



- (51) **International Patent Classification:** Not classified
- (21) **International Application Number:**
PCT/US2012/051060
- (22) **International Filing Date:**
16 August 2012 (16.08.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/524,035 16 August 2011 (16.08.2011) US
13/586,569 15 August 2012 (15.08.2012) US
- (71) **Applicant (for all designated States except US):** **PAN-DUIT CORP.** [US/US]; 18900 Panduit Drive, Tinley Park, Illinois 60487 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** **FROST, James D.** [US/US]; 3304 Lapp Lane, Naperville, Illinois 60564 (US). **DOORHY, Brendan F.** [US/US]; 821 Timber Ridge Court, Westmont, Illinois 60559 (US). **LUKARESKI, Thomas F.** [US/US]; 562 Bishops Gate, New Lenox, Illinois 60451 (US). **CAI, Zeshun** [US/US]; 4621 Howard Street, Skokie, Illinois 60076 (US). **PANOZZO, Guy M.** [US/US]; 16130 Kensington, Tinley Park, Illinois 60477 (US).
- (74) **Agents:** **MCCANN, Robert A.** et al.; Panduit Corp., 6200 West 175th Street, Tinley Park, Illinois 60477 (US).

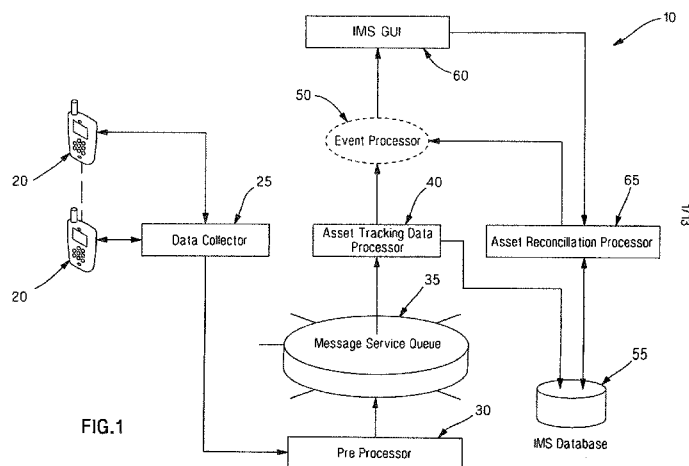
(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP,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

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

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) **Title:** INTEGRATED ASSET TRACKING, TASK MANAGER, AND VIRTUAL CONTAINER FOR DATA CENTER MANAGEMENT



(57) **Abstract:** The present invention provides for the integration of a an infrastructure management software (IMS) asset tracking system, an IMS task manager (ITM) and an IMS virtual container or virtual container feature to alleviate issues such as personnel scheduling issues, lost asset issues and service outages within a data center.

INTEGRATED ASSET TRACKING, TASK MANAGER, AND VIRTUAL CONTAINER FOR DATA CENTER MANAGEMENT

TECHNICAL FIELD

[0001] The present invention generally relates to asset management and tracking, and more specifically to applications and systems for management and tracking of telecommunication equipment in a data center.

BACKGROUND

[0002] A data center is a facility used to house a network of computer systems and associated components, such as telecommunications and storage systems. In addition to that equipment, the data center may include redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. Typically, the data center is managed by a data center manager (DCM) who may need to add, move, or decommission expensive data equipment on an hourly/daily/weekly basis. The highly dynamic environment of the data center routinely may cause personnel scheduling issues, lost asset issues, and service outages. Therefore, it would be desirable to alleviate the issues caused by the highly dynamic environment of the data center and to simplify the workflow for the DCM.

SUMMARY OF THE INVENTION

[0003] Accordingly, the present invention may help to assist the DCM with a highly dynamic environment of the data center and to simplify the workflow

[0004] In one embodiment, the present invention is an asset tracking system which includes the integration of an Infrastructure Management Software (IMS) such as Panduit's Physical Infrastructure Manager, a task manager, and a virtual container or virtual container feature. An IMS is a generally a software application that can facilitate the recording, tracking, and management of data center equipment.

[0005] In another embodiment, the present invention can give the DCM the ability to track the whereabouts of equipment in the network along with equipment's connectivity to that network. The

virtual container can allow the DCM to graphically represent the network equipment in a way that is desirable to the DCM. The graphical representation provided by the virtual container could provide a representation of the network equipment, for example by location, by equipment type, and/or by product line.

[0006] In another embodiment, when the IMS, the task manager, and the virtual container are combined into an integrated system for data center management, the system of the present invention can provide the DCM the ability to schedule when network equipment is added/moved/removed and also identify where the equipment will be located, how it will be connected or disconnected from the network, and/or who will do the work.

[0007] In another embodiment, the present invention includes asset tracking reconciliation, which gives the DCM the ability to accept or reject changes made to the trackable assets by technicians. Through reconciliation, the DCM is given the means to verify that the work is done properly and the DCM is also given the opportunity to approve or reject the work. If the DCM accepts the change made by the technician, the asset information is changed in an IMS database. If the DCM rejects the change, the asset information remains as unchanged.

[0008] A system according to the present invention may provide the DCM with real-time knowledge of where data center equipment is located and if or when the equipment is being worked on. Additionally, the present invention may provide the DCM with the ability to track the whereabouts of each piece of equipment in the network, and within the data center, along with each piece of equipment's connectivity to the rest of the network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The invention can be better understood with reference to the following drawings and description. The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

[0010] FIG. 1 depicts a flow chart illustrating architecture for an asset tracking system according to one embodiment of the present invention using data collection devices.

[0011] FIG. 2 depicts an update asset view from an IMS asset tracking system.

[0012] FIG. 3 depicts a remove asset view from an IMS asset tracking system.

[0013] FIG. 4 depicts a reconciliation of asset view from an IMS asset tracking system.

[0014] FIG. 5 depicts a flow chart illustrating how a virtual container allows for static and dynamic power aggregation for each monitored application when combined with virtualization visualization and an IMS asset tracking system.

[0015] FIG. 6 depicts a flow chart illustrating a virtual container providing boundary and rules pertaining to application security when running in a cloud.

[0016] FIG. 7 depicts a Graphical User Interface (GUI) for a virtual container.

[0017] FIG. 8 depicts a GUI for a virtual chassis for a blade server.

[0018] FIG. 9 depicts a GUI for a virtual chassis for a blade switch.

[0019] FIG. 10 depicts a GUI for a virtual chassis for a Multiple Network Interface Card (Multi-NIC) server.

[0020] FIG. 11 depicts a GUI for a virtual host and virtual machine.

[0021] FIG. 12 depicts the interaction between an IMS task manager client and a third party system.

[0022] FIG. 13 depicts an IMS task manager and the addition of key data center information into a work order.

DETAILED DESCRIPTION

[0023] As used herein, the term “asset tracking” refers to the awareness of the physical location of an individual device. Asset tracking does not necessarily imply asset management; though the two terms may be used interchangeably. Assets may be any piece of equipment found in a data center, including, but not limited to: network equipment such as cabling, switches, routers, patch panels, computer systems, communications devices, power supplies, and modems; and infrastructure such as cabinets, racks, cable ties, communications outlets, and power outlets.

[0024] The tracking system of the present invention can allow a user to select, specify, and track attributes related to automatically discovered assets through IMS discovery and manually discovered assets. An asset is considered to be automatically discovered if the asset is classified as an on-network asset and the asset has been present while a network discovery process was running. The tracking system becomes aware of this class of asset through active actions (e.g. IMS network discovery mechanism, manual or scheduled). An asset is considered manually discovered if the awareness of the asset can only be determined when a technician communicates status changes to the tracking system. The tracking system becomes aware of this class of assets through external means (e.g. data entry via a data entry device). The asset tracking process may also be semi-automated, requiring a user to manually enter attribute information, manually validate asset location, and establish connectivity. In addition, the asset tracking process supports the use of data entry device(s) that allow a user to detect and read asset identifying information such as asset tags to reduce data entry time and improve accuracy. Data entry devices may include any device through which information can be captured or input, such as RFID (radio frequency identification) readers, bar code readers, keyboards, mice, scanners, and/or cameras. Once initial validations are complete, the tracking system will track automatically discovered asset movement across the network, including all asset information previously specified. A process using policy enforcement and data entry devices supports semi-automatically tracking manually discovered asset movement.

[0025] A tracking system according to the present invention may include an Asset Tracking 2.0 Policy which introduces an additional method or tagging system that incorporates ID tags (e.g., barcode or RFID) and data entry devices (e.g., barcode scanners or RFID scanners) to discover and track assets throughout their life cycle within the data center. This tagging system allows for the formation of reliable and unique association between asset data and physical objects associated with the asset data. Using appropriate data entry devices, a tagged asset can be accurately identified, added to the tracking system, and tracked without requiring network connection. As a result, even if an asset is not attached to or connected with the network, certain key asset data can still be gathered and presented to the tracking system of the present invention. The tagging system allows for the addition of assets, and the detection of discrepancy between the asset data and the physical object for non-networking assets. This tagging system expands the scope and categories of assets that may be tracked by the tracking system. In addition, the tagging system enables DCMs to inventory assets at the earliest opportunity (e.g., upon initial possession of assets). The tagging system also supports the capabilities to flag discrepancies between the asset data and device data, which is data generated by a data entry device when reading an ID tag, and to provide a function to guide authorized personnel to reconcile any discrepancies. Authentications and authorizations are also supported by the tracking system of the present invention to insure that asset activities are properly conducted by the authorized personnel. The Asset Tracking 2.0 Policy does not stipulate fixed procedures upon users. Rather, the Asset Tracking 2.0 Policy offers a set of configurable facilities with which users may use to form policies that meet their own practices and needs in adding and tracking assets.

[0026] The workflow of a system 10 according to one embodiment of the present invention is illustrated in FIG. 1. A DCM or any other user employs data entry devices 20 to collect asset tracking (AT) data. This data is collected by an asset tracking data collector 25, which at least in part facilitates the transfer of said data to the IMS. The data collector may include both, software and hardware aspects. The data is then received by a pre-processor 30 which formats the collected data

in preparation for placing it into a message service queue 35. From this queue 35, an asset tracking data processor 40 evaluates the queued data and forwards it to the event processor 50 along with an IMS database 55. When data is received by an even processor 55, it is then formatted and outputted on a graphical user interface (GUI) 60, an example of which is illustrated in FIG. 2. At the same time, the asset reconciliation processor 60 checks the database 55 against an event and if a conflict arises, the processor 65 forwards corresponding data to the event processor 50 to be made visible through the GUI 60.

