(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 February 2017 (16.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/027675 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *G06F 21/57* (2013.01)

(21) International Application Number:
PCT/US2016/046494

(22) International Filing Date:
11 August 2016 (11.08.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/824,143 12 August 2015 (12.08.2015) US

(71) Applicant: **SERVICENOW, INC.** [US/US]; 2225 Lawson Lane, Santa Clara, California 95054 (US).

(72) Inventor: **DELINOCCI, John**; c/o ServiceNow, Inc., 2225 Lawson Lane, Santa Clara, California 95054 (US).

(74) Agents: **MCCLEARY, Ryan T.** et al.; 3001 West Big Beaver Rd., Suite 624, Troy, Michigan 48084 (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

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

(54) **Title**: AUTOMATED ELECTRONIC COMPUTING AND COMMUNICATION SYSTEM EVENT ANALYSIS AND MANAGEMENT

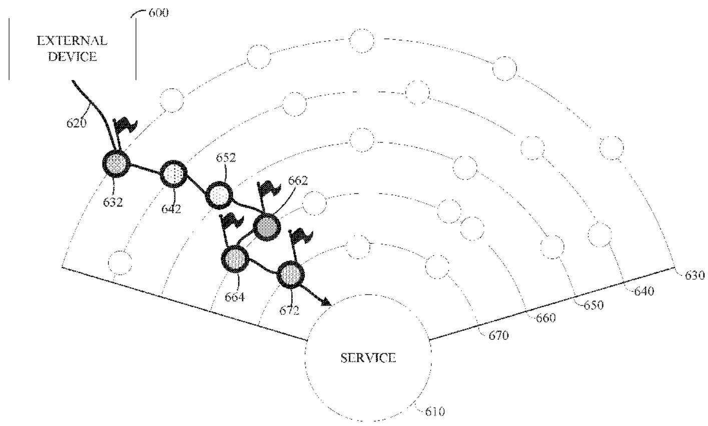

FIG. 6

(57) **Abstract**: Automatic automated electronic computing and communication system event analysis and management includes identifying an event, generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, identifying an element of the electronic computing and communication system based on the representation, identifying a metric for the element, automatically investigating to determine a value for the metric, generating a remediation priority for the element based on a metric weight associated with the metric and a network layer value associated with a network layer associated with a network layer role associated with the element, and generating a graphical representation of the electronic computing and communication system indicating the remediation priority.

WO 2017/027675 A1

AUTOMATED ELECTRONIC COMPUTING AND COMMUNICATION SYSTEM EVENT ANALYSIS AND MANAGEMENT

TECHNICAL FIELD

[0001] The present disclosure is generally related to information technology, and in particular to computer-implemented methods, systems, and apparatuses to analyze events occurring in an electronic computing and communication system.

BACKGROUND

[0002] An electronic computing and communication system may include one or more communicating and computing elements, which, in the course of communicating and computing, generate event information that may indicate an abnormal operating condition, such as a failure, affecting one or more elements of the electronic computing and communication system, such as a service. Accordingly, a method and apparatus for automated electronic computing and communication system event analysis and management may be advantageous.

SUMMARY

[0003] One aspect of the disclosure is a method of automatically analyzing an electronic computing and communication system event. The method may include identifying information indicating an event in an electronic computing and communication system, generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, wherein the computer readable representation represents a plurality of elements of the electronic computing and communication system organized in a hierarchical plurality of network layers, identifying an element of the electronic computing and communication system from plurality of elements based on the computer readable representation of the electronic computing and communication system, identifying a metric for the element of the electronic computing and communication system, and automatically investigating the electronic computing and communication system to determine a value for the metric for the element of the electronic computing and communication system. On a condition that the value is an abnormal value, automatically analyzing an electronic computing and communication system event may include generating a remediation priority for the element of the electronic computing and communication system based on a metric weight associated with the metric and a network layer value associated with a network layer from the hierarchical plurality of network layers, wherein the element is associated with a network layer role corresponding to the network layer. Automatically analyzing an electronic computing and communication system event generating a graphical representation of the electronic computing and communication system, the graphical representation indicating the remediation priority, and outputting or storing the representation.

[0004] Another aspect of the disclosure is a method of automatically analyzing an electronic computing and communication system event. The method may include identifying information indicating an event in an electronic computing and communication system, generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, wherein the computer readable representation represents a plurality of elements of the electronic computing and communication system organized in a hierarchical plurality of network layers, wherein each respective element from the plurality of elements is associated with a respective network layer role corresponding to a respective network layer, identifying a set of elements of the electronic computing and communication system from plurality of elements based on the computer readable representation of the electronic computing and communication system, identifying a plurality of metrics, wherein each element from the set of elements is associated with at least one respective metric from the plurality of metrics, automatically investigating the electronic computing and communication system to determine a plurality of values, wherein each value from the plurality of values corresponds with a respective metric from the plurality of metrics and a respective element from the set of elements, generating a plurality of remediation priorities, wherein each remediation priority from the plurality of remediation priorities corresponds with a respective value from the plurality of values, a respective metric from the plurality of metrics, and a respective element from the set of elements, and wherein each remediation priority from the plurality of remediation priorities is based on a metric weight associated with the respective corresponding metric and a network layer value associated with a respective network layer associated with a respective network layer role associated with the respective element, generating a graphical representation of the electronic computing and communication system, the graphical representation indicating at least some of the remediation priorities, and outputting or storing the representation.

[0005] Another aspect of the disclosure is a method of automatically analyzing an electronic computing and communication system event. The method may include identifying information indicating an event in an electronic computing and communication system, wherein the event is associated with a service, generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, wherein the computer readable representation represents a plurality of elements of the electronic computing and communication system organized in a hierarchical plurality of network layers, wherein each respective element from the plurality of elements is associated with a respective network layer role corresponding to a respective network layer, identifying a set of elements of the electronic computing and communication system from plurality of elements based on the computer readable representation of the electronic computing and communication system, identifying a plurality of metrics, wherein each element from the set of elements is associated with at least one respective metric from the plurality of metrics, automatically investigating the electronic computing and communication system to determine a plurality of values, wherein each value from the plurality of values corresponds with a respective metric from the plurality of metrics and a respective element from the set of elements, generating a plurality of remediation priorities, wherein each remediation priority from the plurality of remediation priorities corresponds with a respective value from the plurality of values, a respective metric from the plurality of metrics, and a respective element from the set of elements, and wherein each remediation priority from the plurality of remediation priorities is based on a metric weight associated with the respective corresponding metric and a network layer value associated with a respective network layer associated with a respective network layer role associated with the respective element, and generating a graphical representation of the electronic computing and communication system. Generating the graphical representation may include generating a graphical representation of the hierarchical plurality of network layers, wherein the service corresponds with a network layer from the hierarchical plurality of network layers, and for each element from the set of elements, generating a graphical representation of the element, and, on a condition that a value from the plurality of values corresponding to the element is an abnormal value, generating a graphical representation indicating that the value is an abnormal value and indicating a category associated with a metric from the plurality of metrics associated with the value. Generating the graphical representation may include generating a graphical representation of a path between an external device and the service, wherein the path intersects with at least one element from the set of elements in each network layer from the hierarchical plurality of network layers. Automatically analyzing an electronic computing and communication system event may include outputting the graphical representation for presentation to a user.

[0006] Variations in and details of these and other aspect of the teachings herein are described in additional detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The description herein makes reference to the accompanying drawings wherein like reference numerals refer to like parts throughout the several views.

[0008] FIG. 1 is a schematic diagram of an example of a cloud computing system in accordance with this disclosure.

[0009] FIG. 2 is a block diagram of an example internal configuration of a computing device in accordance with this disclosure.

[0010] FIG. 3 is a flow diagram of an example of electronic computing and communication system monitoring in accordance with this disclosure.

[0011] FIG. 4 is a flow diagram of an example of automated electronic computing and communication system event analysis and management in accordance with this disclosure.

[0012] FIG. 5 is a flow diagram of an example of electronic computing and communication system automated topology enumeration in accordance with this disclosure.

[0013] FIG. 6 is a diagram of an example of an interface for electronic computing and communication system automated event analysis in accordance with this disclosure.

DETAILED DESCRIPTION

[0014] An electronic computing and communication system may include many elements, such as computers, routers, switches, servers, and the like, in communication internally, within the electronic computing and communication system, and externally, with elements outside the electronic computing and communication system. The elements, individually or in combination, may generate event information messages or signals that may describe the status of the electronic computing and communication system, particularly changes in the status that may indicate a current or potential problem with the electronic computing and communication system. Events can be analyzed to identify how they affect the electronic computing and communication system and to determine how to correct current problems or mitigate the risk of future problems. Event analysis may be performed manually, which may include utilizing significant human resources to investigate and remediate events. For example, a human may manually trace physical wires connecting elements of the electronic computing and communication system or manually review data and interact with the electronic computing and communication system to identify current or historical state information for the electronic computing and communication system.

[0015] Automated electronic computing and communication system event analysis and management desirably reduces the human resource utilization associated with manual event analysis and management, and hence reduce the risk of human error. In some embodiments, automated electronic computing and communication system event analysis and management includes receiving information indicating an event, automatically discovering and enumerating the elements of the electronic computing and communication system to generate a computer readable representation of the current network topology architecture, automatically investigating the electronic computing and communication system to determine current operational state metrics, automatically evaluating the event based on the current operational state metrics and the current network topology architecture to determine respective remediation priorities for the elements of the electronic computing and communication system affected by the event, automatically remediating one or more elements of the electronic computing and communication system, or a combination thereof. Automated electronic computing and communication system event analysis and management may include using one or more monitoring templates, which are generated based on input, such as user input, or automatically based on automatically discovering and enumerating the elements of the electronic computing and communication system.

[0016] FIG. 1 is a schematic of an example of an electronic computing and communication system 100 in accordance with this disclosure. The electronic computing and communication system can include customers, such as customers 110 and 120. A customer may have clients, such as clients 112, 114 for customer 110 and clients 122, 124 for customer 120. A client 112/114/122/124 may be implemented as a computing system, which includes one or more computing devices, such as a mobile phone, a tablet computer, a laptop computer, a notebook computer, a desktop computer, or any other computing device. Although two customers 110/120, each having two clients 112/114/122/124, are shown in FIG. 1, an electronic computing and communication system may include any number of customers or clients or may have a different configuration of customers or clients. For example, there may be hundreds or thousands of customers and each customer may have any number of clients.

