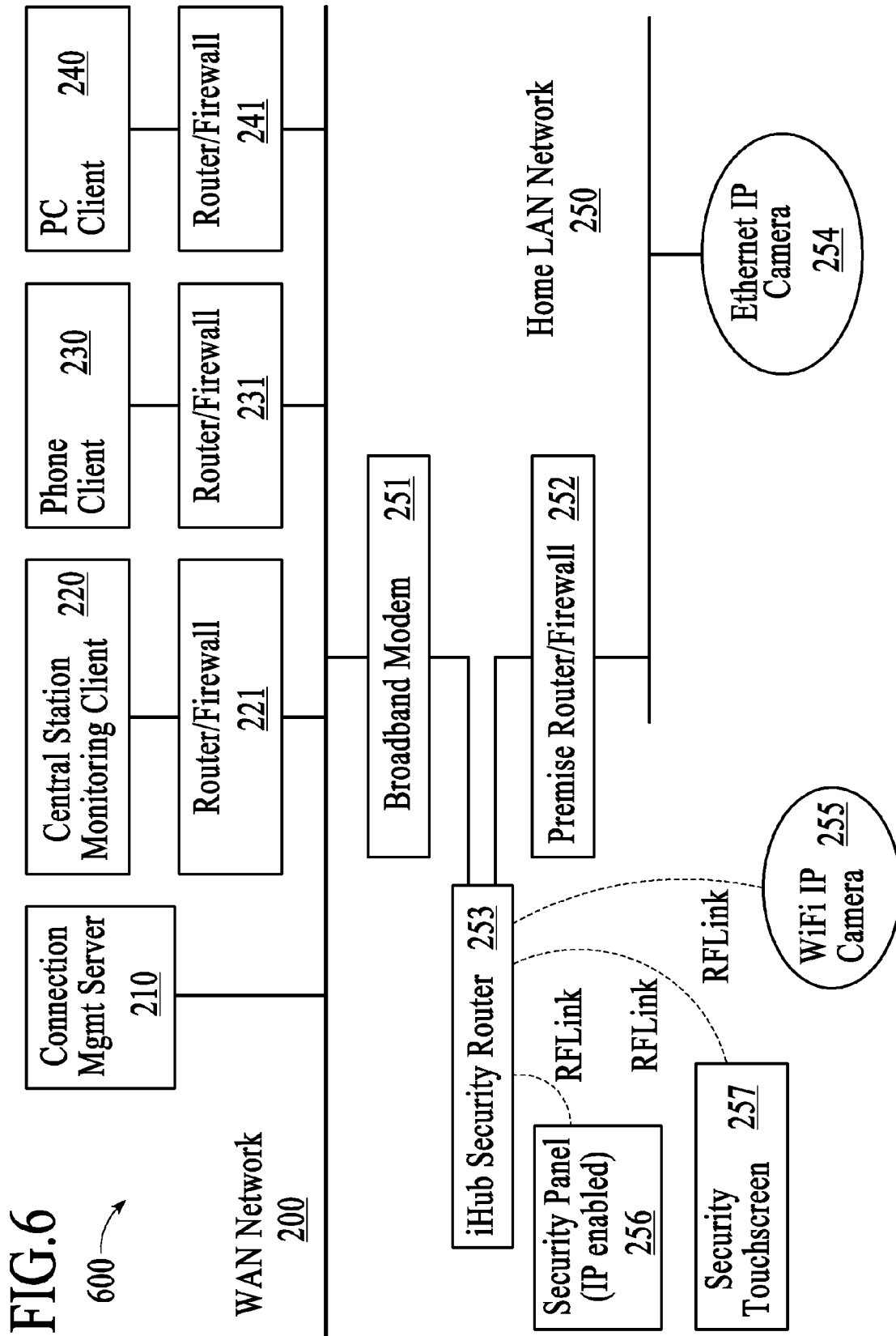


FIG.4





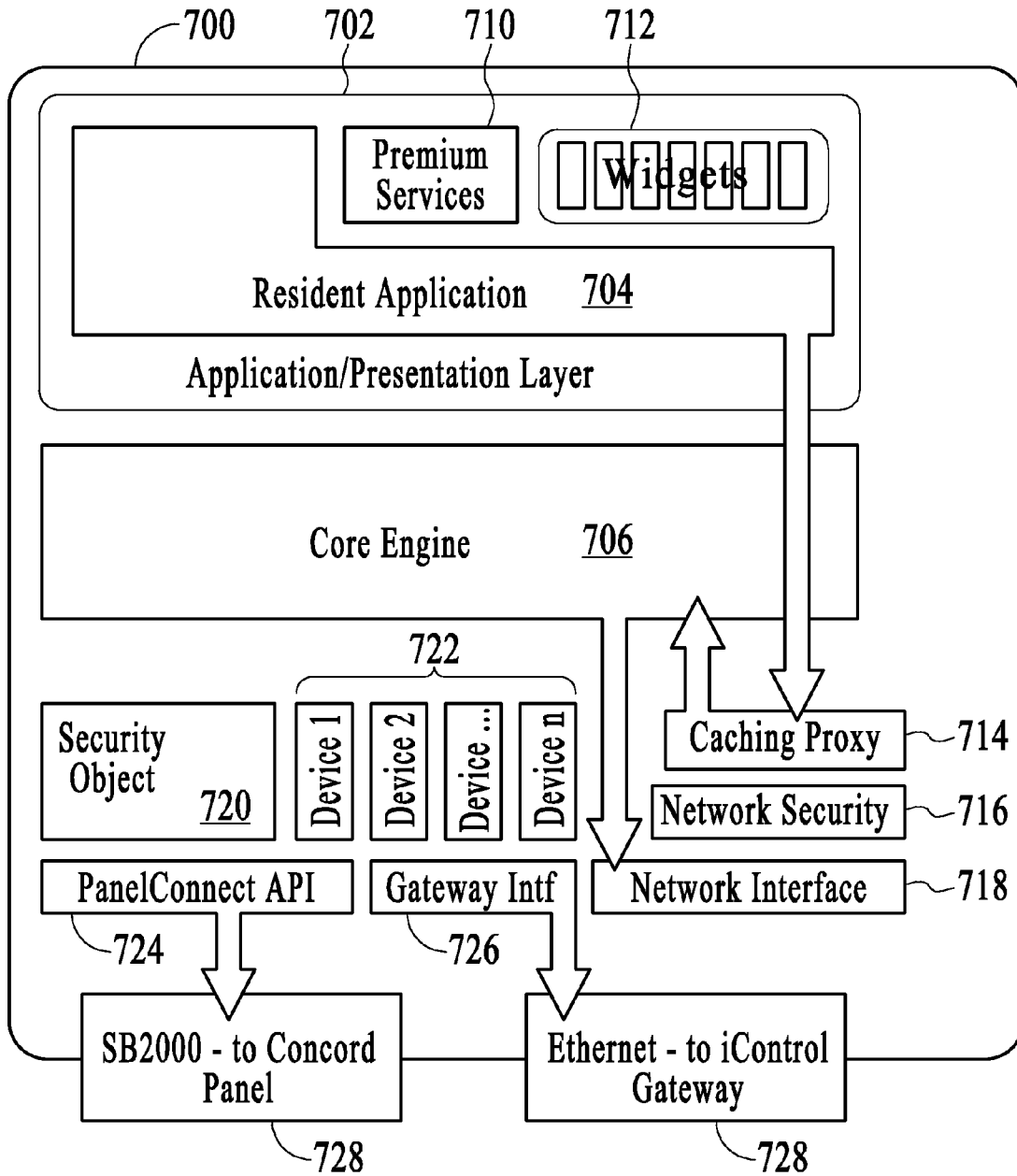


FIG.7

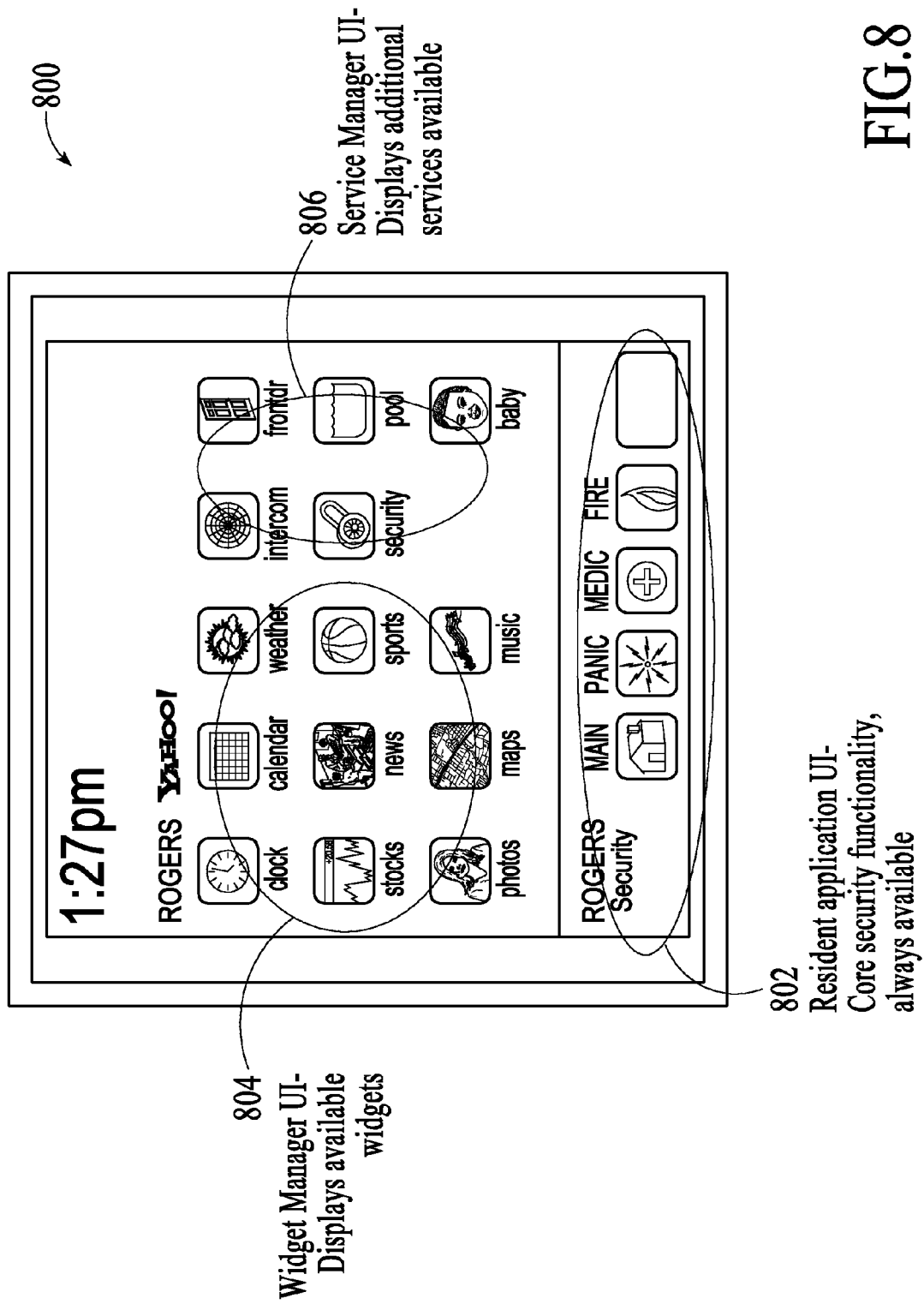
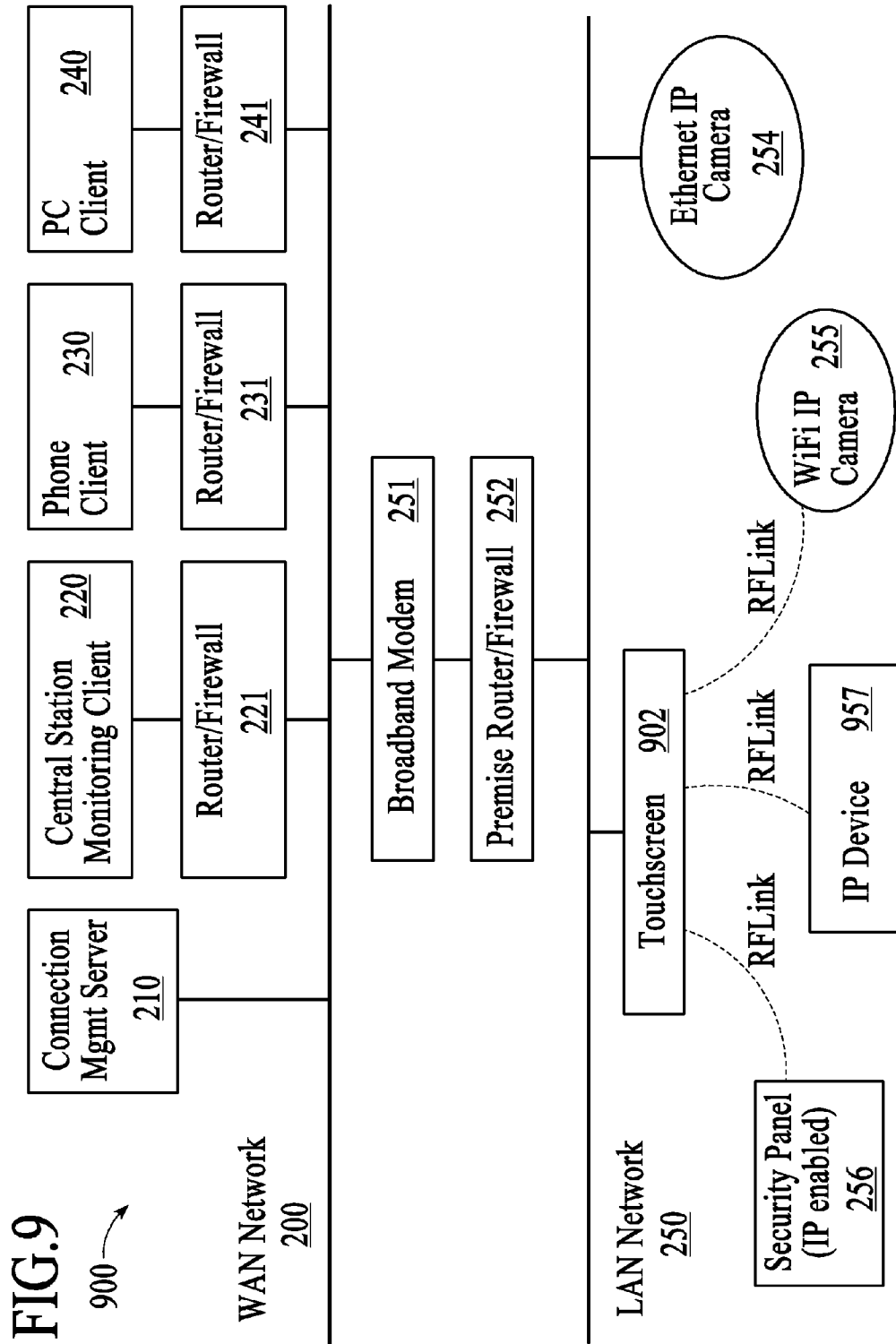
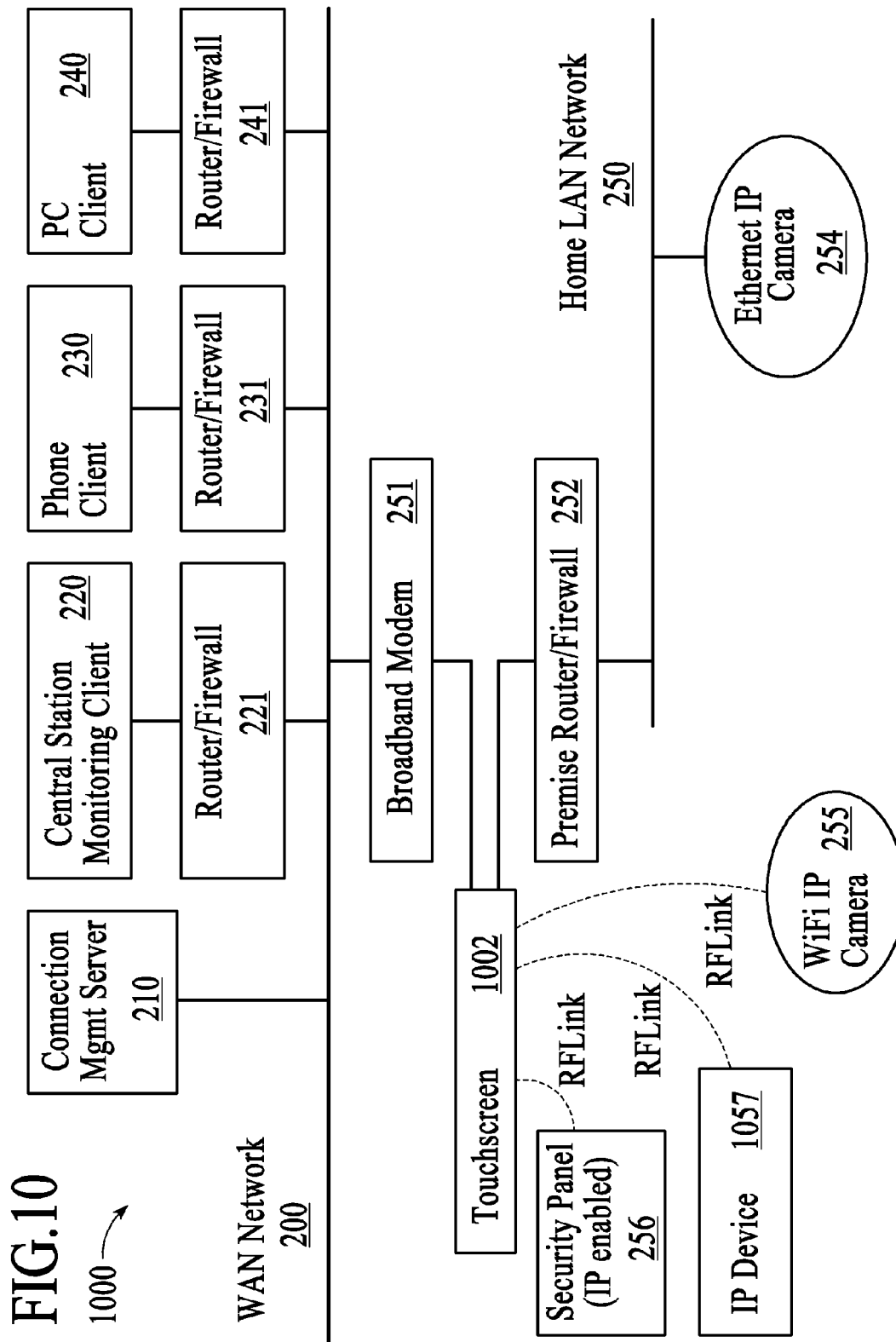