[0027] To add one or more new assets to the tracking system of the present invention, the following preconditions and events, preferably take place: 1) preferably all data reconciliation will be done at the IMS; 2) the data entry device uses a software application to collect key asset data; 3) the data entry device has a method to communicate with the IMS (online/offline); 4) assets are not tagged; 5) a technician or user has a set of pre-printed tags at hand (e.g., tags are printed by a printer or a data entry device); and 6) all rooms/locations within the data center are labeled with tags.

[0028] The events for adding one or more new assets to the tracking system preferably occur in the following sequence: 1) the technician enters a room with a proper credential; 2) the technician signs-in to the data entry device with credentials and the credentials are accepted; 3) the technician selects the room location with the data entry device; 4) for each asset, the technician picks a tag and affixes it to the asset following predetermined recommendation for size and placement; 5) the technician then scans the asset tag with the data entry device; 6) the technician enters additional data into the data entry device (e.g., MAC (media access control), rack, RU (rack unit), UPC (universal product code), serial number, model, vendor), preferably, as much data as available from the asset; 7) the technician repeats steps 4 through 6 until all relevant assets are tagged and scanned; 8) actions taken by the technician are logged into the system or data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 9) the technician instructs the data entry device that the technician is done collecting data, when done; and 10) the data entry device communicates or

transports the collected data to the tracking system, which preferably resides in a remote server or remote computer system.

[0029] After a new asset is added into the tracking system, the newly discovered asset is then updated within the tracking system. In order to update a single newly discovered asset in the tracking system, the following preconditions and events, preferably take place: 1) all data reconciliation needs to be done at the tracking system; 2) the data entry device has a software application used to collect key asset data; 3) the data entry device has a method to communicate with the tracking system (online/offline); 4) the asset is on a rack and is untagged; 5) the tracking system has discovered the asset; 6) the technician has a set of pre-printed tags at hand (e.g., tags are printed by a printer or a data entry device); 7) the building, room, and rack within the data center are labeled with asset tags.

[0030] The events for updating an asset within the tracking system preferably occur in the following sequence: 1) the technician enters the room with proper credential; 2) the technician signs-in on to the data entry device with credential and is accepted; 3) the technician selects the room location; 4) the technician visually searches and finds the asset; 5) the technician picks a tag and affixes it to the asset following predetermined recommendation for size and placement; 6) if asset data is input manually, then the following manual data entry method occurs: a) the technician scans the rack location with the data entry device where the asset was found, b) the technician enters the RU level of the asset into the data entry device, c) the technician scans the asset tag with the data entry device, d) the technician enters additional data into data entry device (e.g., MAC, rack, RU, UPC, serial number, model, vendor) as much data as available from the asset; 7) if data is not input manually, but rather automatically, then the facilitated entry method occurs: a) the tracking system assumes that asset information has been entered previously, b) a report is generated that contains a temporary tag for the asset, c) the technician scans the temporary tag on a printed version of the generated report or the GUI (graphical user interface), d) the technician scans a bar code, or other identifying mark or

device (such as an RFID chip), affixed to the asset; 8) any actions taken by technician are logged into the tracking system or the data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 9) the technician instructs the data entry device that the technician is done collecting data, when done; and 10) the data entry device communicates or transports the collected data to the tracking system.

[0031] As asset information is added, modified, and/or removed, the tracking system can display a sequence of these events in an event-viewer type environment. Such an event-viewer display is shown in FIG. 2, where pane 100 shows the recorded events, pane 110 shows asset information associated with any selected event, and pane 120 shows the transactional information related to the event such as the update-related information.

[0032] After an asset is updated within the tracking system, the tagged asset may also be updated. In order to update a tagged asset in the tracking system, the following preconditions and events, preferably take place: 1) preferably all data reconciliation is to be done with the tracking system; 2) the data entry device has a software application to collect key asset data; 3) the data entry device has a method to communicate with the tracking system (online/offline); 4) the asset is known by the tracking system and is tagged; 5) the tracking system has an entry for the asset, building, room, and rack which are all labeled with asset tags.

[0033] The events for updating a tagged asset within the tracking system preferably occur in the following sequence: 1) the technician enters the room with proper credentials; 2) the technician signs-in on to the data entry device with credential and is accepted; 3) the technician selects the room location; 4) the technician visually searches and finds the asset; 5) if asset data is updated manually, then the following manual data entry occurs: a) the technician scans the rack location with the data entry device where the asset was found, b) the technician enters the rack unit of the asset into the data entry device, c) the technician scans the asset tag with the data entry device, d) the technician enters additional data into data entry device (e.g., MAC, rack, RU, UPC, serial number, model,

vender), preferably, as much data as available from the asset, 6) if necessary, the technician updates the status information for the asset; if the asset is being monitored, the asset status is all that need be updated; 7) any actions taken by technician are logged into the tracking system or data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 8) the technician instructs the data entry device that the technician is done collecting data, when done; 10) the data entry device communicates or transports the collected data to the PIM asset tracking system.

[0034] After an asset is updated within the tracking system, the tagged asset may also be physically removed from a known location. In order to remove a tagged asset from a known location in the tracking system, the following preconditions and events, preferably take place: 1) preferably all data reconciliation is to be done using the tracking system, the remote server may or may not be up and running; 2) the data entry device has software application to collect key asset data; 3) the data entry device has a method to communicate with the tracking system (online/offline); 4) the asset is tagged and the location of the asset is known to tracking system; and 5) a report is available that lists the asset location (e.g. building, room, rack, RU, asset tag barcode); and 6) preferably all rooms within the data center are labeled with tags.

[0035] The events for physically removing a tagged asset from a known location preferably occur in the following sequence: 1) the technician enters the room with proper credentials; 2) the technician signs-in to the data entry device with credentials and the credentials are accepted; 3) the technician selects the location; 4) the technician uses the report to visually search for and find the tagged asset; 5) the technician verifies that the visually found asset matches what the report details; 6) the technician scans the asset tag with the data entry device; 7) the technician selects an option on the data entry device to assign the asset to the technician; 8) the technician physically removes the asset; 9) the asset status should now show Install/Move/Add/Change (IMAC); 10) any actions taken by the technician are logged into the tracking system or the data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 11) the technician instructs data entry device

that technician is done, when done; 10) the data entry device communicates or transports the collected data to the tracking system.

[0036] In order to install an asset into a specified location in the tracking system, the following preconditions and events, preferably take place: 1) all data reconciliation will be done with the tracking system; 2) the data entry device has a software application to collect key asset data; 3) the data entry device has a method to communicate with the tracking system (online/offline); 4) the asset is tagged and in the technicians possession (cart, hand, etc.); 5) a report is available that lists the desired location for the asset to be installed within the data center (e.g. building, room, rack, RU); 6) preferably, all rooms in the data center are labeled with tags.

[0037] The events for installing an asset into a specified location preferably occur in the following sequence: 1) the technician enters the room with proper credentials; 2) the technician signs-in to the data entry device with credentials and the credentials are accepted; 3) the technician selects the specified location with the data entry device; 4) the technician uses the report to visually search for the specified location; 5) the technician visually verifies that asset will fit in the specified location; 6) the technician scans the asset tag with the data entry device; 7) the technician enters asset new location data into data entry device (e.g., room, rack, RU) or scans the asset tag; 8) the technician installs the asset into the specified location; 9) any actions taken by technician are logged into the tracking system or the data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 10) the technician instructs data entry device that technician is done, when done; and 11) the data entry device communicates or transports the collected data to the tracking system.

[0038] With reference to FIG. 3, in order to delete an asset from the tracking system, the following preconditions and events preferably take place: 1) preferably, all data reconciliation will be done with the tracking system; 2) the data entry device has a software application to modify key asset data; 3) the data entry device has a method to communicate with the tracking system (online/offline);

4) the asset is tagged; 5) the asset has been moved (via remove/install use cases) to a location in preparation for decommissioning; 6) preferably, all rooms in the data center are labeled with tags.

[0039] The events for deleting or decommissioning an asset from the tracking system preferably occur in the following sequence: 1) the technician enters the room with proper credentials; 2) the technician signs-in on to the data entry device with credentials and the credentials are accepted; 3) the technician scans the asset tag with the data entry device; 4) the technician validates that the asset matches the data in the tracking system; 5) the technician verifies if any special rules are defined for asset destruction; 6) the technician selects an option to delete the asset; 7) the technician scans his ID to confirm his/her identity; 8) preferably, any actions taken by technician are logged into the tracking system or the data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); 9) the technician instructs data entry device that technician is done, when done; 10) the data entry device communicates or transports the collected data to the tracking system.

[0040] With reference to FIG. 4, when data gathered about off-network or on-network devices, such as the data entry device, is in conflict with the data in the tracking system, reconciliation of an asset record must occur. In order to reconcile an asset record, the following preconditions and events, preferably take place: 1) reconciliation is a manual process performed by the data center manager; 2) reconciliation may be initiated at the GUI for the tracking system or at the data entry device; 3) the reported device data is found to have the following problems but is not limited to: a) one or more (not all) of MAC address, asset number, EPC or barcode mismatch (data in the system doesn't match the reported MAC, asset number, EPC or barcode). Examples of records to be reconciled include: for a server with two NICs (network interface cards), existing system data lists one MAC; data entry device lists other MAC, b) a duplicate MAC, asset number, EPC (electronic product code) or barcode (another device in the system has the same reported MAC, asset number, EPC or barcode), c) the location in the system doesn't match the reported location for the same device or the device is missing in the system, d) a duplicate location (for example: another device in the system already

occupies the reported location), and e) in a link-up report from the switches, the reported device is found in the system; 4) the technician is logged in with credentials that allows (all users will not have permission to perform reconciliation) reconciliation (on server or data entry device).

[0041] The events for reconciliation of an asset record in the tracking system preferably occur in the following sequence: 1) the tracking system (or the data entry device) logs the conflict and raises a security alert (e.g., generates a notification); 2) on the tracking system GUI (e.g., location tree) (or the data entry device), the asset with security alert is marked with special “visibility” for attention, indicating reconciliation is needed; 3) the technician selects the asset to be reconciled; 4) the technician is prompted for one of the following options by the system GUI or data entry device (e.g., on a drop down menu): a) edit the data field or selectively accept the conflicted data (the technician selects the data desired to be accepted) or b) accept new data for the device as is (the new device data will replace the existing device data).

[0042] If option a) is selected, the technician may manually edit additional data fields; the technician completes the change; the technician instructs the system or data entry device to accept the edited/accepted data; the reconciliation is complete and the security alert is cleared; and the asset returns to “normal” visibility within the tracking system. If option b) is selected, the reconciliation is complete and the security alert is cleared and the device returns to “normal” visibility.