[0017] The electronic computing and communication system 100 can include datacenters, such as the two datacenters 130/140 shown. Each datacenter may have servers. For example, as shown the top datacenter 130 includes two servers 132/134, and the bottom datacenter 140 includes two servers 142/144. Each datacenter 130/140 may represent a different location where servers are located, such as a datacenter facility in San Jose, California or Amsterdam, Netherlands. Each server 132/134/142/144 may be implemented as a computing system, which may include one or more computing devices, such as a desktop computer, a server computer, or any other computer capable of operating as a server. Although two datacenters 130/140, each including two servers 132/134/142/144 are shown in FIG. 1, an electronic computing and communication system may have any number of datacenters and servers or may have a different configuration of datacenters and servers. For example, there may be tens of data centers and each data center may have hundreds or any number of servers.

[0018] Clients 112/114/122/124 and servers 132/13/142/144 may be configured to connect to a network 150. In some implementations, the clients of a customer connect to the network 150 via a common connection point. For example, the clients 112/114 of the customer 110 shown at the top left of FIG. 1, are shown as connected via a common connection point or link 116. In other implementations, one or more clients of a customer connect to the network 150 via distinct links. For example, as shown in the bottom left of FIG. 1, a client 122 is connected via a first link 126, and another client 124 is connected via a second link communicating via link 128. A link may be wired, as shown by links 116/126, wireless, as shown by connection point 128, or may include a combination of wired and wireless mediums.

[0019] The network 150 can, for example, be the Internet. The network 150 can also be or include a local area network (LAN), wide area network (WAN), virtual private network (VPN), or any other means of electronic computer communication capable of transferring data between any of clients 112/114/122/124 and servers 132/134/142/144. The network 150, the datacenters 130/140, or any other element, or combination of elements, of the system may include network hardware such as routers, switches, load balancers, other network devices, or combinations thereof. For example, each of datacenters 130/140 may have one or more load balancers for routing traffic from network 150 to various servers, such as servers 132/134/142/144.

[0020] Other implementations of the electronic computing and communication system are also possible. For example, devices other than the clients and servers shown may be included in the electronic computing and communication system. In an implementation, one or more additional servers may operate as an electronic computing and communication system infrastructure control, from which servers, clients, or both, of the cloud infrastructure are monitored, controlled, configured, or a combination thereof. For example, some or all of the techniques described herein may operate on said electronic computing and communication system servers. Alternatively or in addition, some or all of the techniques described herein operate on servers, such as servers 132/134/142/144.

[0021] In some embodiments, one or more of the elements of the electronic computing and communication system 100, such as the clients 112/114/122/124 or the servers 132/134/142/144, are configured to store, manage, and provide one or more databases, tables, or other information sources, or a portion thereof, such as a configuration management database (CMDB), a management information base (MIB), or a combination thereof. A configuration management database includes records representing one or more entities, devices, or units of the electronic computing and communication system, such as the clients 112/114/122/124, the customers 110/120, the datacenters 130/140, the servers 132/134/142/144, the access point 128, the network 150, or any other element, portion of an element, or combination of elements of the electronic computing and communication system 100. The configuration management database may include information describing the configuration, the role, or both, of an element of the electronic computing and communication system 100. In some embodiments, a management information base includes one or more databases listing characteristics of the elements of the electronic computing and communication system 100. An object identifier (OID) may represent object identifiers of objects or elements in the MIB.

[0022] In some embodiments, automated electronic computing and communication system event analysis and management is implemented on a single device, such as a single server. In other embodiments, automated electronic computing and communication system event analysis and management are implemented on a combination of devices, such as a combination of clients 112/114/122/124 and servers 132/134/142/144.

[0023] FIG. 2 is a block diagram of an example internal configuration of a computing device 200, such as a client 112/114/122/124 or a server 132/134/142/144 of the electronic computing and communication system 100 shown in FIG. 1. As previously described, clients or servers may take the form of a computing system including multiple computing devices, or in the form of a single computing device, for example a mobile phone, a tablet computer, a laptop computer, a notebook computer, a desktop computer, a server computer and the like.

[0024] The computing device 200 as shown includes a processor 210, memory 220, a network communication unit or interface 230, a network communication interface 240, a user interface 250, a location identification unit 260, a power source 270, and a bus 280.

[0025] The processor 210 can be a conventional central processing unit (CPU). The processor 210 can include single or multiple processors each having single or multiple processing cores. Alternatively, the processor 210 can include another type of device, or multiple devices, capable of manipulating or processing information now-existing or hereafter developed. The processor 210 can be a general purpose processor or a special purpose processor.

[0026] In some embodiments, the memory 220 may include random access memory (RAM), read only memory (ROM), a disk drive, a solid state drive, or a combination thereof. The memory 220 can include executable instructions and data for immediate access by the processor 210. The memory 220 may alternatively or additionally include one or more DRAM modules such as DDR SDRAM. In brief, the memory 220 can include another type of device, or multiple devices, capable of storing data for processing by the processor 210 now-existing or hereafter developed. The processor 210 can access and manipulate data in the memory 220 via the bus 280. The memory 220 can include executable instructions and application files along with other data. The executable instructions can include, for example, an operating system and one or more application programs for loading in whole or part into the memory 220 and to be executed by the processor 210. The operating system can be, for example, a Windows, Mac OS X, or Linux operating system. The application program can include, for example, a web browser, a web server, a database server, or a combination thereof. Application files include, for example, user files, database catalogs, and configuration information. The memory 220 may comprise one or multiple devices and may utilize one or more types of storage, such as solid state or magnetic.

[0027] In some embodiments, the internal configuration may include one or more input/output devices, such as the network interface 240 and the user interface 250. The network interface 240 and the user interface 250 can be coupled to the processor 210 via the bus 280. The network interface 240 can, for example, provide a connection to a network, such as the network 150 shown in FIG. 1, and may take the form of a wired network interface, such as Ethernet, or a wireless network interface. Other output devices that permit a user to program or otherwise use the computing device 200 can be provided in addition to or as an alternative to the user interface 250. When the output device is or includes a display, the display can be implemented in various ways, including by a liquid crystal display (LCD) or a cathode-ray tube (CRT) or light emitting diode (LED) display, such as an OLED display.

[0028] Other implementations of the internal architecture of clients and servers are also possible. For example, servers may omit location unit 260. The operations of the processor 210 can be distributed across multiple machines, which can be coupled directly or across a local area or other network. The memory 220 can be distributed across multiple machines such as network-based memory or memory in multiple machines performing the operations of clients or servers. Although depicted here as a single bus, the bus 280 can be composed of multiple buses.

[0029] In some implementations, automated electronic computing and communication system event analysis and management includes generating a computer readable representation of an electronic computing and communication system, which may include representing physical elements of the electronic computing and communication system, physical connectivity between elements of the electronic computing and communication system, logical connectivity between elements, or a combination thereof. For example, generating the computer readable representation includes determining a network topology, which may represent physical elements, physical connectivity, or both; a network architecture, which may represent logical connectivity; or a combination thereof. The electronic computing and communication system may be represented by a network topology architecture, which includes a combination of the network architecture and the network topology.

[0030] Physical elements of the electronic computing and communication system, such as servers, routers, wired or wireless links, and the like, may be included in a physical layer, which is represented by the network topology. In some embodiments, the network topology may represent physical elements of the electronic computing and communication system, their physical location, which includes relative physical location, geospatial physical location, or both, and physical connections. For example, an element of the electronic computing and communication system may communicate with another element of the electronic computing and communication system via a physical medium, such as a linear bus, which can be a physical cable. In some configurations, physical elements within the physical layer include other physical elements. For example, as shown in FIG. 2, the computing device 200 includes a communication unit 240, such as an Ethernet interface, which are both physical elements.

[0031] In some implementations, elements of an electronic computing and communication system may communicate via a network stack, which often includes a hierarchy of network communication layers. In some embodiments, the lowest layer of the network stack may be the physical layer and may correspond with the network topology. The electronic computing and communication system may include one or more network stack layers above the physical layer. For example, the electronic computing and communication system may include a data link layer above the physical layer and a network layer above the data link layer. The data link layer may be omitted or combined with the network layer. It is also possible for the electronic computing and communication system to include one or more host or service layers above the network layer. For example, the host layers can include a transport layer above the network layer, a session layer above the transport layer, a presentation layer above the session layer, an application layer above the presentation layer, or a combination thereof. Any one or more layers may be omitted or combined with other layers, and other layers may be included.

[0032] The network architecture may represent the logical organization of the elements of the electronic computing and communication system, which includes representing routing, paths, or flows of information in the electronic computing and communication system. In some embodiments, the network architecture includes a series of functional network architecture layers, which may be oriented relative to a service that is, for example, an instance of an application executed on one or more physical servers. The lowest layer of the network architecture may be the service, or access, layer. The network architecture may also include one or more layers above the service layer. In such cases, each layer may represent a defined degree of separation from, or proximity to, an instance of a service on one or more physical devices.

[0033] In some embodiments, the network architecture may include one or more distribution or aggregation layers above the service layer. The distribution or aggregation layers can include elements of the electronic computing and communication system that distribute information toward the service layer elements, aggregate information from the service layer elements, or both. In an example, the most proximate layer to the service layer, which may be referred to herein as the second layer, includes a Top of Rack (ToR) switch. The next most proximate layer, which may be above the second layer and may be referred to herein as the third layer, includes a Direct Server Return (DSR) load balancer in this example.

[0034] The network architecture may additionally or alternatively include one or more backbone, or core, layers above the service layer. In some embodiments, the backbone layers include elements of the electronic computing and communication system that transport information between distribution or aggregation layer elements, transport communications between the electronic computing and communication system and external systems, or both. For example, the network architecture can include a fourth layer, above the third layer, that is a core layer and represents the broadest scope of communication within the electronic computing and communication system, and a fifth layer, above the fourth layer, that is a border layer and can include, for example, a firewall.

[0035] In some embodiments, the network architecture includes an external interface layer, such as an Internet Service Provider (ISP) layer. The external interface layer may include elements, such as a circuit, on the external side of an interface between the electronic computing and communication system and external systems, such as the Internet, and may include elements, such as a firewall of a backbone layer, on the internal side of the interface between the electronic computing and communication system and external systems.