FIG. 8





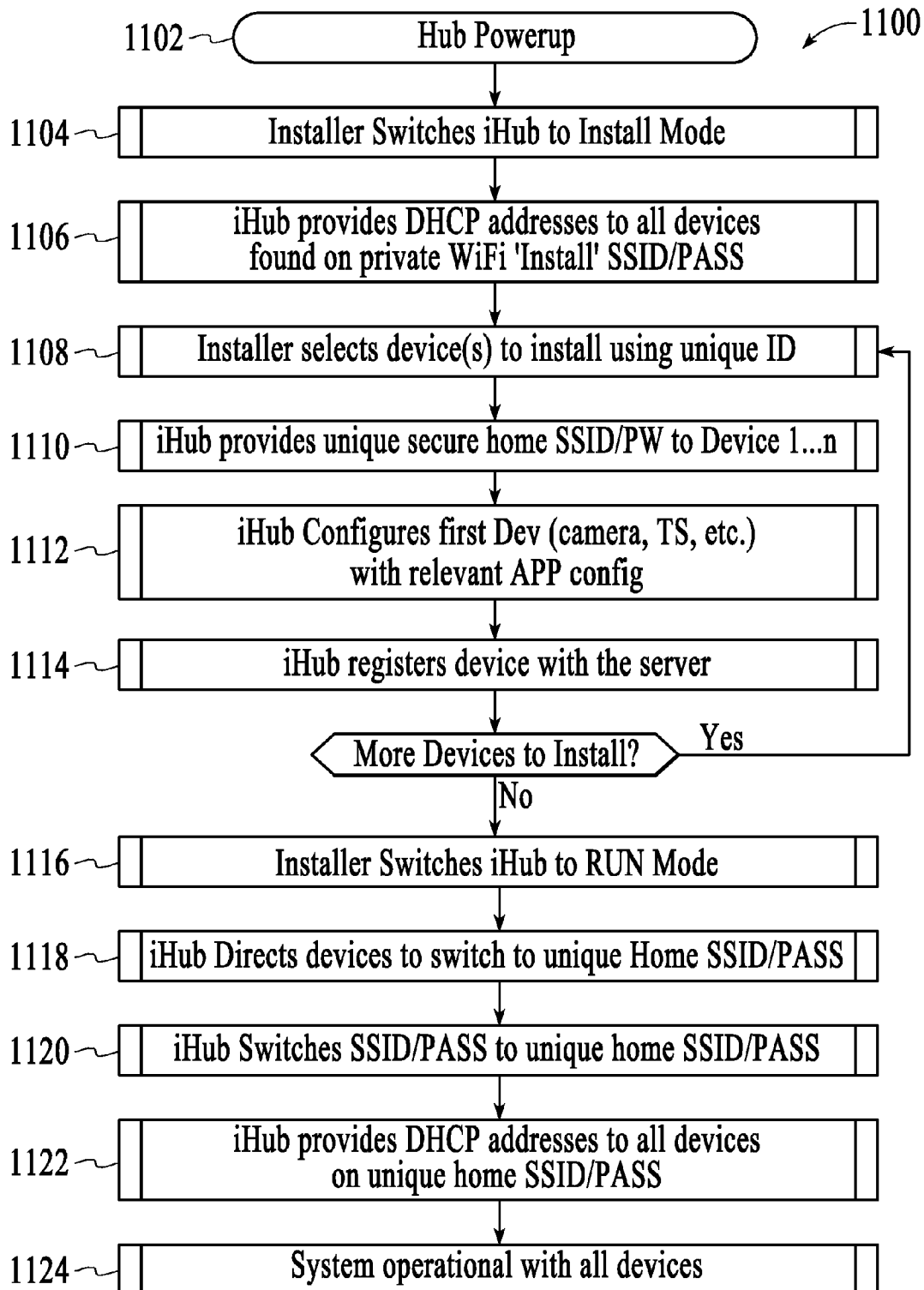


FIG.11

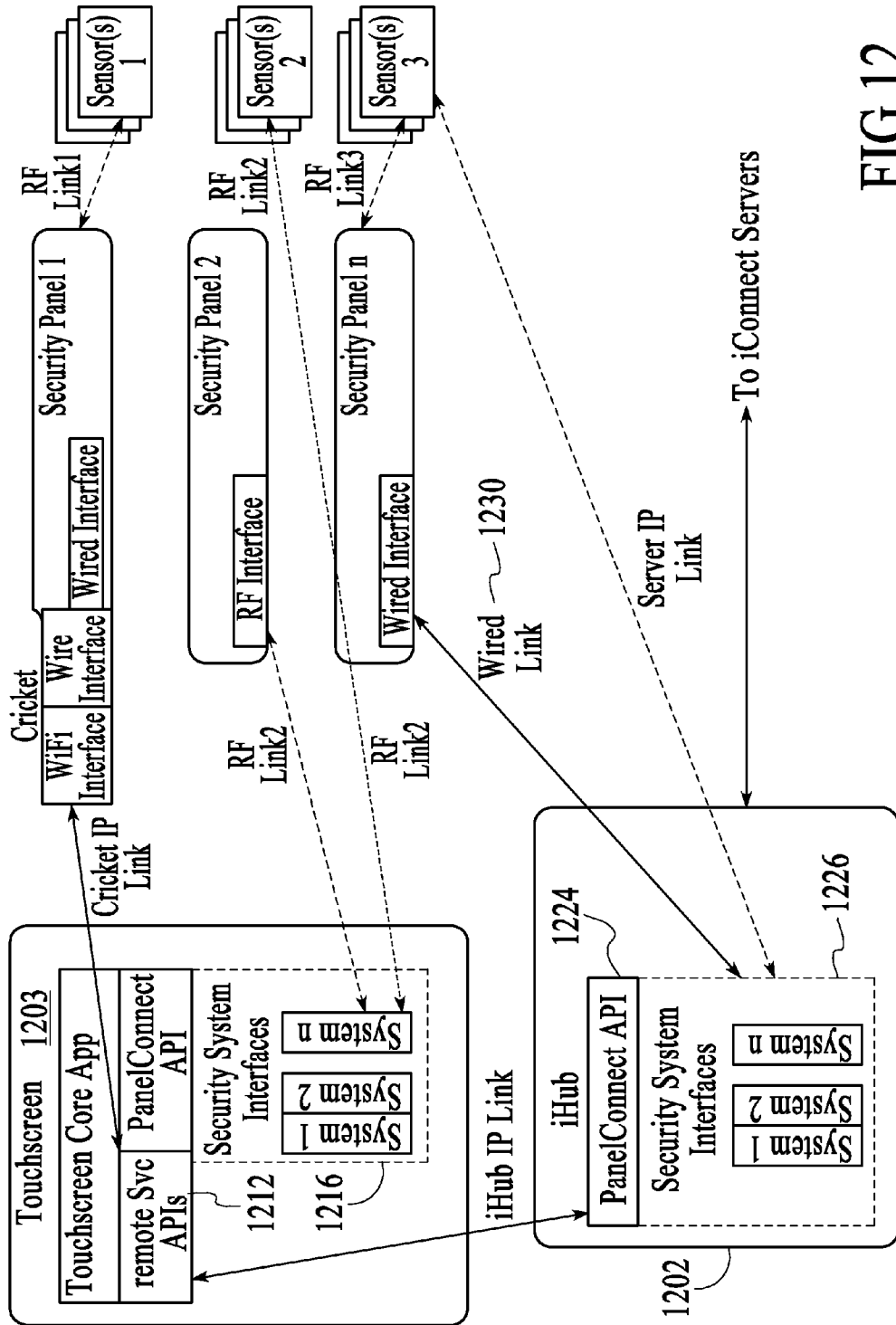


FIG.12

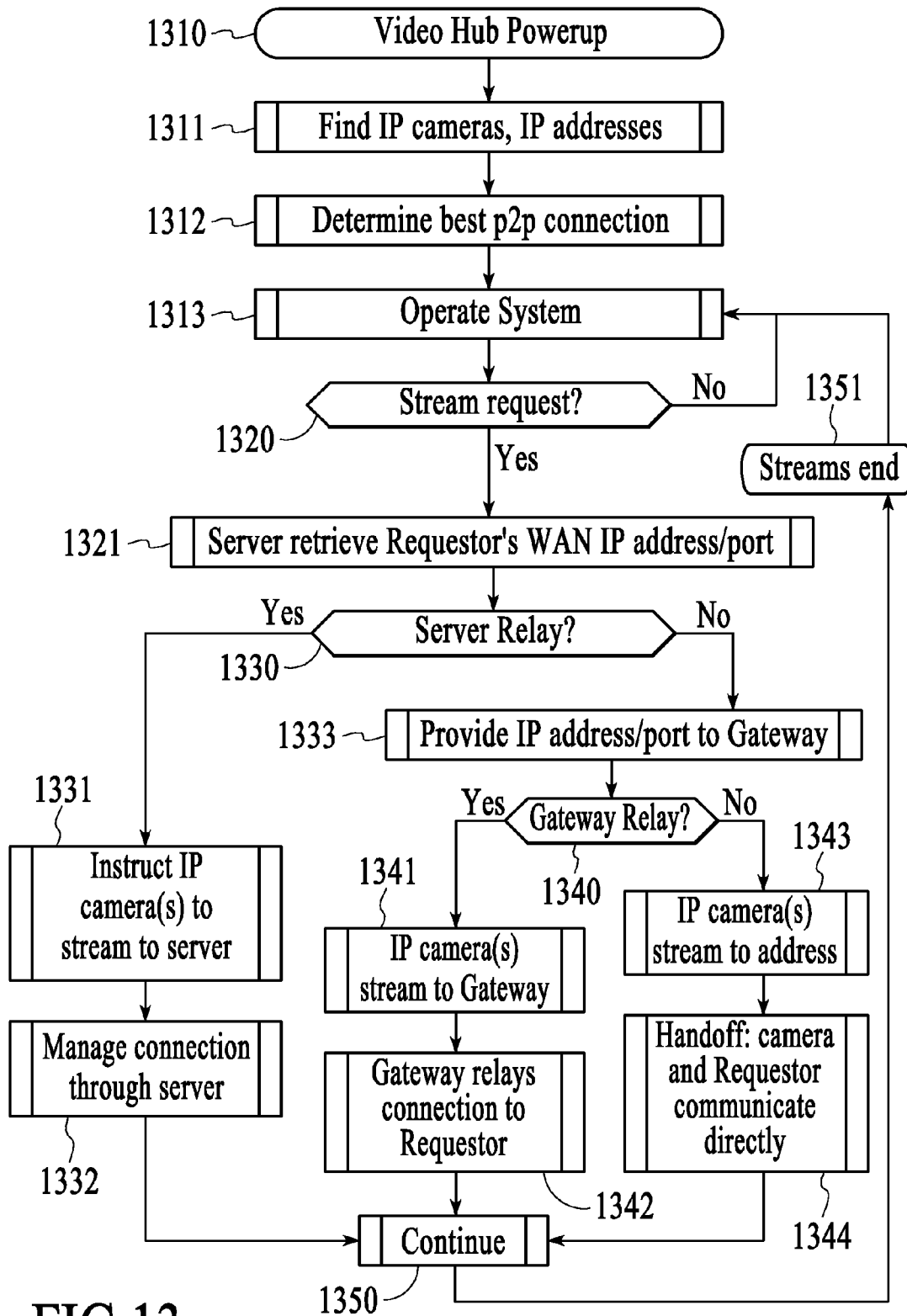


FIG.13

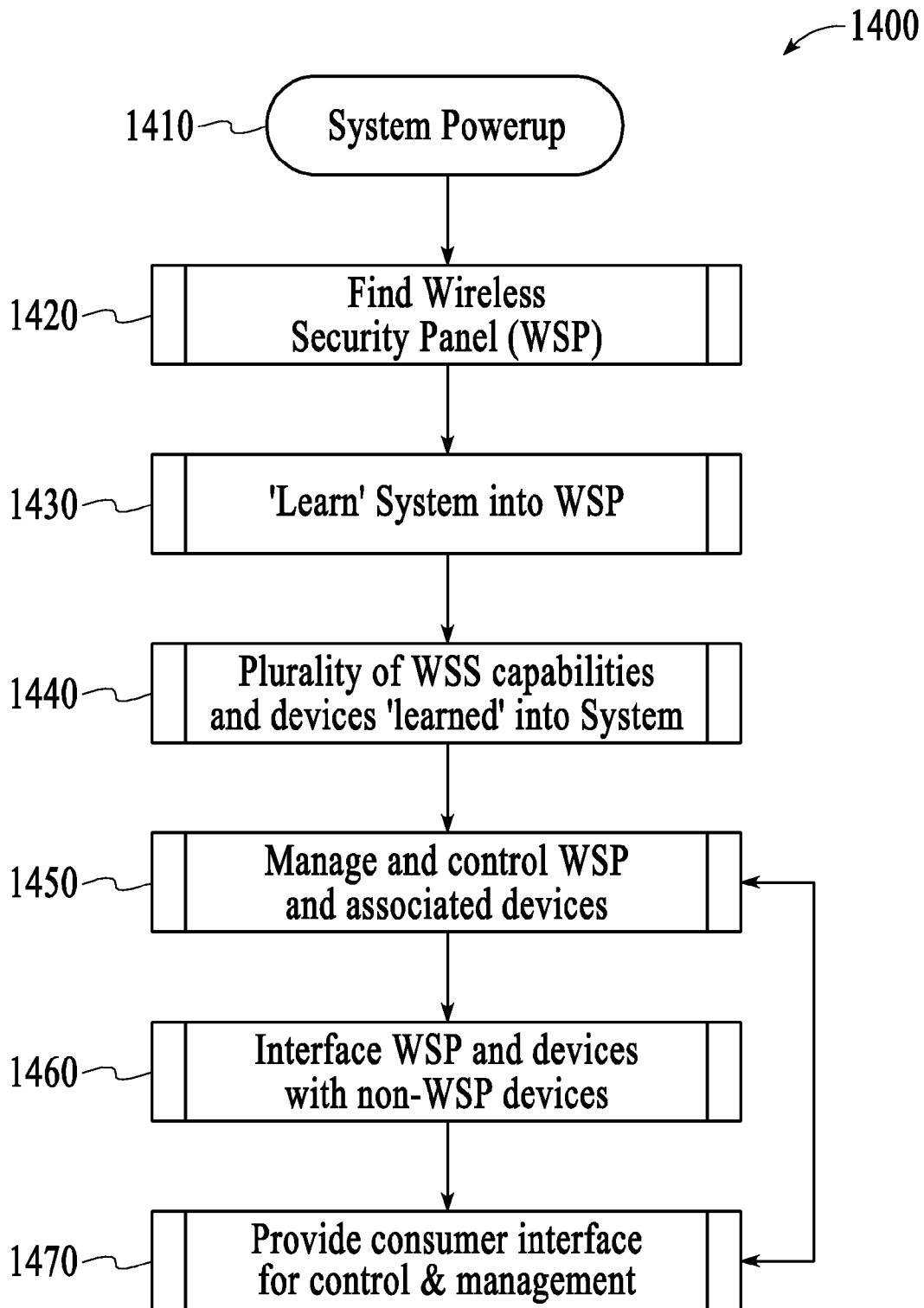


FIG.14

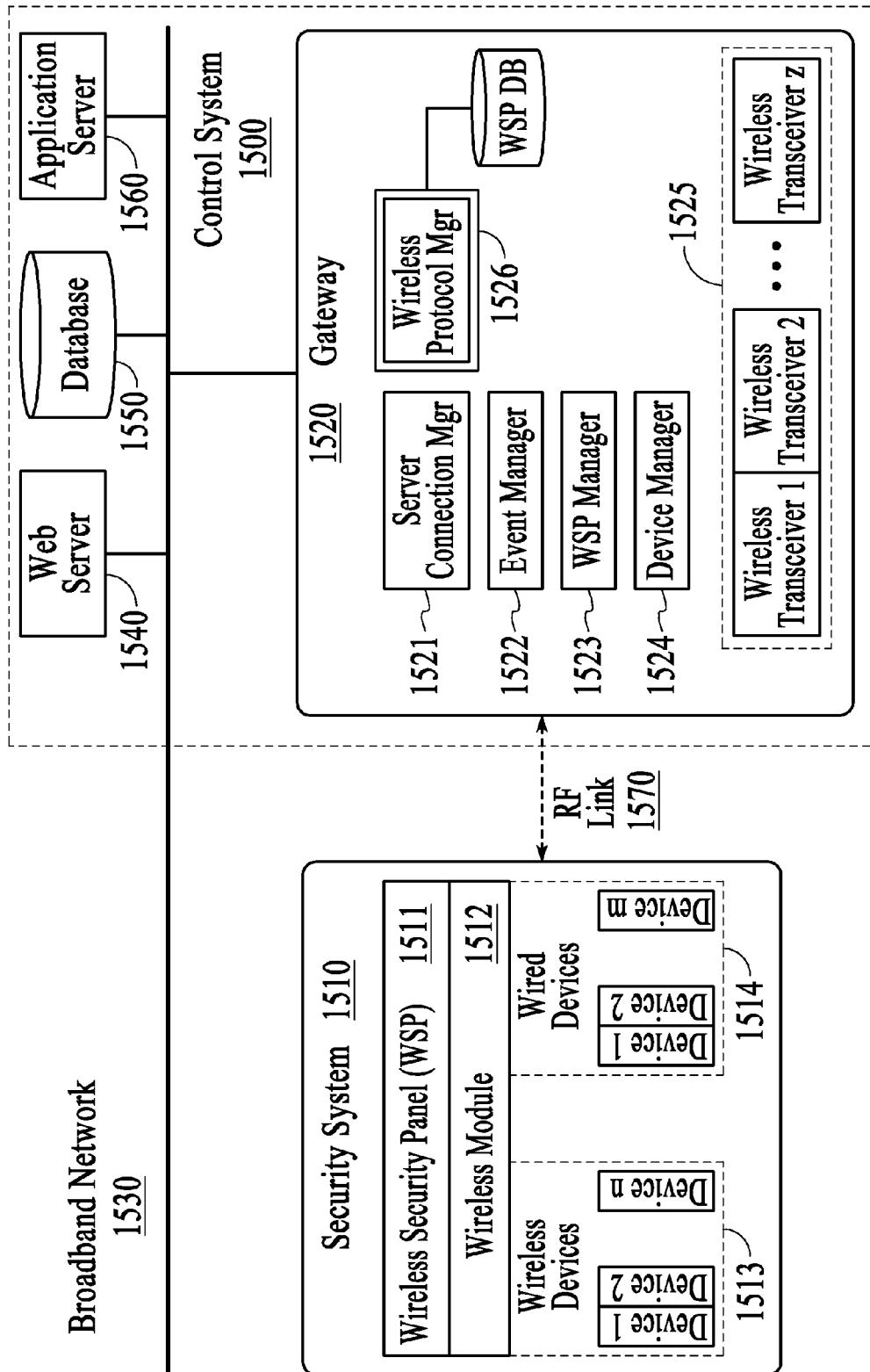


FIG.15

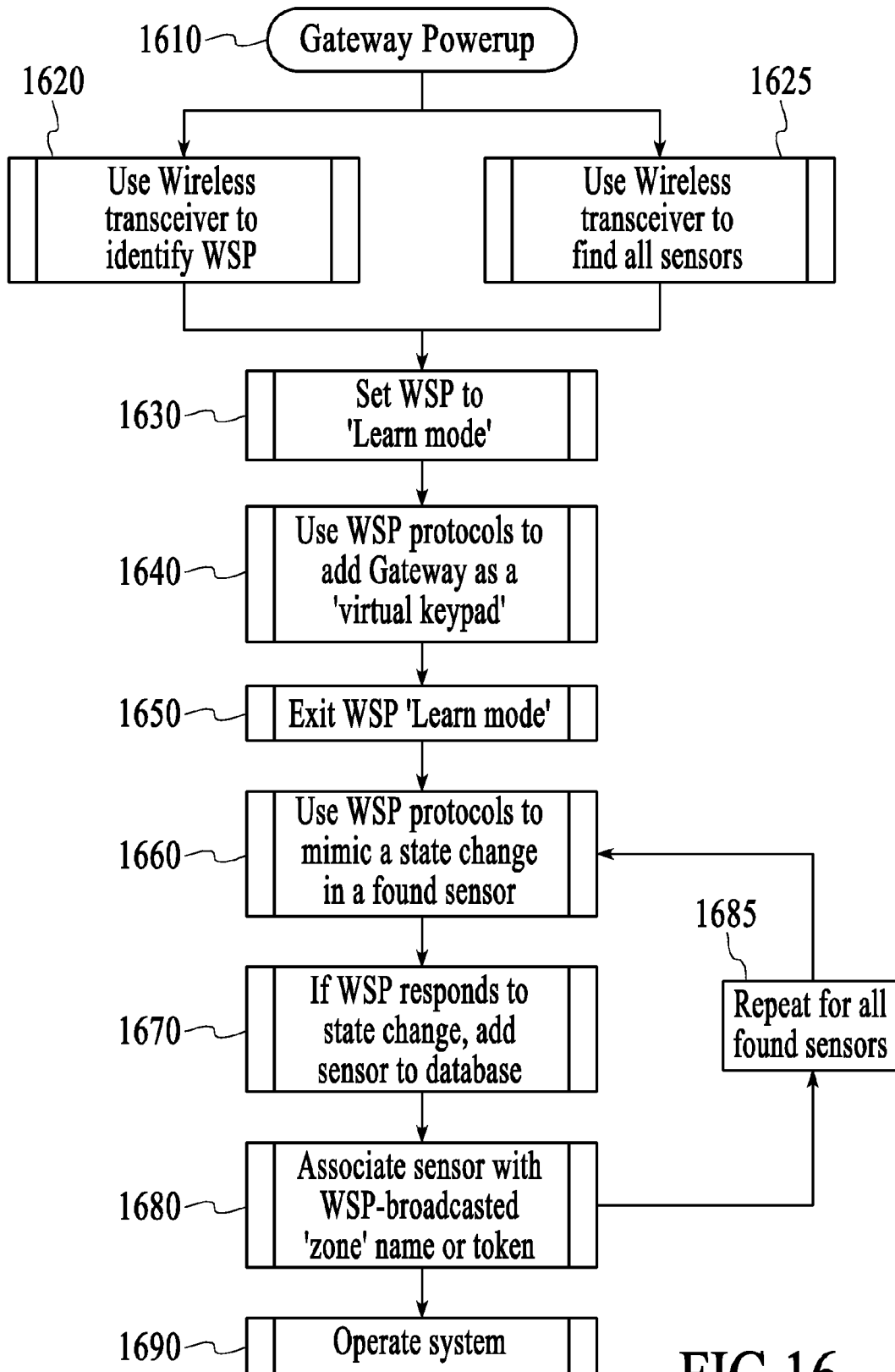


FIG.16

CONTROLLING DATA ROUTING AMONG NETWORKS

RELATED APPLICATIONS

- [0001] This application claims the benefit of U.S. Patent Application No. 60/957,997, filed Aug. 24, 2007.
- [0002] This application claims the benefit of U.S. Patent Application No. 60/968,005, filed Aug. 24, 2007.
- [0003] This application claims the benefit of U.S. Patent Application No. 60/987,359, filed Nov. 12, 2007.
- [0004] This application claims the benefit of U.S. Patent Application No. 60/987,366, filed Nov. 12, 2007.
- [0005] This application claims the benefit of U.S. Patent Application No. 61/019,162, filed Jan. 4, 2008.
- [0006] This application claims the benefit of U.S. Patent Application No. 61/019,167, filed Jan. 4, 2008.
- [0007] This application claims the benefit of U.S. Patent Application No. 61/023,489, filed Jan. 25, 2008.
- [0008] This application claims the benefit of U.S. Patent Application No. 61/023,493, filed Jan. 25, 2008.
- [0009] This application claims the benefit of U.S. Patent Application No. 61/023,496, filed Jan. 25, 2008.
- [0010] This application claims the benefit of U.S. Patent Application No. 61/087,967, filed Aug. 11, 2008.
- [0011] This application is a continuation in part application of U.S. patent application Ser. No. 11/084,232, filed Mar. 16, 2005.
- [0012] This application is a continuation in part application of U.S. patent application Ser. No. 11/761,718, filed Jun. 12, 2007.
- [0013] This application is a continuation in part application of U.S. patent application Ser. No. 11/761,745, filed Jun. 12, 2007.
- [0014] This application is a continuation in part application of U.S. patent application Ser. No. 12/019,554, filed Jan. 24, 2008.
- [0015] This application is a continuation in part application of U.S. patent application Ser. No. 12/019,568, filed Jan. 24, 2008.
- [0016] This application is a continuation in part application of U.S. patent application Ser. No. 12/189,757, filed Aug. 11, 2008.

TECHNICAL FIELD

[0017] The embodiments described herein relate generally to a method and apparatus for improving the capabilities of security systems in home and business applications. More particularly, the embodiments described herein relate to enabling video cameras in a security system or home monitoring application to couple or connect to monitoring and/or control applications residing outside of a Local Area Network (LAN) in which the video cameras are situated.

BACKGROUND

[0018] The field of home and small business security is dominated by technology suppliers who build comprehensive 'closed' security systems, where the individual components (sensors, security panels, keypads) operate solely within the confines of a single vendor solution. For example, a wireless motion sensor from vendor A cannot be used with a security panel from vendor B. Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or

no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-based network (such as an Internet Protocol (IP) network); most installed systems support only a low-bandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.

[0019] Furthermore, with the proliferation of the internet, ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth, low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT) there increasingly exists the networking capability to extend these traditional security systems to offer enhanced functionality. In addition, the proliferation of broadband access has driven a corresponding increase in home and small business networking technologies and devices. It is desirable to extend traditional security systems to encompass enhanced functionality such as the ability to control and manage security systems from the world wide web, cellular telephones, or advanced function internet-based devices. Other desired functionality includes an open systems approach to interface home security systems to home and small business networks.

[0020] Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. Solution providers attempting to address this need are becoming known in the art, including three categories of vendors: traditional proprietary hardware providers such as Honeywell and GE Security; third party hard-wired module providers such as Alarm.com, NextAlarm, and uControl; and new proprietary systems providers such as InGrid.

[0021] A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.

[0022] A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for sys-

tems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.

INCORPORATION BY REFERENCE

[0023] Each patent, patent application, and/or publication mentioned in this specification is herein incorporated by reference in its entirety to the same extent as if each individual patent, patent application, and/or publication was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] FIG. 1 is a block diagram of the integrated security system, under an embodiment.

[0025] FIG. 2 is a block diagram of components of the integrated security system, under an embodiment.

[0026] FIG. 3 is a block diagram of the gateway software or applications, under an embodiment.

[0027] FIG. 4 is a block diagram of the gateway components, under an embodiment.

[0028] FIG. 5 is a block diagram of IP device integration with a premise network, under an embodiment.

[0029] FIG. 6 is a block diagram of IP device integration with a premise network, under an alternative embodiment.

[0030] FIG. 7 is a block diagram of a touchscreen, under an embodiment.

[0031] FIG. 8 is an example screenshot of a networked security touchscreen, under an embodiment.

[0032] FIG. 9 is a block diagram of network or premise device integration with a premise network, under an embodiment.

[0033] FIG. 10 is a block diagram of network or premise device integration with a premise network, under an alternative embodiment.

[0034] FIG. 11 is a flow diagram for installation of an IP device into a private network environment, under an embodiment.

[0035] FIG. 12 is a block diagram showing communications among IP devices of the private network environment, under an embodiment.

[0036] FIG. 13 is a general flow diagram for IP video control, under an embodiment.

[0037] FIG. 14 is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment.

[0038] FIG. 15 is a block diagram of an integrated security system wirelessly interfacing to proprietary security systems, under an embodiment.

[0039] FIG. 16 is a flow diagram for wirelessly 'learning' the gateway into an existing security system and discovering extant sensors, under an embodiment.

DETAILED DESCRIPTION

[0040] An integrated security system is described that integrates broadband and mobile access and control with conventional security systems and premise devices to provide a tri-mode security network (broadband, cellular/GSM, POTS access) that enables users to remotely stay connected to their premises. The integrated security system, while delivering remote premise monitoring and control functionality to conventional monitored premise protection, complements existing premise protection equipment. The integrated security system integrates into the premise network and couples wire-

lessly with the conventional security panel, enabling broadband access to premise security systems. Automation devices (cameras, lamp modules, thermostats, etc.) can be added, enabling users to remotely see live video and/or pictures and control home devices via their personal web portal or webpage, mobile phone, and/or other remote client device. Users can also receive notifications via email or text message when happenings occur, or do not occur, in their home.

[0041] Although the detailed description herein contains many specifics for the purposes of illustration, anyone of ordinary skill in the art will appreciate that many variations and alterations to the following details are within the scope of the embodiments described herein. Thus, the following illustrative embodiments are set forth without any loss of generality to, and without imposing limitations upon, the claimed invention.

[0042] In accordance with the embodiments described herein, a wireless system (e.g., radio frequency (RF)) is provided that enables a security provider or consumer to extend the capabilities of an existing RF-capable security system or a non-RF-capable security system that has been upgraded to support RF capabilities. The system includes an RF-capable Gateway device (physically located within RF range of the RF-capable security system) and associated software operating on the Gateway device. The system also includes a web server, application server, and remote database providing a persistent store for information related to the system.

[0043] The security systems of an embodiment, referred to herein as the iControl security system or integrated security system, extend the value of traditional home security by adding broadband access and the advantages of remote home monitoring and home control through the formation of a security network including components of the integrated security system integrated with a conventional premise security system and a premise local area network (LAN). With the integrated security system, conventional home security sensors, cameras, touchscreen keypads, lighting controls, and/or Internet Protocol (IP) devices in the home (or business) become connected devices that are accessible anywhere in the world from a web browser, mobile phone or through content-enabled touchscreens. The integrated security system experience allows security operators to both extend the value proposition of their monitored security systems and reach new consumers that include broadband users interested in staying connected to their family, home and property when they are away from home.

[0044] The integrated security system of an embodiment includes security servers (also referred to herein as iConnect servers or security network servers) and an iHub gateway (also referred to herein as the gateway, the iHub, or the iHub client) that couples or integrates into a home network (e.g., LAN) and communicates directly with the home security panel, in both wired and wireless installations. The security system of an embodiment automatically discovers the security system components (e.g., sensors, etc.) belonging to the security system and connected to a control panel of the security system and provides consumers with full two-way access via web and mobile portals. The gateway supports various wireless protocols and can interconnect with a wide range of control panels offered by security system providers. Service providers and users can then extend the system's capabilities with the additional IP cameras, lighting modules or security devices such as interactive touchscreen keypads. The integrated security system adds an enhanced value to these secu-

rity systems by enabling consumers to stay connected through email and SMS alerts, photo push, event-based video capture and rule-based monitoring and notifications. This solution extends the reach of home security to households with broadband access.

[0045] The integrated security system builds upon the foundation afforded by traditional security systems by layering broadband and mobile access, IP cameras, interactive touchscreens, and an open approach to home automation on top of traditional security system configurations. The integrated security system is easily installed and managed by the security operator, and simplifies the traditional security installation process, as described below.

[0046] The integrated security system provides an open systems solution to the home security market. As such, the foundation of the integrated security system customer premises equipment (CPE) approach has been to abstract devices, and allows applications to manipulate and manage multiple devices from any vendor. The integrated security system DeviceConnect technology that enables this capability supports protocols, devices, and panels from GE Security and Honeywell, as well as consumer devices using Z-Wave, IP cameras (e.g., Ethernet, wifi, and Homeplug), and IP touchscreens. The DeviceConnect is a device abstraction layer that enables any device or protocol layer to interoperate with integrated security system components. This architecture enables the addition of new devices supporting any of these interfaces, as well as add entirely new protocols.