[0043] A third option, option c) is also possible which is to reject and not accept the reported data (the existing device data is kept in the system and the reported data is discarded). If option c) is selected, the reconciliation is complete, the security alert is cleared, and the device returns to “normal” visibility. A fourth option, option d) is to defer, where the security alert is to be resolved by action other than manipulating the device data and existing device data is kept in the system. Under option d), reconciliation is still required, the device is still in security alert, and action other than manipulating the device data is required to complete the reconciliation. For example, a physical move of the device may be required to correct the problem.

[0044] After selecting an option in step 4), the sequence moves to step 5) whereby any actions taken by technician are logged into the tracking system or the data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps).

[0045] In order to audit a specified location and verify expected inventory vs. actual inventory (e.g. for a SOx (Sarbanes–Oxley) audit), the following preconditions and events, preferably take place: 1) the tracking system has a list of known assets; 2) a report interface exists to generate reports by location (room, rack, etc.); 3) the report interface can print out the asset number and barcode number in barcode format; 4) at least one report is generated per location; 5) the report can be generated via paper or sent to the data entry device or displayed on the GUI of the tracking system.

[0046] The events for auditing a specified location and verifying expected inventory vs. actual inventory, preferably occur in the following sequence: 1) a report is generated that creates a location targeted listing (a room or a rack for example); 2) the report has an ID that can be scanned (e.g. bar code) for the asset number, the room and the location; 3) the technician enters the room with proper credential; 4) the technician signs-in on to the data entry device with credentials and the credentials are accepted; 5) the technician selects the room location with the data entry device; 6) the technician verifies that the technician is in the proper room; 7) the technician scans an asset tag and a barcode from the report that defines the location; 8) the technician scans, preferably, all assets associated with that location; 9) the technician indicates to the data entry device that all assets have been scanned; 10) actions taken by technician are logged into the system or data entry device (e.g., the selected option, the person performing the reconciliation, and timestamps); and 11) the technician closes out the transaction on the data entry device.

[0047] With reference to FIG. 5, the virtual container feature provides the DCM with the ability to graphically represent the network equipment in a way that is desirable to the DCM. The graphical representation provided by the virtual container feature can provide a representation of the network equipment, for example by location, by equipment type, or by product line.

[0048] Data center managers and data center designers often refer to the assets in the data center in terms of their functional, logical, or physical grouping in the data center. The virtual container feature is targeted at that behavior. Within an IMS, assets may be referred to as managed items, which are items that are being managed by an IMS and are shown on a location tree. Managed items may include devices such as switches, Panduit's PViQ panels, POUs (power outlet units), DPEs, power-over-Ethernet panels, computers, other endpoints, and containers such as racks, as well as "virtual chassis," may all be managed items under an IMS. Assets known by the tracking system can be members of multiple virtual containers such as "POD 13", "Container 12", "Accounting Server group 3" and "Development Servers." The concept of a virtual container is a collection of customer defined items. The concept is defined such that a virtual container can contain other virtual containers. Also, a virtual chassis is defined as a "virtual container" under the physical network location tree that is intended to group related devices belonging to a Multi-NIC server, blade chassis server or switch. The virtual container leads to many useful applications: when combined with a virtualization visualization system and the tracking system, the virtual container is capable of determining power aggregation per application. Virtualization visualization gives a user the ability to visually model a network based on virtual containers. For example, there could be a diagram of all of the accounting department's servers in the network based on a virtual container. Also, the virtual container is able to set boundaries and rules for application accessibility running in a cloud computing environment. A cloud computing environment enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Boundaries, such as geographical or security-based boundaries, may be enforced on an application, for example.

[0049] Preferably, the virtual container allows static and dynamic power aggregation per application when combined with a virtualization visualization system and the tracking system. This power

aggregation functionality may enable enterprises to monitor the power usage of different departments. An example of such departments is illustrated in FIG. 5, showing marketing 110, engineering 120, finance 130, human resource (not shown), or research and development (not shown). For instance, all the above mentioned departments may have servers in any cabinet within a data center. By using the virtual container, a user can group all the marketing servers together 140, all the engineering servers together 150, all the finance servers together 160, and the same thing can be done to group other servers per department. Once this happens, with the help of the tracking system, a user can statically monitor the power usage by all or some of a particular group of servers, such as all of the marketing servers, with more ease. Furthermore, a user may also dynamically monitor the power usage by combining the virtual container with virtualization visualization. Virtualization visualization is able to dynamically track applications running by a certain department, such as the marketing department 170. When applications running from a certain department, such as the marketing department, interact with other departments, virtualization visualization is able to track them down and provide an accurate power per application data which can be generated dynamically.

[0050] The virtual container may enable the monitoring of VMware™ which is virtualization software for desktops manufactured by VMware of Palo Alto, CA. The virtual container may track software based applications. The virtual container can show the user where an instance of an Oracle Database is running (e.g. on a server in another city) and provide and display how much processing power and memory is being consumed by that software, for example. For instance, a user can track how many instances of a certain type of software, such as Oracle Database software, is running and the user may also obtain the location of where the each instance of a certain type of software is running at. For example, virtual containers may be used to track all Microsoft Outlook applications in the network or how much memory is consumed by Microsoft Outlook for the accounting team, etc..

[0051] With reference to FIG. 6, the virtual container may provide boundary 200 and rules pertaining to application security when running in a cloud computing environment, known simply as a “cloud.” A user may create a custom boundary and rules to limit the “traveling of an application.” For instance, certain applications may be in a top secret or high level, and a user may use the virtual container to keep those applications on only certain approved servers. Applications may also be prevented from migrating to computing resources in particular locations.

[0052] Managed items 210 may easily be dragged and dropped into a virtual container 220 or chassis. Any time a managed item is dragged into a virtual container or chassis, the presence of the managed item under the network physical location tree should be left intact. Likewise, these managed items can also be copied or cut from a virtual location and be pasted onto another virtual location.

[0053] With reference to FIG. 7, two virtual containers are shown created under a root virtual container node. As an example the two virtual containers are named “My Virtual Container” 250 and “My Virtual Container 1” 260. Under “My Virtual Container,” there are assets 270 being grouped together. This illustrates one of the main functions of a virtual container: to group assets into a user defined virtual container. Under “My Virtual Container 1,” there are two virtual containers named “My Virtual Container 2” 280 and “My Virtual Container 3” 290 which belongs to “My Virtual Container 2.” From this example, we can see that a virtual container is capable of grouping virtual containers within a virtual container. When a virtual container is selected or the assets within a virtual container are selected, a panel on the right-hand side 300 will display any appropriate information.

[0054] With reference to FIG. 8, the hierarchy of a blade server virtual chassis is displayed as: Server 310 – Virtual Chassis 320 – Blade Server 330 – Ports 340. A validation may be done to check what types the source and target devices are, e.g. switch and network capable devices. If the validation fails, then the user will be shown an error message. If the validation is successful, then the

user will be shown a dialog box with an option to create a Multi-NIC device or a virtual chassis. If the user selects the virtual chassis option, a text box for entering the virtual chassis name will be displayed. If the user selects “Cancel” nothing will happen. If user selects “OK” then a new virtual chassis will be created and the source and target device would be shown under the newly created virtual chassis. When the user opens the connectivity for the virtual chassis, the connectivity view shows the ports for the underlying devices.

[0055] With reference to FIG. 9, a structure of a blade switch virtual chassis is displayed as: Switch 350 – Chassis 360 – Blade 370 – Ports 380. When a user selects a virtual chassis, the chassis detail is displayed on the right-hand pane 390. Similarly when the user selects a switch blade under the virtual chassis, any blade details will be displayed on the right-hand pane 390.

[0056] With reference to FIG. 10, a validation may be done to check if source and target devices are e.g., switch and network capable devices, for example. If the validation fails then the user will be shown an error message. If the validation is successful, then the user will be shown a dialog box with an option to create a Multi-NIC device or a virtual chassis. If the user selects the Multi-NIC option and selects the OK button, a new port will be created for the target device with the IP and MAC of the source device. FIG. 10 displays the port details of a highlighted device.

[0057] With reference to FIG. 11, one can observe the relationship between a virtual host and a virtual machine. For example, when viewing FIG. 11, one can observe that “Virtual Machine 1” 400 belongs to “Virtual Host 1” 410 in “rack 1” 420; and likewise, “Virtual Machine 2” 430 belongs to “Virtual Host 2” 440 in “rack 2” 450. Each virtual machine is associated with a virtual host and is represented as a child node of the virtual host.

[0058] With reference to FIGS. 12 and 13, the IMS (in the case of the illustrations, the IMS is Panduit’s PIM) task manager provides the DCM with the ability to view a work order task and to add subtasks to accomplish the work order task. DCMs routinely create and assign work order tasks to technicians to carry out the day to day operations of the data center. These tasks are typically

include but are not limited to installing and removing equipment or assets such as switches, routers and servers from data center racks and cabinets. To simplify technician assignments and track the task from start to finish, DCM's use a third party work order application designed to do so. Examples of third party work order systems include BMC Remedy by BMC and Ground Zero Tech-Works Inc. by AyaNova.

[0059] The IMS Task Manager (ITM) feature provides the DCM the ability to view the work order tasks and to add subtasks to accomplish the work order task. The subtasks can be manual events that must be carried out, or they can be IMS related tasks that use existing IMS features like a Device Catalog, Infrastructure Manager, and Connectivity Creation Screens (available in Panduit's PIM software) to create detailed tasks that can be carried out by technicians or by an IMS automatically.

[0060] The ITM consists of three pieces: a third party work order system, an IMS, and an API (application programming interface) to connect the two. The third party work order system serves as the engine for creating and processing work orders. When a task on a work order is identified as an IMS related task, the task will be sent to the IMS, using API calls, for Data Center Manager and Network Engineer input. When a new work order task is received from the third party work order system, the IMS will store the task for processing, adding a timestamp. The DCM may then process the task within the IMS, creating any subtasks that are required at the IMS level. When finished, the updated task will be exported back to the third party work order system, which will add the subtasks into the work order. The IMS will then track the progress of the automatic subtasks and notify the third party work order system when a task is complete.

[0061] In one embodiment, only network connections will be processed by the IMS and a notification will be sent to the third party work order system. All other status updates will come down from the third party work order system.

[0062] One primary method for accessing and provisioning the tasks will be handled by a link on the third party work order system. This link will open an IMS client and take the user to a ITM landing

page. This landing page will display the work orders for that user and will allow the provisioning of tasks for the work orders. The IMS allows a user to save a device, location or connection (connect/disconnect) to a task. The necessary information required to do the task will be placed in the task.