[0036] An element of the electronic computing and communication system may operate within one or more network architecture layers and its operation identified as a role for the element. For simplicity and clarity, elements of the electronic computing and communication system operating according to roles in a network architecture layer are described herein relative to an identified, or current, layer. For example, elements operating in the current layer are referred to herein as lateral elements, elements operating in a layer below the current layer, which may be closer to the service layer, are referred to herein as lower layer elements, and elements operating in layers above the current layer, which may be further from the service layer than the current layer, are referred to herein as higher layer elements.

[0037] FIG. 3 is a flow diagram of an example of electronic computing and communication system monitoring in accordance with this disclosure. In some embodiments, automated electronic computing and communication system event analysis and management includes monitoring and is implemented in one or more computing devices, such as one or more of the clients 112/114/122/124, the servers 132/134/142/144, or a combination thereof as shown in FIG 1.

[0038] As shown in FIG. 3, an electronic computing and communication system includes automated topology enumeration at 300, generating monitoring templates 310, and monitoring the electronic computing and communication system at 320.

[0039] In some embodiments, automatic network topology enumeration at 300 includes automatically discovering one or more elements, such as devices or units, in the electronic computing and communication system, discovering communication connections between the elements, determining a logical organization of network communication, or a combination thereof. Automated topology enumeration at 300 may be similar to the automated topology enumeration shown in FIG. 5 and described below.

[0040] One or more monitoring templates is generated at 310. A monitoring template may indicate one or more elements of the electronic computing and communication system to be monitored. Generating monitoring templates at 310 may include manually generating monitoring templates, automatically generating monitoring templates, or both.

[0041] Where a monitoring template is manually generated at 310, the monitoring template may be generated by copying or modifying a previously generated monitoring template, in response to input, such as user input. In an example, a first monitoring template is associated with a device manufacturer and a second monitoring template is generated based on the first monitoring template and is associated with a device manufactured by the device manufacturer.

[0042] Automatically generating a monitoring template at 310 may include automatically copying or modifying a previously generated monitoring template that is based on the topology of the electronic computing and communication system, such as the topology automatically enumerated at 300. For example, one or more monitoring templates may be generated automatically based on the SNMP discovery information.

[0043] In some embodiments, one or more monitoring templates are stored in a data store, such as a configuration management database (CMDB). The stored monitoring templates may be associated with, or mapped to, information indicating the discovered elements of the electronic computing and communication system, such as the manufacturer of the element, the device type of the element, the model of the element, the firmware version for the element, one or more hardware components of the element, or a combination thereof.

[0044] Elements of the electronic computing and communication system are monitored at 320 based on monitoring templates. For example, the electronic computing and communication system may be monitored at 320 based on defined monitoring templates, based on the monitoring templates generated at 310, or based on a combination of defined monitoring templates and automatically generated monitoring templates. A monitoring template may be associated with one or more metrics, or conditions, such that monitoring at 320 includes determining whether to include a monitoring template in the monitoring based on the associated metrics. In an example, generating the monitoring templates at 320 includes determining metrics, or values thereof, for respective monitoring templates based on, for example, the information identified at 310. Additionally or alternatively, one or more metrics, or values thereof, may be determined in response to input, such as user input.

[0045] FIG. 4 is a flow diagram of an example of automated electronic computing and communication system event analysis and management in accordance with this disclosure. Automated electronic computing and communication system event analysis and management may be implemented in one or more computing devices, such as one or more of the clients 112/114/122/124, the servers 132/134/142/144, or a combination thereof as shown in FIG. 1.

[0046] As shown, automated electronic computing and communication system event analysis and management includes identifying an event at 400, automated topology enumeration at 410, automated system investigation at 420, automated event analysis at 430, and automated remediation at 440.

[0047] Identifying an event at 400 may include identifying information indicating an event in an electronic computing and communication system. In some embodiments, a diagnostic unit receives event information, such as a message, notification, or a signal, indicating an event or incident in the electronic computing and communication system. The diagnostic unit may be an element of the electronic computing and communication system, for example a server such as a server 132/134/142/144 shown in FIG. 1.

[0048] An event, or incident, notification may include information representing a network or device event, an alarm condition, the opening of a service ticket, or any other occurrence describing a change in the electronic computing and communication system. In some embodiments, an event or incident represents an adverse state of one or more elements of the electronic computing and communication system. An event may be a network layer event, a host layer event, or an event associated with any other network communication layer. An event notification may describe an event affecting one or more network communication layers, such as the network layer, the host or service layer, or any other network communication layer. The event notification can be received from a system or component external to the elements implementing automated electronic computing and communication system event analysis and management.

[0049] An event may be associated with a subject that represents a failed or affected service, such as an application that provides a service, such as a data storage service, a data manipulation service, a presentation service, a communication service, or the like. For example, the subject service may be an e-mail service, a printing service, a network file system, directory services, a file sharing service, an instant messaging service, a video telephony service, a world wide web service, a time service, or any other service that may be included in the electronic computing and communication system.

[0050] In an example, an event notification is a machine-readable communication, message, or other signal automatically generated by one or more of the elements of the electronic computing and communication system that experienced or detected the event.

[0051] Identifying an event at 400 may include receiving a message at the diagnostic unit and evaluating the message to determine whether the message indicates an event notice. For example, the diagnostic unit can evaluate a list, or other data store, of defined events based on information included in the message to determine whether the message indicates an event. In some embodiments, a message is identified as an event notice in response to input, such user input, indicating that the message is an event notice.

[0052] The electronic computing and communication system topology is automatically enumerated at 410. Automated topology enumeration may be performed at 410 in response to receiving the event notification at 400 and may be similar to the automated topology enumeration at 300 in FIG. 3 or the automated topology enumeration described below with respect to FIG. 5. In some embodiments, automated topology enumeration at 410 includes associating one or more discovered elements of the network with the event notification identified at 400. For example, information describing the discovered element, such as a list of enumerated network devices, can be associated with or included in an incident ticket, such as by including the information describing the discovered device in a work note associated with the incident ticket.

[0053] The electronic computing and communication system is automatically investigated at 420 by, e.g., identifying an element of the electronic computing and communication system based on the computer readable representation of the electronic computing and communication system generated at 410. In some embodiments, the investigation also includes identifying a metric for the element of the electronic computing and communication system. Automatically investigating the electronic computing and communication system at 420 can also include determining a value for the metric for the element of the electronic computing and communication system.

[0054] The electronic computing and communication system topology generated at 410 may indicate one or more elements and one or more metrics for respective elements such that automatically investigating the electronic computing and communication system at 420 includes determining values, such as current status values, for the one or more metrics for one or more elements of the electronic computing and communication system.

[0055] Automatically investigating the electronic computing and communication system at 420 may include evaluating, such as iteratively, the elements of the electronic computing and communication system identified at 410.

[0056] Current status or metric values may be determined using polling or otherwise querying one or more of the elements of the electronic computing and communication system. Current status or metric values may also be determined by retrieving stored or historical information from ongoing or previously executed metrics collection. Automatically investigating the electronic computing and communication system at 420 may include evaluating the identified current metric values to identify a probability that the respective status may affect a related service.

[0057] The metrics can be categorized based on the network architecture, the currently running services, or the like. For example, the categories may include change, availability, performance, capacity, variance, etc.

[0058] In some embodiments, one or more values of one or more metrics are identified as abnormal, which may indicate a current problem or likely future problem, and the metric is identified, or flagged, for further evaluation.

[0059] Automatically investigating the electronic computing and communication system at 420 can also include identifying network reporting information, such as by querying a network reporting layer generated using SNMP polling, SNMP traps, Syslog data, Netflow data, transaction collection data, or the like.

[0060] The automatic investigation of the electronic computing and communication system at 420 may further include identifying relevant change management information. Change management information indicates configuration changes occurring in one or more of the enumerated electronic computing and communication system elements. In one example, a change management system, which can be an external system, is queried or polled to identify recent or current tracked changes to the electronic computing and communication system. One or more configuration management data sources, whether provided by internal systems within the electronic computing and communication system or by external systems, may be queried to identify configuration changes omitted from the change management system. In addition, one or more external maintenance or configuration systems, such as a vendor system, may be queried to identify changes to elements that affect the electronic computing and communication system and are omitted from internal change and configuration management data sources. For example, external changes can include changes by an ISP, such as circuit maintenance.

[0061] Automatically investigating the electronic computing and communication system at 420 can include identifying availability information. Availability information includes a category of metrics pertaining to availability of an element of the electronic computing and communication system, one or more components thereof, or a group of elements and related components. For example, information indicating an abnormal availability affecting a relatively large portion of the electronic computing and communication system may be associated with a relatively high weight.

[0062] Automatically investigating the electronic computing and communication system at 420 may include identifying performance information. Performance information includes a category of metrics pertaining to the performance of an element of the electronic computing and communication system, one or more components thereof, or a group of elements and related components. For example, information indicating an abnormal performance condition or state that affect a relatively large portion of the electronic computing and communication system may be associated with a relatively high weight. Performance information includes, for example, CPU utilization, memory utilization, traffic utilization, or the like.

[0063] Automatically investigating the electronic computing and communication system at 420 may include identifying capacity information. Capacity information includes a category of metrics representing utilization, such as peak or average utilization, relative to maximum capacity or capability for a feature of an element of the electronic computing and communication system, one or more components thereof, or a group of elements and related components.

[0064] Automatically investigating the electronic computing and communication system at 420 may include identifying variance information. Variance information includes information indicating a variance in a metric value that exceeds a defined range, such as a range, which may be positive, negative, or both, defined from a defined baseline value for an element of the electronic computing and communication system, one or more components thereof, or a group of elements and related components. For example, a load balancer can balance a volume or amount of traffic for a server pool within a defined range. If the load balancer starts blocking all inbound traffic to the server pool, the traffic volume of that pool may drop to zero without otherwise generating an error. This can indicate a variance greater than the defined range.

[0065] The topology enumeration at 410, the system investigation at 420, or both, may be used to identify one or more services that are affected by the event identified at 400.

[0066] The event identified at 400 is automatically analyzed at 430. In some embodiments, the automated event analysis at 430 may include evaluating the network elements enumerated at 410, the metric values determined at 420, or both.