[0047] The benefit of DeviceConnect is that it provides supplier flexibility. The same consistent touchscreen, web, and mobile user experience operate unchanged on whatever security equipment selected by a security system provider, with the system provider's choice of IP cameras, backend data center and central station software.

[0048] The integrated security system provides a complete system that integrates or layers on top of a conventional host security system available from a security system provider. The security system provider therefore can select different components or configurations to offer (e.g., CDMA, GPRS, no cellular, etc.) as well as have iControl modify the integrated security system configuration for the system provider's specific needs (e.g., change the functionality of the web or mobile portal, add a GE or Honeywell-compatible TouchScreen, etc.).

[0049] The integrated security system integrates with the security system provider infrastructure for central station reporting directly via Broadband and GPRS alarm transmissions. Traditional dial-up reporting is supported via the standard panel connectivity. Additionally, the integrated security system provides interfaces for advanced functionality to the CMS, including enhanced alarm events, system installation optimizations, system test verification, video verification, 2-way voice over IP and GSM.

[0050] The integrated security system is an IP centric system that includes broadband connectivity so that the gateway augments the existing security system with broadband and GPRS connectivity. If broadband is down or unavailable GPRS may be used, for example. The integrated security system supports GPRS connectivity using an optional wireless package that includes a GPRS modem in the gateway. The integrated security system treats the GPRS connection as a higher cost though flexible option for data transfers. In an embodiment the GPRS connection is only used to route alarm events (e.g., for cost), however the gateway can be configured

(e.g., through the iConnect server interface) to act as a primary channel and pass any or all events over GPRS. Consequently, the integrated security system does not interfere with the current plain old telephone service (POTS) security panel interface. Alarm events can still be routed through POTS; however the gateway also allows such events to be routed through a broadband or GPRS connection as well. The integrated security system provides a web application interface to the CSR tool suite as well as XML web services interfaces for programmatic integration between the security system provider's existing call center products. The integrated security system includes, for example, APIs that allow the security system provider to integrate components of the integrated security system into a custom call center interface. The APIs include XML web service APIs for integration of existing security system provider call center applications with the integrated security system service. All functionality available in the CSR Web application is provided with these API sets. The Java and XML-based APIs of the integrated security system support provisioning, billing, system administration, CSR, central station, portal user interfaces, and content management functions, to name a few. The integrated security system can provide a customized interface to the security system provider's billing system, or alternatively can provide security system developers with APIs and support in the integration effort.

[0051] The integrated security system provides or includes business component interfaces for provisioning, administration, and customer care to name a few. Standard templates and examples are provided with a defined customer professional services engagement to help integrate OSS/BSS systems of a Service Provider with the integrated security system.

[0052] The integrated security system components support and allow for the integration of customer account creation and deletion with a security system. The iConnect APIs provides access to the provisioning and account management system in iConnect and provide full support for account creation, provisioning, and deletion. Depending on the requirements of the security system provider, the iConnect APIs can be used to completely customize any aspect of the integrated security system backend operational system.

[0053] The integrated security system includes a gateway that supports the following standards-based interfaces, to name a few: Ethernet IP communications via Ethernet ports on the gateway, and standard XML/TCP/IP protocols and ports are employed over secured secure socket layer (SSL) sessions; USB 2.0 via ports on the gateway; 802.11b/g/n IP communications; GSM/GPRS RF WAN communications; CDMA 1xRTT RF WAN communications (optional, can also support EVDO and 3G technologies).

[0054] The gateway supports the following proprietary interfaces, to name a few: interfaces including Dialog RF network (319.5 MHz) and RS485 Superbus 2000 wired interface; RF mesh network (908 MHz); and interfaces including RF network (345 MHz) and RS485/RS232bus wired interfaces.

[0055] Regarding security for the IP communications (e.g., authentication, authorization, encryption, anti-spoofing, etc), the integrated security system uses SSL to encrypt all IP traffic, using server and client-certificates for authentication, as well as authentication in the data sent over the SSL-encrypted channel. For encryption, integrated security system

issues public/private key pairs at the time/place of manufacture, and certificates are not stored in any online storage in an embodiment.

[0056] The integrated security system does not need any special rules at the customer premise and/or at the security system provider central station because the integrated security system makes outgoing connections using Transmission Control Protocol (TCP) over the standard Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) ports. Provided outbound TCP connections are allowed then no special requirements on the firewalls are necessary.

[0057] FIG. 1 is a block diagram of the integrated security system 100, under an embodiment. The integrated security system 100 of an embodiment includes the gateway 102 and the security servers 104 coupled to the conventional home security system 110. At a customer's home or business, the gateway 102 connects and manages the diverse variety of home security and self-monitoring devices. The gateway 102 communicates with the iConnect Servers 104 located in the service provider's data center 106 (or hosted in integrated security system data center), with the communication taking place via a communication network 108 or other network (e.g., cellular network, internet, etc.). These servers 104 manage the system integrations necessary to deliver the integrated system service described herein. The combination of the gateway 102 and the iConnect servers 104 enable a wide variety of remote client devices 120 (e.g., PCs, mobile phones and PDAs) allowing users to remotely stay in touch with their home, business and family. In addition, the technology allows home security and self-monitoring information, as well as relevant third party content such as traffic and weather, to be presented in intuitive ways within the home, such as on advanced touchscreen keypads.

[0058] The integrated security system service (also referred to as iControl service) can be managed by a service provider via browser-based Maintenance and Service Management applications that are provided with the iConnect Servers. Or, if desired, the service can be more tightly integrated with existing OSS/BSS and service delivery systems via the iConnect web services-based XML APIs.

[0059] The integrated security system service can also coordinate the sending of alarms to the home security Central Monitoring Station (CMS) 199. Alarms are passed to the CMS 199 using standard protocols such as Contact ID or SIA and can be generated from the home security panel location as well as by iConnect server 104 conditions (such as lack of communications with the integrated security system). In addition, the link between the security servers 104 and CMS 199 provides tighter integration between home security and self-monitoring devices and the gateway 102. Such integration enables advanced security capabilities such as the ability for CMS personnel to view photos taken at the time a burglary alarm was triggered. For maximum security, the gateway 102 and iConnect servers 104 support the use of a mobile network (both GPRS and CDMA options are available) as a backup to the primary broadband connection.

[0060] The integrated security system service is delivered by hosted servers running software components that communicate with a variety of client types while interacting with other systems. FIG. 2 is a block diagram of components of the integrated security system 100, under an embodiment. Following is a more detailed description of the components.

[0061] The iConnect servers 104 support a diverse collection of clients 120 ranging from mobile devices, to PCs, to in-home security devices, to a service provider's internal systems. Most clients 120 are used by end-users, but there are also a number of clients 120 that are used to operate the service.

[0062] Clients 120 used by end-users of the integrated security system 100 include, but are not limited to, the following:

[0063] Clients based on gateway client applications 202 (e.g., a processor-based device running the gateway technology that manages home security and automation devices).

[0064] A web browser 204 accessing a Web Portal application, performing end-user configuration and customization of the integrated security system service as well as monitoring of in-home device status, viewing photos and video, etc. Device and user management can also be performed by this portal application.

[0065] A mobile device 206 (e.g., PDA, mobile phone, etc.) accessing the integrated security system Mobile Portal. This type of client 206 is used by end-users to view system status and perform operations on devices (e.g., turning on a lamp, arming a security panel, etc.) rather than for system configuration tasks such as adding a new device or user.

[0066] PC or browser-based "widget" containers 208 that present integrated security system service content, as well as other third-party content, in simple, targeted ways (e.g. a widget that resides on a PC desktop and shows live video from a single in-home camera). "Widget" as used herein means applications or programs in the system.

[0067] Touchscreen home security keypads 208 and advanced in-home devices that present a variety of content widgets via an intuitive touchscreen user interface.

[0068] Notification recipients 210 (e.g., cell phones that receive SMS-based notifications when certain events occur (or don't occur), email clients that receive an email message with similar information, etc.).

[0069] Custom-built clients (not shown) that access the iConnect web services XML API to interact with users' home security and self-monitoring information in new and unique ways. Such clients could include new types of mobile devices, or complex applications where integrated security system content is integrated into a broader set of application features.

[0070] In addition to the end-user clients, the iConnect servers 104 support PC browser-based Service Management clients that manage the ongoing operation of the overall service. These clients run applications that handle tasks such as provisioning, service monitoring, customer support and reporting.

[0071] There are numerous types of server components of the iConnect servers 104 of an embodiment including, but not limited to, the following: Business Components which manage information about all of the home security and self-monitoring devices; End-User Application Components which display that information for users and access the Business Components via published XML APIs; and Service Management Application Components which enable operators to administer the service (these components also access the Business Components via the XML APIs, and also via published SNMP MIBs).

[0072] The server components provide access to, and management of, the objects associated with an integrated security system installation. The top-level object is the “network.” It is a location where a gateway **102** is located, and is also commonly referred to as a site or premises; the premises can include any type of structure (e.g., home, office, warehouse, etc.) at which an gateway **102** is located. Users can only access the networks to which they have been granted permission. Within a network, every object monitored by the gateway **102** is called a device. Devices include the sensors, cameras, home security panels and automation devices, as well as the controller or processor-based device running the gateway applications.

[0073] Various types of interactions are possible between the objects in a system. Automations define actions that occur as a result of a change in state of a device. For example, take a picture with the front entry camera when the front door sensor changes to “open”. Notifications are messages sent to users to indicate that something has occurred, such as the front door going to “open” state, or has not occurred (referred to as an iWatch notification). Schedules define changes in device states that are to take place at predefined days and times. For example, set the security panel to “Armed” mode every weeknight at 11:00 pm.

[0074] The iConnect Business Components are responsible for orchestrating all of the low-level service management activities for the integrated security system service. They define all of the users and devices associated with a network (site), analyze how the devices interact, and trigger associated actions (such as sending notifications to users). All changes in device states are monitored and logged. The Business Components also manage all interactions with external systems as required, including sending alarms and other related self-monitoring data to the home security Central Monitoring System (CMS) **199**. The Business Components are implemented as portable Java J2EE Servlets, but are not so limited.

[0075] The following iConnect Business Components manage the main elements of the integrated security system service, but the embodiment is not so limited:

[0076] A Registry Manager **220** defines and manages users and networks. This component is responsible for the creation, modification and termination of users and networks. It is also where a user’s access to networks is defined.

[0077] A Network Manager **222** defines and manages security and self-monitoring devices that are deployed on a network (site). This component handles the creation, modification, deletion and configuration of the devices, as well as the creation of automations, schedules and notification rules associated with those devices.

[0078] A Data Manager **224** manages access to current and logged state data for an existing network and its devices. This component specifically does not provide any access to network management capabilities, such as adding new devices to a network, which are handled exclusively by the Network Manager **222**.

[0079] To achieve optimal performance for all types of queries, data for current device states is stored separately from historical state data (a.k.a. “logs”) in the database. A Log Data Manager **226** performs ongoing transfers of current device state data to the historical data log tables.

[0080] Additional iConnect Business Components handle direct communications with certain clients and other systems, for example:

[0081] An iHub Manager **228** directly manages all communications with gateway clients, including receiving information about device state changes, changing the configuration of devices, and pushing new versions of the gateway client to the hardware it is running on.

[0082] A Notification Manager **230** is responsible for sending all notifications to clients via SMS (mobile phone messages), email (via a relay server like an SMTP email server), etc.

[0083] An Alarm and CMS Manager **232** sends critical server-generated alarm events to the home security Central Monitoring Station (CMS) and manages all other communications of integrated security system service data to and from the CMS.

[0084] The Element Management System (EMS) **234** is an iControl Business Component that manages all activities associated with service installation, scaling and monitoring, and filters and packages service operations data for use by service management applications. The SNMP MIBs published by the EMS can also be incorporated into any third party monitoring system if desired.

[0085] The iConnect Business Components store information about the objects that they manage in the iControl Service Database **240** and in the iControl Content Store **242**. The iControl Content Store is used to store media objects like video, photos and widget content, while the Service Database stores information about users, networks, and devices. Database interaction is performed via a JDBC interface. For security purposes, the Business Components manage all data storage and retrieval.

[0086] The iControl Business Components provide web services-based APIs that application components use to access the Business Components’ capabilities. Functions of application components include presenting integrated security system service data to end-users, performing administrative duties, and integrating with external systems and back-office applications.

[0087] The primary published APIs for the iConnect Business Components include, but are not limited to, the following:

[0088] A Registry Manager API **252** provides access to the Registry Manager Business Component’s functionality, allowing management of networks and users.

[0089] A Network Manager API **254** provides access to the Network Manager Business Component’s functionality, allowing management of devices on a network.

[0090] A Data Manager API **256** provides access to the Data Manager Business Component’s functionality, such as setting and retrieving (current and historical) data about device states.

[0091] A Provisioning API **258** provides a simple way to create new networks and configure initial default properties.

[0092] Each API of an embodiment includes two modes of access: Java API or XML API. The XML APIs are published as web services so that they can be easily accessed by applications or servers over a network. The Java APIs are a programmer-friendly wrapper for the XML APIs. Application components and integrations written in Java should generally use the Java APIs rather than the XML APIs directly.

[0093] The iConnect Business Components also have an XML-based interface **260** for quickly adding support for new devices to the integrated security system. This interface **260**, referred to as DeviceConnect **260**, is a flexible, standards-based mechanism for defining the properties of new devices and how they can be managed. Although the format is flexible enough to allow the addition of any type of future device, pre-defined XML profiles are currently available for adding common types of devices such as sensors (SensorConnect), home security panels (PanelConnect) and IP cameras (CameraConnect).

[0094] The iConnect End-User Application Components deliver the user interfaces that run on the different types of clients supported by the integrated security system service. The components are written in portable Java J2EE technology (e.g., as Java Servlets, as JavaServer Pages (JSPs), etc.) and they all interact with the iControl Business Components via the published APIs.

[0095] The following End-User Application Components generate CSS-based HTML/JavaScript that is displayed on the target client. These applications can be dynamically branded with partner-specific logos and URL links (such as Customer Support, etc.). The End-User Application Components of an embodiment include, but are not limited to, the following:

[0096] An iControl Activation Application **270** that delivers the first application that a user sees when they set up the integrated security system service. This wizard-based web browser application securely associates a new user with a purchased gateway and the other devices included with it as a kit (if any). It primarily uses functionality published by the Provisioning API.

[0097] An iControl Web Portal Application **272** runs on PC browsers and delivers the web-based interface to the integrated security system service. This application allows users to manage their networks (e.g. add devices and create automations) as well as to view/change device states, and manage pictures and videos. Because of the wide scope of capabilities of this application, it uses three different Business Component APIs that include the Registry Manager API, Network Manager API, and Data Manager API, but the embodiment is not so limited.

[0098] An iControl Mobile Portal **274** is a small-footprint web-based interface that runs on mobile phones and PDAs. This interface is optimized for remote viewing of device states and pictures/videos rather than network management. As such, its interaction with the Business Components is primarily via the Data Manager API.

[0099] Custom portals and targeted client applications can be provided that leverage the same Business Component APIs used by the above applications.

[0100] A Content Manager Application Component **276** delivers content to a variety of clients. It sends multimedia-rich user interface components to widget container clients (both PC and browser-based), as well as to advanced touchscreen keypad clients. In addition to providing content directly to end-user devices, the Content Manager **276** provides widget-based user interface components to satisfy requests from other Application Components such as the iControl Web **272** and Mobile **274** portals.

[0101] A number of Application Components are responsible for overall management of the service. These pre-defined applications, referred to as Service Management Application Components, are configured to offer off-the-shelf solutions for production management of the integrated security system service including provisioning, overall service monitoring, customer support, and reporting, for example. The Service Management Application Components of an embodiment include, but are not limited to, the following:

[0102] A Service Management Application **280** allows service administrators to perform activities associated with service installation, scaling and monitoring/alerting. This application interacts heavily with the Element Management System (EMS) Business Component to execute its functionality, and also retrieves its monitoring data from that component via protocols such as SNMP MIBs.

[0103] A Kitting Application **282** is used by employees performing service provisioning tasks. This application allows home security and self-monitoring devices to be associated with gateways during the warehouse kitting process.

[0104] A CSR Application and Report Generator **284** is used by personnel supporting the integrated security system service, such as CSRs resolving end-user issues and employees enquiring about overall service usage. Pushes of new gateway firmware to deployed gateways is also managed by this application.

[0105] The iConnect servers **104** also support custom-built integrations with a service provider's existing OSS/BSS, CSR and service delivery systems **290**. Such systems can access the iConnect web services XML API to transfer data to and from the iConnect servers **104**. These types of integrations can compliment or replace the PC browser-based Service Management applications, depending on service provider needs.

[0106] As described above, the integrated security system of an embodiment includes a gateway, or iHub. The gateway of an embodiment includes a device that is deployed in the home or business and couples or connects the various third-party cameras, home security panels, sensors and devices to the iConnect server over a WAN connection as described in detail herein. The gateway couples to the home network and communicates directly with the home security panel in both wired and wireless sensor installations. The gateway is configured to be low-cost, reliable and thin so that it complements the integrated security system network-based architecture.

[0107] The gateway supports various wireless protocols and can interconnect with a wide range of home security control panels. Service providers and users can then extend the system's capabilities by adding IP cameras, lighting modules and additional security devices. The gateway is configurable to be integrated into many consumer appliances, including set-top boxes, routers and security panels. The small and efficient footprint of the gateway enables this portability and versatility, thereby simplifying and reducing the overall cost of the deployment.

[0108] FIG. 3 is a block diagram of the gateway **102** including gateway software or applications, under an embodiment. The gateway software architecture is relatively thin and efficient, thereby simplifying its integration into other consumer appliances such as set-top boxes, routers, touch screens and security panels. The software architecture also provides a

high degree of security against unauthorized access. This section describes the various key components of the gateway software architecture.

[0109] The gateway application layer **302** is the main program that orchestrates the operations performed by the gateway. The Security Engine **304** provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine **304** of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

- [0110] Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.
- [0111] Bi-directional authentication between the gateway and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.
- [0112] Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The gateway provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.
- [0113] 802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.
- [0114] An gateway-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying gateway-enabled devices have the knowledge that only an gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

[0115] As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

[0116] A Remote Firmware Download module **306** allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server **104**, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Gateway firmware can be remotely download either for one gateway at a time, a group of gateways, or in batches.

[0117] The Automations engine **308** manages the user-defined rules of interaction between the different devices (e.g., when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

[0118] DeviceConnect **310** includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module **310** offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect **312** is provided for adding new sensors, CameraConnect **316** for adding IP cameras, and PanelConnect **314** for adding home security panels.

[0119] The Schedules engine **318** is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application. The Schedules Engine **318** then interfaces with SensorConnect **312** to ensure that scheduled events occur at precisely the desired time.

[0120] The Device Management module **320** is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters—to simplify the user experience and reduce the customer support burden, the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

[0121] The video routing engine **322** is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

[0122] FIG. 4 is a block diagram of components of the gateway **102**, under an embodiment. Depending on the specific set of functionality desired by the service provider deploying the integrated security system service, the gateway **102** can use any of a number of processors **402**, due to the small footprint of the gateway application firmware. In an embodiment, the gateway could include the Broadcom BCM5354 as the processor for example. In addition, the gateway **102** includes memory (e.g., FLASH **404**, RAM **406**, etc.) and any number of input/output (I/O) ports **408**.

[0123] Referring to the WAN portion **410** of the gateway **102**, the gateway **102** of an embodiment can communicate with the iConnect server using a number of communication types and/or protocols, for example Broadband **412**, GPRS **414** and/or Public Switched Telephone Network (PSTN) **416** to name a few. In general, broadband communication **412** is the primary means of connection between the gateway **102** and the iConnect server **104** and the GPRS/CDMA **414** and/or PSTN **416** interfaces acts as back-up for fault tolerance in case the user's broadband connection fails for whatever reason, but the embodiment is not so limited.

[0124] Referring to the LAN portion **420** of the gateway **102**, various protocols and physical transceivers can be used to communicate to off-the-shelf sensors and cameras. The

gateway **102** is protocol-agnostic and technology-agnostic and as such can easily support almost any device networking protocol. The gateway **102** can, for example, support GE and Honeywell security RF protocols **422**, Z-Wave **424**, serial (RS232 and RS485) **426** for direct connection to security panels as well as WiFi **428** (802.11b/g) for communication to WiFi cameras.

[0125] The integrated security system includes couplings or connections among a variety of IP devices or components, and the device management module is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system of an embodiment uses a “sandbox” network to discover and manage all IP devices coupled or connected as components of the system. The IP devices of an embodiment include wired devices, wireless devices, cameras, interactive touchscreens, and security panels to name a few. These devices can be wired via ethernet cable or Wifi devices, all of which are secured within the sandbox network, as described below. The “sandbox” network is described in detail below.

[0126] FIG. **5** is a block diagram **500** of network or premise device integration with a premise network **250**, under an embodiment. In an embodiment, network devices **255-257** are coupled to the gateway **102** using a secure network coupling or connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption). The network coupling or connection between the gateway **102** and the network devices **255-257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled to the premise router/firewall **252** via a coupling with a premise LAN **250**. The premise router/firewall **252** is coupled to a broadband modem **251**, and the broadband modem **251** is coupled to a WAN **200** or other network outside the premise. The gateway **102** thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN **250** of the host premises. The gateway sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

[0127] FIG. **6** is a block diagram **600** of network or premise device integration with a premise network **250**, under an alternative embodiment. The network or premise devices **255-257** are coupled to the gateway **102**. The network coupling or connection between the gateway **102** and the network devices **255-257** is a private coupling or connection in that it is segregated from any other network couplings or connections. The gateway **102** is coupled or connected between the premise router/firewall **252** and the broadband modem **251**. The broadband modem **251** is coupled to a WAN **200** or other network outside the premise, while the premise router/firewall **252** is coupled to a premise LAN **250**. As a result of its location between the broadband modem **251** and the premise router/firewall **252**, the gateway **102** can be configured or function as the premise router routing specified data between the outside network (e.g., WAN **200**) and the premise router/firewall **252** of the LAN **250**. As described above, the gateway

102 in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices **255-257** and is coupled or connected between the LAN **250** of the host premises and the WAN **200**. The gateway sub-network can include, but is not limited to, any number of network or premise devices **255-257** like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The gateway **102** manages or controls the sub-network separately from the LAN **250** and transfers data and information between components of the sub-network and the LAN **250**/WAN **200**, but is not so limited. Additionally, other network devices **254** can be coupled to the LAN **250** without being coupled to the gateway **102**.

[0128] The examples described above with reference to FIGS. **5** and **6** are presented only as examples of IP device integration. The integrated security system is not limited to the type, number and/or combination of IP devices shown and described in these examples, and any type, number and/or combination of IP devices is contemplated within the scope of this disclosure as capable of being integrated with the premise network.

[0129] The integrated security system of an embodiment includes a touchscreen (also referred to as the iControl touchscreen or integrated security system touchscreen), as described above, which provides core security keypad functionality, content management and presentation, and embedded systems design. The networked security touchscreen system of an embodiment enables a consumer or security provider to easily and automatically install, configure and manage the security system and touchscreen located at a customer premise. Using this system the customer may access and control the local security system, local IP devices such as cameras, local sensors and control devices (such as lighting controls or pipe freeze sensors), as well as the local security system panel and associated security sensors (such as door/window, motion, and smoke detectors). The customer premise may be a home, business, and/or other location equipped with a wired or wireless broadband IP connection.

[0130] The system of an embodiment includes a touchscreen with a configurable software user interface and/or a gateway device (e.g., iHub) that couples or connects to a premise security panel through a wired or wireless connection, and a remote server that provides access to content and information from the premises devices to a user when they are remote from the home. The touchscreen supports broadband and/or WAN wireless connectivity. In this embodiment, the touchscreen incorporates an IP broadband connection (e.g., Wifi radio, Ethernet port, etc.), and/or a cellular radio (e.g., GPRS/GSM, CDMA, WiMax, etc.). The touchscreen described herein can be used as one or more of a security system interface panel and a network user interface (UI) that provides an interface to interact with a network (e.g., LAN, WAN, internet, etc.).

[0131] The touchscreen of an embodiment provides an integrated touchscreen and security panel as an all-in-one device. Once integrated using the touchscreen, the touchscreen and a security panel of a premise security system become physically co-located in one device, and the functionality of both may even be co-resident on the same CPU and memory (though this is not required).

[0132] The touchscreen of an embodiment also provides an integrated IP video and touchscreen UI. As such, the touchscreen supports one or more standard video CODECs/players (e.g., H.264, Flash Video, MOV, MPEG4, MJPEG, etc.). The

touchscreen UI then provides a mechanism (such as a camera or video widget) to play video. In an embodiment the video is streamed live from an IP video camera. In other embodiments the video comprises video clips or photos sent from an IP camera or from a remote location.

[0133] The touchscreen of an embodiment provides a configurable user interface system that includes a configuration supporting use as a security touchscreen. In this embodiment, the touchscreen utilizes a modular user interface that allows components to be modified easily by a service provider, an installer, or even the end user. Examples of such a modular approach include using Flash widgets, HTML-based widgets, or other downloadable code modules such that the user interface of the touchscreen can be updated and modified while the application is running. In an embodiment the touchscreen user interface modules can be downloaded over the internet. For example, a new security configuration widget can be downloaded from a standard web server, and the touchscreen then loads such configuration app into memory, and inserts it in place of the old security configuration widget. The touchscreen of an embodiment is configured to provide a self-install user interface.