[0063] The ITM displays a main page which provides links to a device catalog, an infrastructure manager, and a connectivity creation page, allowing for easy access to areas for finding devices, locations, and connections. The selected device information, location, and connection information may be added into a task that is being configured when the user saves the selection to the task.

[0064] As a result, the IMS seamlessly integrates with the 3rd party system (that is, it appears to be a part of the 3rd party work order system when using the 3rd party work order system). Additionally, the ITM allows extension and enhancement of the 3rd party functionality in a unique manner. The IMS provides the ability to define connectivity, RU Reservation, POU outlet reservation and asset tagging work order subtasks. As the subtasks are defined using IMS features, they are transferred to a ITM holding container module. Once subtasks are encapsulated in the ITM holding container module they can be reordered/deleted/added/modified as a part of the overall work order within the 3rd party work order system. Work orders are normally initiated from the 3rd party work order system, however, the IMS can have the capability of initiating a work order and transfer that set of tasks/subtasks to the 3rd party system.

[0065] Those having skill in the art will recognize that the state of the art has progressed to the point where there is little distinction left between hardware and software implementations of aspects of systems; the use of hardware or software is generally (but not always, in that in certain contexts the choice between hardware and software can become significant) a design choice representing cost vs. efficiency tradeoffs. Those having skill in the art will appreciate that there are various vehicles by which processes and/or systems and/or other technologies described herein can be effected (e.g., hardware, software, and/or firmware), and that the preferred vehicle will vary with the context in

which the processes and/or systems and/or other technologies are deployed. For example, if an implementer determines that speed and accuracy are paramount, the implementer may opt for a mainly hardware and/or firmware vehicle; alternatively, if flexibility is paramount, the implementer may opt for a mainly software implementation; or, yet again alternatively, the implementer may opt for some combination of hardware, software, and/or firmware. Hence, there are several possible vehicles by which the processes and/or devices and/or other technologies described herein may be effected, none of which is inherently superior to the other in that any vehicle to be utilized is a choice dependent upon the context in which the vehicle will be deployed and the specific concerns (e.g., speed, flexibility, or predictability) of the implementer, any of which may vary. Those skilled in the art will recognize that optical aspects of implementations will typically employ optically-oriented hardware, software, and or firmware.

[0066] The foregoing detailed description has set forth various embodiments of the devices and/or processes via the use of block diagrams, flowcharts, and/or examples. Insofar as such block diagrams, flowcharts, and/or examples contain one or more functions and/or operations, it will be understood by those within the art that each function and/or operation within such block diagrams, flowcharts, or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. In one embodiment, several portions of the subject matter described herein may be implemented via Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs), digital signal processors (DSPs), or other integrated formats. However, those skilled in the art will recognize that some aspects of the embodiments disclosed herein, in whole or in part, can be equivalently implemented in integrated circuits, as one or more computer programs running on one or more computers (e.g., as one or more programs running on one or more computer systems), as one or more programs running on one or more processors (e.g., as one or more programs running on one or more microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing

the code for the software and or firmware would be well within the skill of one of skill in the art in light of this disclosure. In addition, those skilled in the art will appreciate that the mechanisms of the subject matter described herein are capable of being distributed as a program product in a variety of forms, and that an illustrative embodiment of the subject matter described herein applies regardless of the particular type of signal bearing medium used to actually carry out the distribution. Examples of a signal bearing medium include, but are not limited to, the following: a recordable type medium such as a floppy disk, a hard disk drive, a Compact Disc (CD), a Digital Video Disk (DVD), a digital tape, a computer memory, etc.; and a transmission type medium such as a digital and/or an analog communication medium (e.g., a fiber optic cable, a waveguide, a wired communications link, a wireless communication link, etc.)

[0067] The herein described subject matter sometimes illustrates different components contained within, or connected with, different other components. It is to be understood that such depicted architectures are merely exemplary, and that in fact many other architectures can be implemented which achieve the same functionality. In a conceptual sense, any arrangement of components to achieve the same functionality is effectively "associated" such that the desired functionality is achieved. Hence, any two components herein combined to achieve a particular functionality can be seen as "associated with" each other such that the desired functionality is achieved, irrespective of architectures or intermedial components. Likewise, any two components so associated can also be viewed as being "operably connected", or "operably coupled", to each other to achieve the desired functionality, and any two components capable of being so associated can also be viewed as being "operably couplable", to each other to achieve the desired functionality. Specific examples of operably couplable include but are not limited to physically mateable and/or physically interacting components and/or wirelessly interactable and/or wirelessly interacting components and/or logically interacting and/or logically interactable components.

[0068] Those skilled in the art will recognize that it is common within the art to implement devices and/or processes and/or systems in the fashion(s) set forth herein, and thereafter use engineering and/or business practices to integrate such implemented devices and/or processes and/or systems into more comprehensive devices and/or processes and/or systems. That is, at least a portion of the devices and/or processes and/or systems described herein can be integrated into comprehensive devices and/or processes and/or systems via a reasonable amount of experimentation. Those having skill in the art will recognize that examples of such comprehensive devices and/or processes and/or systems might include--as appropriate to context and application--all or part of devices and/or processes and/or systems of (a) an air conveyance (e.g., an airplane, rocket, hovercraft, helicopter, etc.), (b) a ground conveyance (e.g., a car, truck, locomotive, tank, armored personnel carrier, etc.), (c) a building (e.g., a home, warehouse, office, etc.), (d) an appliance (e.g., a refrigerator, a washing machine, a dryer, etc.), (e) a communications system (e.g., a networked system, a telephone system, a Voice over IP system, etc.), (f) a business entity (e.g., an Internet Service Provider (ISP) entity such as Comcast Cable, Quest, Southwestern Bell, etc.); or (g) a wired/wireless services entity such as Sprint, Cingular, Nextel, etc.), etc.

[0069] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject matter lies in less than all features of a single disclosed embodiment. Thus the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

[0070] While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that other embodiments and implementations are possible within the scope of the invention. Accordingly, the invention is not to be restricted except in light of the attached claims and their equivalents.

We claim:

1. An asset tracking system for tracking assets within a data center, said asset tracking system comprising:

an infrastructure management software;

a task manager; and

a virtual container,

said asset tracking system having a means for recording, tracking, and managing information associated with equipment within said data center, said asset tracking system further having a means for asset tracking reconciliation,

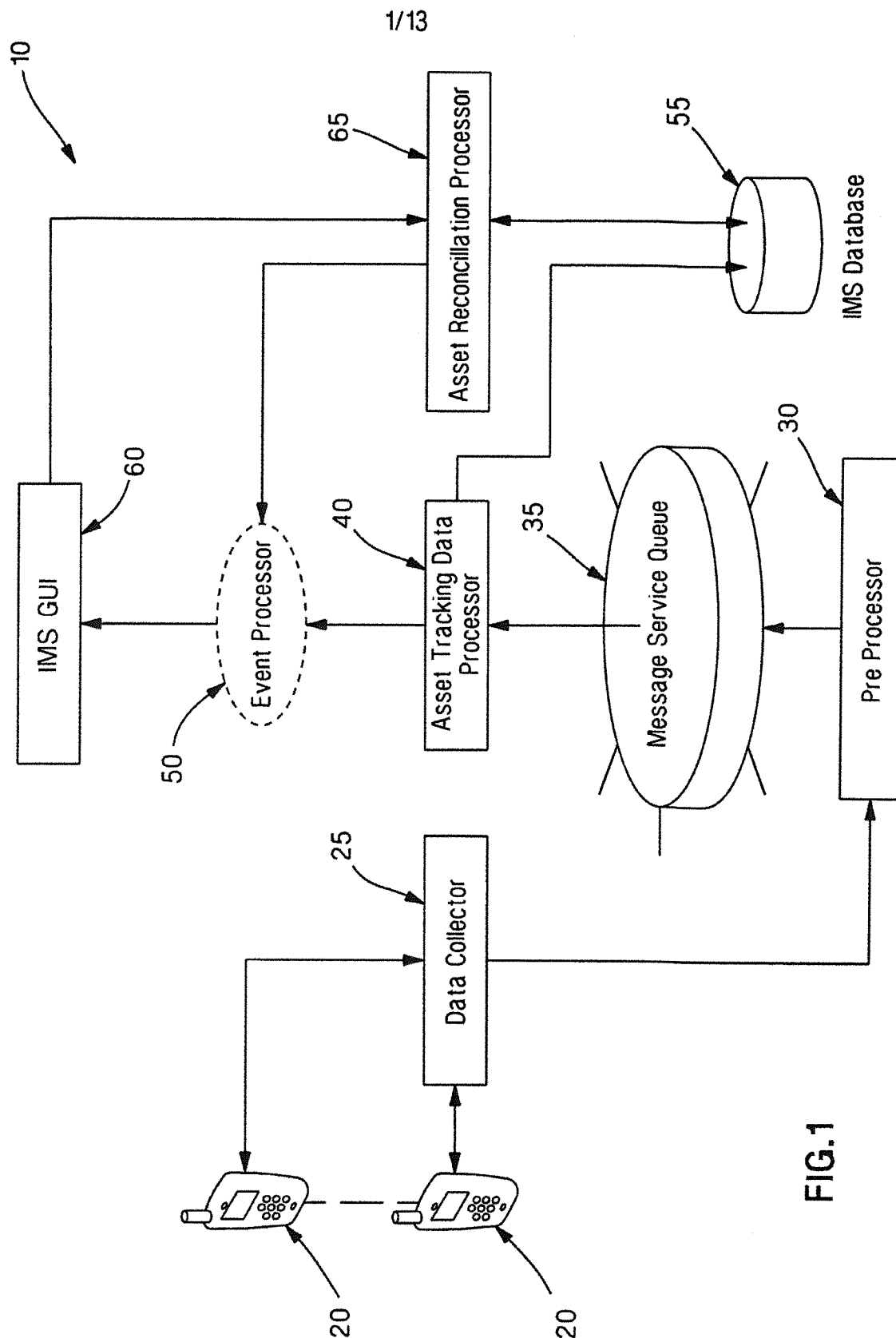
said task manager having a means for viewing information associated with at least one of adding a new asset, updating a newly discovered asset, updating a tagged asset, installing an asset, and removing an asset,

said virtual container providing a graphical representation of a network at least partially connected to said data center.

2. The asset tracking system of claim 1, wherein said means for recording, tracking, and managing information associated with equipment includes means for recording, tracking, and managing information associated with equipment that is not connected to said network.