[0067] Automated event analysis at 430 may include determining whether a metric value associated with an element of the electronic computing and communication system indicates an abnormal value, such as a value that exceeds a defined threshold or a value outside a defined expected range associated with the metric. As a result, the element, and the element, the metric, or both, can be identified for further evaluation. For example, an element may be associated with a flag indicating that an abnormal value was identified for the element.

[0068] Automated event analysis at 430 may include generating output, such as a summary report, that identifies one or more elements of the electronic computing and communication system for remediation, such as auto-remediation at 440. For example, elements may be identified for remediation based on a probability of failure for the element, a measure of the expected affect that an identified abnormality at the element may have on other elements of the electronic computing and communication system, or a combination thereof.

[0069] One or more flags, representing abnormal values, may be associated with one or more categories, such as the change category, the availability category, the performance category, the capacity category, the variance category, or the like. In some embodiments, a flag is associated with a value, such as a weighted value, that represents an indication of a priority for remediating the element in response to the event. In an example, a relatively low value associated with a flag indicates a low priority for remediating the element and a relatively high value associated with the flag indicates a high priority for remediating the element. Flags associated with the availability category may be associated with a relatively high weight, such as 255, flags associated with the change category may be associated with a weight lower than the availability weight, such as 200, flags associated with the performance category may be associated with a weight lower than the change weight, such as 150, and flags associated with the capacity category may be associated with a weight lower than the performance weight, such as 100.

[0070] In some embodiments, the flag value for the metrics within a category are identified based on the category. For example, performance metrics can be associated with the flag value of 150. One or more metrics may be associated with a flag value relative to, or independent of, the category flag value. In an example, the performance category includes a latency metric, and a latency flag associated with an abnormal value of the latency metric is associated with a latency flag value, which may differ from the performance flag value.

[0071] It is also possible for each layer in the network topology architecture to be associated with a value, such as a weighted value, that represents the expected affect that an abnormality of an element of the electronic computing and communication system within the respective layer may have on other, related, elements of the electronic computing and communication system, such as the expected affect that the abnormality may have on a service in communication with the element associated with the abnormality. In some embodiments, the network topology architecture layer values are based on the relative distance of the network topology architecture layer from the service. The network topology architecture layer values may be inversely proportional to the relative distance from the lowest layer. For example, a routing layer, adjacent to the service layer, can have a relatively high network topology architecture layer value, such as 255, a distribution layer, such as a load balancing layer that is above or more remote than the routing layer, can have a network topology architecture layer value lower than the routing layer value, such as 200, a core layer that is above the distribution layer can have a network topology architecture layer value lower than the distribution layer value, such as 150, a border layer that is above the core layer can have a network topology architecture layer value lower than the core layer value, such as 100, and an Internet layer that is above the border layer can have a network topology architecture layer value lower than the border layer, such as 50.

[0072] Flag values, including category flag values and metric flag values, the network topology architecture layer values, or a combination thereof, may be identified in some cases based on input, such as user input.

[0073] Automated event analysis at 430 may include generating a remediation priority for the element of the electronic computing and communication system based on a metric weight a network layer value. The remediation priority indicates a priority, or order, of elements of the electronic computing and communication system, for remediating, further investigating, repairing, or the like, the electronic computing and communication system in response to the event.

[0074] In some embodiments, automated event analysis at 430 includes generating, storing, outputting, or both, one or more reports representing a result of the automated event analysis, such as the example graphical representation shown in FIG 6 and described below.

[0075] Automated event analysis at 430 may include receiving external information indicating a measure of accuracy for the automated event analysis. For example, input, such as user input, indicating a measurement of accuracy of the automated event analysis may be received in response to outputting the automated event analysis information. The input may be stored in association with the automated event analysis information.

[0076] One or more elements of the electronic computing and communication system is automatically remediated at 440. Automatic remediation, or auto-remediation, at 440 includes automatically configuring, or adjusting the configuration of, one or more elements of the electronic computing and communication system. In some embodiments, auto-remediation at 440 includes generating one or more remediation records and storing the remediation records in association with one or more of the elements enumerated at 410, one or more of the metric values determined at 420, the automated event analysis information, or a portion thereof, identified at 430, or a combination thereof. In an example, the event is associated with a service ticket and the auto-remediation information is included in, or stored in association with, the service ticket.

[0077] In some embodiments, auto-remediation at 440 includes executing one or more defined procedures. Auto-remediation may include determining whether to perform auto-remediation based on a measure of accuracy for the analysis determined at 430, or for one or more similar analyses. For example, one or more auto-remediation procedures can be defined for a scope, such as an event type, a subject, an element, an element type, a role, a metric, a metric category, a metric value, a layer, or any other aspect, or combination of aspects, of the electronic computing and communication system. Then, responsive to an aggregate, maximum, or most recent, value of automated event analysis corresponding to the scope exceeding a defined threshold, the auto-remediation procedures may be implemented. The threshold can be defined in response to input, such as user input. Where the value for the automated event analysis is within the defined threshold, or auto-remediation procedures are unavailable, auto-remediation may be omitted.

[0078] FIG. 5 is a flow diagram of an example of electronic computing and communication system automated topology enumeration in accordance with this disclosure. Automated topology enumeration may be implemented in one or more computing devices, such as one or more of the clients 112/114/122/124, the servers 132/134/142/144, or a combination thereof as shown in FIG 1.

[0079] Automated, or automatic, topology enumeration is performed at 500, which may include generating a computer readable representation of the electronic computing and communication system using automated topology enumeration. The computer readable representation may represent a plurality of elements of the electronic computing and communication system organized in a hierarchy of network layers.

[0080] Implementations of automated topology enumeration at 500 as shown in FIG. 5 include generating information representing physical topology at 510 and generating information representing logical topology at 520. In some embodiments, the physical topology represents the physical configuration of elements of the electronic computing and communication system, such as routers, switches, computers, servers, cables, and the like. The logical topology may also represent the organization of the flow of information in the electronic computing and communication system, such as routing information.

[0081] Automated network topology enumeration at 500 may include generating or collecting a machine-readable description of one or more devices in the electronic computing and communication system, one or more subcomponents of the devices, or a combination thereof. Automated network topology enumeration at 500 can additionally include identifying physical interconnections of the devices and subcomponents. In some embodiments, automated network topology enumeration at 500 includes generating a machine-readable description of connections between physical servicers and a network topology stack. Automated network topology enumeration at 500 may also include generating a description of logical network connectivity.

[0082] Automated enumeration at 500 can include automatically discovering substantially all of the elements of the electronic computing and communication system is some examples.

[0083] Automated enumeration at 500 can include automatically discovering elements based on one or more direct or indirect logical or physical relationships with a defined subject, such as a service affected by an identified event. In some embodiments, one or more elements of the electronic computing and communication system within a defined relationship distance from an affected service are automatically discovered, detected, or identified. For example, a portion of the electronic computing and communication system may include elements communicating with external devices via an internet service provider, and the defined relationship distance may include the elements communicating with external devices via the internet service provider, such that automated enumeration at 500 includes discovering the internet service provider, or a portion thereof, discovering ports on switches, or any other element or combination of elements. One or more elements or types of element may correspond with a network edge, hence indicating an outer limit for automated topology enumeration.

[0084] Information representing physical connectivity is generated at 510. Generating the information representing the physical connectivity layer at 510 may include enumerating the physical elements of the electronic computing and communication system, enumerating the respective physical components of each physical element, generating information representing connections between the elements and the respective components thereof, or a combination thereof, as indicated at 512. For example, the components of a physical element of the electronic computing and communication system can include attached interfaces, ports, port-channels, virtual local area networks, or the like.

[0085] In the information generated at 510, a connection, such as a connection between two physical elements of the electronic computing and communication system, can be represented as a sequence alternating between physical elements, such as a device or a component, and relationship descriptions, such as consistsOf, connectedTo, partOf, or the like. As used in herein, these topology relationship descriptions are non-limiting. For example, an element that 'consistsOf' a component may also 'consistOf' other components.

[0086] In some embodiments, automated network topology enumeration may include physical discovery, such as simple network management protocol (SNMP) discovery as shown at 513. Generally, a SNMP collector performs SNMP discovery. Physical discovery may include using a discovery function of a software-as-a-service (SaaS) platform.

[0087] SNMP discovery at 513 may include identifying information describing one or more elements of the electronic computing and communication system, which includes information indicating a manufacturer of the element, a device type of the element, a model of the element, a firmware version for the element, one or more hardware components of the element, or a combination thereof. SNMP discovery at 513 may include evaluating, or processing, one or more SNMP management information bases (MIBs), and enumerating one or more object identifiers indicated in a respective management information base, each of which may represent a respective element of the electronic computing and communication system. In some embodiments, one or more SNMP MIBs are identified from an MIB repository, are provided by a vendor, or both.

[0088] Automated topology enumeration at 500 may also include generating information describing connections between the enumerated elements, such as an interface to interface connection between an interface of a first device and an interface of a second device as shown at 514. Generating information describing connections between the enumerated elements (i.e., interface connectivity) at 514 may include identifying network protocol information for the elements, such as Cisco Discovery Protocol (CDP) information, Link Layer Discovery Protocol (LLDP) information, or a combination thereof. In some embodiments, the network protocol information is determined by recovering, or pulling, the information, or a portion thereof, from one or more network devices. Component connectivity information, such as interface connectivity information at 514, may then be generated based on the network protocol information. For example, the component connectivity information can indicate that a first component of a first device is connected to a second component of a second device. The information describing connections between the enumerated elements may include data link layer information.

[0089] The physical device connectivity information, such as the information identified using SNMP discovery and the interface connectivity information, such as the information identified using CDP and LLDP information, may be combined. For example, a first element of the electronic computing and communication system, 'deviceA', can include a first interface component, such as a first Ethernet port, 'eth0', and a second element of the electronic computing and communication system, 'deviceB', can include a second interface component, such as a second Ethernet port, 'eth1'. The first device communicates with the second device using the first interface component and the second interface component respectively. The physical device connectivity information, such as the information identified using SNMP discovery, identifies the first device, the first interface, that the first device includes (consistsOf), and communicates via, the first interface, the second device, the second interface, and that the second device includes (consistsOf), and communicates via, the second interface. The interface connectivity information, such as the information identified using CDP and LLDP information, indicates the connectivity between the first device and the second device via the first interface and the second interface respectively. In some embodiments, the combined information may be expressed directionally. For example, the combined information can express the connectivity from the first device to the second device, from the second device to the first device, or both, which may be expressed as the following:

deviceA→consistsOf→eth0→connectedTo→eth1→partOf→deviceB,

deviceB→consistsOf→eth1→connectedTo→eth0→partOf→deviceA.