[0134] Embodiments of the networked security touchscreen system described herein include a touchscreen device with a user interface that includes a security toolbar providing one or more functions including arm, disarm, panic, medic, and alert. The touchscreen therefore includes at least one screen having a separate region of the screen dedicated to a security toolbar. The security toolbar of an embodiment is present in the dedicated region at all times that the screen is active.

[0135] The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing home-based functions. The home-based functions of an embodiment include managing, viewing, and/or controlling IP video cameras. In this embodiment, regions of the home screen are allocated in the form of widget icons; these widget icons (e.g. for cameras, thermostats, lighting, etc) provide functionality for managing home systems. So, for example, a displayed camera icon, when selected, launches a Camera Widget, and the Camera widget in turn provides access to video from one or more cameras, as well as providing the user with relevant camera controls (take a picture, focus the camera, etc.)

[0136] The touchscreen of an embodiment includes a home screen having a separate region of the screen allocated to managing, viewing, and/or controlling internet-based content or applications. For example, the Widget Manager UI presents a region of the home screen (up to and including the entire home screen) where internet widgets icons such as weather, sports, etc. may be accessed). Each of these icons may be selected to launch their respective content services.

[0137] The touchscreen of an embodiment is integrated into a premise network using the gateway, as described above. The gateway as described herein functions to enable a separate wireless network, or sub-network, that is coupled, connected, or integrated with another network (e.g., WAN, LAN of the host premises, etc.). The sub-network enabled by the gateway optimizes the installation process for IP devices, like the touchscreen, that couple or connect to the sub-network by segregating these IP devices from other such devices on the network. This segregation of the IP devices of the sub-network further enables separate security and privacy policies to be implemented for these IP devices so that, where the IP

devices are dedicated to specific functions (e.g., security), the security and privacy policies can be tailored specifically for the specific functions. Furthermore, the gateway and the sub-network it forms enables the segregation of data traffic, resulting in faster and more efficient data flow between components of the host network, components of the sub-network, and between components of the sub-network and components of the network.

[0138] The touchscreen of an embodiment includes a core functional embedded system that includes an embedded operating system, required hardware drivers, and an open system interface to name a few. The core functional embedded system can be provided by or as a component of a conventional security system (e.g., security system available from GE Security). These core functional units are used with components of the integrated security system as described herein. Note that portions of the touchscreen description below may include reference to a host premise security system (e.g., GE security system), but these references are included only as an example and do not limit the touchscreen to integration with any particular security system.

[0139] As an example, regarding the core functional embedded system, a reduced memory footprint version of embedded Linux forms the core operating system in an embodiment, and provides basic TCP/IP stack and memory management functions, along with a basic set of low-level graphics primitives. A set of device drivers is also provided or included that offer low-level hardware and network interfaces. In addition to the standard drivers, an interface to the RS 485 bus is included that couples or connects to the security system panel (e.g., GE Concord panel). The interface may, for example, implement the Superbus 2000 protocol, which can then be utilized by the more comprehensive transaction-level security functions implemented in PanelConnect technology (e.g. SetAlarmLevel (int level, int partition, char *access-Code)). Power control drivers are also provided.

[0140] FIG. 7 is a block diagram of a touchscreen 700 of the integrated security system, under an embodiment. The touchscreen 700 generally includes an application/presentation layer 702 with a resident application 704, and a core engine 706. The touchscreen 700 also includes one or more of the following, but is not so limited: applications of premium services 710, widgets 712, a caching proxy 714, network security 716, network interface 718, security object 720, applications supporting devices 722, PanelConnect API 724, a gateway interface 726, and one or more ports 728.

[0141] More specifically, the touchscreen, when configured as a home security device, includes but is not limited to the following application or software modules: RS 485 and/or RS-232 bus security protocols to conventional home security system panel (e.g., GE Concord panel); functional home security classes and interfaces (e.g. Panel ARM state, Sensor status, etc.); Application/Presentation layer or engine; Resident Application; Consumer Home Security Application; installer home security application; core engine; and System bootloader/Software Updater. The core Application engine and system bootloader can also be used to support other advanced content and applications. This provides a seamless interaction between the premise security application and other optional services such as weather widgets or IP cameras.

[0142] An alternative configuration of the touchscreen includes a first Application engine for premise security and a second Application engine for all other applications. The

integrated security system application engine supports content standards such as HTML, XML, Flash, etc. and enables a rich consumer experience for all 'widgets', whether security-based or not. The touchscreen thus provides service providers the ability to use web content creation and management tools to build and download any 'widgets' regardless of their functionality.

[0143] As discussed above, although the Security Applications have specific low-level functional requirements in order to interface with the premise security system, these applications make use of the same fundamental application facilities as any other 'widget', application facilities that include graphical layout, interactivity, application handoff, screen management, and network interfaces, to name a few.

[0144] Content management in the touchscreen provides the ability to leverage conventional web development tools, performance optimized for an embedded system, service provider control of accessible content, content reliability in a consumer device, and consistency between 'widgets' and seamless widget operational environment. In an embodiment of the integrated security system, widgets are created by web developers and hosted on the integrated security system Content Manager (and stored in the Content Store database). In this embodiment the server component caches the widgets and offers them to consumers through the web-based integrated security system provisioning system. The servers interact with the advanced touchscreen using HTTPS interfaces controlled by the core engine and dynamically download widgets and updates as needed to be cached on the touchscreen. In other embodiments widgets can be accessed directly over a network such as the Internet without needing to go through the iControl Content Manager.

[0145] Referring to FIG. 7, the touchscreen system is built on a tiered architecture, with defined interfaces between the Application/Presentation Layer (the Application Engine) on the top, the Core Engine in the middle, and the security panel and gateway APIs at the lower level. The architecture is configured to provide maximum flexibility and ease of maintenance.

[0146] The application engine of the touchscreen provides the presentation and interactivity capabilities for all applications (widgets) that run on the touchscreen, including both core security function widgets and third party content widgets. FIG. 8 is an example screenshot 800 of a networked security touchscreen, under an embodiment. This example screenshot 800 includes three interfaces or user interface (UI) components 802-806, but is not so limited. A first UI 802 of the touchscreen includes icons by which a user controls or accesses functions and/or components of the security system (e.g., "Main", "Panic", "Medic", "Fire", state of the premise alarm system (e.g., disarmed, armed, etc.), etc.); the first UI 802, which is also referred to herein as a security interface, is always presented on the touchscreen. A second UI 804 of the touchscreen includes icons by which a user selects or interacts with services and other network content (e.g., clock, calendar, weather, stocks, news, sports, photos, maps, music, etc.) that is accessible via the touchscreen. The second UI 804 is also referred to herein as a network interface or content interface. A third UI 806 of the touchscreen includes icons by which a user selects or interacts with additional services or components (e.g., intercom control, security, cameras coupled to the system in particular regions (e.g., front door, baby, etc.) available via the touchscreen.

[0147] A component of the application engine is the Presentation Engine, which includes a set of libraries that implement the standards-based widget content (e.g., XML, HTML, JavaScript, Flash) layout and interactivity. This engine provides the widget with interfaces to dynamically load both graphics and application logic from third parties, support high level data description language as well as standard graphic formats. The set of web content-based functionality available to a widget developer is extended by specific touchscreen functions implemented as local web services by the Core Engine.

[0148] The resident application of the touchscreen is the master service that controls the interaction of all widgets in the system, and enforces the business and security rules required by the service provider. For example, the resident application determines the priority of widgets, thereby enabling a home security widget to override resource requests from a less critical widget (e.g. a weather widget). The resident application also monitors widget behavior, and responds to client or server requests for cache updates.

[0149] The core engine of the touchscreen manages interaction with other components of the integrated security system, and provides an interface through which the resident application and authorized widgets can get information about the home security system, set alarms, install sensors, etc. At the lower level, the Core Engine's main interactions are through the PanelConnect API, which handles all communication with the security panel, and the gateway Interface, which handles communication with the gateway. In an embodiment, both the iHub Interface and PanelConnect API are resident and operating on the touchscreen. In another embodiment, the PanelConnect API runs on the gateway or other device that provides security system interaction and is accessed by the touchscreen through a web services interface.

[0150] The Core Engine also handles application and service level persistent and cached memory functions, as well as the dynamic provisioning of content and widgets, including but not limited to: flash memory management, local widget and content caching, widget version management (download, cache flush new/old content versions), as well as the caching and synchronization of user preferences. As a portion of these services the Core engine incorporates the bootloader functionality that is responsible for maintaining a consistent software image on the touchscreen, and acts as the client agent for all software updates. The bootloader is configured to ensure full update redundancy so that unsuccessful downloads cannot corrupt the integrated security system.

[0151] Video management is provided as a set of web services by the Core Engine. Video management includes the retrieval and playback of local video feeds as well as remote control and management of cameras (all through iControl CameraConnect technology).

[0152] Both the high level application layer and the mid-level core engine of the touchscreen can make calls to the network. Any call to the network made by the application layer is automatically handed off to a local caching proxy, which determines whether the request should be handled locally. Many of the requests from the application layer are web services API requests; although such requests could be satisfied by the iControl servers, they are handled directly by the touchscreen and the gateway. Requests that get through the caching proxy are checked against a white list of acceptable sites, and, if they match, are sent off through the network interface to the gateway. Included in the Network Subsystem is a set of network services including HTTP, HTTPS, and server-level authentication functions to manage the secure client-server interface. Storage and management of certificates is incorporated as a part of the network services layer.

[0153] Server components of the integrated security system servers support interactive content services on the touchscreen. These server components include, but are not limited to the content manager, registry manager, network manager, and global registry, each of which is described herein.

[0154] The Content Manager oversees aspects of handling widget data and raw content on the touchscreen. Once created and validated by the service provider, widgets are 'ingested' to the Content Manager, and then become available as downloadable services through the integrated security system Content Management APIs. The Content manager maintains versions and timestamp information, and connects to the raw data contained in the backend Content Store database. When a widget is updated (or new content becomes available) all clients registering interest in a widget are systematically updated as needed (a process that can be configured at an account, locale, or system-wide level).

[0155] The Registry Manager handles user data, and provisioning accounts, including information about widgets the user has decided to install, and the user preferences for these widgets.

[0156] The Network Manager handles getting and setting state for all devices on the integrated security system network (e.g., sensors, panels, cameras, etc.). The Network manager synchronizes with the gateway, the advanced touchscreen, and the subscriber database.

[0157] The Global Registry is a primary starting point server for all client services, and is a logical referral service that abstracts specific server locations/addresses from clients (touchscreen, gateway 102, desktop widgets, etc.). This approach enables easy scaling/migration of server farms.

[0158] The touchscreen of an embodiment operates wirelessly with a premise security system. The touchscreen of an embodiment incorporates an RF transceiver component that either communicates directly with the sensors and/or security panel over the panel's proprietary RF frequency, or the touchscreen communicates wirelessly to the gateway over 802.11, Ethernet, or other IP-based communications channel, as described in detail herein. In the latter case the gateway implements the PanelConnect interface and communicates directly to the security panel and/or sensors over wireless or wired networks as described in detail above.

[0159] The touchscreen of an embodiment is configured to operate with multiple security systems through the use of an abstracted security system interface. In this embodiment, the PanelConnect API can be configured to support a plurality of proprietary security system interfaces, either simultaneously or individually as described herein. In one embodiment of this approach, the touchscreen incorporates multiple physical interfaces to security panels (e.g. GE Security RS-485, Honeywell RF, etc.) in addition to the PanelConnect API implemented to support multiple security interfaces. The change needed to support this in PanelConnect is a configuration parameter specifying the panel type connection that is being utilized.

[0160] So for example, the setARMState() function is called with an additional parameter (e.g., Armstate=setARMState(type="ARM STAY|ARM AWAY|DISARM", Parameters="ExitDelay=30|Lights=OFF", panelType="GE Concord4 RS485"). The 'panelType' parameter is used by the setARMState function (and in practice by all of the PanelConnect functions) to select an algorithm appropriate to the specific panel out of a plurality of algorithms.

[0161] The touchscreen of an embodiment is self-installable. Consequently, the touchscreen provides a 'wizard' approach similar to that used in traditional computer installations (e.g. InstallShield). The wizard can be resident on the touchscreen, accessible through a web interface, or both. In one embodiment of a touchscreen self-installation process, the service provider can associate devices (sensors, touchscreens, security panels, lighting controls, etc.) remotely using a web-based administrator interface.

[0162] The touchscreen of an embodiment includes a battery backup system for a security touchscreen. The touchscreen incorporates a standard Li-ion or other battery and charging circuitry to allow continued operation in the event of a power outage. In an embodiment the battery is physically located and connected within the touchscreen enclosure. In another embodiment the battery is located as a part of the power transformer, or in between the power transformer and the touchscreen.

[0163] The example configurations of the integrated security system described above with reference to FIGS. 5 and 6 include a gateway that is a separate device, and the touchscreen couples to the gateway. However, in an alternative embodiment, the gateway device and its functionality can be incorporated into the touchscreen so that the device management module, which is now a component of or included in the touchscreen, is in charge of the discovery, installation and configuration of the IP devices coupled or connected to the system, as described above. The integrated security system with the integrated touchscreen/gateway uses the same "sandbox" network to discover and manage all IP devices coupled or connected as components of the system.

[0164] The touchscreen of this alternative embodiment integrates the components of the gateway with the components of the touchscreen as described herein. More specifically, the touchscreen of this alternative embodiment includes software or applications described above with reference to FIG. 3. In this alternative embodiment, the touchscreen includes the gateway application layer 302 as the main program that orchestrates the operations performed by the gateway. A Security Engine 304 of the touchscreen provides robust protection against intentional and unintentional intrusion into the integrated security system network from the outside world (both from inside the premises as well as from the WAN). The Security Engine 304 of an embodiment comprises one or more sub-modules or components that perform functions including, but not limited to, the following:

[0165] Encryption including 128-bit SSL encryption for gateway and iConnect server communication to protect user data privacy and provide secure communication.

[0166] Bi-directional authentication between the touchscreen and iConnect server in order to prevent unauthorized spoofing and attacks. Data sent from the iConnect server to the gateway application (or vice versa) is digitally signed as an additional layer of security. Digital signing provides both authentication and validation that the data has not been altered in transit.

[0167] Camera SSL encapsulation because picture and video traffic offered by off-the-shelf networked IP cameras is not secure when traveling over the Internet. The touchscreen provides for 128-bit SSL encapsulation of the user picture and video data sent over the internet for complete user security and privacy.

[0168] 802.11b/g/n with WPA-2 security to ensure that wireless camera communications always takes place using the strongest available protection.

[0169] A touchscreen-enabled device is assigned a unique activation key for activation with an iConnect server. This ensures that only valid gateway-enabled devices can be activated for use with the specific instance of iConnect server in use. Attempts to activate gateway-enabled devices by brute force are detected by the Security Engine. Partners deploying touchscreen-enabled devices have the knowledge that only a gateway with the correct serial number and activation key can be activated for use with an iConnect server. Stolen devices, devices attempting to masquerade as gateway-enabled devices, and malicious outsiders (or insiders as knowledgeable but nefarious customers) cannot effect other customers' gateway-enabled devices.

[0170] As standards evolve, and new encryption and authentication methods are proven to be useful, and older mechanisms proven to be breakable, the security manager can be upgraded "over the air" to provide new and better security for communications between the iConnect server and the gateway application, and locally at the premises to remove any risk of eavesdropping on camera communications.

[0171] A Remote Firmware Download module 306 of the touchscreen allows for seamless and secure updates to the gateway firmware through the iControl Maintenance Application on the server 104, providing a transparent, hassle-free mechanism for the service provider to deploy new features and bug fixes to the installed user base. The firmware download mechanism is tolerant of connection loss, power interruption and user interventions (both intentional and unintentional). Such robustness reduces down time and customer support issues. Touchscreen firmware can be remotely download either for one touchscreen at a time, a group of touchscreen, or in batches.

[0172] The Automations engine 308 of the touchscreen manages the user-defined rules of interaction between the different devices (e.g. when door opens turn on the light). Though the automation rules are programmed and reside at the portal/server level, they are cached at the gateway level in order to provide short latency between device triggers and actions.

[0173] DeviceConnect 310 of the touchscreen includes definitions of all supported devices (e.g., cameras, security panels, sensors, etc.) using a standardized plug-in architecture. The DeviceConnect module 310 offers an interface that can be used to quickly add support for any new device as well as enabling interoperability between devices that use different technologies/protocols. For common device types, pre-defined sub-modules have been defined, making supporting new devices of these types even easier. SensorConnect 312 is provided for adding new sensors, CameraConnect 316 for adding IP cameras, and PanelConnect 314 for adding home security panels.

[0174] The Schedules engine 318 of the touchscreen is responsible for executing the user defined schedules (e.g., take a picture every five minutes; every day at 8 am set temperature to 65 degrees Fahrenheit, etc.). Though the schedules are programmed and reside at the iConnect server level they are sent to the scheduler within the gateway application of the touchscreen. The Schedules Engine 318 then interfaces with SensorConnect 312 to ensure that scheduled events occur at precisely the desired time.

[0175] The Device Management module 320 of the touchscreen is in charge of all discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras,

etc.) coupled or connected to the system. Networked IP devices, such as those used in the integrated security system, require user configuration of many IP and security parameters, and the device management module of an embodiment handles the details of this configuration. The device management module also manages the video routing module described below.

[0176] The video routing engine 322 of the touchscreen is responsible for delivering seamless video streams to the user with zero-configuration. Through a multi-step, staged approach the video routing engine uses a combination of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing.

[0177] FIG. 9 is a block diagram 900 of network or premise device integration with a premise network 250, under an embodiment. In an embodiment, network devices 255, 256, 957 are coupled to the touchscreen 902 using a secure network connection such as SSL over an encrypted 802.11 link (utilizing for example WPA-2 security for the wireless encryption), and the touchscreen 902 coupled to the premise router/firewall 252 via a coupling with a premise LAN 250. The premise router/firewall 252 is coupled to a broadband modem 251, and the broadband modem 251 is coupled to a WAN 200 or other network outside the premise. The touchscreen 902 thus enables or forms a separate wireless network, or sub-network, that includes some number of devices and is coupled or connected to the LAN 250 of the host premises. The touchscreen sub-network can include, but is not limited to, any number of other devices like WiFi IP cameras, security panels (e.g., IP-enabled), and IP devices, to name a few. The touchscreen 902 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the touchscreen 902.

[0178] FIG. 10 is a block diagram 1000 of network or premise device integration with a premise network 250, under an alternative embodiment. The network or premise devices 255, 256, 1057 are coupled to the touchscreen 1002, and the touchscreen 1002 is coupled or connected between the premise router/firewall 252 and the broadband modem 251. The broadband modem 251 is coupled to a WAN 200 or other network outside the premise, while the premise router/firewall 252 is coupled to a premise LAN 250. As a result of its location between the broadband modem 251 and the premise router/firewall 252, the touchscreen 1002 can be configured or function as the premise router routing specified data between the outside network (e.g., WAN 200) and the premise router/firewall 252 of the LAN 250. As described above, the touchscreen 1002 in this configuration enables or forms a separate wireless network, or sub-network, that includes the network or premise devices 255, 156, 1057 and is coupled or connected between the LAN 250 of the host premises and the WAN 200. The touchscreen sub-network can include, but is not limited to, any number of network or premise devices 255, 256, 1057 like WiFi IP cameras, security panels (e.g., IP-enabled), and security touchscreens, to name a few. The touchscreen 1002 manages or controls the sub-network separately from the LAN 250 and transfers data and information between components of the sub-network and the LAN 250/WAN 200, but is not so limited. Additionally, other network devices 254 can be coupled to the LAN 250 without being coupled to the touchscreen 1002.

[0179] The gateway of an embodiment, whether a stand-alone component or integrated with a touchscreen, enables couplings or connections and thus the flow or integration of information between various components of the host premises and various types and/or combinations of IP devices, where the components of the host premises include a network (e.g., LAN) and/or a security system or subsystem to name a few. Consequently, the gateway controls the association between and the flow of information or data between the components of the host premises. For example, the gateway of an embodiment forms a sub-network coupled to another network (e.g., WAN, LAN, etc.), with the sub-network including IP devices. The gateway further enables the association of the IP devices of the sub-network with appropriate systems on the premises (e.g., security system, etc.). Therefore, for example, the gateway can form a sub-network of IP devices configured for security functions, and associate the sub-network only with the premises security system, thereby segregating the IP devices dedicated to security from other IP devices that may be coupled to another network on the premises.

[0180] In an example embodiment, FIG. 11 is a flow diagram 1100 for integration or installation of an IP device into a private network environment, under an embodiment. The IP device includes any IP-capable device which, for example, includes the touchscreen of an embodiment. The variables of an embodiment set at time of installation include, but are not limited to, one or more of a private SSID/Password, an gateway identifier, a security panel identifier, a user account TS, and a Central Monitoring Station account identification.

[0181] An embodiment of the IP device discovery and management begins with a user or installer activating 1102 the gateway and initiating 1104 the install mode of the system. This places the gateway in an install mode. Once in install mode, the gateway shifts to a default (Install) Wifi configuration. This setting will match the default setting for other integrated security system-enabled devices that have been pre-configured to work with the integrated security system. The gateway will then begin to provide 1106 DHCP addresses for these IP devices. Once the devices have acquired a new DHCP address from the gateway, those devices are available for configuration into a new secured Wifi network setting.

[0182] The user or installer of the system selects 1108 all devices that have been identified as available for inclusion into the integrated security system. The user may select these devices by their unique IDs via a web page, Touchscreen, or other client interface. The gateway provides 1110 data as appropriate to the devices. Once selected, the devices are configured 1112 with appropriate secured Wifi settings, including SSID and WPA/WPA-2 keys that are used once the gateway switches back to the secured sandbox configuration from the "Install" settings. Other settings are also configured as appropriate for that type of device. Once all devices have been configured, the user is notified and the user can exit install mode. At this point all devices will have been registered 1114 with the integrated security system servers.

[0183] The installer switches 1116 the gateway to an operational mode, and the gateway instructs or directs 1118 all newly configured devices to switch to the "secured" Wifi sandbox settings. The gateway then switches 1120 to the "secured" Wifi settings. Once the devices identify that the gateway is active on the "secured" network, they request new DHCP addresses from the gateway which, in response, pro-

vides 1122 the new addresses. The devices with the new addresses are then operational 1124 on the secured network.

[0184] In order to ensure the highest level of security on the secured network, the gateway can create or generate a dynamic network security configuration based on the unique ID and private key in the gateway, coupled with a randomizing factor that can be based on online time or other inputs. This guarantees the uniqueness of the gateway secured network configuration.

[0185] To enable the highest level of performance, the gateway analyzes the RF spectrum of the 802.11x network and determines which frequency band/channel it should select to run.

[0186] An alternative embodiment of the camera/IP device management process leverages the local ethernet connection of the sandbox network on the gateway. This alternative process is similar to the Wifi discovery embodiment described above, except the user connects the targeted device to the ethernet port of the sandbox network to begin the process. This alternative embodiment accommodates devices that have not been pre-configured with the default "Install" configuration for the integrated security system.

[0187] This alternative embodiment of the IP device discovery and management begins with the user/installer placing the system into install mode. The user is instructed to attach an IP device to be installed to the sandbox Ethernet port of the gateway. The IP device requests a DHCP address from the gateway which, in response to the request, provides the address. The user is presented the device and is asked if he/she wants to install the device. If yes, the system configures the device with the secured Wifi settings and other device-specific settings (e.g., camera settings for video length, image quality etc.). The user is next instructed to disconnect the device from the ethernet port. The device is now available for use on the secured sandbox network.

[0188] FIG. 12 is a block diagram showing communications among integrated IP devices of the private network environment, under an embodiment. The IP devices of this example include a security touchscreen 1203, gateway 1202 (e.g., "iHub"), and security panel (e.g., "Security Panel 1", "Security Panel 2", "Security Panel n"), but the embodiment is not so limited. In alternative embodiments any number and/or combination of these three primary component types may be combined with other components including IP devices and/or security system components. For example, a single device which comprises an integrated gateway, touchscreen, and security panel is merely another embodiment of the integrated security system described herein. The description that follows includes an example configuration that includes a touchscreen hosting particular applications. However, the embodiment is not limited to the touchscreen hosting these applications, and the touchscreen should be thought of as representing any IP device.

[0189] Referring to FIG. 12, the touchscreen 1203 incorporates an application 1210 that is implemented as computer code resident on the touchscreen operating system, or as a web-based application running in a browser, or as another type of scripted application (e.g., Flash, Java, Visual Basic, etc.). The touchscreen core application 1210 represents this application, providing user interface and logic for the end user to manage their security system or to gain access to networked information or content (Widgets). The touchscreen core application 1210 in turn accesses a library or libraries of functions to control the local hardware (e.g., screen

display, sound, LEDs, memory, etc.) as well as specialized librarie(s) to couple or connect to the security system.