3. The asset tracking system of claim 2, wherein said means for recording, tracking, and managing information associated with equipment that is not connected to said network includes at least one identification tag placed on said equipment and at least one data entry device capable of gathering information from said at least one identification tag.

4. The asset tracking system of claim 3, wherein said identification tag includes at least one of a radio frequency identification tag and a bar code tag, and wherein said data entry device includes at least one of a radio frequency identification tag scanner and a bar code tag scanner.
5. The asset tracking system of claim 1, wherein said virtual container determines power aggregation for at least one application executed on at least one server.
6. The asset tracking system of claim 5, wherein said virtual container determines power aggregation for all applications associated with at least one department.
7. The asset tracking system of claim 1, wherein said virtual container sets security boundaries for applications executed on servers virtually placed within said virtual container.
8. The asset tracking system of claim 1, wherein said virtual container sets security boundaries for all applications placed within said virtual container.
9. The asset tracking system of claim 1 further comprising an application programming interface (API), said API connecting said infrastructure management software and a third party application.
10. The asset tracking system of claim 9, wherein said third party application is a work order system capable of creating and processing work orders for said data center.



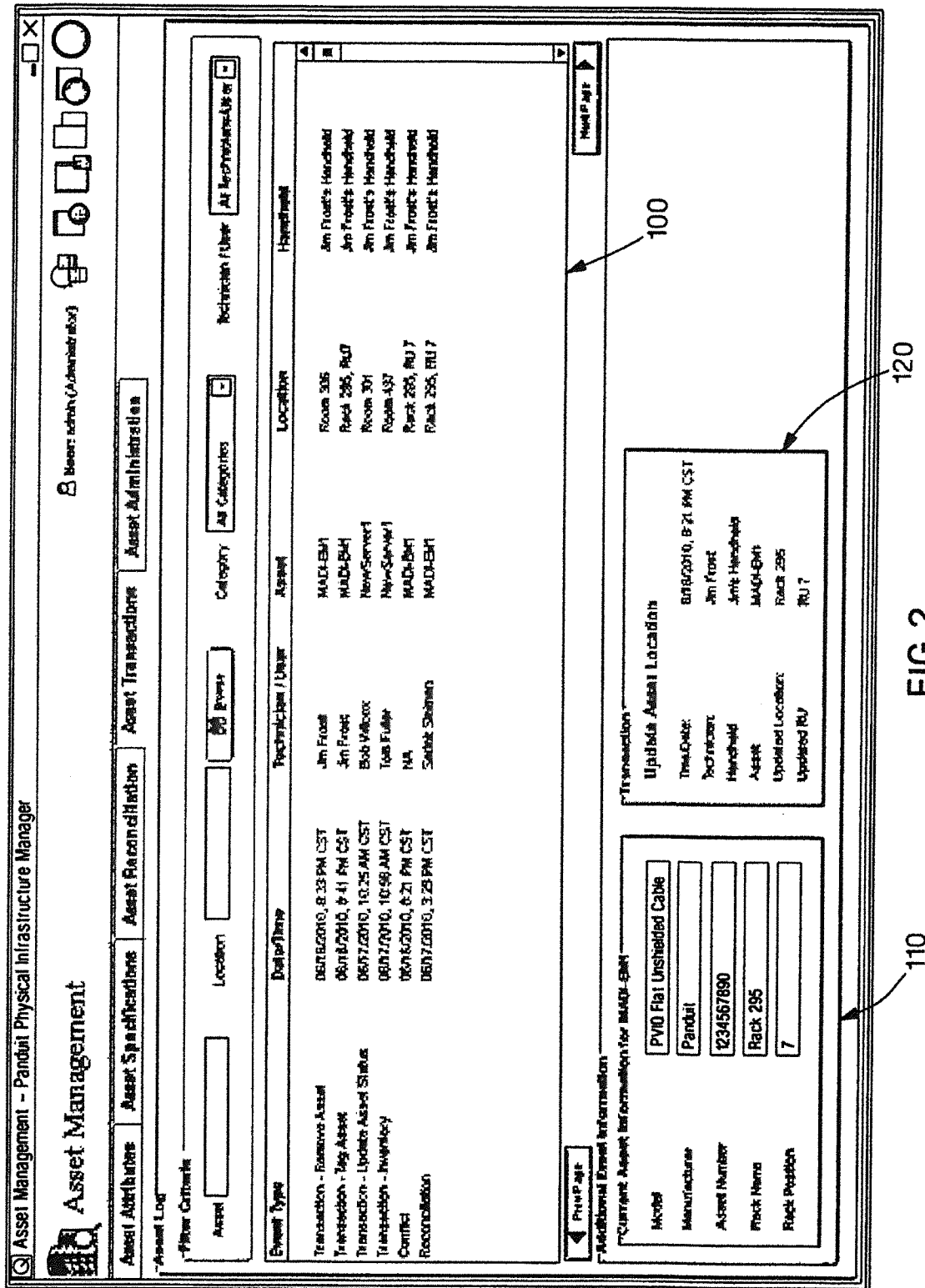


FIG.2

Asset Management - Panduit Physical Infrastructure Manager							
User: admin (Administrator)							
Asset Management							
Asset Attributes		Asset Specifications		Asset Reconciliation		Asset Transactions	
<input checked="" type="radio"/> Display All Assets <input type="radio"/> Display Single Asset							
Asset Reconciliation							
Transaction	Date/Time	Technician	Handfield	Asset	Location	Issue	
Remove Asset	06/16/2010, 8:21 PM CST	Jim Frost	Jim's Handfield	MADU-EM1	Room 306	Asset removed from a container/location it was not in	
	06/16/2010, 8:33 PM CST	Jim Frost	Jim's Handfield	MADU-EM1	N/A	Status changed to a status that is no longer in the system	
	06/16/2010, 8:41 PM CST	Jim Frost	Jim's Handfield	MADU-EM1	Rack 295, RU 7	Location updated to an RU that is already occupied	
	06/17/2010, 10:25 AM CST	Bob Wilcox	Common H-H	NewServer1	Room 301	Asset tagged with barcode that already exists	
	06/17/2010, 10:58 AM CST	Tom Fuller	Common HH2	[NEW_ASSET]	Room 437	Asset added with specified RU size that differs from Device Catalog	
	06/17/2010, 2:47 PM CST	Socet Station	SMSL-HH-01	N/A	Room 303	Item scanned during inventory that should not be in container/location	
Conflict							
This transaction removed MADU-EM1 from Room 306, and the system records show it was in that container/location.							
MADU-EM1 - Additional Information							
Model	PV10 Flat Unshielded Cable						
Manufacturer	Panduit						
Asset Number	1234567890						
Bar Code	192837 465192837465						
Serial Number	987654321						
MAC Address							
IP Address							
Rack Name							
Rack Position							
RU Height							
Remove Asset							
Time/Date:		06/16/2010, 8:21 PM CST					
Technician:		Jim Frost					
Handfield:		Jim's Handfield					
Asset:		MADU-EM1					
Removed Location:		Room 306					
Removed RU:							
Reconciliation							
Accept Transaction							
<input checked="" type="checkbox"/>		Accept will accept the transaction as is, and put the asset into the In-Transit state even though it was not in the container/location specified.					
Reject Transaction							
<input checked="" type="checkbox"/>		Reject will throw out the entire transaction.					

FIG. 3

4/13

Asset Management - Panduit Physical Infrastructure Manager

Asset Management

User: admin (Administrator)

Asset Administration
Asset Specifications
Asset Reconciliation
Asset Transactions
Asset Administration

Asset Reconciliation
Display All Assets
Display Single Asset

Transaction	Date/Time	Technician	Handheld	Asset	Location	Issue
Remove Asset	06/16/2010, 8:21 PM CST	Jim Frost	Jim's Handheld	MAD-BM1	Room 306	Asset removed from a container location it was not in
Update Asset Status	06/16/2010, 8:39 PM CST	Jim Frost	Jim's Handheld	MAD-BM1	NA	Status changed to a status that is no longer in the system
Update Asset Location	06/16/2010, 8:41 PM CST	Jim Frost	Jim's Handheld	MAD-BM1	Rack 295, RU7	Location updated to RU7 that is already occupied
Tag Asset	06/17/2010, 10:25 AM CST	Bob Wilcox	Compass HH1	NewServer1	Room 301	Asset tagged with barcode that already exists
Add Asset	06/17/2010, 10:46 AM CST	Tom Fuler	Compass HH2	[NEW_ASSET]	Room 437	Asset added with specified RU sets that differs from Device Catalog
Inventory	06/17/2010, 2:47 PM CST	Sasha Steiner	EM65-HH101	NA	Room 303	Item scanned during inventory that should not be in container location

Transaction

Update Asset Location

Date/Time: 06/16/2010, 8:41 PM CST
 Technician: Jim Frost
 Handheld: Jim's Handheld
 Asset: MAD-BM1
 Updated Location: Rack 295
 Updated RU: RU 7

Reconciliation

Accept Transaction ☒ Accept

Accept will accept the transaction as is, and add the asset to the RU even though it is already occupied.

Reject Transaction ☒ Reject

Reject will throw out the entire transaction.