[0090] Automatic network topology enumeration may include generating information representing physical device network connectivity, such as connectivity for a server or a server instance to communicate on a physical network portion or segment as shown at 516. Information representing physical device network connectivity (also called instance connectivity) describes how a physical element of the electronic computing and communication system connects with the network topology stack. The information representing physical device connectivity may be identified based on server media access control (MAC) address to Top of Rack (ToR) switch port mapping. This information can be retrieved from a table, or other information store, such as a CnsCamTable generated by Cisco networking services (CNS) including layer 2 discovery information, such as port mapping information, as shown at 517. For example, information describing physical connectivity between a first element of the electronic computing and communication system, 'serverA', and a second element of the electronic computing and communication system, 'switchA', can be expressed as the following:

serverA→consistsOf→interface/MAC→connectedTo→switchPort→partOf→switch.

[0091] Automated network topology enumeration may include using a dynamic table in a network switch that maps MAC addresses to ports, such as a content addressable memory (CAM) table, a MAC table, a filter table, or any network routing or addressing information store. In some embodiments, a dynamic table collection may be used to create a topology map that includes network devices, such as servers.

[0092] Automated network topology enumeration can include circuit providers, internet service providers, or both, in the topology. To define device roles and respective weighted values, hence building a network architecture aware topology, automated network topology enumeration may integrate with the CMDB. Automated network topology enumeration may include collecting information to determine information traffic flow patterns, such as paths, that include information such as dynamic routing tables, failover status of devices, and address resolution protocol (ARP) to port mapping.

[0093] Automatic network topology enumeration can include associating a customer instance with a network interface, such as a ToR switch port. In some embodiments, a customer instance may represent an application or service associated with a customer and executing, at least in part, on a physical server. Information (e.g., stored in the CMDB) can indicate an association between a customer instance and one or more servers and can be combined with the physical device network connectivity information so as to map customer instances to identified ToR switch ports.

[0094] Automatic network topology enumeration include generating information representing logical connectivity for the electronic computing and communication system as shown at 520. In some embodiments, the logical connectivity information at 520 is generated based on, for example, network architecture information, routing protocol status information, default gateway information, circuit connectivity information, ISP connectivity information, hot standby router protocol (HSRP) status information, such as active or passive status, virtual router redundancy protocol (VRRP) status information, netscreen standby routing protocol (NSRP) status information, or the like, as shown at 522.

[0095] The logical network architecture may include a hierarchy of logical network architecture layers, and an element of the electronic computing and communication system, such as a router or a switch, may operate in one or more logical network architecture layers. One or more device roles defined and stored, such as in the CMDB, can represent the operation of an element of electronic computing and communication system in an identified logical network architecture layer.

[0096] In some embodiments, a network architecture layer value is associated with a defined device role. A network architecture layer value indicates a network layer associated with a defined role. Relative network layer orientation of elements in the electronic computing and communication system may then be identified based on the associated network architecture layer values. For example, determining whether an element of the electronic computing and communication system is above, below, or lateral to another element of the electronic computing and communication system can be based on the respective network architecture layer values associated with the roles associated with the respective elements.

[0097] One or more elements of the electronic computing and communication system may operate using an active mode or a passive mode. In some embodiments, the physical connectivity information and the logical connectivity information are combined and routing information, such as network traffic patterns or paths, are identified by polling elements of the electronic computing and communication system to identify the active or passive status of the respective elements, as shown at 523. The polling may be SNMP polling.

[0098] An electronic computing and communication system can use dynamic routing protocols to route traffic. In some embodiments, such as embodiments that include using dynamic routing protocols to route traffic, the routing information is identified based on open shortest path first (OSPF) routing protocol, border gateway protocol (BGP), or the like. One or more elements of the electronic computing and communication system, such as a server, may perform a hashing function to determine a route, and a corresponding pair of network devices may be included in a network path.

[0099] Automated network topology enumeration may include providing, using, or both, a topology application programming interface (API) as shown at 530. For example, a function exposed by the topology API can receive an identifier of an element of the electronic computing and communication system, such as a network device or a server, and respond with information indicating one or more elements of the electronic computing and communication system that may be in communication with the identified element, such as elements on the same network architecture layer as the identified element, elements in the network architecture layers below the identified element, elements in the network architecture layers above the identified element, or a combination thereof.

[0100] The topology API can receive a topology request for the an element of the electronic computing and communication system associated with a DSR role, and respond with information indicating elements of the electronic computing and communication system lateral to, or in the same network architecture layer as, the DSR role, such as the third network architecture layer, elements of the electronic computing and communication system in the network architecture layers above the DSR layer, such as the fourth, fifth, and sixth network architecture layers, and elements of the electronic computing and communication system in the network architecture layers below the DSR layer, such as the first and second network architecture layers.

[0101] FIG. 6 is a diagram of an example of an interface for electronic computing and communication system automated event analysis in accordance with this disclosure. Automated event analysis, such as the automated event analysis shown at 430 in FIG. 4, may include generating, storing, outputting, presenting, etc., one or more reports representing a result of the automated event analysis.

[0102] The graphical representation of the automated event analysis as shown includes a graphical representation of an external device 600 in communication with a service 610 via a path 620. The graphical representation includes one or more elements of the electronic computing and communication system, shown as small circles, within one or more network topology architecture layers 630/640/650/660/670. In this example, the path 620 includes one or more of the more elements of the electronic computing and communication system, such as element 632 in layer 630, element 642 in layer 640, element 652 in layer 650, elements 662 and 664 in layer 660, and element 672 in layer 670. Although a single path is shown for simplicity and clarity, elements of the electronic computing and communication system may communicate with other elements of the electronic computing and communication system or with external communicating elements, such as the external device 600, via any number of paths.

[0103] In some embodiments, the network topology architecture layers 630/640/650/660/670 correspond with respective network topology architecture layer values. For example, the layer 630 most remote from the service 610 represents the Internet layer and is associated with relatively low value, such as 50, the layer 640 inside, or below, the Internet layer 630, represents the border layer and is associated with value greater than the Internet layer 630 value, such as 100, the layer 650 inside, or below, the border layer 640, represents a core layer and is associated with a value greater than the border layer 640 value, such as 150, the layer 660 inside, or below, the core layer 650, represents a distribution layer and is associated with value greater than the core layer 650 value, such as 200, and the layer 670 inside, or below, the distribution layer 660, represents an aggregation layer and is associated with value greater than the distribution layer 650 value, such as 255. Although not shown in FIG. 6, the layer values may be shown in accordance with the layers in some embodiments.

[0104] In some embodiments, the network topology architecture layer values may be defined values, such as values identified in response to input, such as user input. These defined network topology architecture layer values can be adjusted based on system investigation, such as the system investigation shown at 420 in FIG. 4.

[0105] Whether an element of the electronic computing and communication system is in the communication path 620 may be indicated graphically, or visually. For example, elements in the communication path 620 are shown using a color or size that differs from elements omitted from the communication path 620. Here, elements omitted from the communication path 620 are shown as small white circles with thin borders, and elements 632/642/652/662/664/672 included in the communication path 620 are shown as small circles with thick borders.

[0106] The graphical representation may indicate that one or more of the elements 632/642/652/662/664/672 included in the communication path 620 corresponds with an abnormal metric value. For example, a flag is shown in association with one or more elements 632/642/652/662/664/672 identified as corresponding with an abnormal metric value. Although shown as black flags in FIG. 6, a flag may graphically represent a corresponding metric category in some embodiments. For example, the flag associated with the element 632 in the Internet layer 630 may be colored orange to indicate that the flag is associated with a performance metric, the flag associated with the right element 662 in the distribution layer 660 may be colored yellow to indicate that the flag is associated with a change metric, the flag associated with the left element 664 in the distribution layer 660 may be colored blue to indicate that the flag is associated with a capacity metric, and the flag associated with the element 672 in the aggregation layer 670 may be colored red to indicate that the flag is associated with an availability metric. The graphical representation of an element may also indicate whether the element is associated with an abnormal metric value. For example, the color of elements included in the communication path that are not associated with abnormal metric values can be shown in a color that differs from the color of elements included in the communication path that are associated with abnormal metric values. As shown in the example of FIG. 6, the element 642 in the border layer 640 and the element 652 in the core layer 650 may be shown in a color, such as green, that differs from the color, such as red, of elements 632/662/664/672 included in the communication path 620 that are associated with abnormal metric values. In FIG. 6, the elements 642/652 included in the communication path 620 that are not associated with abnormal metric values are shown with light stippling and the color of elements 632/662/664/672 included in the communication path 620 that are associated with abnormal metric values are shown with heavy stippling.

[0107] Although not shown separately in FIG. 6, a remediation priority may be determined and presented for each of the elements 632/642/652/662/664/672 included in the communication path 620 based on, for example, the respective layer value and metric category value. For example, a list of the elements 632/642/652/662/664/672 included in the communication path 620 ordered by remediation priority is possible.

[0108] In the example shown in FIG. 6, the external device 620 communicates with the service 610 via an element 632 in the Internet layer 630 that is associated with an abnormal performance metric value. The layer value for the Internet layer 630 may be 50, the metric category value for the abnormal performance metric may be 150, and the remediation priority for the element 632 in the Internet layer 630 may be, for example, a product of the layer value and the metric category value (i.e., 7500).

[0109] The communication path traverses the network from the element 632 in the Internet layer 630 to the element 642 in the border layer 640, which may not be associated with an abnormal metric value. The layer value for the border layer 640 may be 100. Where a value of zero indicates that the element 642 is not associated with an abnormal metric value, the remediation priority for the element 642 in the border layer 640 may be 0.

[0110] The communication path traverses the network from the element 642 in the border layer 640 to the element 652 in the core layer 650, which may not be associated with an abnormal metric value. The layer value for the core layer 650 may be 150. Where a value of zero indicates that the element 652 is not associated with an abnormal metric value, the remediation priority for the element 652 in the core layer 650 may be 0.

[0111] The communication path traverses the network from the element 652 in the core layer 650 to the right element 662 in the distribution layer 660, which may which may be associated with an abnormal change metric value. The layer value for the distribution layer 660 may be 200, the metric category value for the abnormal change metric may be 200, and the remediation priority for the right element 662 in the distribution layer 660 may be their product (i.e., 40000).