[0190] In an embodiment of this security system connection, the touchscreen **1203** communicates to the gateway **1202**, and has no direct communication with the security panel. In this embodiment, the touchscreen core application **1210** accesses the remote service APIs **1212** which provide security system functionality (e.g. ARM/DISARM panel, sensor state, get/set panel configuration parameters, initiate or get alarm events, etc.). In an embodiment, the remote service APIs **1212** implement one or more of the following functions, but the embodiment is not so limited: Armstate=setARMState(type="ARM STAY|ARM AWAY|DISARM", Parameters="ExitDelay=30|Lights=OFF"); sensorState=getSensors (type="ALL|SensorName|SensorNameList"); result=setSensorState(SensorName, parameters="Option1, Options2, . . . Option n"); interruptHandler=SensorEvent(); and, interruptHandler=alarmEvent().

[0191] Functions of the remote service APIs **1212** of an embodiment use a remote PanelConnect API **1224** which resides in memory on the gateway **1202**. The touchscreen **1203** communicates with the gateway **1202** through a suitable network interface such as an Ethernet or 802.11 RF connection, for example. The remote PanelConnect API **1224** provides the underlying Security System Interfaces **1226** used to communicate with and control one or more types of security panel via wired link **1230** and/or RF link **3**. The PanelConnect API **1224** provides responses and input to the remote services APIs **1226**, and in turn translates function calls and data to and from the specific protocols and functions supported by a specific implementation of a Security Panel (e.g. a GE Security Simon XT or Honeywell Vista 20P). In an embodiment, the PanelConnect API **1224** uses a 345 MHz RF transceiver or receiver hardware/firmware module to communicate wirelessly to the security panel and directly to a set of 345 MHz RF-enabled sensors and devices, but the embodiment is not so limited.

[0192] The gateway of an alternative embodiment communicates over a wired physical coupling or connection to the security panel using the panel's specific wired hardware (bus) interface and the panel's bus-level protocol.

[0193] In an alternative embodiment, the Touchscreen **1203** implements the same PanelConnect API **1214** locally on the Touchscreen **1203**, communicating directly with the Security Panel **2** and/or Sensors **2** over the proprietary RF link or over a wired link for that system. In this embodiment the Touchscreen **1203**, instead of the gateway **1202**, incorporates the 345 MHz RF transceiver to communicate directly with Security Panel **2** or Sensors **2** over the RF link **2**. In the case of a wired link the Touchscreen **1203** incorporates the real-time hardware (e.g. a PIC chip and RS232-variant serial link) to physically connect to and satisfy the specific bus-level timing requirements of the SecurityPanel2.

[0194] In yet another alternative embodiment, either the gateway **1202** or the Touchscreen **1203** implements the remote service APIs. This embodiment includes a Cricket device ("Cricket") which comprises but is not limited to the following components: a processor (suitable for handling 802.11 protocols and processing, as well as the bus timing requirements of SecurityPanel1); an 802.11 (WiFi) client IP

interface chip; and, a serial bus interface chip that implements variants of RS232 or RS485, depending on the specific Security Panel.

[0195] The Cricket also implements the full PanelConnect APIs such that it can perform the same functions as the case where the gateway implements the PanelConnect APIs. In this embodiment, the touchscreen core application **1210** calls functions in the remote service APIs **1212** (such as setArmState()). These functions in turn couple or connect to the remote Cricket through a standard IP connection ("Cricket IP Link") (e.g., Ethernet, Homeplug, the gateway's proprietary Wifi network, etc.). The Cricket in turn implements the PanelConnect API, which responds to the request from the touchscreen core application, and performs the appropriate function using the proprietary panel interface. This interface uses either the wireless or wired proprietary protocol for the specific security panel and/or sensors.

[0196] Components of the gateway of the integrated security system described herein control discovery, installation and configuration of both wired and wireless IP devices (e.g., cameras, etc.) coupled or connected to the system, as described above with reference to FIGS. 1-4, as well as management of video routing using a video routing module or engine. The video routing engine initiates communication paths for the transfer of video from a streaming source device to a requesting client device, and delivers seamless video streams to the user via the communication paths using one or more of UPnP port-forwarding, relay server routing and STUN/TURN peer-to-peer routing, each of which is described below.

[0197] By way of reference, conventional video cameras have the ability to stream digital video in a variety of formats and over a variety of networks. Internet protocol (IP) video cameras, which include video cameras using an IP transport network (e.g., Ethernet, WiFi (IEEE 802.11 standards), etc.) are prevalent and increasingly being utilized in home monitoring and security system applications. With the proliferation of the internet, Ethernet and WiFi local area networks (LANs) and advanced wide area networks (WANs) that offer high bandwidth, low latency connections (broadband), as well as more advanced wireless WAN data networks (e.g. GPRS or CDMA 1xRTT), there increasingly exists the networking capability to extend traditional security systems to offer IP-based video. However, a fundamental reason for such IP video in a security system is to enable a user or security provider to monitor live or otherwise streamed video from outside the host premises (and the associated LAN).

[0198] The conventional solution to this problem has involved a technique known as 'port forwarding', whereby a 'port' on the LAN's router/firewall is assigned to the specific LAN IP address for an IP camera, or a proxy to that camera. Once a port has been 'forwarded' in this manner, a computer external to the LAN can address the LAN's router directly, and request access to that port. This access request is then forwarded by the router directly to the IP address specified, the IP camera or proxy. In this way an external device can directly access an IP camera within the LAN and view or control the streamed video.

[0199] The issues with this conventional approach include the following: port forwarding is highly technical and most users do not know how/why to do it; automatic port forwarding is difficult and problematic using emerging standards like UPnP; the camera IP address is often reset in response to a power outage/router reboot event; there are many different

routers with different ways/capabilities for port forwarding. In short, although port forwarding can work, it is frequently less than adequate to support a broadly deployed security solution utilizing IP cameras.

[0200] Another approach to accessing streaming video externally to a LAN utilizes peer-to-peer networking technology. So-called peer-to-peer networks, which includes networks in which a device or client is connected directly to another device or client, typically over a Wide Area Network (WAN) and without a persistent server connection, are increasingly common. In addition to being used for the sharing of files between computers (e.g., Napster and KaZaa), peer-to-peer networks have also been more recently utilized to facilitate direct audio and media streaming in applications such as Skype. In these cases, the peer-to-peer communications have been utilized to enable telephony-style voice communications and video conferencing between two computers, each enabled with an IP-based microphone, speaker, and video camera. A fundamental reason for adopting such peer-to-peer technology is the ability to transparently ‘punch through’ LAN firewalls to enable external access to the streaming voice and video content, and to do so in a way that scales to tens of millions of users without creating an untenable server load.

[0201] A limitation of the conventional peer-to-peer video transport lies in the personal computer (PC)-centric nature of the solution. Each of the conventional solutions uses a highly capable PC connected to the video camera, with the PC providing the advanced software functionality required to initiate and manage the peer-to-peer connection with the remote client. A typical security or remote home monitoring system requires multiple cameras, each with its own unique IP address, and only a limited amount of processing capability in each camera such that the conventional PC-centric approach cannot easily solve the need. Instead of a typical PC-centric architecture with three components (a “3-way IP Video System”) that include a computer device with video camera, a mediating server, and a PC client with video display capability, the conventional security system adds a plurality of fourth components that are standalone IP video cameras (requiring a “4-way IP Video System”), another less-than-ideal solution.

[0202] In accordance with the embodiments described herein, IP camera management systems and methods are provided that enable a consumer or security provider to easily and automatically configure and manage IP cameras located at a customer premise. Using this system IP camera management may be extended to remote control and monitoring from outside the firewall and router of the customer premise.

[0203] With reference to FIGS. 5 and 6, the system includes a gateway 253 having a video routing component so that the gateway 253 can manage and control, or assist in management and control, or video routing. The system also includes one or more cameras (e.g., WiFi IP camera 254, Ethernet IP camera 255, etc.) that communicate over the LAN 250 using an IP format, as well as a connection management server 210 located outside the premise firewall 252 and connected to the gateway 253 by a Wide Area Network (WAN) 200. The system further includes one or more devices 220, 230, 240 located outside the premise and behind other firewalls 221, 231, 241 and connected to the WAN 200. The other devices 220, 230, 240 are configured to access video or audio content from the IP cameras within the premise, as described above.

[0204] Alternatively, with reference to FIGS. 9 and 10, the system includes a touchscreen 902 or 1002 having a video

routing component so that the touchscreen 902 or 1002 can manage and control, or assist in management and control, or video routing. The system also includes one or more cameras (e.g., WiFi IP camera 254, Ethernet IP camera 255, etc.) that communicate over the LAN 250 using an IP format, as well as a connection management server 210 located outside the premise firewall 252 and connected to the gateway 253 by a Wide Area Network (WAN) 200. The system further includes one or more devices 220, 230, 240 located outside the premise and behind other firewalls 221, 231, 241 and connected to the WAN 200. The other devices 220, 230, 240 are configured to access video or audio content from the IP cameras within the premise, as described above.

[0205] FIG. 13 is a general flow diagram for IP video control, under an embodiment. The IP video control interfaces, manages, and provides WAN-based remote access to a plurality of IP cameras in conjunction with a home security or remote home monitoring system. The IP video control allows for monitoring and controlling of IP video cameras from a location remote to the customer premise, outside the customer premise firewall, and protected by another firewall. Operations begin when the system is powered on 1310, involving at a minimum the power-on of the gateway, as well as the power-on of at least one IP camera coupled or connected to the premise LAN. The gateway searches 1311 for available IP cameras and associated IP addresses. The gateway selects 1312 from one or more possible approaches to create connections between the IP camera and a device external to the firewall. Once an appropriate connection path is selected, the gateway begins operation 1313, and awaits 1320 a request for a stream from one of the plurality of IP video cameras available on the LAN. When a stream request is present the server retrieves 1321 the requestor’s WAN IP address/port.

[0206] When a server relay is present 1330, the IP camera is instructed 1331 to stream to the server, and the connection is managed 1332 through the server. In response to the stream terminating 1351, operations return to gateway operation 1313, and waits to receive another request 1320 for a stream from one of the plurality of IP video cameras available on the LAN.

[0207] When a server relay is not present 1330, the requestor’s WAN IP address/port is provided 1333 to the gateway or gateway relay. When a gateway relay is present 1340, the IP camera is instructed 1341 to stream to the gateway, and the gateway relays 1342 the connection to the requestor. In response to the stream terminating 1351, operations return to gateway operation 1313, and waits to receive another request 1320 for a stream from one of the plurality of IP video cameras available on the LAN. When a gateway relay is not present 1340, the IP camera is instructed 1343 to stream to an address, and a handoff 1344 is made resulting in direct communication between the camera and the requester. In response to the stream terminating 1351, operations return to gateway operation 1313, and waits to receive another request 1320 from one of the plurality of IP video cameras available on the LAN.

[0208] The integrated security system of an embodiment supports numerous video stream formats or types of video streams. Supported video streams include, but are not limited to, Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP), MPEG-4 over Hypertext Transfer Protocol (HTTP), and Motion Joint Photographic Experts Group (JPEG) (MJPEG).

[0209] The integrated security system of an embodiment supports the MPEG-4/RTSP video streaming method (supported by video servers and clients) which uses RTSP for the control channel and Real-time Transport Protocol (RTP) for the data channel. Here the RTSP channel is over Transmission Control Protocol (TCP) while the data channel uses User Datagram Protocol (UDP). This method is widely supported by both streaming sources (e.g., cameras) and stream clients (e.g., remote client devices, Apple Quicktime, VideoLAN, IPTV mobile phones, etc).

[0210] Encryption can be added to the two channels under MPEG-4/RTSP. For example, the RTSP control channel can be encrypted using SSL/TLS. The data channel can also be encrypted.

[0211] If the camera or video stream source inside the home does not support encryption for either RTSP or RTP channels, the gateway located on the LAN can facilitate the encrypted RTSP method by maintaining separate TCP sessions with the video stream source device and with the encrypted RTSP client outside the LAN, and relay all communication between the two sessions. In this situation, any communication between the gateway and the video stream source that is not encrypted could be encrypted by the gateway before being relayed to the RTSP client outside the LAN. In many cases the gateway is an access point for the encrypted and private Wifi network on which the video stream source device is located. This means that communication between the gateway and the video stream source device is encrypted at the network level, and communication between the gateway and the RTSP client is encrypted at the transport level. In this fashion the gateway can compensate for a device that does not support encrypted RTSP.

[0212] The integrated security system of an embodiment also supports reverse RTSP. Reverse RTSP includes taking a TCP-based protocol like RTSP, and reversing the roles of client and server (references to "server" include the iControl server, also referred to as the iConnect server) when it comes to TCP session establishment. For example, in standard RTSP the RTSP client is the one that establishes the TCP connection with the stream source server (the server listens on a port for incoming connections). In Reverse RTSP, the RTSP client listens on a port for incoming connections from the stream source server. Once the TCP connection is established, the RTSP client begins sending commands to the server over the TCP connection just as it would in standard RTSP.

[0213] When using Reverse RTSP, the video stream source is generally on a LAN, protected by a firewall. Having a device on the LAN initiate the connection to the RTSP client outside the firewall enables easy network traversal.

[0214] If the camera or video stream source inside the LAN does not support Reverse RTSP, then the gateway facilitates the Reverse RTSP method by initiating separate TCP sessions with the video stream source device and with the Reverse RTSP client outside the LAN, and then relays all communication between the two sessions. In this fashion the gateway compensates for a stream source device that does not support Reverse RTSP.

[0215] As described in the encryption description above, the gateway can further compensate for missing functionalities on the device such as encryption. If the device does not support encryption for either RTSP or RTP channels, the gateway can communicate with the device using these unencrypted streams, and then encrypt the streams before relaying them out of the LAN to the RTSP Reverse client.

[0216] Servers of the integrated security system can compensate for RTSP clients that do not support Reverse RTSP. In this situation, the server accepts TCP connections from both the RTSP client and the Reverse RTSP video stream source (which could be a gateway acting on behalf of a stream source device that does not support Reverse RTSP). The server then relays the control and video streams from the Reverse RTSP video stream source to the RTSP client. The server can further compensate for the encryption capabilities of the RTSP client; if the RTSP client does not support encryption then the server can provide an unencrypted stream to the RTSP client even though an encrypted stream was received from the Reverse RTSP streaming video source.

[0217] The integrated security system of an embodiment also supports Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing. STUN and Turn are techniques for using a server to help establish a peer-to-peer UDP data stream (it does not apply to TCP streams). The bandwidth consumed by the data channel of a video stream is usually many thousands of times larger than that used by the control channel. Consequently, when a peer-to-peer connection for both the RTSP and RTP channels is not possible, there is still a great incentive to use STUN/TURN techniques in order to achieve a peer-to-peer connection for the RTP data channel.

[0218] Here, a method referred to herein as RTSP with STUN/TURN is used by the integrated security system. The RTSP with STUN/TURN is a method in which the video streaming device is instructed over the control channel to stream its UDP data channel to a different network address than that of the other end of the control TCP connection (usually the UDP data is simply streamed to the IP address of the RTSP client). The result is that the RTSP or Reverse RTSP TCP channel can be relayed using the gateway and/or the server, while the RTP UDP data channel can flow directly from the video stream source device to the video stream client.

[0219] If a video stream source device does not support RTSP with STUN/TURN, the gateway can compensate for the device by relaying the RTSP control channel via the server to the RTSP client, and receiving the RTP data channel and then forwarding it directly to the RTSP with STUN/TURN enabled client. Encryption can also be added here by the gateway.

[0220] The integrated security system of an embodiment supports MPEG-4 over HTTP. MPEG-4 over HTTP is similar to MPEG-4 over RTSP except that both the RTSP control channel and the RTP data channel are passed over an HTTP TCP session. Here a single TCP session can be used, splitting it into multiple channels using common HTTP techniques like chunked transfer encoding.

[0221] The MPEG-4 over HTTP is generally supported by many video stream clients and server devices, and encryption can easily be added to it using SSL/TLS. Because it uses TCP for both channels, STUN/TURN techniques may not apply in the event that a direct peer-to-peer TCP session between client and server cannot be established.

[0222] As described above, encryption can be provided using SSL/TLS taking the form of HTTPS. And as with MPEG-4 over RTSP, a gateway can compensate for a stream source device that does not support encryption by relaying the TCP streams and encrypting the TCP stream between the gateway and the stream client. In many cases the gateway is

an access point for the encrypted and private Wifi network on which the video stream source device is located. This means that communication between the gateway and the video stream source device is encrypted at the network level, and communication between the gateway and the video stream client is encrypted at the transport level. In this fashion the gateway can compensate for a device that does not support HTTPS.

[0223] As with Reverse RTSP, the integrated security system of an embodiment supports Reverse HTTP. Reverse HTTP includes taking a TCP-based protocol like HTTP, and reversing the roles of client and server when it comes to TCP session establishment. For example, in conventional HTTP the HTTP client is the one that establishes the TCP connection with the server (the server listens on a port for incoming connections). In Reverse HTTP, the HTTP client listens on a port for incoming connections from the server. Once the TCP connection is established, the HTTP client begins sending commands to the server over the TCP connection just as it would in standard HTTP.

[0224] When using Reverse HTTP, the video stream source is generally on a LAN, protected by a firewall. Having a device on the LAN initiate the connection to the HTTP client outside the firewall enables easy network traversal.

[0225] If the camera or video stream source inside the LAN does not support Reverse HTTP, then the gateway can facilitate the Reverse HTTP method by initiating separate TCP sessions with the video stream source device and with the Reverse HTTP client outside the LAN, and then relay all communication between the two sessions. In this fashion the gateway can compensate for a stream source device that does not support Reverse HTTP.

[0226] As described in the encryption description above, the gateway can further compensate for missing functionalities on the device such as encryption. If the device does not support encrypted HTTP (e.g., HTTPS), then the gateway can communicate with the device using HTTP, and then encrypt the TCP stream(s) before relaying out of the LAN to the Reverse HTTP client.

[0227] The servers of an embodiment can compensate for HTTP clients that do not support Reverse HTTP. In this situation, the server accepts TCP connections from both the HTTP client and the Reverse HTTP video stream source (which could be a gateway acting on behalf of a stream source device that does not support Reverse HTTP). The server then relays the TCP streams from the Reverse HTTP video stream source to the HTTP client. The server can further compensate for the encryption capabilities of the HTTP client; if the HTTP client does not support encryption then the server can provide an unencrypted stream to the HTTP client even though an encrypted stream was received from the Reverse HTTP streaming video source.

[0228] The integrated security system of an embodiment supports MJPEG as described above. MJPEG is a streaming technique in which a series of JPG images are sent as the result of an HTTP request. Because MJPEG streams are transmitted over HTTP, HTTPS can be employed for encryption and most MJPEG clients support the resulting encrypted stream. And as with MPEG-4 over HTTP, a gateway can compensate for a stream source device that does not support encryption by relaying the TCP streams and encrypting the TCP stream between the gateway and the stream client. In many cases the gateway is an access point for the encrypted and private Wifi network on which the video stream source

device is located. This means that communication between the gateway and the video stream source device is encrypted at the network level, and communication between the gateway and the video stream client is encrypted at the transport level. In this fashion the gateway can compensate for a device that does not support HTTPS.

[0229] The integrated system of an embodiment supports Reverse HTTP. Reverse HTTP includes taking a TCP-based protocol like HTTP, and reversal of the roles of client and server when it comes to TCP session establishment can be employed for MJPEG streams. For example, in standard HTTP the HTTP client is the one who establishes the TCP connection with the server (the server listens on a port for incoming connections). In Reverse HTTP, the HTTP client listens on a port for incoming connections from the server. Once the TCP connection is established, the HTTP client begins sending commands to the server over the TCP connection just as it would in standard HTTP.

[0230] When using Reverse HTTP, the video stream source is generally on a LAN, protected by a firewall. Having a device on the LAN initiate the connection to the HTTP client outside the firewall enables network traversal.

[0231] If the camera or video stream source inside the LAN does not support Reverse HTTP, then the gateway can facilitate the Reverse HTTP method by initiating separate TCP sessions with the video stream source device and with the Reverse HTTP client outside the LAN, and then relay all communication between the two sessions. In this fashion the gateway can compensate for a stream source device that does not support Reverse HTTP.

[0232] As described in the encryption description above, the gateway can further compensate for missing functionalities on the device such as encryption. If the device does not support encrypted HTTP (e.g., HTTPS), then the gateway can communicate with the device using HTTP, and then encrypt the TCP stream(s) before relaying out of the LAN to the Reverse HTTP client.

[0233] The servers can compensate for HTTP clients that do not support Reverse HTTP. In this situation, the server accepts TCP connections from both the HTTP client and the Reverse HTTP video stream source (which could be a gateway acting on behalf of a stream source device that does not support Reverse HTTP). The server then relays the TCP streams from the Reverse HTTP video stream source to the HTTP client. The server can further compensate for the encryption capabilities of the HTTP client; if the HTTP client does not support encryption then the server can provide an unencrypted stream to the HTTP client even though an encrypted stream was received from the Reverse HTTP streaming video source.

[0234] The integrated security system of an embodiment considers numerous parameters in determining or selecting one of the streaming formats described above for use in transferring video streams. The parameters considered in selecting a streaming format include, but are not limited to, security requirements, client capabilities, device capabilities, and network/system capabilities.

[0235] The security requirements for a video stream are considered in determining an applicable streaming format in an embodiment. Security requirements fall into two categories, authentication and privacy, each of which is described below.

[0236] Authentication as a security requirement means that stream clients must present credentials in order to obtain a

stream. Furthermore, this presentation of credentials should be done in a way that is secure from network snooping and replays. An example of secure authentication is Basic Authentication over HTTPS. Here a username and password are presented over an encrypted HTTPS channel so snooping and replays are prevented. Basic Authentication alone, however, is generally not sufficient for secure authentication.

[0237] Because not all streaming clients support SSL/TLS, authentication methods that do not require it are desirable. Such methods include Digest Authentication and one-time requests. A one-time request is a request that can only be made by a client one time, and the server prevents a reuse of the same request. One-time requests are used to control access to a stream source device by stream clients that do not support SSL/TLS. An example here is providing video access to a mobile phone. Typical mobile phone MPEG-4 viewers do not support encryption. In this case, one of the MPEG-4 over RTSP methods described above can be employed to get the video stream relayed to a server. The server can then provide the mobile phone with a one-time request Universal Resource Locator (URL) for the relayed video stream source (via a Wireless Application Protocol (WAP) page). Once the stream ends, the mobile phone would need to obtain another one-time request URL from the server (via WAP, for example) in order to view the stream again.

[0238] Privacy as a security requirement means that the contents of the video stream must be encrypted. This is a requirement that may be impossible to satisfy on clients that do not support video stream encryption, for example many mobile phones. If a client supports encryption for some video stream format(s), then the “best” of those formats should be selected. Here “best” is determined by the stream type priority algorithm.

[0239] The client capabilities are considered in determining an applicable streaming format in an embodiment. In considering client capabilities, the selection depends upon the supported video stream formats that include encryption, and the supported video stream formats that do not support encryption.

[0240] The device capabilities are considered in determining an applicable streaming format in an embodiment. In considering device capabilities, the selection depends upon the supported video stream formats that include encryption, the supported video stream formats that do not support encryption, and whether the device is on an encrypted private Wifi network managed by the gateway (in which case encryption at the network level is not required).

[0241] The network/system capabilities are considered in determining an applicable streaming format in an embodiment. In considering network/system capabilities, the selection depends upon characteristics of the network or system across which the stream must travel. The characteristics considered include, for example, the following: whether there is a gateway and/or server on the network to facilitate some of the fancier video streaming types or security requirements; whether the client is on the same LAN as the gateway, meaning that network firewall traversal is not needed.

[0242] Streaming methods with the highest priority are peer-to-peer because they scale best with server resources. Universal Plug and Play (UPnP) can be used by the gateway to open ports on the video stream device’s LAN router and direct traffic through those ports to the video stream device. This allows a video stream client to talk directly with the

video stream device or talk directly with the gateway which can in turn facilitate communication with the video stream device.

[0243] Another factor in determining the best video stream format to use is the success of STUN and TURN methods for establishing direct peer-to-peer UDP communication between the stream source device and the stream client. Again, the gateway and the server can help with the setup of this communication.

[0244] Client bandwidth availability and processing power are other factors in determining the best streaming methods. For example, due to its bandwidth overhead an encrypted MJPEG stream should not be considered for most mobile phone data networks.

[0245] Device bandwidth availability can also be considered in choosing the best video stream format. For example, consideration can be given to whether the upstream bandwidth capabilities of the typical residential DSL support two or more simultaneous MJPEG streams.

[0246] Components of the integrated security system of an embodiment, while considering various parameters in selecting a video streaming format to transfer video streams from streaming source devices and requesting client devices, prioritize streaming formats according to these parameters. The parameters considered in selecting a streaming format include, as described above, security requirements, client capabilities, device capabilities, and network/system capabilities. Components of the integrated security system of an embodiment select a video streaming format according to the following priority, but alternative embodiments can use other priorities.

[0247] The selected format is UPnP or peer-to-peer MPEG-4 over RTSP with encryption when both requesting client device and streaming source device support this format.

[0248] The selected format is UPnP or peer-to-peer MPEG-4 over RTSP with authentication when the requesting client device does not support encryption or UPnP or peer-to-peer MPEG-4 over RTSP with encryption.