Model PVD Flat Unshielded Panel

Manufacturer Panduit

Asset Number 1234567890

Bar Code 192837 465192837465

Serial Number 987654321

MAC Address 84:2B:4C:91:00:21

IP Address 192.168.0.111

Rack Name Rack 295

Rack Position 7

RU Height 1

Jim's PM - Additional Information

Model PVD Flat Unshielded Panel

Manufacturer Panduit

Asset Number 1234567890

Bar Code 192837 465192837465

Serial Number 987654321

MAC Address 84:2B:4C:91:00:21

IP Address 192.168.0.111

Rack Name Rack 295

Rack Position 7

RU Height 1

FIG.4

5/13

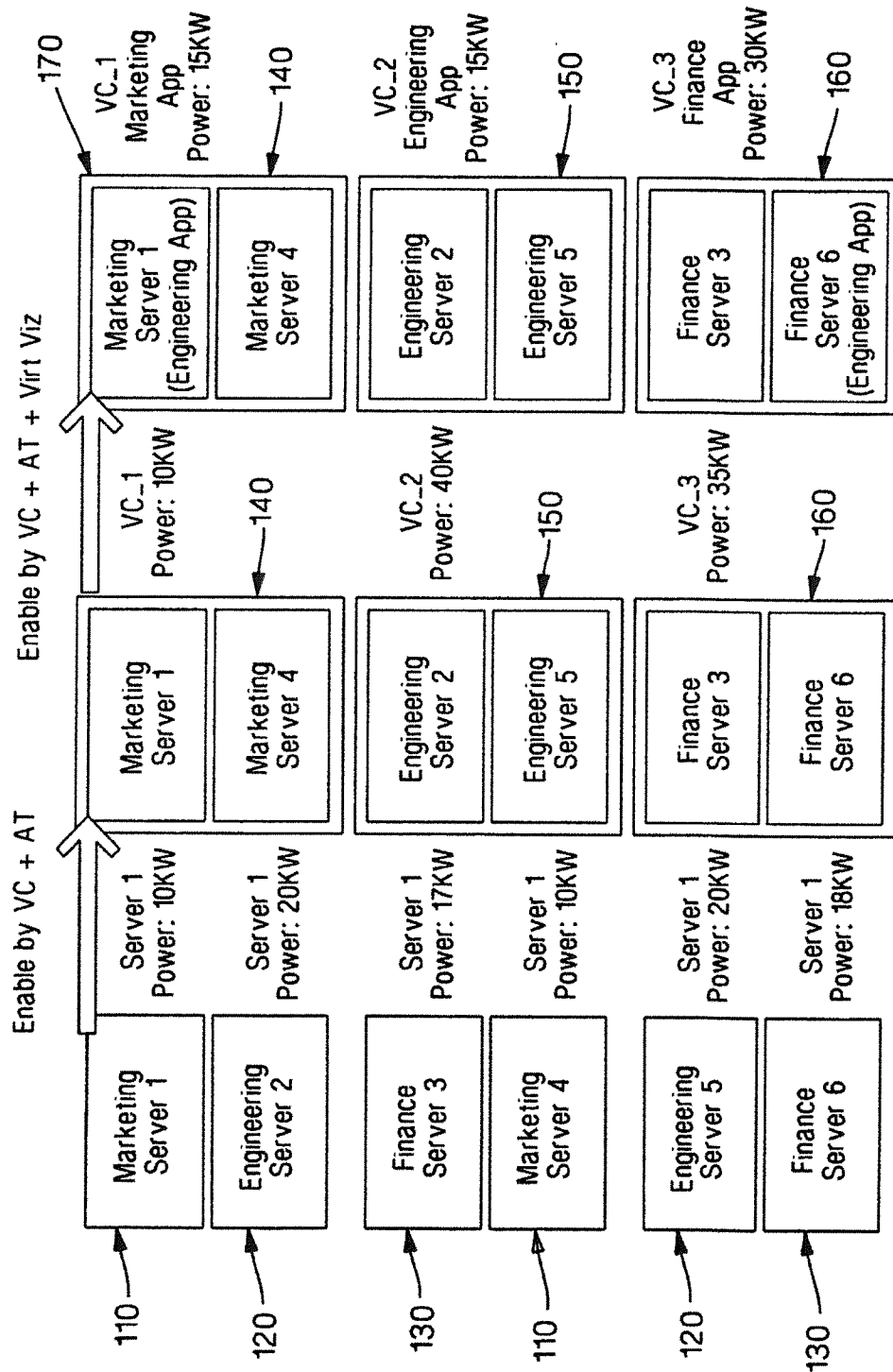
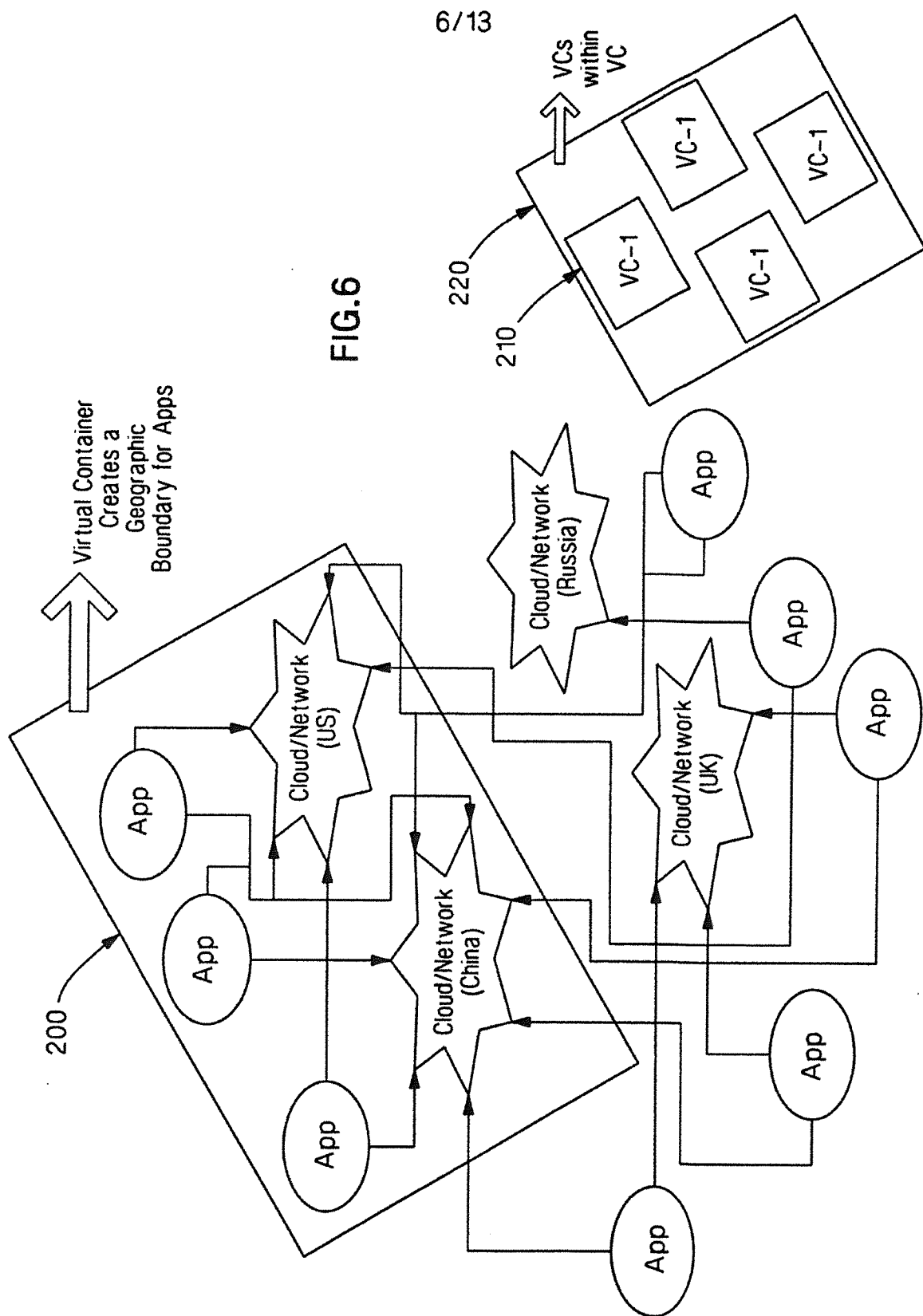