[0112] The communication path traverses the network from the right element 662 in the distribution layer 650 to the left element 664 in the distribution layer 660, which may which may be associated with an abnormal capacity metric value. The layer value for the distribution layer 660 may be 200, the metric category value for the abnormal capacity metric may be 100, and the remediation priority for the left element 664 in the distribution layer 660 may be their product (i.e., 20000).

[0113] The communication path traverses the network from the left element 654 in the distribution layer 660 to the element 672 in the aggregation layer 670, which may be associated with an abnormal availability metric value. The layer value for the aggregation layer 670 may be 255, the metric category value for the abnormal availability metric may be 255, and the remediation priority for the element 672 in the aggregation layer 670 may be their product (i.e., 65025).

[0114] The elements can presented in remediation priority order with the element 672 in the aggregation layer 670, having the highest remediation priority, first, followed by the right element 662 in the distribution layer 660, the left element 664 in the distribution layer 660, the element 632 in the Internet layer 630, the element 642 in the border layer 640, and the element 652 in the core layer 650.

[0115] The implementations of the electronic computing and communication system including clients 112/114/122/124 and servers 132/134/142/144 (and the algorithms, methods, instructions, etc. stored thereon and/or executed thereby) can be realized in hardware, software, or any combination thereof. The hardware can include, for example, computers, intellectual property (IP) cores, application-specific integrated circuits (ASICs), programmable logic arrays, optical processors, programmable logic controllers, microcontrollers, servers, microprocessors, digital signal processors or any other suitable circuit. In the claims, the term “processor” should be understood as encompassing any of the foregoing hardware, either singly or in combination. The terms “signal” and “data” are used interchangeably. Further, portions of clients 112/114/122/124 and servers 132/134/142/144 are not necessarily implemented in the same manner.

[0116] Further, in an embodiment, for example, clients 112/114/122/124 and servers 132/134/142/144 can be implemented using a special purpose computer/processor, which can contain specialized hardware for carrying out any of the methods, algorithms, or instructions described herein.

[0117] Further, all or a portion of embodiments of the present invention can be implemented using a special purpose computer/processor with a computer program that, when executed, carries out any of the respective techniques, algorithms and/or instructions described herein, and which can contain specialized hardware for carrying out any of the techniques, algorithms, or instructions described herein.

[0118] Implementations or portions of implementations of the above disclosures can take the form of a computer program product accessible from, for example, a computer-usable or computer-readable medium. A computer-usable or computer-readable medium can be any device that can, for example, tangibly contain, store, communicate, or transport a program or data structure for use by or in connection with any processor. The medium can be, for example, an electronic, magnetic, optical, electromagnetic, or a semiconductor device. Other suitable mediums are also available. Such computer-usable or computer-readable media can be referred to as non-transitory memory or media, and may include RAM or other volatile memory or storage devices that may change over time.

[0119] As used herein, the terminology “determine” and “identify”, or any variations thereof, includes selecting, ascertaining, computing, looking up, receiving, determining, establishing, obtaining, or otherwise identifying or determining in any manner whatsoever using one or more of the devices shown and described herein. As used herein, the terminology “generating”, or any variations thereof, includes combining, calculating, computing, aggregating, rendering, laying out, drawing, or otherwise producing in any manner whatsoever using one or more of the devices shown and described herein. As used herein, the terminology “automatic”, “automatically”, “automated”, or any variation thereof, including use of the prefix “auto-“, includes initiating or executing by one or more of the devices shown and described herein without human intervention. As used herein, the terminology “cardinality” includes a number or count of elements or items in a set, group, plurality, or any other collection of zero or more elements. As used herein, the terminology “receiving” includes receiving via a network, retrieving from memory, or otherwise ascertaining the identified information.

[0120] The above-described embodiments have been described in order to allow easy understanding of the present invention and do not limit the present invention. On the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims, which scope is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structure as is permitted under the law.

What is claimed is:

1. A method of automatically analyzing an electronic computing and communication system event, the method comprising:

identifying information indicating an event in an electronic computing and communication system;

generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, wherein the representation represents a plurality of elements of the electronic computing and communication system organized in a hierarchical plurality of network layers;

identifying an element of the electronic computing and communication system from the plurality of elements based on the computer readable representation of the electronic computing and communication system;

identifying a metric for the element of the electronic computing and communication system;

automatically investigating the electronic computing and communication system to determine a value for the metric;

on a condition that the value is an abnormal value, generating a remediation priority for the element of the electronic computing and communication system based on a metric weight associated with the metric and a network layer value associated with a network layer from the hierarchical plurality of network layers, wherein the element is associated with a network layer role corresponding to the network layer;

generating a graphical representation of the electronic computing and communication system, the graphical representation indicating the remediation priority; and

outputting or storing the graphical representation.

2. The method of claim 1, wherein automated topology enumeration includes:

automatically discovering the plurality of elements;

generating a computer readable representation of physical connectivity for the plurality of elements; and

generating a computer readable representation of logical connectivity for the plurality of elements.

3. The method of claim 1, wherein automated topology enumeration includes:

identifying the network layer role associated with the element; and identifying the network layer associated with the element based on the network layer role.

4. The method of claim 3, wherein identifying the network layer role includes:

identifying information representing the element; and

determining the network layer role by evaluating a configuration management database based on the information representing the element.

5. The method of claim 1, wherein automated topology enumeration includes:

identifying simple network management protocol discovery information indicating the element and, if available, information indicating a component of the element.

6. The method of claim 1, wherein automated topology enumeration includes:

identifying network protocol information for the element, wherein the network protocol information for the element indicates a physical connection between the element and a second element of the electronic computing and communication system.

7. The method of claim 6, wherein identifying the network protocol information for the element includes identifying network protocol information that indicates that the physical connection physical connection between the element and the second element includes a physical connection between a component of the element and a component of the second element.

8. The method of claim 1, wherein identifying the metric includes:

identifying a plurality of metric categories;

identifying a metric category for the metric from the plurality of metric categories; and

identifying the metric weight associated with the metric based on the metric category.

9. The method of claim 8, wherein the plurality of metric categories includes:

a change category including a plurality of change metrics, wherein each change metric from the plurality of change metrics represents a respective managed change information element representing a managed change to the electronic computing and communication system;

an availability category including a plurality of availability metrics, wherein each availability metric from the plurality of availability metrics represents a respective availability of an element of the electronic computing and communication system;

a performance category including a plurality of performance metrics, wherein each performance metric from the plurality of performance metrics represents a respective performance of an element of the electronic computing and communication system;

a capacity category including a plurality of capacity metrics, wherein each capacity metric from the plurality of capacity metrics represents a respective available capacity of an element of the electronic computing and communication system; or

a variance category including a plurality of variance metrics, wherein each variance metric from the plurality of variance metrics represents a respective variance of another metric from a corresponding defined metric value for an element of the electronic computing and communication system.

10. The method of claim 1, further comprising:

automatically remediating the electronic computing and communication system including:

identifying a remediation procedure associated with the element and the event; and

performing the remediation procedure.

11. The method of claim 1, wherein generating the graphical representation includes generating the graphical representation such that the graphical representation includes:

a graphical representation of the hierarchical plurality of network layers, including a graphical representation of the network layer;

a graphical representation of the element spatially corresponding to the graphical representation of the network layer;

on a condition that the value is an abnormal value, a graphical representation indicating that the value is an abnormal value and indicating a category associated with the metric.

12. A method of automatically analyzing an electronic computing and communication system event, the method comprising:

identifying information indicating an event in an electronic computing and communication system;

generating a computer readable representation of the electronic computing and communication system using automated topology enumeration, wherein the computer readable representation represents a plurality of elements of the electronic computing and communication system organized in a hierarchical plurality of network layers, wherein each respective element from the plurality of elements is associated with a respective network layer role corresponding to a respective network layer;

identifying a set of elements of the electronic computing and communication system from plurality of elements based on the computer readable representation of the electronic computing and communication system;

identifying a plurality of metrics, wherein each element from the set of elements is associated with at least one respective metric from the plurality of metrics;

automatically investigating the electronic computing and communication system to determine a plurality of values, wherein each value from the plurality of values corresponds with a respective metric from the plurality of metrics and a respective element from the set of elements;

generating a plurality of remediation priorities, wherein each remediation priority from the plurality of remediation priorities corresponds with a respective value from the plurality of values, a respective metric from the plurality of metrics, and a respective element from the set of elements, and wherein each remediation priority from the plurality of remediation priorities is based on a metric weight associated with the respective corresponding metric and a network layer value associated with a respective network layer associated with a respective network layer role associated with the respective element;

generating a graphical representation of the electronic computing and communication system, the graphical representation indicating at least some of the remediation priorities; and

outputting or storing the representation.

13. The method of claim 12, wherein automated topology enumeration includes:

automatically discovering the plurality of elements;

generating a computer readable representation of physical connectivity for the plurality of elements; and

generating a computer readable representation of logical connectivity for the plurality of elements.

14. The method of claim 13, wherein automatically discovering the plurality of elements includes automatically discovering an internet service provider.

15. The method of claim 12, wherein, for each element from the plurality of elements, automated topology enumeration includes:

identifying the respective network layer role associated with the element; and

identifying the network layer associated with the element based on the network layer role.

16. The method of claim 15, wherein identifying the network layer role includes:

identifying information representing the element; and

determining the network layer role by evaluating a configuration management database based on the information representing the element.

17. The method of claim 12, wherein generating the graphical representation includes generating the graphical representation such that the graphical representation includes:

a graphical representation of the hierarchical plurality of network layers;

a graphical representation of each element from the set of elements; and

for each element from the set of elements, on a condition that the corresponding value is an abnormal value, a graphical representation indicating that the respective value is an abnormal value and indicating a category associated with the corresponding metric.

18. The method of claim 12, wherein the event is associated with a service, and wherein generating the graphical representation of the electronic computing and communication system comprises:

generating a graphical representation of the hierarchical plurality of network layers, wherein the service corresponds with a network layer from the hierarchical plurality of network layers;

for each element from the set of elements:

generating a graphical representation of the element; and

on a condition that a value from the plurality of values corresponding to the element is an abnormal value, generating a graphical representation indicating that the value is an abnormal value and indicating a category associated with a metric from the plurality of metrics associated with the value; and

generating a graphical representation of a path between an external device and the service, wherein the path intersects with at least one element from the set of elements in each network layer from the hierarchical plurality of network layers; and wherein outputting or storing the representation comprises:

outputting the graphical representation for presentation to a user.

