randomly combined or divided based on specific implementation.

[0019] According to a third aspect, a data processing apparatus is provided. The apparatus includes a processor and a memory, where

the memory is configured to store a computer program, where the computer program includes program instructions; and

the processor is configured to invoke the computer program to implement the data processing method according to any implementation of the first aspect.

[0020] According to a fourth aspect, a computer storage medium is provided. The computer storage medium stores instructions; and when the instructions are executed by a processor, the data processing method according to any implementation of the first aspect is implemented.

[0021] According to a fifth aspect, a chip is provided. The chip includes a programmable logic circuit and/or program instructions. When the chip runs, the data processing method according to any implementation of the first aspect is implemented.

[0022] Beneficial effects brought by the technical solutions provided in this application include at least the following:

[0023] After obtaining the network data of the target network, the management device processes the network data, to generate the knowledge graph of the target network. The knowledge graph of the target network can intuitively reflect the network entities in the target network and the relationship between different network entities, that is, can be used to visualize the network data. When needing to obtain the network information in the target network, the user only needs to view the knowledge graph of the target network without manually querying the command line. Therefore, the efficiency of obtaining the network information by the user is improved. In addition, after the fault occurs in the target network, the management device may further identify the abnormal network entities on the knowledge graph of the target network, to intuitively reflect abnormal locations in the target network. Further, the management device may further determine the root-cause fault network entity in the abnormal network entities on the knowledge graph of the target network based on the fault propagation relationship between network entities, to implement the automated inference and locating of the network fault root cause.

network devices in FIG. 1 are merely used as an example, and are not used as a limitation on the application scenario of the data processing method provided in embodiments of this application. The communication network may be a data center network (DCN), a metropolitan area network, a wide area network, a campus network, a virtual local area network (VLAN), a virtual extensible local area network (VXLAN), or the like. A type of the communication network is not limited in embodiments of this application.

[0036] Optionally, the management device 101 may be one server or a server cluster including several servers, or may be a cloud computing service center. The network device 102 may be a switch, a router, or the like. Optionally, still refer to FIG. 1. The application scenario may further include a control device 103. The control device 103 is configured to manage and control the network device 102 in the communication network. The management device 101 is connected to the control device 103 through a wired network or a wireless network, and the control device 103 is connected to the network device 102 through a wired network or a wireless network. The control device 103 may be a network controller, a network management device, a gateway, or another device having a control capability. The control device 103 may be one or more devices.

[0037] The control device 103 may store a network topology of the communication network managed by the control device 103. The control device 103 is further configured to collect device information of the network device 102 in the communication network, an abnormal event generated in the communication network, and the like, and provide the management device 101 with the network topology of the communication network, the device information of the network device 102, the abnormal event generated in the communication network, and the like. The device information of the network device includes network configuration information, a routing entry, and/or the like of the network device. The network configuration information usually includes interface configuration information, protocol configuration information, service configuration information, and the like. Optionally, the control device 103 may periodically collect the device information of the network device 102 and the abnormal event generated in the communication network. Alternatively, when the device information of the network device 102 changes, the network device 102 actively reports changed device information to the control device 103. When a fault occurs in the communication network, the network device 102 actively reports a generated abnormal event to the control device 103. Certainly, in some application scenarios, the

management device may alternatively be directly connected to the network device in the communication network. In other words, the application scenarios may not include the control device. This is not limited in embodiments of this application.

[0038] FIG. 2 is a flowchart of a data processing method according to an embodiment of this application. The data processing method may be applied to the management device 101 in the application scenario shown in FIG. 1. As shown in FIG. 2, the method includes the following steps.

[0039] Step 201: Obtain network data of a target network.

[0040] The network data includes a network topology of the target network and device information of a plurality of network devices in the target network. The device information of the network device includes network configuration information of the network device, and specifically includes one or more of interface configuration information, protocol configuration information, and service configuration information. The device information may further include a routing entry and the like. Optionally, the interface configuration information of the network device includes an Internet Protocol (IP) address of an interface, a protocol type supported by the interface, a service type supported by the interface, and the like. The protocol configuration information of the network device includes an identifier of a protocol, where the identifier of the protocol is used to uniquely identify the protocol, and may be represented by a character, a letter, a digit, and/or the like. The service configuration information of the network device includes a service used by the network device, for example, a virtual private network (VPN) service and/or a dynamic host configuration protocol (DHCP) service.

[0041] Optionally, an implementation process of step 201 includes: The management device receives the network data of the target network that is sent by a control device of the target network.

[0042] Step 202: Extract a plurality of knowledge graph triplets from the network data of the target network.

[0043] Each knowledge graph triplet includes two network entities and a relationship between the two network entities. For example, the relationship between the two network entities may be a dependency relationship, a subordinate relationship, or an equivalence relationship.