FIG.5



7/13

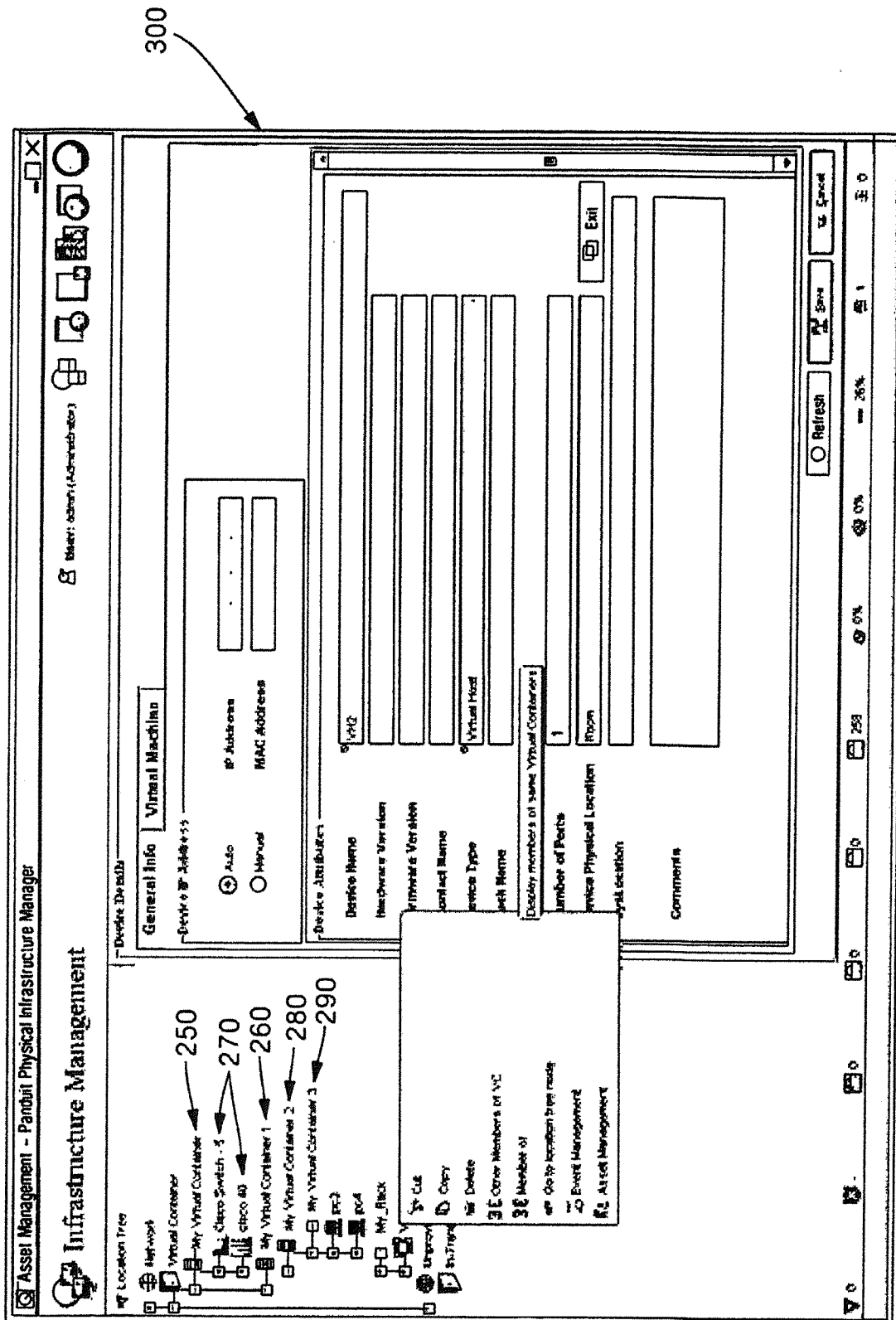


FIG.7

8/13

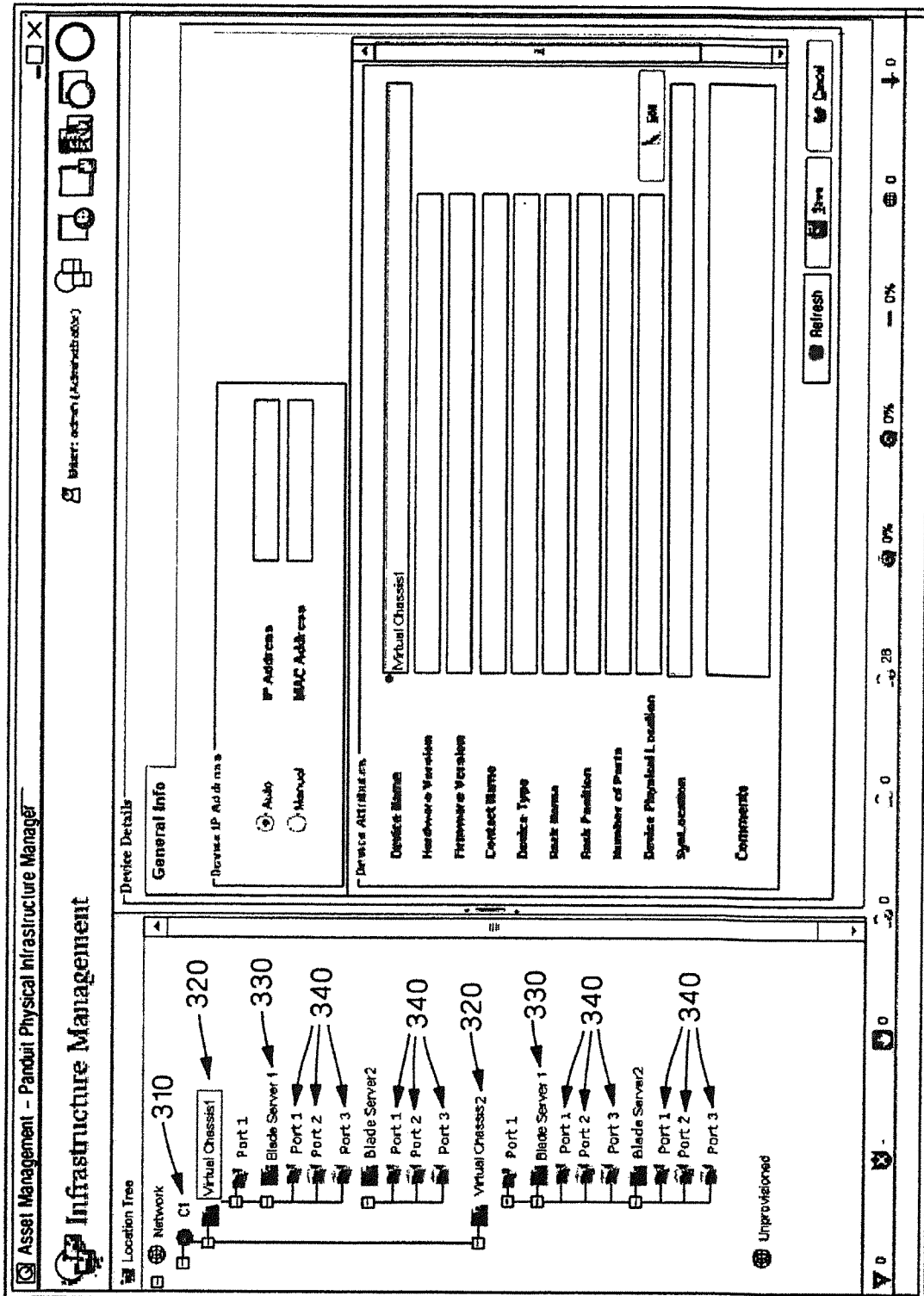


FIG.8

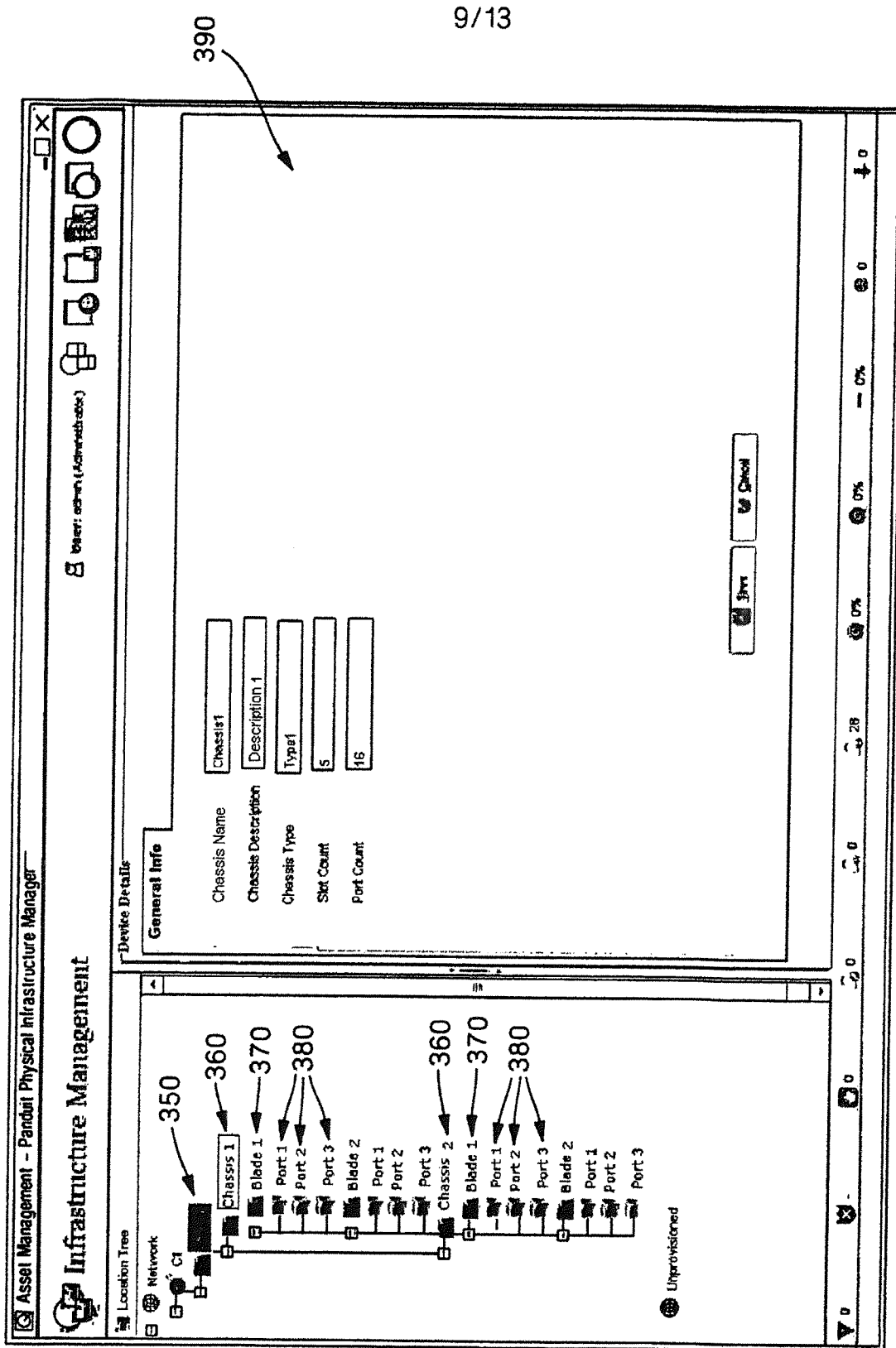


FIG.9

10/13