19. The method of claim 12, wherein automatically investigating the electronic computing and communication system includes:

identifying a monitoring template associated with at least one element from the set of elements; and

identifying at least one value from the plurality of values using the monitoring template.

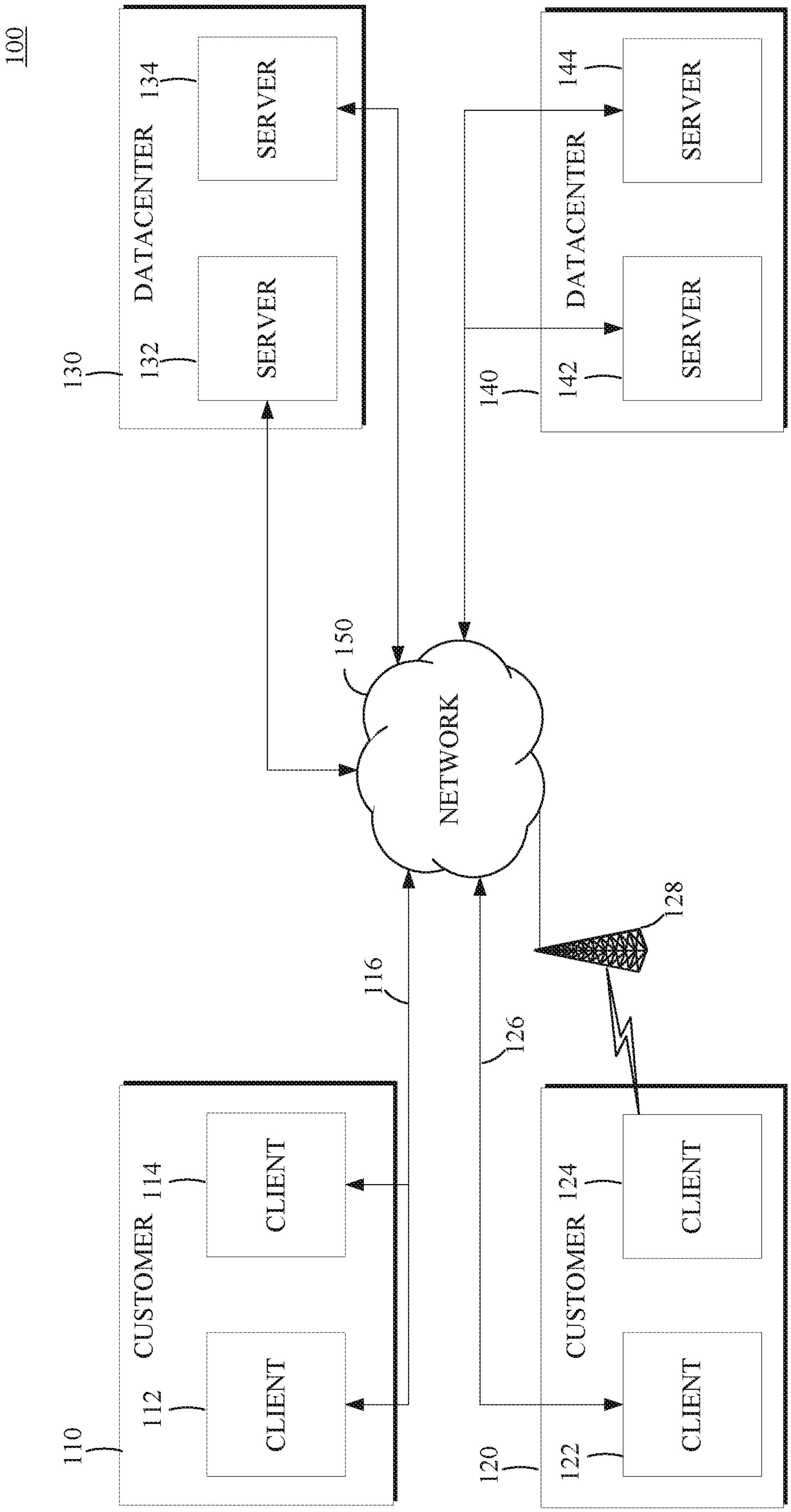
100
DATACENTER
130
SERVER
132
SERVER
134
DATACENTER
140
SERVER
142
SERVER
144
NETWORK
150
116
126
128
CUSTOMER
110
CLIENT
112
CLIENT
114
CUSTOMER
120
CLIENT
122
CLIENT
124

FIG. 1

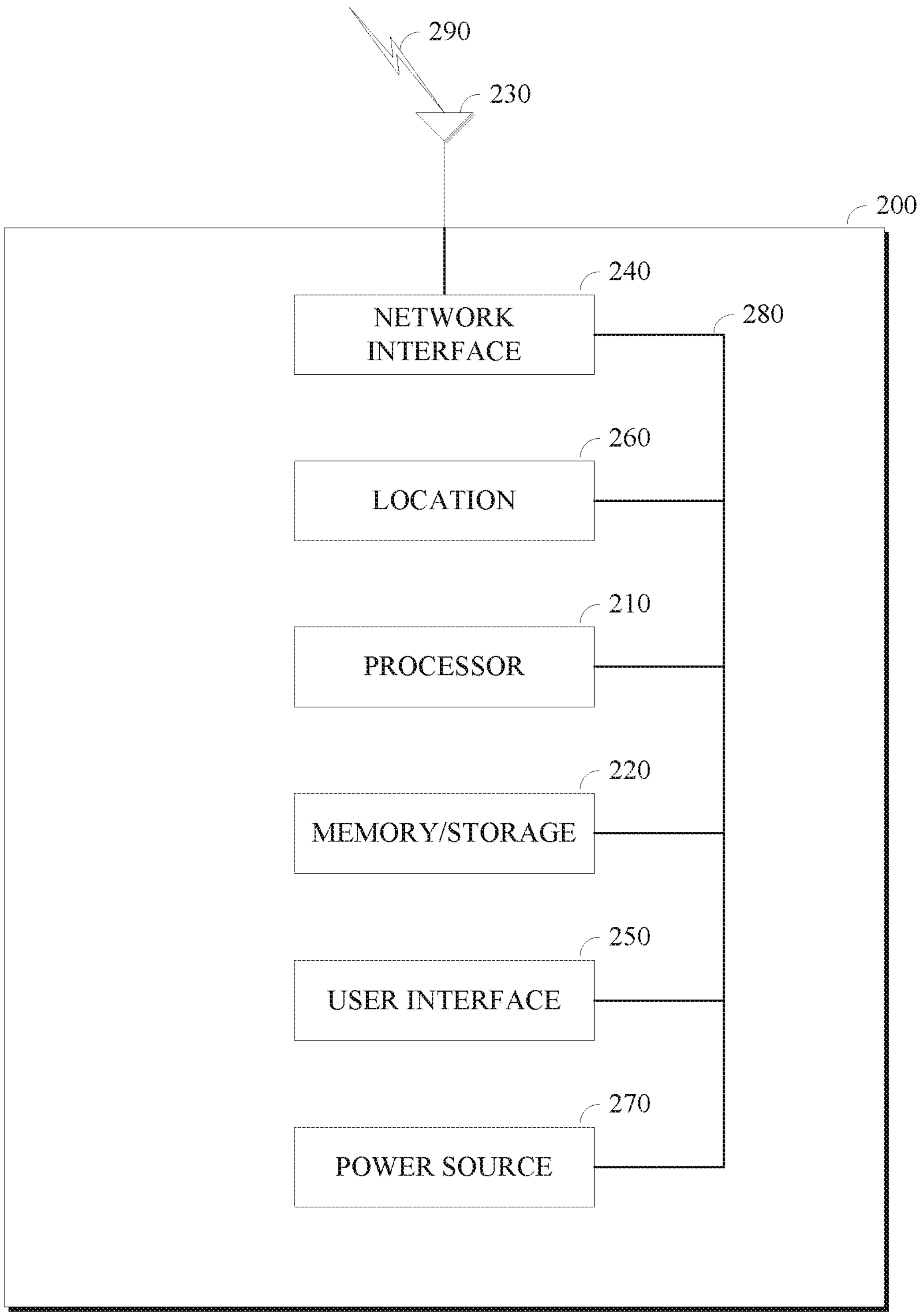
290
230
200
240
NETWORK INTERFACE
280
260
LOCATION
210
PROCESSOR
220
MEMORY/STORAGE
250
USER INTERFACE
270
POWER SOURCE

FIG. 2

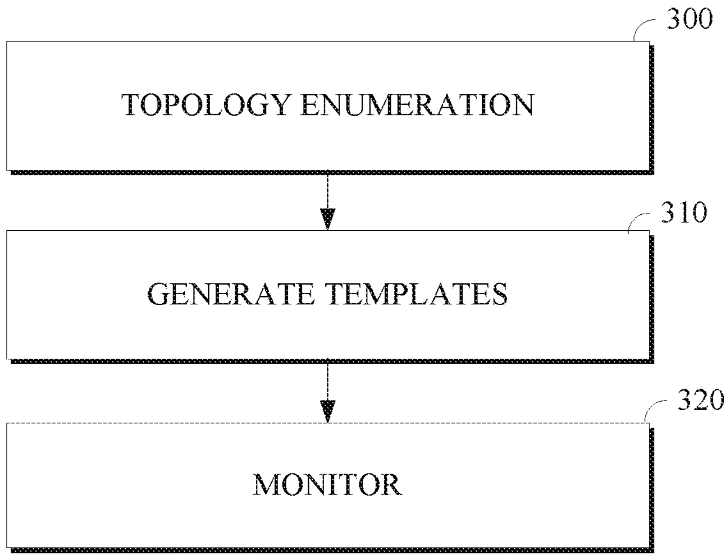
300
TOPOLOGY ENUMERATION
310
GENERATE TEMPLATES
320
MONITOR