[0249] The selected format is UPnP (peer-to-peer) MPEG-4 over HTTPS when both requesting client device and streaming source device support this format.

[0250] The selected format is UPnP (peer-to-peer) MPEG-4 over HTTP when the requesting client device does not support encryption or UPnP (peer-to-peer) MPEG-4 over HTTPS.

[0251] The selected format is UPnP (peer-to-peer) MPEG-4 over RTSP facilitated by gateway or touchscreen (including or incorporating gateway components) (to provide encryption), when the requesting client device supports encrypted RTSP and the streaming source device supports MPEG-4 over RTSP.

[0252] The selected format is UPnP (peer-to-peer) MPEG-4 over HTTPS facilitated by gateway or touchscreen (including or incorporating gateway components) (to provide encryption) when the requesting client device supports MPEG-4 over HTTPS and the streaming source device supports MPEG-4 over HTTP.

[0253] The selected format is UPnP (peer-to-peer) MJPEG over HTTPS when the networks and devices can handle the bandwidth and both requesting client device and streaming source device support MJPEG over HTTPS.

[0254] The selected format is Reverse RTSP with STUN/TURN facilitated by the server when the streaming source device initiates SSL/TLS TCP to server, the streaming source

device supports Reverse RTSP over SSL/TLS with STUN/TURN, and the requesting client device supports RTSP with STUN/TURN.

[0255] The selected format is Reverse RTSP with STUN/TURN facilitated by server and gateway or touchscreen (including or incorporating gateway components) when the gateway initiates SSL/TLS TCP to the server and to the streaming source device, the streaming source device supports RTSP, and the requesting client device supports RTSP with STUN/TURN.

[0256] The selected format is Reverse MPEG over RTSP/HTTP facilitated by the server when the streaming source device initiates SSL/TLS TCP to server, the streaming source device supports Reverse RTSP or HTTP over SSL/TLS, and the requesting client device supports MPEG over RTSP/HTTP.

[0257] The selected format is Reverse MPEG over RTSP/HTTP facilitated by server and gateway or touchscreen (including or incorporating gateway components) when the gateway initiates SSL/TLS TCP to server and to streaming source device, the streaming source device supports MPEG over RTSP or HTTP, and the requesting client device supports MPEG over RTSP/HTTP.

[0258] The selected format is UPnP (peer-to-peer) MJPEG over HTTP when the networks and devices can handle the bandwidth and when the requesting client device does not support encryption and does not support MPEG-4.

[0259] The selected format is Reverse MJPEG over HTTPS facilitated by the server when the streaming source device initiates SSL/TLS TCP to server, the streaming source device supports Reverse MJPEG over SSL/TLS, and the requesting client device supports MJPEG.

[0260] The selected format is Reverse MJPEG over HTTPS facilitated by server and gateway or touchscreen (including or incorporating gateway components) when the gateway initiates SSL/TLS TCP to the server and to the streaming source device, the streaming source device supports MJPEG, and the requesting client device supports MJPEG.

[0261] FIG. 14 is a flow diagram of a method of integrating an external control and management application system with an existing security system, under an embodiment. Operations begin when the system is powered on **1410**, involving at a minimum the power-on of the gateway device, and optionally the power-on of the connection between the gateway device and the remote servers. The gateway device initiates **1420** a software and RF sequence to locate the extant security system. The gateway and installer initiate and complete **1430** a sequence to 'learn' the gateway into the security system as a valid and authorized control device. The gateway initiates **1440** another software and RF sequence of instructions to discover and learn the existence and capabilities of existing RF devices within the extant security system, and store this information in the system. These operations under the system of an embodiment are described in further detail below.

[0262] Unlike conventional systems that extend an existing security system, the system of an embodiment operates utilizing the proprietary wireless protocols of the security system manufacturer. In one illustrative embodiment, the gateway is an embedded computer with an IP LAN and WAN connection and a plurality of RF transceivers and software protocol modules capable of communicating with a plurality of security systems each with a potentially different RF and software protocol interface. After the gateway has completed the discovery and learning **1440** of sensors and has been

integrated **1450** as a virtual control device in the extant security system, the system becomes operational. Thus, the security system and associated sensors are presented **1450** as accessible devices to a potential plurality of user interface subsystems.

[0263] The system of an embodiment integrates **1460** the functionality of the extant security system with other non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms, which may be controlled via RF, wired, or powerline-based networking mechanisms supported by the gateway or servers.

[0264] The system of an embodiment provides a user interface subsystem **1470** enabling a user to monitor, manage, and control the system and associated sensors and security systems. In an embodiment of the system, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX/Flash presentation of a monitoring and control application, enabling users to view the state of all sensors and controllers in the extant security system from a web browser or equivalent operating on a computer, PDA, mobile phone, or other consumer device.

[0265] In another illustrative embodiment of the system described herein, a user interface subsystem is an HTML/XML/Javascript/Java/AJAX presentation of a monitoring and control application, enabling users to combine the monitoring and control of the extant security system and sensors with the monitoring and control of non-security devices including but not limited to IP cameras, touchscreens, lighting controls, door locking mechanisms.

[0266] In another illustrative embodiment of the system described herein, a user interface subsystem is a mobile phone application enabling users to monitor and control the extant security system as well as other non-security devices.

[0267] In another illustrative embodiment of the system described herein, a user interface subsystem is an application running on a keypad or touchscreen device enabling users to monitor and control the extant security system as well as other non-security devices.

[0268] In another illustrative embodiment of the system described herein, a user interface subsystem is an application operating on a TV or set-top box connected to a TV enabling users to monitor and control the extant security system as well as other non-security devices.

[0269] FIG. 15 is a block diagram of an integrated security system **1500** wirelessly interfacing to proprietary security systems, under an embodiment. A security system **1510** is coupled or connected to a Gateway **1520**, and from Gateway **1520** coupled or connected to a plurality of information and content sources across a network **1530** including one or more web servers **1540**, system databases **1550**, and applications servers **1560**. While in one embodiment network **1530** is the Internet, including the World Wide Web, those of skill in the art will appreciate that network **1530** may be any type of network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non-TCP/IP based network.

[0270] Moreover, other elements of the system of an embodiment may be conventional, well-known elements that need not be explained in detail herein. For example, security system **1510** could be any type home or business security system, such devices including but not limited to a standalone RF home security system or a non-RF-capable wired home security system with an add-on RF interface module. In the integrated security system **1500** of this example, security

system 1510 includes an RF-capable wireless security panel (WSP) 1511 that acts as the master controller for security system 1510. Well-known examples of such a WSP include the GE Security Concord, Networx, and Simon panels, the Honeywell Vista and Lynx panels, and similar panels from DSC and Napco, to name a few. A wireless module 1514 includes the RF hardware and protocol software necessary to enable communication with and control of a plurality of wireless devices 1513. WSP 1511 may also manage wired devices 1514 physically connected to WSP 1511 with an RS232 or RS485 or Ethernet connection or similar such wired interface.

[0271] In an implementation consistent with the systems and methods described herein, Gateway 1520 provides the interface between security system 1510 and LAN and/or WAN for purposes of remote control, monitoring, and management. Gateway 1520 communicates with an external web server 1540, database 1550, and application server 1560 over network 1530 (which may comprise WAN, LAN, or a combination thereof). In this example system, application logic, remote user interface functionality, as well as user state and account are managed by the combination of these remote servers. Gateway 1520 includes server connection manager 1521, a software interface module responsible for all server communication over network 1530. Event manager 1522 implements the main event loop for Gateway 1520, processing events received from device manager 1524 (communicating with non-security system devices including but not limited to IP cameras, wireless thermostats, or remote door locks). Event manager 1522 further processes events and control messages from and to security system 1510 by utilizing WSP manager 1523.

[0272] WSP manager 1523 and device manager 1524 both rely upon wireless protocol manager 1526 which receives and stores the proprietary or standards-based protocols required to support security system 1510 as well as any other devices interfacing with gateway 1520. WSP manager 1523 further utilizes the comprehensive protocols and interface algorithms for a plurality of security systems 1510 stored in the WSP DB client database associated with wireless protocol manager 1526. These various components implement the software logic and protocols necessary to communicate with and manager devices and security systems 1510. Wireless Transceiver hardware modules 1525 are then used to implement the physical RF communications link to such devices and security systems 1510. An illustrative wireless transceiver 1525 is the GE Security Dialog circuit board, implementing a 319.5 MHz two-way RF transceiver module. In this example, RF Link 1570 represents the 319.5 MHz RF communication link, enabling gateway 1520 to monitor and control WSP 1511 and associated wireless and wired devices 1513 and 1514, respectively.

[0273] In one embodiment, server connection manager 1521 requests and receives a set of wireless protocols for a specific security system 1510 (an illustrative example being that of the GE Security Concord panel and sensors) and stores them in the WSP DB portion of the wireless protocol manager 1526. WSP manager 1523 then utilizes such protocols from wireless protocol manager 1526 to initiate the sequence of processes detailed in FIG. 14 and FIG. 15 for learning gateway 1520 into security system 1510 as an authorized control device. Once learned in, as described with reference to FIG. 15 (and above), event manager 1522 processes all events and messages detected by the combination of WSP manager 1523 and the GE Security wireless transceiver module 1525.

[0274] In another embodiment, gateway 1520 incorporates a plurality of wireless transceivers 1525 and associated protocols managed by wireless protocol manager 1526. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP 1511, wireless devices 1513, and wired devices 1514. For example a wireless sensor from one manufacturer may be utilized to control a device using a different protocol from a different manufacturer.

[0275] In another embodiment, gateway 1520 incorporates a wired interface to security system 1510, and incorporates a plurality of wireless transceivers 1525 and associated protocols managed by wireless protocol manager 1526. In this embodiment events and control of multiple heterogeneous devices may be coordinated with WSP 1511, wireless devices 1513, and wired devices 1514.

[0276] Of course, while an illustrative embodiment of an architecture of the system of an embodiment is described in detail herein with respect to FIG. 15, one of skill in the art will understand that modifications to this architecture may be made without departing from the scope of the description presented herein. For example, the functionality described herein may be allocated differently between client and server, or amongst different server or processor-based components. Likewise, the entire functionality of the gateway 1520 described herein could be integrated completely within an existing security system 1510. In such an embodiment, the architecture could be directly integrated with a security system 1510 in a manner consistent with the currently described embodiments.

[0277] FIG. 16 is a flow diagram for wirelessly 'learning' the Gateway into an existing security system and discovering extant sensors, under an embodiment. The learning interfaces gateway 1520 with security system 1510. Gateway 1520 powers up 1610 and initiates software sequences 1620 and 1625 to identify accessible WSPs 1511 and wireless devices 1513, respectively (e.g., one or more WSPs and/or devices within range of gateway 1520). Once identified, WSP 1511 is manually or automatically set into 'learn mode' 1630, and gateway 1520 utilizes available protocols to add 1640 itself as an authorized control device in security system 1510. Upon successful completion of this task, WSP 1511 is manually or automatically removed from 'learn mode' 1650.

[0278] Gateway 1520 utilizes the appropriate protocols to mimic 1660 the first identified device 1514. In this operation gateway 1520 identifies itself using the unique or pseudo-unique identifier of the first found device 1514, and sends an appropriate change of state message over RF Link 1570. In the event that WSP 1511 responds to this change of state message, the device 1514 is then added 1670 to the system in database 1550. Gateway 1520 associates 1680 any other information (such as zone name or token-based identifier) with this device 1514 in database 1550, enabling gateway 1520, user interface modules, or any application to retrieve this associated information.

[0279] In the event that WSP 1511 does not respond to the change of state message, the device 1514 is not added 1670 to the system in database 1550, and this device 1514 is identified as not being a part of security system 1510 with a flag, and is either ignored or added as an independent device, at the discretion of the system provisioning rules. Operations here-under repeat 1685 operations 1660, 1670, 1680 for all devices 1514 if applicable. Once all devices 1514 have been tested in this way, the system begins operation 1690.

[0280] In another embodiment, gateway 1520 utilizes a wired connection to WSP 1511, but also incorporates a wireless transceiver 1525 to communicate directly with devices 1514. In this embodiment, operations under 1620 above are removed, and operations under 1640 above are modified so the system of this embodiment utilizes wireline protocols to add itself as an authorized control device in security system 1510.

[0281] A description of an example embodiment follows in which the Gateway (FIG. 15, element 1520) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. In this example the gateway is “automatically” installed with a security system.

[0282] The automatic security system installation begins with the assignment of an authorization key to components of the security system (e.g., gateway, kit including the gateway, etc.). The assignment of an authorization key is done in lieu of creating a user account. An installer later places the gateway in a user’s premises along with the premises security system. The installer uses a computer to navigate to a web portal (e.g., integrated security system web interface), logs in to the portal, and enters the authorization key of the installed gateway into the web portal for authentication. Once authenticated, the gateway automatically discovers devices at the premises (e.g., sensors, cameras, light controls, etc.) and adds the discovered devices to the system or “network”. The installer assigns names to the devices, and tests operation of the devices back to the server (e.g., did the door open, did the camera take a picture, etc.). The security device information is optionally pushed or otherwise propagated to a security panel and/or to the server network database. The installer finishes the installation, and instructs the end user on how to create an account, username, and password. At this time the user enters the authorization key which validates the account creation (uses a valid authorization key to associate the network with the user’s account). New devices may subsequently be added to the security network in a variety of ways (e.g., user first enters a unique ID for each device/sensor and names it in the server, after which the gateway can automatically discover and configure the device).

[0283] A description of another example embodiment follows in which the security system (FIG. 15, element 1510) is a Dialog system and the WSP (FIG. 15, element 1511) is a SimonXT available from General Electric Security, and the Gateway (FIG. 15, element 1520) is the iHub available from iControl Networks, Palo Alto, Calif., and described in detail herein. Descriptions of the install process for the SimonXT and iHub are also provided below.

[0284] GE Security’s Dialog network is one of the most widely deployed and tested wireless security systems in the world. The physical RF network is based on a 319.5 MHz unlicensed spectrum, with a bandwidth supporting up to 19 Kbps communications. Typical use of this bandwidth—even in conjunction with the integrated security system—is far less than that. Devices on this network can support either one-way communication (either a transmitter or a receiver) or two-way communication (a transceiver). Certain GE Simon, Simon XT, and Concord security control panels incorporate a two-way transceiver as a standard component. The gateway also incorporates the same two-way transceiver card. The physical link layer of the network is managed by the transceiver module hardware and firmware, while the coded payload bit-streams are made available to the application layer for processing.

[0285] Sensors in the Dialog network typically use a 60-bit protocol for communicating with the security panel transceiver, while security system keypads and the gateway use the encrypted 80-bit protocol. The Dialog network is configured for reliability, as well as low-power usage. Many devices are supervised, i.e. they are regularly monitored by the system ‘master’ (typically a GE security panel), while still maintaining excellent power usage characteristics. A typical door window sensor has a battery life in excess of 5-7 years.

[0286] The gateway has two modes of operation in the Dialog network: a first mode of operation is when the gateway is configured or operates as a ‘slave’ to the GE security panel; a second mode of operation is when the gateway is configured or operates as a ‘master’ to the system in the event a security panel is not present. In both configurations, the gateway has the ability to ‘listen’ to network traffic, enabling the gateway to continually keep track of the status of all devices in the system. Similarly, in both situations the gateway can address and control devices that support setting adjustments (such as the GE wireless thermostat).

[0287] In the configuration in which the gateway acts as a ‘slave’ to the security panel, the gateway is ‘learned into’ the system as a GE wireless keypad. In this mode of operation, the gateway emulates a security system keypad when managing the security panel, and can query the security panel for status and ‘listen’ to security panel events (such as alarm events).

[0288] The gateway incorporates an RF Transceiver manufactured by GE Security, but is not so limited. This transceiver implements the Dialog protocols and handles all network message transmissions, receptions, and timing. As such, the physical, link, and protocol layers of the communications between the gateway and any GE device in the Dialog network are totally compliant with GE Security specifications.

[0289] At the application level, the gateway emulates the behavior of a GE wireless keypad utilizing the GE Security 80-bit encrypted protocol, and only supported protocols and network traffic are generated by the gateway. Extensions to the Dialog RF protocol of an embodiment enable full control and configuration of the panel, and iControl can both automate installation and sensor enrollment as well as direct configuration downloads for the panel under these protocol extensions.

[0290] As described above, the gateway participates in the GE Security network at the customer premises. Because the gateway has intelligence and a two-way transceiver, it can ‘hear’ all of the traffic on that network. The gateway makes use of the periodic sensor updates, state changes, and supervisory signals of the network to maintain a current state of the premises. This data is relayed to the integrated security system server (e.g., FIG. 2, element 260) and stored in the event repository for use by other server components. This usage of the GE Security RF network is completely non-invasive; there is no new data traffic created to support this activity.

[0291] The gateway can directly (or indirectly through the Simon XT panel) control two-way devices on the network. For example, the gateway can direct a GE Security Thermostat to change its setting to ‘Cool’ from ‘Off’, as well as request an update on the current temperature of the room. The gateway performs these functions using the existing GE Dialog protocols, with little to no impact on the network; a gateway device control or data request takes only a few dozen bytes of data in a network that can support 19 Kbps.

[0292] By enrolling with the Simon XT as a wireless keypad, as described herein, the gateway includes data or information of all alarm events, as well as state changes relevant to the security panel. This information is transferred to the gateway as encrypted packets in the same way that the information is transferred to all other wireless keypads on the network.

[0293] Because of its status as an authorized keypad, the gateway can also initiate the same panel commands that a keypad can initiate. For example, the gateway can arm or disarm the panel using the standard Dialog protocol for this activity. Other than the monitoring of standard alarm events like other network keypads, the only incremental data traffic on the network as a result of the gateway is the infrequent remote arm/disarm events that the gateway initiates, or infrequent queries on the state of the panel.

[0294] The gateway is enrolled into the Simon XT panel as a 'slave' device which, in an embodiment, is a wireless keypad. This enables the gateway for all necessary functionality for operating the Simon XT system remotely, as well as combining the actions and information of non-security devices such as lighting or door locks with GE Security devices. The only resource taken up by the gateway in this scenario is one wireless zone (sensor ID).

[0295] The gateway of an embodiment supports three forms of sensor and panel enrollment/installation into the integrated security system, but is not limited to this number of enrollment/installation options. The enrollment/installation options of an embodiment include installer installation, kitting, and panel, each of which is described below.

[0296] Under the installer option, the installer enters the sensor IDs at time of installation into the integrated security system web portal or iScreen. This technique is supported in all configurations and installations.

[0297] Kits can be pre-provisioned using integrated security system provisioning applications when using the kitting option. At kitting time, multiple sensors are automatically associated with an account, and at install time there is no additional work required.

[0298] In the case where a panel is installed with sensors already enrolled (i.e. using the GE Simon XT enrollment process), the gateway has the capability to automatically extract the sensor information from the system and incorporate it into the user account on the integrated security system server.

[0299] The gateway and integrated security system of an embodiment uses an auto-learn process for sensor and panel enrollment in an embodiment. The deployment approach of an embodiment can use additional interfaces that GE Security is adding to the Simon XT panel. With these interfaces, the gateway has the capability to remotely enroll sensors in the panel automatically. The interfaces include, but are not limited to, the following: EnrollDevice(ID, type, name, zone, group); SetDeviceParameters(ID, type, Name, zone, group); GetDeviceParameters(zone); and RemoveDevice(zone).

[0300] The integrated security system incorporates these new interfaces into the system, providing the following install process. The install process can include integrated security system logistics to handle kitting and pre-provisioning. Pre-kitting and logistics can include a pre-provisioning kitting tool provided by integrated security system that enables a security system vendor or provider ("provider") to offer pre-packaged initial 'kits'. This is not required but is recommended for simplifying the install process. This example

assumes a 'Basic' kit is preassembled and includes one (1) Simon XT, three (3) Door/window sensors, one (1) motion sensor, one (1) gateway, one (1) keyfob, two (2) cameras, and ethernet cables. The kit also includes a sticker page with all Zones (1-24) and Names (full name list).

[0301] The provider uses the integrated security system kitting tool to assemble 'Basic' kit packages. The contents of different types of starter kits may be defined by the provider. At the distribution warehouse, a worker uses a bar code scanner to scan each sensor and the gateway as it is packed into the box. An ID label is created that is attached to the box. The scanning process automatically associates all the devices with one kit, and the new ID label is the unique identifier of the kit. These boxes are then sent to the provider for distribution to installer warehouses. Individual sensors, cameras, etc. are also sent to the provider installer warehouse. Each is labeled with its own barcode/ID.

[0302] An installation and enrollment procedure of a security system including an gateway is described below as one example of the installation process.

1. Order and Physical Install Process

[0303] a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the provider for assignment to an installer.

[0304] b. The assigned installer picks up his/her ticket(s) and fills his/her truck with Basic and/or Advanced starter kits. He/she also keeps a stock of individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.

[0305] c. The installer arrives at the address on the ticket, and pulls out the Basic kit. The installer determines sensor locations from a tour of the premises and discussion with the homeowner. At this point assume the homeowner requests additional equipment including an extra camera, two (2) additional door/window sensors, one (1) glass break detector, and one (1) smoke detector.

[0306] d. Installer mounts SimonXT in the kitchen or other location in the home as directed by the homeowner, and routes the phone line to Simon XT if available. GPRS and Phone numbers pre-programmed in SimonXT to point to the provider Central Monitoring Station (CMS).

[0307] e. Installer places gateway in the home in the vicinity of a router and cable modem. Installer installs an ethernet line from gateway to router and plugs gateway into an electrical outlet.

2. Associate and Enroll gateway into SimonXT

[0308] a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with installer ID/pass.

[0309] b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer for kit ID (on box's barcode label).

[0310] c. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad. It is noted that this step is for security only and can be automated in an embodiment.

- [0311] d. Installer enters the installer code into the Simon XT. Installer Learns 'gateway' into the panel as a wireless keypad as a group 1 device.
- [0312] e. Installer goes back to Web portal, and clicks the 'Finished Adding SimonXT' button.
3. Enroll Sensors into SimonXT via iControl
- [0313] a. All devices in the Basic kit are already associated with the user's account.
- [0314] b. For additional devices, Installer clicks 'Add Device' and adds the additional camera to the user's account (by typing in the camera ID/Serial
- [0315] c. Installer clicks 'Add Device' and adds other sensors (two (2) door/window sensors, one (1) glass break sensor, and one (1) smoke sensor) to the account (e.g., by typing in IDs).
- [0316] d. As part of Add Device, Installer assigns zone, name, and group to the sensor. Installer puts appropriate Zone and Name sticker on the sensor temporarily.
- [0317] e. All sensor information for the account is pushed or otherwise propagated to the iConnect server, and is available to propagate to CMS automation software through the CMS application programming interface (API).
- [0318] f. Web interface displays 'Installing Sensors in System . . .' and automatically adds all of the sensors to the Simon XT panel through the GE RF link.
- [0319] g. Web interface displays 'Done Installing'-->all sensors show green.
4. Place and Tests Sensors in Home
- [0320] a. Installer physically mounts each sensor in its desired location, and removes the stickers.
- [0321] b. Installer physically mounts WiFi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
- [0322] c. Installer goes to Web interface and is prompted for automatic camera install. Each camera is provisioned as a private, encrypted Wifi device on the gateway secured sandbox network, and firewall NAT traversal is initiated. Upon completion the customer is prompted to test the security system.
- [0323] d. Installer selects the 'Test System' button on the web portal—the SimonXT is put into Test mode by the gateway over GE RF.
- [0324] e. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
- [0325] f. gateway sends test data directly to CMS over broadband link, as well as storing the test data in the user's account for subsequent report generation.
- [0326] g. Installer exits test mode from the Web portal.
5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the iControl web and mobile portals. Customer creates a username/password at this time.
6. Installer instructs customer how to change Simon XT user code from the Web interface. Customer changes user code which is pushed to SimonXT automatically over GE RF.
- [0327] An installation and enrollment procedure of a security system including an gateway is described below as an alternative example of the installation process. This installa-

tion process is for use for enrolling sensors into the SimonXT and integrated security system and is compatible with all existing GE Simon panels.

[0328] The integrated security system supports all pre-kitting functionality described in the installation process above. However, for the purpose of the following example, no kitting is used.

[0329] 1. Order and Physical Install Process

[0330] a. Once an order is generated in the iControl system, an account is created and an install ticket is created and sent electronically to the security system provider for assignment to an installer.

[0331] b. The assigned installer picks up his/her ticket (s) and fills his/her truck with individual sensors, cameras, iHubs, Simon XTs, etc. Optionally, the installer can also stock homeplug adapters for problematic installations.

[0332] c. The installer arrives at the address on the ticket, and analyzes the house and talks with the homeowner to determine sensor locations. At this point assume the homeowner requests three (3) cameras, five (5) door/window sensors, one (1) glass break detector, one (1) smoke detector, and one (1) keyfob.

[0333] d. Installer mounts SimonXT in the kitchen or other location in the home. The installer routes a phone line to Simon XT if available. GPRS and Phone numbers are pre-programmed in SimonXT to point to the provider CMS.

[0334] e. Installer places gateway in home in the vicinity of a router and cable modem, and installs an ethernet line from gateway to the router, and plugs gateway into an electrical outlet.

[0335] 2. Associate and Enroll gateway into SimonXT

[0336] a. Installer uses either his/her own laptop plugged into router, or homeowners computer to go to the integrated security system web interface and log in with an installer ID/pass.