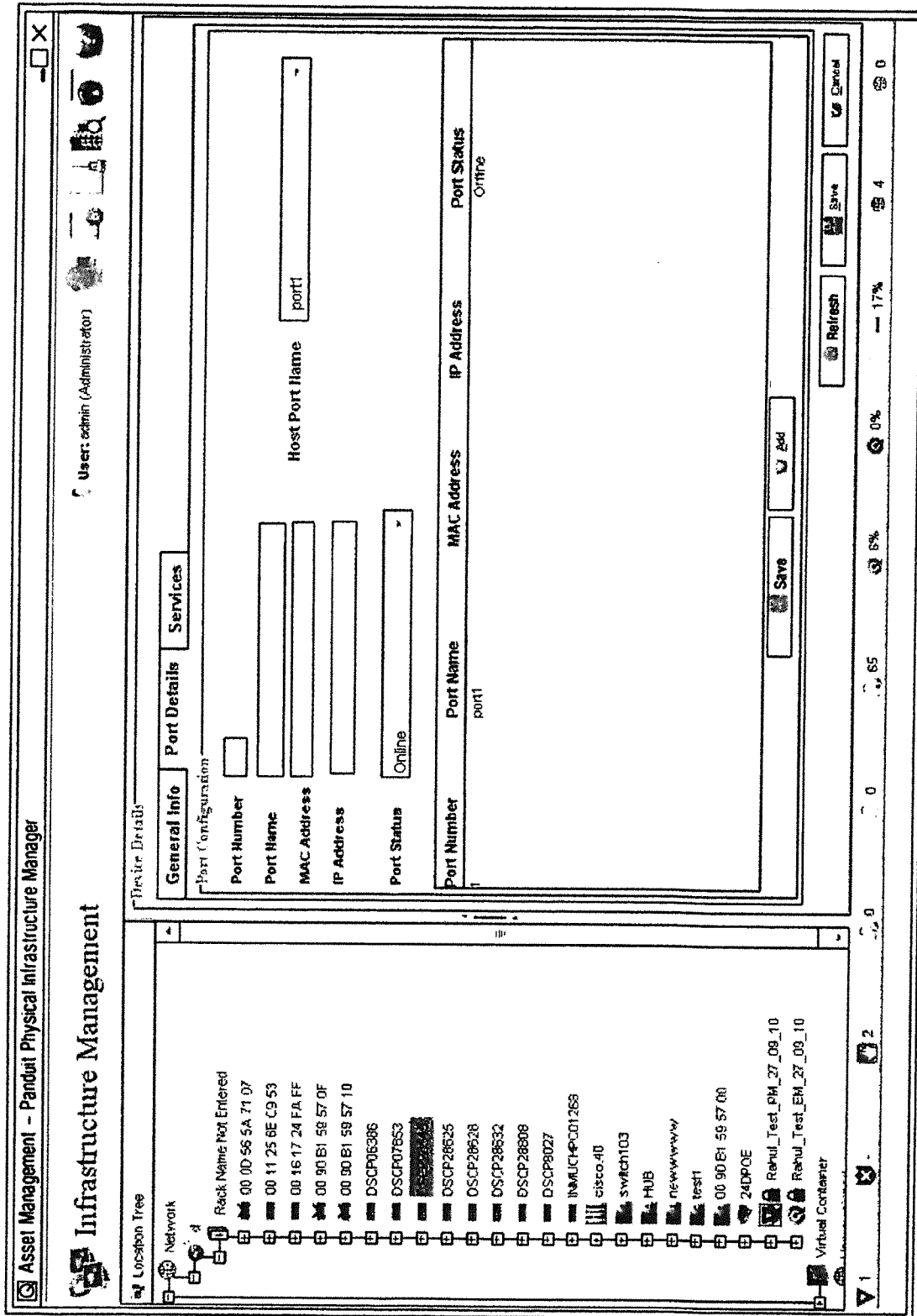


FIG. 10

11/13

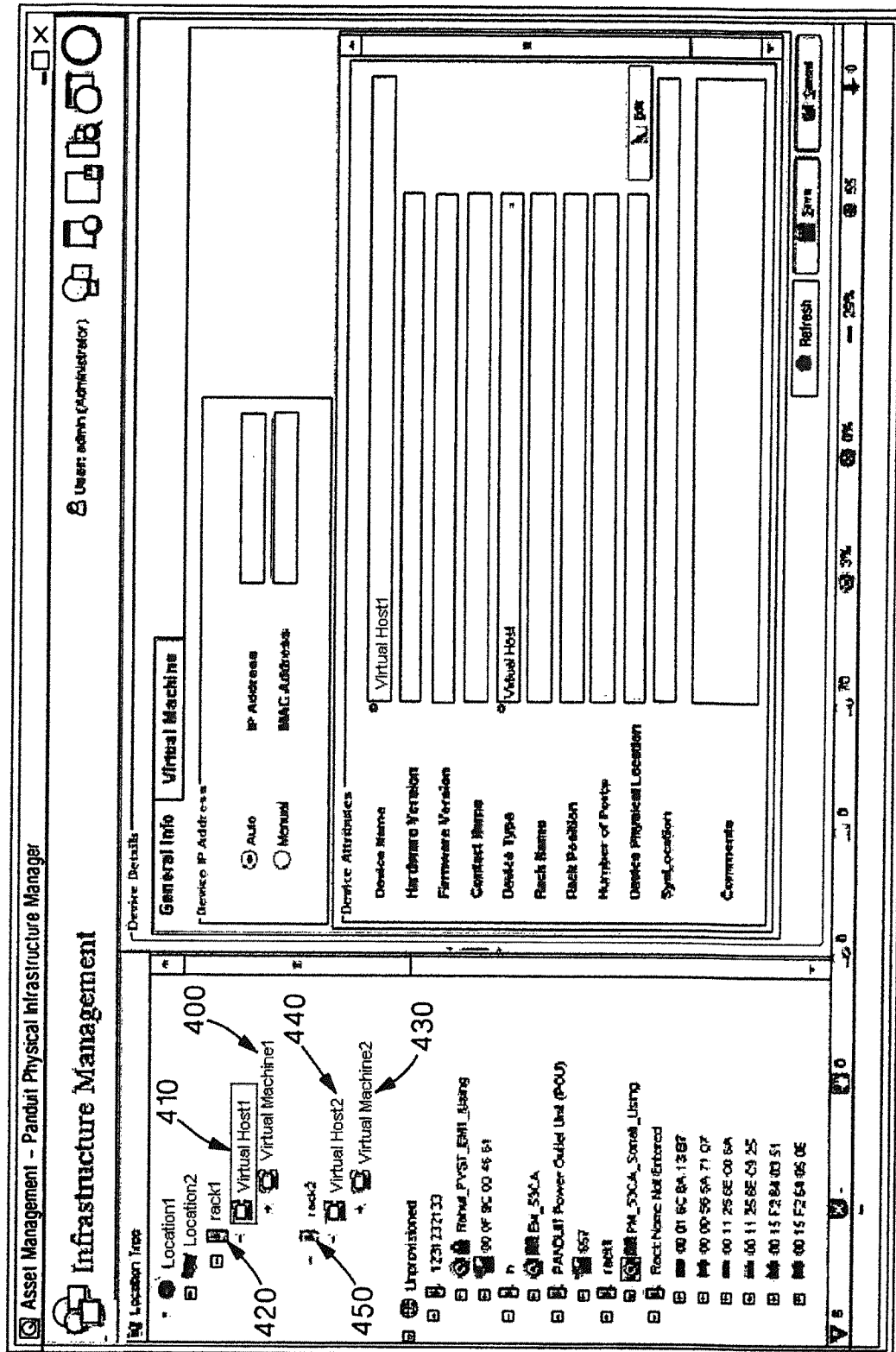


FIG. 11

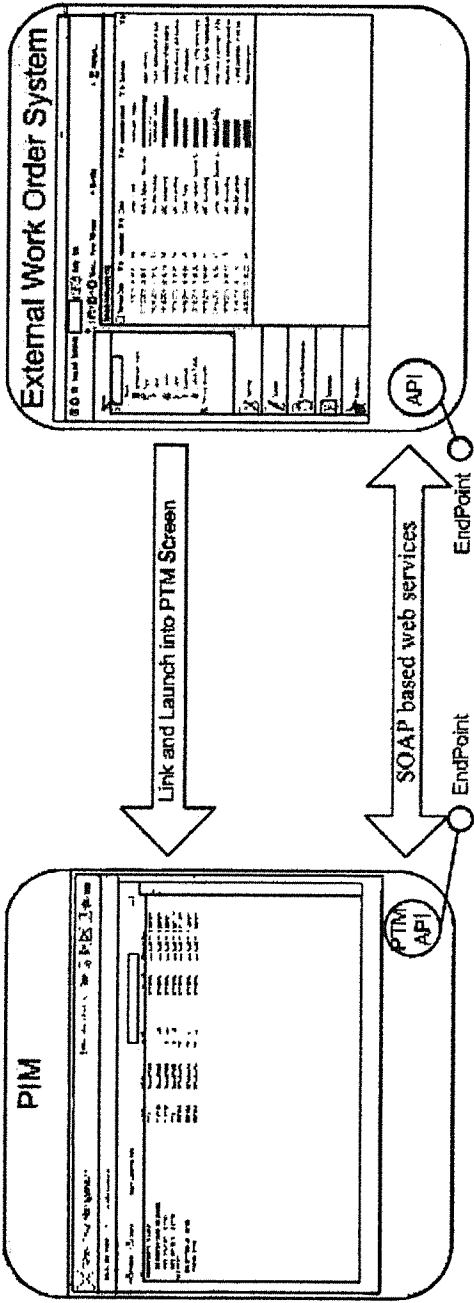
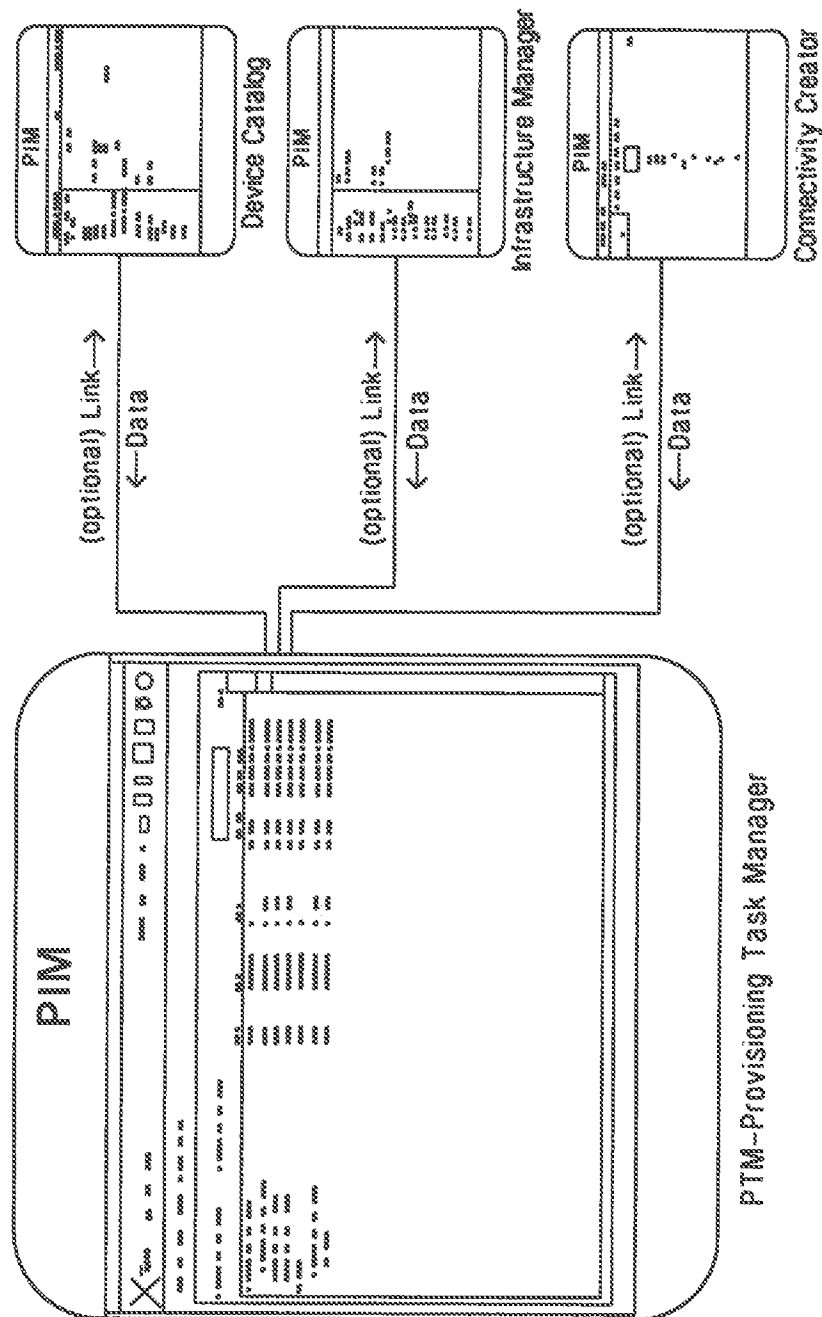


FIG.12



മുഖ്യമന്ത്രി