[0044] In embodiments of this application, a type of the network entity may be a network device, an interface, a protocol, or a service. For example, when two network entities on a knowledge graph triplet are a network device and an interface, a relationship between the two

network entities is a subordinate relationship, that is, the interface belongs to the network device. For another example, when two network entities on a knowledge graph triplet are two interfaces between which a communication connection is established, a relationship between the two network entities is an equivalence relationship.

[0045] Optionally, a network entity whose type is a network device may be represented by a name, a media access control (MAC) address, or a hardware address of the network device, or another identifier that can uniquely identify the network device. A network entity whose type is an interface may be represented by a name of the interface. A network entity whose type is a protocol may be represented by an identifier of the protocol. The knowledge graph triplet is represented in a graph form. The knowledge graph triplet includes two basic elements, namely, a point and an edge, where the point represents a network entity, and the edge represents a relationship between two network entities. The edge on the knowledge graph triplet may be directional or directionless. The edge on the knowledge graph triplet may be further used to indicate a specific relationship, for example, a dependency relationship, a subordinate relationship, or an equivalence relationship, between two network entities. For example, when two network entities are in an equivalence relationship, a directionless edge may be used to connect the two network entities. When two network entities are in a dependency relationship or a subordinate relationship, a directional edge (for example, an arrow) may be used to connect the two network entities, and the directional edge points from a depending network entity to a depended network entity, or the directional edge points from a belonging network entity to a belonged network entity.

[0046] For example, assuming that the network data obtained by the management device includes a piece of data that "a network device 1 has an interface named "10GE1/0/6"", the management device may extract a knowledge graph triplet shown in FIG. 3. Refer to FIG. 3. On the knowledge graph triplet, types of two network entities are respectively a network device and an interface, and an arrow points from the interface to the network device. This indicates that the interface named "10GE1/0/6" belongs to the network device 1, in other words, the knowledge graph triplet can reflect that the network device 1 has the interface named "10GE1/0/6".

[0047] Optionally, an implementation process of step 202 includes: The management device extracts the plurality of knowledge graph triplets from the network data based on an abstract service model corresponding to a network type of the target network, where the abstract service model is used to reflect a relationship between different network entities. Different network types

may correspond to different abstract service models. The abstract service model is essentially a data object used to define a dependency relationship between different network entities. For example, it may be defined in the abstract service model that, each network device has one or more interfaces, in other words, the interface belongs to the network device; the interface may carry a forwarding service, for example, the interface may carry a layer 3 IP forwarding service, and this means that the interface supports packet forwarding using an interior gateway protocol (IGP), in other words, the layer 3 IP forwarding service or the IGP depends on the interface; the layer 3 IP forwarding service may carry a VXLAN tunnel, a traffic engineering (TE) tunnel, and a border gateway protocol (BGP), in other words, the VXLAN tunnel, the TE tunnel, and the BGP depend on the layer 3 IP forwarding service; the TE tunnel may carry a VPN service, in other words, the VPN service depends on the TE tunnel; and so on. That the layer 3 IP forwarding service may carry the VXLAN tunnel indicates that an interface that carries the layer 3 IP forwarding service may be used as an endpoint of the VXLAN tunnel. That the layer 3 IP forwarding service may carry the TE tunnel indicates that an interface that carries the layer 3 IP forwarding service may be used as an endpoint of the TE tunnel. That the layer 3 IP forwarding service may carry the BGP indicates that an interface that carries the layer 3 IP forwarding service may be configured to send and receive a BGP-based protocol packet. That the TE tunnel may carry the VPN service indicates that an interface that carries the TE tunnel may support the VPN service.

[0048] Optionally, the management device may extract the knowledge graph triplets from the network configuration information of the network device, or may obtain the knowledge graph triplets based on the routing entry of the network device.

[0049] For example, it is assumed that content of the knowledge graph triplet extracted by the management device based on the network configuration information of the network device includes: The network device 1 has the interface named "10GE1/0/6"; the interface "10GE1/0/6" supports a layer 3 IP forwarding service, and an IP address of the interface "10GE1/0/6" is 192.168.1.1; and the network device 1 has a VXLAN tunnel, a source IP address of the VXLAN tunnel is 192.168. 1.1, and a destination IP address of the VXLAN tunnel is 192.168. 10.1. To determine a relationship between the VXLAN tunnel and the interface, the management device may search the routing entry by using 192.168.10.1 as the destination IP address. If it is determined, based on the routing entry, that an outbound interface reaching the destination IP address is the

interface "10GE1/0/6", content of the knowledge graph triplet obtained by the management device based on the routing entry is: An endpoint of the VXLAN tunnel is located on the interface "10GE1/0/6" of the network device 1.