[0337] b. Installer enters ticket number into admin interface, and clicks 'New Install' button. Screen prompts installer to add devices.

[0338] c. Installer types in ID of gateway, and it is associated with the user's account.

[0339] d. Installer clicks 'Add Device' and adds the cameras to the user's account (by typing in the camera ID/Serial #).

[0340] e. Installer clicks 'Add SimonXT'. Instructions prompt installer to put Simon XT into install mode, and add gateway as a wireless keypad.

[0341] f. Installer goes to Simon XT and enters the installer code into the Simon XT. Learns 'gateway' into the panel as a wireless keypad as group 1 type sensor.

[0342] g. Installer returns to Web portal, and clicks the 'Finished Adding SimonXT' button.

[0343] h. Gateway now is alerted to all subsequent installs over the security system RF.

[0344] 3. Enroll Sensors into SimonXT via iControl

[0345] a. Installer clicks 'Add Simon XT Sensors'—Displays instructions for adding sensors to Simon XT.

[0346] b. Installer goes to Simon XT and uses Simon XT install process to add each sensor, assigning zone, name, group. These assignments are recorded for later use.

- [0347] c. The gateway automatically detects each sensor addition and adds the new sensor to the integrated security system.
- [0348] d. Installer exits install mode on the Simon XT, and returns to the Web portal.
- [0349] e. Installer clicks 'Done Adding Devices'.
- [0350] f. Installer enters zone/sensor naming from recorded notes into integrated security system to associate sensors to friendly names.
- [0351] g. All sensor information for the account is pushed to the iConnect server, and is available to propagate to CMS automation software through the CMS API.
- [0352] 4. Place and Tests Sensors in Home
- [0353] a. Installer physically mounts each sensor in its desired location.
- [0354] b. Installer physically mounts Wifi cameras in their location and plugs into AC power. Optional fishing of low voltage wire through wall to remove dangling wires. Camera transformer is still plugged into outlet but wire is now inside the wall.
- [0355] c. Installer puts SimonXT into Test mode from the keypad.
- [0356] d. Installer manually tests the operation of each sensor, receiving an audible confirmation from SimonXT.
- [0357] e. Installer exits test mode from the Simon XT keypad.
- [0358] f. Installer returns to web interface and is prompted to automatically set up cameras. After waiting for completion cameras are now provisioned and operational.
- [0359] 5. Installer instructs customer on use of the Simon XT, and shows customer how to log into the integrated security system web and mobile portals. Customer creates a username/password at this time.
- [0360] 6. Customer and Installer observe that all sensors/cameras are green.
- [0361] 7. Installer instructs customer how to change Simon XT user code from the keypad. Customer changes user code and stores in SimonXT.
- [0362] 8. The first time the customer uses the web portal to Arm/Disarm system the web interface prompts the customer for the user code, which is then stored securely on the server. In the event the user code is changed on the panel the web interface once again prompts the customer.
- [0363] The panel of an embodiment can be programmed remotely. The CMS pushes new programming to SimonXT over a telephone or GPRS link. Optionally, iControl and GE provide a broadband link or coupling to the gateway and then a link from the gateway to the Simon XT over GE RF.
- [0364] As described above, computer networks suitable for use with the embodiments described herein include local area networks (LAN), wide area networks (WAN), Internet, or other connection services and network variations such as the world wide web, the public internet, a private internet, a private computer network, a public network, a mobile network, a cellular network, a value-added network, and the like. Computing devices coupled or connected to the network may be any microprocessor controlled device that permits access to the network, including terminal devices, such as personal computers, workstations, servers, mini computers, main-frame computers, laptop computers, mobile computers, palm

top computers, hand held computers, mobile phones, TV set-top boxes, or combinations thereof. The computer network may include one of more LANs, WANs, Internets, and computers. The computers may serve as servers, clients, or a combination thereof.

[0365] The integrated security system can be a component of a single system, multiple systems, and/or geographically separate systems. The integrated security system can also be a subcomponent or subsystem of a single system, multiple systems, and/or geographically separate systems. The integrated security system can be coupled to one or more other components (not shown) of a host system or a system coupled to the host system.

[0366] One or more components of the integrated security system and/or a corresponding system or application to which the integrated security system is coupled or connected includes and/or runs under and/or in association with a processing system. The processing system includes any collection of processor-based devices or computing devices operating together, or components of processing systems or devices, as is known in the art. For example, the processing system can include one or more of a portable computer, portable communication device operating in a communication network, and/or a network server. The portable computer can be any of a number and/or combination of devices selected from among personal computers, personal digital assistants, portable computing devices, and portable communication devices, but is not so limited. The processing system can include components within a larger computer system.

[0367] The processing system of an embodiment includes at least one processor and at least one memory device or subsystem. The processing system can also include or be coupled to at least one database. The term "processor" as generally used herein refers to any logic processing unit, such as one or more central processing units (CPUs), digital signal processors (DSPs), application-specific integrated circuits (ASIC), etc. The processor and memory can be monolithically integrated onto a single chip, distributed among a number of chips or components, and/or provided by some combination of algorithms. The methods described herein can be implemented in one or more of software algorithm(s), programs, firmware, hardware, components, circuitry, in any combination.

[0368] The components of any system that includes the integrated security system can be located together or in separate locations. Communication paths couple the components and include any medium for communicating or transferring files among the components. The communication paths include wireless connections, wired connections, and hybrid wireless/wired connections. The communication paths also include couplings or connections to networks including local area networks (LANs), metropolitan area networks (MANs), wide area networks (WANs), proprietary networks, interoffice or backend networks, and the Internet. Furthermore, the communication paths include removable fixed mediums like floppy disks, hard disk drives, and CD-ROM disks, as well as flash RAM, Universal Serial Bus (USB) connections, RS-232 connections, telephone lines, buses, and electronic mail messages.

[0369] Embodiments of the integrated security system described herein include a system comprising: a gateway located at a first location; a video engine coupled to the gateway, the video engine automatically establishing a coupling with a camera device installed at the first location,

wherein the video engine forms a segregated network with the camera device via the coupling; and a security server located at a second location different from the first location, the security server coupled to the gateway, the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location.

[0370] The gateway of an embodiment is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location.

[0371] The gateway of an embodiment is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

[0372] The gateway of an embodiment is coupled to the security server via the internet.

[0373] The routing of an embodiment is Universal Plug and Play port forwarding.

[0374] The routing of an embodiment is relay server routing.

[0375] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0376] The video stream of an embodiment is encrypted.

[0377] The gateway of an embodiment encrypts the video stream received from the camera device.

[0378] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream.

[0379] The requesting client device of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the security server.

[0380] The security server of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device.

[0381] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0382] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Hypertext Transfer Protocol (HTTP) video stream.

[0383] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0384] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0385] The video stream of an embodiment is a Motion Joint Photographic Experts Group (JPEG) (MJPEG) video stream.

[0386] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0387] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0388] A format of the video stream of an embodiment is automatically selected by at least one of the gateway and the security server.

[0389] The format of an embodiment is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

[0390] The format of an embodiment is selected based on a capability of the requesting client device.

[0391] The format of an embodiment is selected based on a capability of the camera device.

[0392] The format of an embodiment is selected based on an authentication requirement of the requesting client device.

[0393] The format of an embodiment is selected based on a privacy requirement of the requesting client device.

[0394] The format of an embodiment is selected based on a determined capability of a network coupling the gateway to the requesting client device, wherein the determined capability is determined by at least one of the gateway and the security server.

[0395] The determined capability of an embodiment is relative success among a plurality of routings of the video stream.

[0396] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0397] The determined capability of an embodiment is relative success of Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0398] The determined capability of an embodiment is bandwidth availability of the requesting client device.

[0399] The determined capability of an embodiment is processing capability of the requesting client device.

[0400] The determined capability of an embodiment is bandwidth availability of the camera device.

[0401] The format of the video stream of an embodiment is automatically selected according to a priority.

[0402] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a first priority.

[0403] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a second priority.

[0404] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a third priority.

[0405] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol (HTTP) video stream has a fourth priority.

[0406] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream has a fifth priority, wherein the gateway encrypts the video stream from the camera device.

[0407] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a sixth priority, wherein the gateway encrypts the video stream from the camera device.

[0408] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) Hyper-

text Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a seventh priority.

[0409] The system of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has an eighth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0410] The system of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has a ninth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein one of the gateway and the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0411] The system of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has a tenth priority, wherein the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0412] The system of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has an eleventh priority, wherein one of the gateway and the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0413] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol (HTTP) video stream has a twelfth priority.

[0414] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a thirteenth priority, wherein the security server facilitates routing.

[0415] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a fourteenth priority, wherein one of the gateway and the security server facilitates routing.

[0416] The requesting client device of an embodiment includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

[0417] The gateway of an embodiment performs audio streaming between a first device and a second device, wherein the first device is located behind the gateway at the first location and the second device is located outside the gateway at a remote location.

[0418] The gateway of an embodiment performs a data transfer between a first device and a second device, wherein the first device is located behind the gateway at the first location and the second device is located outside the gateway at a remote location.

[0419] The data transfer of an embodiment uses Transmission Control Protocol (TCP).

[0420] The data transfer of an embodiment uses User Datagram Protocol (UDP).

[0421] The data transfer of an embodiment uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

[0422] The gateway of an embodiment is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

[0423] The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

[0424] The gateway of an embodiment automatically discovers the security system components.

[0425] The gateway of an embodiment includes protocols of the security system from the security server and uses the protocols to discover the security system components.

[0426] The gateway of an embodiment requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components.

[0427] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0428] The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

[0429] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0430] The gateway of an embodiment includes definitions of the security system components.

[0431] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0432] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0433] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0434] The secondary communication link of an embodiment includes a broadband coupling.

[0435] The secondary communication link of an embodiment includes a cellular coupling.

[0436] The gateway of an embodiment transmits messages comprising event data of the security system components to the requesting client device over the secondary communication link.

[0437] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0438] The gateway of an embodiment receives control data for control of the security system components from the requesting client device via the secondary communication link.

[0439] Embodiments of the integrated security system described herein include a system comprising: a gateway including a video engine located at a first location, the gateway coupled to a local area network (LAN) of the first location, the video engine automatically establishing a coupling with a camera device installed at the first location, wherein the video engine forms a segregated network with the camera device via the coupling; and a security server located at a second location different from the first location, wherein the security server is coupled to the gateway using a wide area network (WAN), the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location.

[0440] Embodiments of the integrated security system described herein include a system comprising: a gateway located at a first location, the gateway coupled to a local area network (LAN) of the first location; a video engine coupled to the gateway, the video engine automatically establishing a coupling with a camera device installed at the first location, wherein the video engine forms a segregated network with the camera device via the coupling; and a security server located at a second location different from the first location, wherein the security server is coupled to the gateway using a wide area network (WAN), the security server and the video engine communicating to control routing of a video stream from the camera device to a requesting client device, the requesting client device remote to the first location and the second location.

[0441] Embodiments of the integrated security system described herein include a system comprising: a gateway including a video engine located at a first location, the gateway coupled to a local area network (LAN) of the first location, the video engine automatically establishing a coupling with a camera device installed at the first location, wherein the video engine forms a segregated network with the camera device via the coupling; a security server located at a second location different from the first location, wherein the security server is coupled to the gateway using a wide area network (WAN), the security server and the video engine communicating to; and an interface coupled to the gateway and the security server, the interface receiving requests from a requesting client device for a video stream from the camera device and providing the video stream from the camera device to the requesting client device, the requesting client device remote to the first location and the second location.

[0442] Embodiments of the integrated security system described herein include a system comprising: a security network comprising a gateway coupled to a security system and located at a first location, the security system including a plurality of security system components, the security network comprising a plurality of camera devices installed at the first location and coupled to the gateway via a secure network, wherein the gateway automatically establishes a coupling with the camera devices; and a security server located at a second location different from the first location, the security server coupled to the gateway, the security server and the gateway communicating to control routing of a video stream from the camera devices to a requesting client device, the requesting client device remote to the first location and the second location.

[0443] The gateway of an embodiment is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location.

[0444] The gateway of an embodiment is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

[0445] The gateway of an embodiment is coupled to the security server via the internet.

[0446] The routing of an embodiment is Universal Plug and Play port forwarding.

[0447] The routing of an embodiment is relay server routing.

[0448] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0449] The video stream of an embodiment is encrypted.

[0450] The gateway of an embodiment encrypts the video stream received from the camera device.

[0451] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream.

[0452] The requesting client device of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the security server.

[0453] The security server of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device.

[0454] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0455] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Hypertext Transfer Protocol (HTTP) video stream.

[0456] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0457] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0458] The video stream of an embodiment is a Motion Joint Photographic Experts Group (JPEG) (MJPEG) video stream.

[0459] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0460] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0461] A format of the video stream of an embodiment is automatically selected by at least one of the gateway and the security server.

[0462] The format of an embodiment is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

[0463] The format of an embodiment is selected based on a capability of the requesting client device.

[0464] The format of an embodiment is selected based on a capability of the camera device.

[0465] The format of an embodiment is selected based on an authentication requirement of the requesting client device.

[0466] The format of an embodiment is selected based on a privacy requirement of the requesting client device.

[0467] The format of an embodiment is selected based on a determined capability of a network coupling the gateway to the requesting client device, wherein the determined capability is determined by at least one of the gateway and the security server.

[0468] The determined capability of an embodiment is relative success among a plurality of routings of the video stream.

[0469] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0470] The determined capability of an embodiment is relative success of Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0471] The determined capability of an embodiment is bandwidth availability of the requesting client device.

[0472] The determined capability of an embodiment is processing capability of the requesting client device.

[0473] The determined capability of an embodiment is bandwidth availability of the camera device.

[0474] The format of the video stream of an embodiment is automatically selected according to a priority.

[0475] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a first priority.

[0476] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a second priority.

[0477] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a third priority.

[0478] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol (HTTP) video stream has a fourth priority.

[0479] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream has a fifth priority, wherein the gateway encrypts the video stream from the camera device.

[0480] The system of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a sixth priority, wherein the gateway encrypts the video stream from the camera device.

[0481] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a seventh priority.

[0482] The system of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has an eighth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server facilitates Simple Traversal of User Datagram Protocol

(UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0483] The system of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has a ninth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein one of the gateway and the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0484] The system of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has a tenth priority, wherein the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0485] The system of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has an eleventh priority, wherein one of the gateway and the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0486] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol (HTTP) video stream has a twelfth priority.

[0487] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a thirteenth priority, wherein the security server facilitates routing.

[0488] The system of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a fourteenth priority, wherein one of the gateway and the security server facilitates routing.

[0489] The requesting client device of an embodiment includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

[0490] The gateway of an embodiment is coupled via a wireless coupling to the security system installed at the first location, wherein the gateway integrates communications and functions of the security system components into the security network via the wireless coupling.

[0491] The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

[0492] The gateway of an embodiment automatically discovers the security system components.

[0493] The gateway of an embodiment includes protocols of the security system from the security server and uses the protocols to discover the security system components.

[0494] The gateway of an embodiment requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components.

[0495] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0496] The gateway of an embodiment automatically establishes the coupling with the security system including the security system components.

[0497] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0498] The gateway of an embodiment includes definitions of the security system components.

[0499] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0500] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0501] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0502] The secondary communication link of an embodiment includes a broadband coupling.

[0503] The secondary communication link of an embodiment includes a cellular coupling.

[0504] The gateway of an embodiment transmits messages comprising event data of the security system components to the requesting client device over the secondary communication link.

[0505] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0506] The gateway of an embodiment receives control data for control of the security system components from the requesting client device via the secondary communication link.

[0507] The security network of an embodiment comprises network devices coupled to the gateway via a wireless coupling.

[0508] The gateway of an embodiment automatically discovers the network devices.

[0509] The gateway of an embodiment automatically installs the network devices in the security network.

[0510] The gateway of an embodiment automatically configures the network devices for operation in the security network.

[0511] The gateway of an embodiment controls communications between the network devices, the security system components, and the security server.

[0512] The gateway of an embodiment transmits event data of the network devices to the requesting client device over at least one of a plurality of communication links.

[0513] The gateway of an embodiment receives control data for control of the network devices from the requesting client device via at least one of the plurality of communication links.

[0514] The event data of an embodiment comprises changes in device states of the network devices, data of the network devices, and data received by the network devices.

[0515] The security server of an embodiment creates, modifies and terminates couplings between the gateway and the network devices.

[0516] The security server of an embodiment performs creation, modification, deletion and configuration of the network devices.

[0517] The security server of an embodiment creates automations, schedules and notification rules associated with the network devices.

[0518] The security server of an embodiment manages access to current and logged state data for the network devices.

[0519] The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the network devices.

[0520] The security server of an embodiment manages communications with the network devices.

[0521] The network device of an embodiment is an Internet Protocol device.

[0522] The network device of an embodiment is a camera.

[0523] The network device of an embodiment is a touch-screen.

[0524] The network device of an embodiment is a device controller that controls an attached device.

[0525] The network device of an embodiment is a sensor.

[0526] The security server of an embodiment creates, modifies and terminates users corresponding to the security system.

[0527] The security server of an embodiment creates, modifies and terminates couplings between the gateway and the security system components.

[0528] The security server of an embodiment performs creation, modification, deletion and configuration of the security system components.

[0529] The security server of an embodiment creates automations, schedules and notification rules associated with the security system components.

[0530] The security server of an embodiment manages access to current and logged state data for the security system components.

[0531] The security server of an embodiment manages access to current and logged state data for couplings between the gateway and the security system components.

[0532] The security server of an embodiment manages communications with the security system components.

[0533] The security server of an embodiment generates and transfers notifications to the requesting client device, the notifications comprising event data.

[0534] The notifications of an embodiment include one or more of short message service messages and electronic mail messages.

[0535] The event data of an embodiment is event data of the security system components.

[0536] The security system components of an embodiment include one or more of sensors, cameras, input/output (I/O) devices, and accessory controllers.

[0537] Embodiments of the integrated security system described herein include a system comprising: a security network comprising a gateway coupled to a security system and located at a first location, the security system including a plurality of security system components, the security network comprising a plurality of camera devices installed at the first location and coupled to the gateway via a secure network, wherein the gateway electronically integrates communications and functions of the camera devices with the security system components; and a security server located at a second location different from the first location, the security server coupled to the security network via the gateway, the security server and the gateway communicating to control routing of a

video stream from the camera devices to a requesting client device, the requesting client device remote to the first location and the second location.

[0538] Embodiments of the integrated security system described herein include a system comprising: a security network comprising a gateway coupled to a security server, wherein the gateway is located at a first location and coupled to a security system, the security system including security system components located at the first location, wherein the security server is located at a second location different from the first location; and a plurality of premise devices including cameras located at the first location and coupled to the gateway, wherein the gateway electronically integrates communications and functions of the plurality of premise devices and the security system components into the security network, wherein the gateway controls routing of a video stream from the cameras to a requesting client device, the requesting client device remote to the first location and the second location.

[0539] Embodiments of the integrated security system described herein include a security network comprising: a gateway, wherein the gateway is coupled to a security system that includes a plurality of security system components that are proprietary to the security system; a plurality of cameras coupled to the gateway, wherein the gateway forms a premise security network at a first location and couples the premise security network to a local area network of the first location, wherein the gateway forms the premise security network by automatically establishing a coupling with the plurality of cameras; and an application server located at a second location different from the first location, the application server coupled to the premise security network via the gateway and a communication network, the application server and the gateway controlling delivery of a video stream from the plurality of cameras to a remote client device.

[0540] Embodiments of the integrated security system described herein include a device comprising: a gateway comprising a processor, the gateway located at a first location; a connection management component coupled to the processor, the connection management component automatically establishing a coupling with a security system installed at the first location, the security system including security system components, wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the coupling; and a video engine coupled to the processor, the video engine automatically forming a segregated network including a camera device installed at the first location, the video engine controlling routing of a video stream from the camera device to a requesting client device that is remote to the first location.

[0541] The gateway of an embodiment is connected to a local area network (LAN) at the first location, and the LAN is coupled to a wide area network (WAN) via a router at the first location.

[0542] The gateway of an embodiment is coupled to a security server located at a second location different from the first location, wherein the security server is coupled to the WAN, the security server and the video engine communicating to control the routing of the video stream from the camera device to a requesting client device, the requesting client device remote to the second location.

[0543] The gateway of an embodiment is coupled to a wide area network (WAN) and is coupled to a local area network (LAN) at the first location via the connection management

component and a router at the first location, wherein the security server is coupled to the WAN.

[0544] The gateway of an embodiment is coupled to a security server located at a second location different from the first location, wherein the security server is coupled to the WAN, the security server and the video engine communicating to control the routing of the video stream from the camera device to a requesting client device, the requesting client device remote to the second location.

[0545] The routing of an embodiment is Universal Plug and Play port forwarding.

[0546] The routing of an embodiment is relay server routing.

[0547] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0548] The video stream of an embodiment is encrypted.

[0549] The gateway of an embodiment encrypts the video stream received from the camera device.

[0550] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream.

[0551] The video stream of an embodiment is a reverse of the MPEG-4/RTSP video stream such that a security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server is located at a second location different from the first location.

[0552] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0553] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Hypertext Transfer Protocol (HTTP) video stream.

[0554] The video stream of an embodiment is a reverse of the MPEG-4 over HTTP video stream such that a security server initiates and establishes a HTTP Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server is located at a second location different from the first location.

[0555] The video stream of an embodiment is a Motion Joint Photographic Experts Group (JPEG) (MJPEG) video stream.

[0556] The video stream of an embodiment is a reverse of the MJPEG video stream such that a security server initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server is located at a second location different from the first location.

[0557] A format of the video stream of an embodiment is automatically selected by at least one of a gateway and a security server, wherein the security server is located at a second location different from the first location.

[0558] The format of an embodiment is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

[0559] The format of an embodiment is selected based on a capability of the requesting client device.

[0560] The format of an embodiment is selected based on a capability of the camera device.

[0561] The format of an embodiment is selected based on an authentication requirement of the requesting client device.

[0562] The format of an embodiment is selected based on a privacy requirement of the requesting client device.

[0563] The format of an embodiment is selected based on a determined capability of a network coupling the gateway to the requesting client device, wherein the determined capability is determined by at least one of the gateway and a security server, wherein the security server is located at a second location different from the first location.

[0564] The determined capability of an embodiment is relative success among a plurality of routings of the video stream.

[0565] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0566] The determined capability of an embodiment is relative success of Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0567] The determined capability of an embodiment is bandwidth availability of the requesting client device.

[0568] The determined capability of an embodiment is processing capability of the requesting client device.

[0569] The determined capability of an embodiment is bandwidth availability of the camera device.

[0570] The format of the video stream of an embodiment is automatically selected according to a priority.

[0571] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a first priority.

[0572] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a second priority.

[0573] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a third priority.

[0574] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol (HTTP) video stream has a fourth priority.

[0575] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream has a fifth priority, wherein the gateway encrypts the video stream from the camera device.

[0576] The device of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a sixth priority, wherein the gateway encrypts the video stream from the camera device.

[0577] The device of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a seventh priority.

[0578] The device of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has an eighth priority, wherein a security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing,

wherein the security server is located at a second location different from the first location.

[0579] The device of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has a ninth priority, wherein a security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein one of the gateway and the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing, wherein the security server is located at a second location different from the first location.

[0580] The device of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has a tenth priority, wherein a security server facilitates Hypertext Transfer Protocol (HTTP) routing, wherein the security server is located at a second location different from the first location.

[0581] The device of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has an eleventh priority, wherein one of the gateway and a security server facilitates Hypertext Transfer Protocol (HTTP) routing, wherein the security server is located at a second location different from the first location.

[0582] The device of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol (HTTP) video stream has a twelfth priority.

[0583] The device of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a thirteenth priority, wherein a security server facilitates routing, wherein the security server is located at a second location different from the first location.

[0584] The device of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a fourteenth priority, wherein one of the gateway and a security server facilitates routing, wherein the security server is located at a second location different from the first location.

[0585] The requesting client device of an embodiment includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

[0586] The gateway of an embodiment is coupled via a wireless coupling to the security system.

[0587] The device of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

[0588] The gateway of an embodiment automatically discovers the security system components.

[0589] The gateway of an embodiment uses protocols of the security system to discover the security system components.

[0590] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0591] The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

[0592] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0593] The gateway of an embodiment includes definitions of the security system components.

[0594] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0595] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0596] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0597] The secondary communication link of an embodiment includes a broadband coupling.

[0598] The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

[0599] The gateway of an embodiment transmits messages comprising event data of the security system components to the requesting client device over the secondary communication link.

[0600] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0601] The gateway of an embodiment receives control data for control of the security system components from the requesting client device via the secondary communication link.

[0602] Embodiments of the integrated security system described herein include a device comprising: a gateway including a video engine and a connection management component located at a first location, the gateway coupled to a local area network (LAN) of the first location; wherein the video engine automatically forms a device network including a plurality of camera devices installed at the first location by coupling with the plurality of camera devices; wherein the connection management component automatically forms a security network by coupling with security system components of a security system installed at the first location; wherein the security network integrates communications and functions of the device network and the security system.