FIG. 3

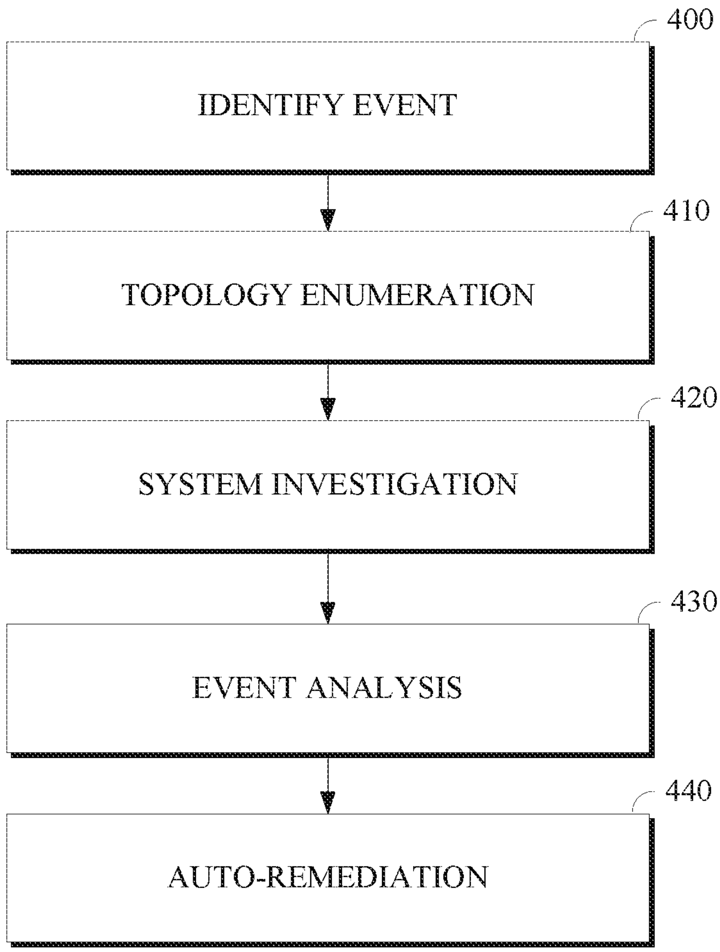
400
IDENTIFY EVENT
410
TOPOLOGY ENUMERATION
420
SYSTEM INVESTIGATION
430
EVENT ANALYSIS
440
AUTO-REMEDIATION

FIG. 4

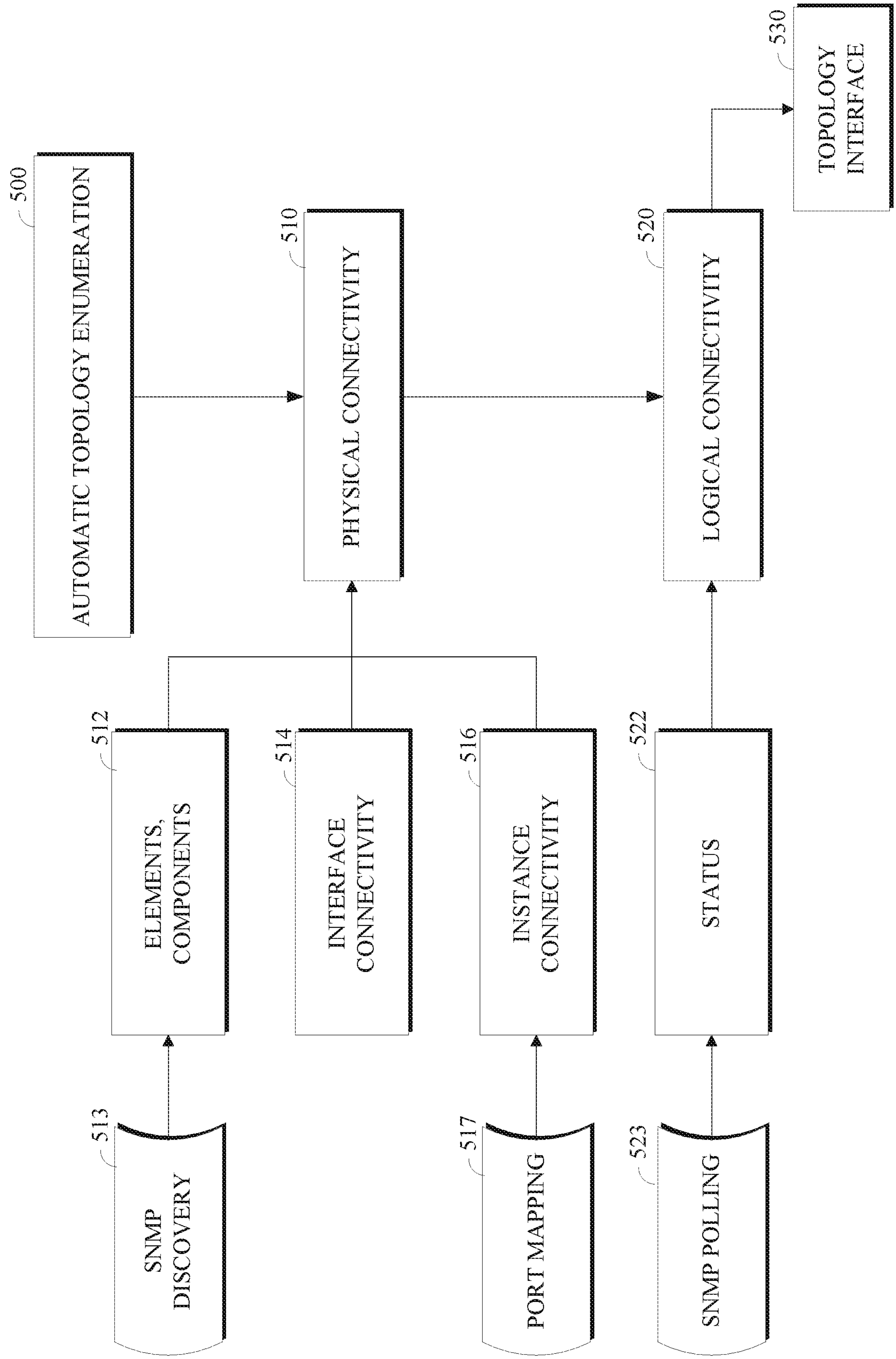
500
AUTOMATIC TOPOLOGY ENUMERATION
510
PHYSICAL CONNECTIVITY
520
LOGICAL CONNECTIVITY
530
TOPOLOGY INTERFACE
512
ELEMENTS, COMPONENTS
514
INTERFACE CONNECTIVITY
516
INSTANCE CONNECTIVITY
522
STATUS
513
SNMP DISCOVERY
517
PORT MAPPING
523
SNMP POLLING

FIG. 5

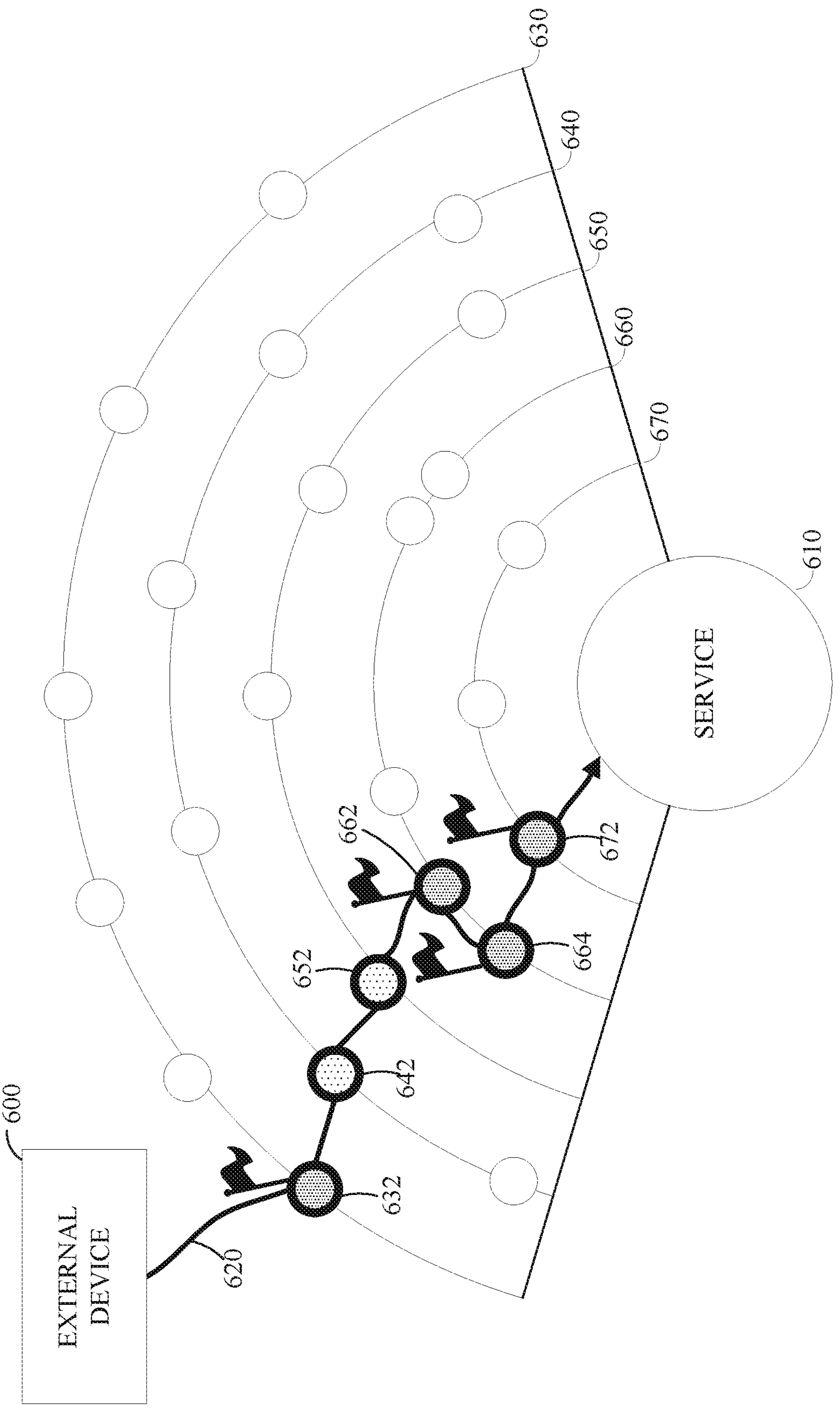
EXTERNAL DEVICE
600
620
632
642
652
662
664
672
630
640
650
660
670
SERVICE
610

FIG. 6