[0050] Step 203: Generate a knowledge graph of the target network based on the plurality of knowledge graph triplets.

[0051] For example, it is assumed that the target network includes two network devices: a network device A and a network device B. The network device A has three interfaces, and names of the three interfaces are: 10GE1/0/1, 10GE1/0/2, and 10GE1/0/3. The network device B has four interfaces, and names of the four interfaces are: 10GE3/0/1, 10GE3/0/2, 10GE3/0/3, and 10GE3/0/4. Both the network device A and the network device B support the open shortest path first (OSPF) protocol, where the OSPF protocol is an IGP. An identifier of the OSPF protocol on the network device A is represented by 10.89.46.25, and the OSPF protocol on the network device A includes three route IP addresses: 11.11.11.11, 11.11.11.12, and 11.11.11.13. An identifier of the OSPF protocol on the network device B is represented by 10.89.49.37, and the OSPF protocol on the network device B includes four route IP addresses: 11.12.11.11, 11.12.11.12, 11.12.11.13, and 11.12.11.14. The interface "10GE1/0/2" of the network device A is connected to the interface "10GE3/0/2" of the network device B, and the OSPF protocol is used for communication between the two interfaces. The interface "10GE1/0/2" of the network device A uses the route IP address 11.11.11.11, and the interface "10GE3/0/2" of the network device B uses the route IP address 11.12.11.14. Therefore, a knowledge graph shown in FIG. 4 may be obtained based on the foregoing network data. Refer to FIG. 4. Device information of the network device A and the network device B in the target network is expressed in a graph form on the knowledge graph.

[0052] Optionally, after generating the knowledge graph of the target network, the management device may send the knowledge graph of the target network to an operations support system (OSS) or a terminal device connected to the management device, so that the OSS or the terminal device displays the knowledge graph. Certainly, if the management device has a display function, the management device may alternatively directly display the knowledge graph of the target network on a display interface of the management device.

[0053] In this embodiment of this application, after obtaining the network data of the target network, the management device processes the network data, to generate the knowledge graph of

embodiment of this application.

[0059] Optionally, after identifying the abnormal network entities on the knowledge graph of the target network, the management device may send the knowledge graph of the target network to the OSS or the terminal device connected to the management device, so that the OSS or the terminal device displays the knowledge graph. This helps an operation and maintenance engineer view the abnormal network entities in the target network. The management device may further send the abnormal events corresponding to the abnormal network entities to the OSS or the terminal device connected to the management device, so that the OSS or the terminal device displays the abnormal events. This helps an operation and maintenance engineer obtain abnormal types of the abnormal network entities.

[0060] The knowledge graph generated in step 203 may also be referred to as an initial knowledge graph. The knowledge graph on which the abnormal network entities are identified in step 205 may also be referred to as a first knowledge graph.

[0061] Step 206: Determine one or more root-cause fault network entities from all the abnormal network entities on the knowledge graph of the target network based on the fault propagation relationship between network entities.

[0062] The root-cause fault network entity is an abnormal network entity that is a root cause of the fault.

[0063] Optionally, a process in which the management device obtains the fault propagation relationship includes: The management device obtains a plurality of knowledge graph samples, where each knowledge graph sample is identified with all abnormal network entities that generate, when a fault occurs in a network to which the knowledge graph sample belongs, abnormal events in the network to which the knowledge graph sample belongs and a root-cause fault network entity. The management device determines the fault propagation relationship based on the plurality of knowledge graph samples. Each knowledge graph sample is a fault case, and the abnormal network entities and the root-cause fault network entity in the knowledge graph sample may be manually determined. Optionally, the management device may learn the fault propagation relationship in the plurality of knowledge graph samples by using a graph embedding algorithm or the like. Alternatively, when a probability that two network entities on a same knowledge graph triplet are simultaneously abnormal is greater than a threshold, the management device may determine that fault propagation is performed between the two network entities.

[0064] For example, on the knowledge graph shown in FIG. 4, when a fault occurs on the interface "10GE1/0/2" of the network device A, normal communication cannot be performed on the interface, and consequently the route IP address "11.12.11.14" used by the interface is unreachable. Therefore, the management device may obtain a fault propagation relationship: The fault of the interface causes the route IP address used by the interface to be unreachable. When the management device obtains a first abnormal event used to indicate the fault of the interface and a second abnormal event used to indicate that the route IP address used by the interface is unreachable, the management device determines that the first abnormal event is a root-cause abnormal event, and determines the interface as a root-cause fault network entity.

[0065] Optionally, the network to which the knowledge graph sample belongs is the target network, or the network to which the knowledge graph sample belongs is another network of the same network type as the target network. The plurality of knowledge graph samples may belong to a same network, or may belong to a plurality of networks. This is not limited in this embodiment of this application.