[0603] Embodiments of the integrated security system described herein include a device comprising: a gateway comprising a processor, the gateway located at a first location; a connection management component coupled to the processor, the connection management component automatically establishing a coupling with a security system installed at the first location, the security system including security system components, wherein the connection management component forms a security network that integrates communications and functions of the security system components into the security network via the coupling; and a video engine coupled to the processor, the video engine automatically forming a segregated network including a plurality of premise devices installed at the first location, the plurality of premise devices including at least one camera device, the video engine con-

trolling routing of a data from the premise devices to a requesting client device that is remote to the first location.

[0604] Embodiments of the integrated security system described herein include a system comprising: a gateway located at a first location; a plurality of camera devices installed at the first location and coupled to the gateway via a secure network, wherein the gateway establishes the secure network; a firewall coupled between the gateway and a wide area network (WAN); a server coupled to the gateway via the WAN, the server located at a second location; the gateway and the server communicating to control routing of a video stream from at least one camera device of the plurality of camera devices to the client device in response to a request for live video received from the client device, wherein the routing uses a network protocol selected from a plurality of network protocols in response to capabilities of the firewall, wherein the client device is remote to the first location and the second location.

[0605] The network protocol of an embodiment is Universal Plug and Play (UPnP) port forwarding, wherein the UPnP opens a port of the firewall.

[0606] The system of an embodiment, wherein, if UPnP port forwarding fails, the gateway and the server use Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN) to bypass the firewall and establish a peer-to-peer coupling.

[0607] The system of an embodiment, wherein, if STUN fails, the server relays the video stream.

[0608] The video stream of an embodiment is encrypted.

[0609] The gateway of an embodiment encrypts the video stream received from the camera devices.

[0610] A format of the video stream of an embodiment is automatically selected by at least one of the gateway and the server.

[0611] The format of an embodiment is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

[0612] The format of an embodiment is selected based on a capability of the client device.

[0613] The format of an embodiment is selected based on a capability of the camera device.

[0614] The format of an embodiment is selected based on an authentication requirement of the client device.

[0615] The format of an embodiment is selected based on a privacy requirement of the client device.

[0616] The format of an embodiment is selected based on a determined capability of the WAN, wherein the determined capability is determined by at least one of the gateway and the server.

[0617] The determined capability of an embodiment is relative success among a plurality of routings of the video stream.

[0618] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0619] The determined capability of an embodiment is relative success of peer-to-peer routing.

[0620] The determined capability of an embodiment is bandwidth availability of the client device.

[0621] The determined capability of an embodiment is processing capability of the client device.

[0622] The determined capability of an embodiment is bandwidth availability of the camera devices.

[0623] The format of the video stream of an embodiment is automatically selected according to a priority.

[0624] The client device of an embodiment includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

[0625] The gateway of an embodiment is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

[0626] The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network via the client device.

[0627] The gateway of an embodiment automatically discovers the security system components.

[0628] The gateway of an embodiment includes protocols of the security system from the server and uses the protocols to discover the security system components.

[0629] The gateway of an embodiment requests and receives protocols of the security system from the server, wherein the gateway uses the protocols received to discover the security system components.

[0630] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0631] The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

[0632] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0633] The gateway of an embodiment includes definitions of the security system components.

[0634] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0635] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0636] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0637] The event data of an embodiment comprises changes data and information of the plurality of camera devices.

[0638] The secondary communication link of an embodiment includes a broadband coupling.

[0639] The secondary communication link of an embodiment includes a cellular coupling.

[0640] The gateway of an embodiment transmits messages comprising event data of the security system components to the client device over the secondary communication link.

[0641] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0642] The gateway of an embodiment receives control data for control of the security system components from the client device via the secondary communication link.

[0643] Embodiments of the integrated security system described herein include a system comprising: a gateway located at a first location; a plurality of Internet Protocol (IP) devices installed at the first location and coupled to the gateway via a private network, wherein the private network is segregated from any other network at the first location, the gateway automatically establishing the private network, the establishing comprising provisioning identifiers and passwords to the plurality of IP devices; a router coupled between the gateway and a wide area network (WAN), the router providing WAN access to the gateway and the plurality of IP devices; and a server coupled to the gateway, the server located at a second location different from the first location.

[0644] The gateway of an embodiment is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

[0645] The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network via a client device remote to the first location and the second location.

[0646] The gateway of an embodiment automatically discovers the security system components.

[0647] The gateway of an embodiment includes protocols of the security system from the server and uses the protocols to discover the security system components.

[0648] The gateway of an embodiment requests and receives protocols of the security system from the server, wherein the gateway uses the protocols received to discover the security system components.

[0649] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0650] The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

[0651] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0652] The gateway of an embodiment includes definitions of the security system components.

[0653] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0654] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0655] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0656] The event data of an embodiment comprises changes data and information of the plurality of IP devices.

[0657] The secondary communication link of an embodiment includes a broadband coupling.

[0658] The secondary communication link of an embodiment includes a cellular coupling.

[0659] The gateway of an embodiment transmits messages comprising event data of the security system components to a client device over the secondary communication link, wherein the client device is remote to the first location and the second location.

[0660] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0661] The gateway of an embodiment receives control data for control of the security system components from a client device via the secondary communication link, wherein the client device is remote to the first location and the second location.

[0662] The gateway and the server of an embodiment communicate to control routing of a data stream from at least one IP device of the plurality of IP devices to a client device in response to a request for the data stream received from the client device, wherein the routing uses a network protocol selected from a plurality of network protocols in response to capabilities of the firewall, wherein the client device is remote to the first location and the second location.

[0663] The network protocol of an embodiment is Universal Plug and Play (UPnP) port forwarding, wherein the UPnP opens a port of the firewall.

[0664] The system of an embodiment, wherein, if UPnP port forwarding fails, the gateway and the server use Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN) to bypass the firewall and establish a peer-to-peer coupling.

[0665] The system of an embodiment, wherein, if STUN fails, the server relays the data stream.

[0666] The data stream of an embodiment is encrypted.

[0667] The gateway of an embodiment encrypts the data stream received from the IP devices.

[0668] A format of the data stream of an embodiment is automatically selected by at least one of the gateway and the server.

[0669] The format of an embodiment is selected based on a capability of the client device.

[0670] The format of an embodiment is selected based on a capability of the IP device.

[0671] The format of an embodiment is selected based on an authentication requirement of the client device.

[0672] The format of an embodiment is selected based on a privacy requirement of the client device.

[0673] The format of an embodiment is selected based on a determined capability of the WAN, wherein the determined capability is determined by at least one of the gateway and the server.

[0674] The determined capability of an embodiment is relative success among a plurality of routings of the data stream.

[0675] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0676] The determined capability of an embodiment is relative success of peer-to-peer routing.

[0677] The determined capability of an embodiment is bandwidth availability of the client device.

[0678] The determined capability of an embodiment is processing capability of the client device.

[0679] The determined capability of an embodiment is bandwidth availability of the IP devices.

[0680] The format of the data stream of an embodiment is automatically selected according to a priority.

[0681] Embodiments of the integrated security system described herein include a system comprising: a gateway located at a first location and coupled to a wide area network (WAN); a plurality of Internet Protocol (IP) devices installed at the first location and coupled to the gateway via a private network, wherein the private network is segregated from any other network at the first location, the gateway automatically establishing the private network, the establishing comprising provisioning identifiers and passwords to the plurality of IP devices; a router coupled between the gateway and a local area network (LAN) of the first location, the gateway providing WAN access to the plurality of IP devices and the LAN; and a server coupled to the gateway, the server located at a second location different from the first location.

[0682] Embodiments of the integrated security system described herein include a method comprising: coupling a gateway comprising a video engine to a network located at a first location; forming a device network by automatically establishing a coupling between the video engine and a camera device installed at the first location; establishing communication between the gateway and a security server located at a second location different from the first location; and controlling routing of a video stream from the camera device to a requesting client device via communications between the security server and the video engine, the requesting client device remote to the first location and the second location.

[0683] The gateway of an embodiment is connected to a local area network at the first location, and the local area network is coupled to a wide area network via a router at the first location.

[0684] The gateway of an embodiment is coupled to a wide area network and is coupled to a local area network at the first location via the connection management component and a router at the first location.

[0685] The gateway of an embodiment is coupled to the security server via the internet.

[0686] The routing of an embodiment is Universal Plug and Play port forwarding.

[0687] The routing of an embodiment is relay server routing.

[0688] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0689] The method of an embodiment comprises encrypting the video stream.

[0690] The gateway of an embodiment encrypts the video stream received from the camera device. The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream.

[0691] The requesting client device of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the security server.

[0692] The security server of an embodiment initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device.

[0693] The routing of an embodiment is Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0694] The video stream of an embodiment is a Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Hypertext Transfer Protocol (HTTP) video stream.

[0695] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0696] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0697] The video stream of an embodiment is a Motion Joint Photographic Experts Group (JPEG) (MJPEG) video stream.

[0698] The requesting client device of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the security server.

[0699] The security server of an embodiment initiates and establishes a Hypertext Transfer Protocol (HTTP) Transmission Control Protocol (TCP) connection with the requesting client device.

[0700] The system of an embodiment comprises at least one of the gateway and the security server automatically selecting a format of the video stream.

[0701] The format of an embodiment is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

[0702] The format of an embodiment is selected based on a capability of the requesting client device.

[0703] The format of an embodiment is selected based on a capability of the camera device.

[0704] The format of an embodiment is selected based on an authentication requirement of the requesting client device.

[0705] The format of an embodiment is selected based on a privacy requirement of the requesting client device.

[0706] The format of an embodiment is selected based on a determined capability of a network coupling the gateway to the requesting client device, wherein the determined capability is determined by at least one of the gateway and the security server.

[0707] The determined capability of an embodiment is relative success among a plurality of routings of the video stream.

[0708] The determined capability of an embodiment is relative success of Universal Plug and Play port forwarding.

[0709] The determined capability of an embodiment is relative success of Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0710] The determined capability of an embodiment is bandwidth availability of the requesting client device.

[0711] The determined capability of an embodiment is processing capability of the requesting client device.

[0712] The determined capability of an embodiment is bandwidth availability of the camera device.

[0713] The system of an embodiment comprises automatically selecting the format of the video stream according to a priority.

[0714] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a first priority.

[0715] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream with encryption has a second priority.

[0716] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a third priority.

[0717] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol (HTTP) video stream has a fourth priority.

[0718] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) video stream has a fifth priority, wherein the gateway encrypts the video stream from the camera device.

[0719] The method of an embodiment, wherein a Motion Picture Experts Group (MPEG)-4 (MPEG-4) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a sixth priority, wherein the gateway encrypts the video stream from the camera device.

[0720] The method of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a seventh priority.

[0721] The method of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has an eighth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0722] The method of an embodiment, wherein a Reverse Real-Time Streaming Protocol (RTSP) video stream has a ninth priority, wherein the security server initiates and establishes a Transmission Control Protocol (TCP) connection with the requesting client device, wherein one of the gateway and the security server facilitates Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN)/Traversal Using Relay NAT (TURN) peer-to-peer routing.

[0723] The method of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has a tenth priority, wherein the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0724] The method of an embodiment, wherein a Reverse Motion Picture Experts Group (MPEG)-4 (MPEG-4) over Real-Time Streaming Protocol (RTSP) video stream has an eleventh priority, wherein one of the gateway and the security server facilitates Hypertext Transfer Protocol (HTTP) routing.

[0725] The method of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol (HTTP) video stream has a twelfth priority.

[0726] The method of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a thirteenth priority, wherein the security server facilitates routing.

[0727] The method of an embodiment, wherein a Motion Joint Photographic Experts Group (JPEG) (MJPEG) over Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) video stream has a fourteenth priority, wherein one of the gateway and the security server facilitates routing.

[0728] The requesting client device of an embodiment includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

[0729] The system of an embodiment comprises coupling the gateway via a wireless coupling to a security system installed at the first location, the security system including security system components, the gateway forming a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

[0730] The system of an embodiment comprises an interface coupled to the security network, wherein the interface allows control of the functions of the security network by a user.

[0731] The gateway of an embodiment automatically discovers the security system components.

[0732] The gateway of an embodiment includes protocols of the security system from the security server and uses the protocols to discover the security system components.

[0733] The gateway of an embodiment requests and receives protocols of the security system from the security server, wherein the gateway uses the protocols received to discover the security system components.

[0734] The gateway of an embodiment automatically establishes and controls the communications with the security system components.

[0735] The gateway of an embodiment automatically establishes a coupling with the security system including the security system components.

[0736] The gateway of an embodiment manages rules of interaction between the gateway and the security system components.

[0737] The gateway of an embodiment includes definitions of the security system components.

[0738] The security system of an embodiment is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

[0739] The gateway of an embodiment transmits event data of the security system components to the central monitoring station over the secondary communication link.

[0740] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0741] The secondary communication link of an embodiment includes a broadband coupling.

[0742] The secondary communication link of an embodiment includes a General Packet Radio Service (GPRS) coupling.

[0743] The gateway of an embodiment transmits messages comprising event data of the security system components to the requesting client device over the secondary communication link.

[0744] The event data of an embodiment comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

[0745] The gateway of an embodiment receives control data for control of the security system components from the requesting client device via the secondary communication link.

[0746] Embodiments of the integrated security system described herein include a method comprising: coupling a gateway including a video engine and a connection management component to a local area network (LAN) located at a first location; automatically forming a device network by establishing a coupling between the video engine and a plurality of camera devices installed at the first location; and automatically forming a security network by establishing a coupling between the connection management component and security system components of a security system installed at the first location, wherein the security network integrates communications and functions of the device network and the security system.

[0747] Embodiments of the integrated security system described herein include a method comprising: coupling a gateway comprising a processor to a network located at a first location; forming a security network by automatically establishing a coupling between a connection management component coupled to the processor and a security system installed at the first location, the security system including security system components, wherein forming the security network includes integrating communications and functions of the security system components into the security network; forming a device network by automatically establishing a coupling between a video engine coupled to the processor and a camera device installed at the first location; and controlling via the gateway routing of a video stream from the camera device to a requesting client device that is remote to the first location.

[0748] Aspects of the integrated security system and corresponding systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the integrated security system and corresponding systems and methods include: microcontrollers with memory (such as electronically erasable programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the integrated security system and corresponding systems and methods may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies

like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

[0749] It should be noted that any system, method, and/or other components disclosed herein may be described using computer aided design tools and expressed (or represented), as data and/or instructions embodied in various computer-readable media, in terms of their behavioral, register transfer, logic component, transistor, layout geometries, and/or other characteristics. Computer-readable media in which such formatted data and/or instructions may be embodied include, but are not limited to, non-volatile storage media in various forms (e.g., optical, magnetic or semiconductor storage media) and carrier waves that may be used to transfer such formatted data and/or instructions through wireless, optical, or wired signaling media or any combination thereof. Examples of transfers of such formatted data and/or instructions by carrier waves include, but are not limited to, transfers (uploads, downloads, e-mail, etc.) over the Internet and/or other computer networks via one or more data transfer protocols (e.g., HTTP, FTP, SMTP, etc.). When received within a computer system via one or more computer-readable media, such data and/or instruction-based expressions of the above described components may be processed by a processing entity (e.g., one or more processors) within the computer system in conjunction with execution of one or more other computer programs.

[0750] Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise,” “comprising,” and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of “including, but not limited to.” Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words “herein,” “hereunder,” “above,” “below,” and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. When the word “or” is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.

[0751] The above description of embodiments of the integrated security system and corresponding systems and methods is not intended to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the integrated security system and corresponding systems and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems and methods, as those skilled in the relevant art will recognize. The teachings of the integrated security system and corresponding systems and methods provided herein can be applied to other systems and methods, not only for the systems and methods described above.

[0752] The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the integrated security system and corresponding systems and methods in light of the above detailed description.

[0753] In general, in the following claims, the terms used should not be construed to limit the integrated security system and corresponding systems and methods to the specific embodiments disclosed in the specification and the claims, but should be construed to include all systems that operate

under the claims. Accordingly, the integrated security system and corresponding systems and methods is not limited by the disclosure, but instead the scope is to be determined entirely by the claims.

[0754] While certain aspects of the integrated security system and corresponding systems and methods are presented below in certain claim forms, the inventors contemplate the various aspects of the integrated security system and corresponding systems and methods in any number of claim forms. Accordingly, the inventors reserve the right to add additional claims after filing the application to pursue such additional claim forms for other aspects of the integrated security system and corresponding systems and methods.

What is claimed is:

1. A system comprising:

a gateway located at a first location;

a plurality of camera devices installed at the first location and coupled to the gateway via a secure network, wherein the gateway establishes the secure network;

a firewall coupled between the gateway and a wide area network (WAN);

a server coupled to the gateway via the WAN, the server located at a second location;

the gateway and the server communicating to control routing of a video stream from at least one camera device of the plurality of camera devices to the client device in response to a request for live video received from the client device, wherein the routing uses a network protocol selected from a plurality of network protocols in response to capabilities of the firewall, wherein the client device is remote to the first location and the second location.

2. The system of claim 1, wherein the network protocol is Universal Plug and Play (UPnP) port forwarding, wherein the UPnP opens a port of the firewall.

3. The system of claim 2, wherein, if UPnP port forwarding fails, the gateway and the server use Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN) to bypass the firewall and establish a peer-to-peer coupling.

4. The system of claim 3, wherein, if STUN fails, the server relays the video stream.

5. The system of claim 1, wherein the video stream is encrypted.

6. The system of claim 5, wherein the gateway encrypts the video stream received from the camera devices.

7. The system of claim 1, wherein a format of the video stream is automatically selected by at least one of the gateway and the server.

8. The system of claim 7, wherein the format is one of Motion Picture Experts Group (MPEG)-4 (MPEG-4)/Real-Time Streaming Protocol (RTSP) format, a MPEG-4 over Hypertext Transfer Protocol (HTTP) format, and a Motion Joint Photographic Experts Group (JPEG) (MJPEG) format.

9. The system of claim 7, wherein the format is selected based on a capability of the client device.

10. The system of claim 7, wherein the format is selected based on a capability of the camera device.

11. The system of claim 7, wherein the format is selected based on an authentication requirement of the client device.

12. The system of claim 7, wherein the format is selected based on a privacy requirement of the client device.

13. The system of claim 7, wherein the format is selected based on a determined capability of the WAN, wherein the determined capability is determined by at least one of the gateway and the server.

14. The system of claim 13, wherein the determined capability is relative success among a plurality of routings of the video stream.

15. The system of claim 14, wherein the determined capability is relative success of Universal Plug and Play port forwarding.

16. The system of claim 14, wherein the determined capability is relative success of peer-to-peer routing.

17. The system of claim 13, wherein the determined capability is bandwidth availability of the client device.

18. The system of claim 13, wherein the determined capability is processing capability of the client device.

19. The system of claim 13, wherein the determined capability is bandwidth availability of the camera devices.

20. The system of claim 7, wherein the format of the video stream is automatically selected according to a priority.

21. The system of claim 1, wherein the client device includes one or more of a personal computer, a personal digital assistant, a cellular telephone, and a mobile computing device.

22. The system of claim 1, wherein the gateway is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

23. The system of claim 22, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network via the client device.

24. The system of claim 22, wherein the gateway automatically discovers the security system components.

25. The system of claim 24, wherein the gateway includes protocols of the security system from the server and uses the protocols to discover the security system components.

26. The system of claim 24, wherein the gateway requests and receives protocols of the security system from the server, wherein the gateway uses the protocols received to discover the security system components.

27. The system of claim 22, wherein the gateway automatically establishes and controls the communications with the security system components.

28. The system of claim 22, wherein the gateway automatically establishes a coupling with the security system including the security system components.

29. The system of claim 22, wherein the gateway manages rules of interaction between the gateway and the security system components.

30. The system of claim 22, wherein the gateway includes definitions of the security system components.

31. The system of claim 22, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

32. The system of claim 31, wherein the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link.

33. The system of claim 32, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

34. The system of claim 32, wherein the event data comprises changes data and information of the plurality of camera devices.

35. The system of claim 31, wherein the secondary communication link includes a broadband coupling.

36. The system of claim 31, wherein the secondary communication link includes a cellular coupling.

37. The system of claim 31, wherein the gateway transmits messages comprising event data of the security system components to the client device over the secondary communication link.

38. The system of claim 37, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

39. The system of claim 31, wherein the gateway receives control data for control of the security system components from the client device via the secondary communication link.

40. A system comprising:

a gateway located at a first location;

a plurality of Internet Protocol (IP) devices installed at the first location and coupled to the gateway via a private network, wherein the private network is segregated from any other network at the first location, the gateway automatically establishing the private network, the establishing comprising provisioning identifiers and passwords to the plurality of IP devices;

a router coupled between the gateway and a wide area network (WAN), the router providing WAN access to the gateway and the plurality of IP devices; and

a server coupled to the gateway, the server located at a second location different from the first location.

41. The system of claim 40, wherein the gateway is coupled via a wireless coupling to a security system installed at the first location, the security system including security system components, wherein the gateway forms a security network that integrates communications and functions of the security system components into the security network via the wireless coupling.

42. The system of claim 41, comprising an interface coupled to the security network, wherein the interface allows control of the functions of the security network via a client device remote to the first location and the second location.

43. The system of claim 41, wherein the gateway automatically discovers the security system components.

44. The system of claim 43, wherein the gateway includes protocols of the security system from the server and uses the protocols to discover the security system components.

45. The system of claim 43, wherein the gateway requests and receives protocols of the security system from the server, wherein the gateway uses the protocols received to discover the security system components.

46. The system of claim 41, wherein the gateway automatically establishes and controls the communications with the security system components.

47. The system of claim 41, wherein the gateway automatically establishes a coupling with the security system including the security system components.

48. The system of claim 41, wherein the gateway manages rules of interaction between the gateway and the security system components.

49. The system of claim 41, wherein the gateway includes definitions of the security system components.

50. The system of claim 41, wherein the security system is coupled to a central monitoring station via a primary communication link, wherein the gateway is coupled to the central monitoring station via a secondary communication link that is different than the primary communication link, wherein the central monitoring station is located at a third location different from the first location and the second location.

51. The system of claim 50, wherein the gateway transmits event data of the security system components to the central monitoring station over the secondary communication link.

52. The system of claim 51, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

53. The system of claim 51, wherein the event data comprises changes data and information of the plurality of IP devices.

54. The system of claim 50, wherein the secondary communication link includes a broadband coupling.

55. The system of claim 50, wherein the secondary communication link includes a cellular coupling.

56. The system of claim 50, wherein the gateway transmits messages comprising event data of the security system components to a client device over the secondary communication link, wherein the client device is remote to the first location and the second location.

57. The system of claim 56, wherein the event data comprises changes in device states of the security system components, data of the security system components, and data received by the security system components.

58. The system of claim 50, wherein the gateway receives control data for control of the security system components from a client device via the secondary communication link, wherein the client device is remote to the first location and the second location.

59. The system of claim 40, wherein the gateway and the server communicate to control routing of a data stream from at least one IP device of the plurality of IP devices to a client device in response to a request for the data stream received from the client device, wherein the routing uses a network protocol selected from a plurality of network protocols in response to capabilities of the firewall, wherein the client device is remote to the first location and the second location.

60. The system of claim 59, wherein the network protocol is Universal Plug and Play (UPnP) port forwarding, wherein the UPnP opens a port of the firewall.

61. The system of claim 60, wherein, if UPnP port forwarding fails, the gateway and the server use Simple Traversal of

User Datagram Protocol (UDP) through Network Address Translators (NAT) (STUN) to bypass the firewall and establish a peer-to-peer coupling.

62. The system of claim 61, wherein, if STUN fails, the server relays the data stream.

63. The system of claim 59, wherein the data stream is encrypted.

64. The system of claim 63, wherein the gateway encrypts the data stream received from the IP devices.

65. The system of claim 59, wherein a format of the data stream is automatically selected by at least one of the gateway and the server.

66. The system of claim 65, wherein the format is selected based on a capability of the client device.

67. The system of claim 65, wherein the format is selected based on a capability of the IP device.

68. The system of claim 65, wherein the format is selected based on an authentication requirement of the client device.

69. The system of claim 65, wherein the format is selected based on a privacy requirement of the client device.

70. The system of claim 65, wherein the format is selected based on a determined capability of the WAN, wherein the determined capability is determined by at least one of the gateway and the server.

71. The system of claim 70, wherein the determined capability is relative success among a plurality of routings of the data stream.

72. The system of claim 71, wherein the determined capability is relative success of Universal Plug and Play port forwarding.

73. The system of claim 71, wherein the determined capability is relative success of peer-to-peer routing.

74. The system of claim 70, wherein the determined capability is bandwidth availability of the client device.

75. The system of claim 70, wherein the determined capability is processing capability of the client device.

76. The system of claim 70, wherein the determined capability is bandwidth availability of the IP devices.

77. The system of claim 65, wherein the format of the data stream is automatically selected according to a priority.

78. A system comprising:

a gateway located at a first location and coupled to a wide area network (WAN);

a plurality of Internet Protocol (IP) devices installed at the first location and coupled to the gateway via a private network, wherein the private network is segregated from any other network at the first location, the gateway automatically establishing the private network, the establishing comprising provisioning identifiers and passwords to the plurality of IP devices;

a router coupled between the gateway and a local area network (LAN) of the first location, the gateway providing WAN access to the plurality of IP devices and the LAN; and

a server coupled to the gateway, the server located at a second location different from the first location.

* * * * *