[0066] In this embodiment of this application, the management device may learn the fault propagation relationship between network entities by using the plurality of knowledge graph samples, and determine, based on the fault propagation relationship, the root-cause fault network entity in the abnormal network entities on the knowledge graph of the target network. This implements automated inference and locating of a network fault root cause.

[0067] Optionally, the fault propagation relationship between network entities may alternatively be determined by another device and then sent to the management device. For a manner in which the another device determines the fault propagation relationship between network entities, refer to the foregoing manner in which the management device determines the fault propagation relationship between network entities. Details are not described herein in this embodiment of this application.

[0068] Step 207: Identify the one or more root-cause fault network entities on the knowledge graph of the target network.

[0069] Optionally, after identifying the root-cause fault network entity on the knowledge graph of the target network, the management device may send the knowledge graph of the target network to the OSS or a terminal device connected to the management device, so that the OSS or the terminal device displays the knowledge graph. This helps an operation and maintenance

engineer view the root-cause fault network entity in the target network and quickly locate the fault, thereby improving fault repair efficiency. That is, a time period that the network device takes to switch from a faulty state to a working state is shortened. The time period that the network device takes to switch from the faulty state to the working state may also be referred to as a mean time to repair (MTTR).

[0070] Optionally, in this embodiment of this application, the management device may include one device or a plurality of devices. When the management device includes one device, step 201 to step 207 are all performed by the device. Alternatively, when the management device includes a plurality of devices, for example, a first device and a second device, step 201 to step 205 and step 207 may be performed by the first device, and step 206 may be performed by the second device. To be specific, the first device generates the knowledge graph of the target network, and identifies the abnormal network entities on the knowledge graph of the target network; the first device sends the knowledge graph that is identified with the abnormal network entities to the second device; the second device determines the root-cause fault network entity from the abnormal network entities based on the fault propagation relationship between network entities; the second device sends an identifier of the root-cause fault network entity to the first device; and the first device identifies the root-cause fault network entity on the knowledge graph of the target network based on the received identifier of the root-cause fault network entity.

[0071] A sequence of the steps in the data processing method provided in this embodiment of this application may be properly adjusted, and a step may be correspondingly added or deleted based on a situation. For example, step 207 may alternatively not be performed. After determining the root-cause fault network entity on the knowledge graph of the target network, the management device directly outputs a root-cause abnormal event corresponding to the root-cause fault network entity. Any variation method readily figured out by a person skilled in the art within the technical scope disclosed in this application shall fall within the protection scope of this application. Therefore, details are not described herein.

[0072] In conclusion, according to the data processing method provided in this embodiment of this application, after obtaining the network data of the target network, the management device processes the network data, to generate the knowledge graph of the target network. The knowledge graph of the target network can intuitively reflect the network entities in the target network and the relationship between different network entities, that is, can be used to visualize the network

data. When needing to obtain the network information in the target network, the user only needs to view the knowledge graph of the target network without manually querying the command line. Therefore, the efficiency of obtaining the network information by the user is improved. In addition, after the fault occurs in the target network, the management device may further identify the abnormal network entities on the knowledge graph of the target network, to intuitively reflect abnormal locations in the target network. Further, the management device may further determine the root-cause fault network entity in the abnormal network entities on the knowledge graph of the target network based on the fault propagation relationship between network entities, to implement the automated inference and locating of the network fault root cause.

[0073] It should be noted that the management device may include a plurality of devices that are separately configured to perform different steps. If two adjacent steps are performed by different devices, a device that performs a previous step sends an execution result of the previous step to a device that is to perform a next step. It is assumed that the management device includes a device A and a device B. In an implementation, steps 201 to 203 may be performed by the device A, and steps 204 to 207 are performed by the device B, where the device A sends the initial knowledge graph generated through steps 201 to 203 to the device B, and the device B performs steps 204 to 207 based on the initial knowledge graph received from the device A. In another implementation, steps 201 to 205 may be performed by the device A, and steps 206 and 207 are performed by the device B, where the device A sends the first knowledge graph generated through steps 201 to 205 to the device B, and the device B performs steps 206 and 207 based on the first knowledge graph received from device A.

[0074] FIG. 5 is a schematic diagram of a structure of a data processing apparatus 50 according to an embodiment of this application. The data processing apparatus 50 may be applied to the management device 101 in the application scenario shown in FIG. 1. As shown in FIG. 5, the apparatus 50 includes:

a first obtaining module 501, configured to obtain network data of a target network, where the network data includes a network topology of the target network and device information of a plurality of network devices in the target network, and the device information includes one or more of interface configuration information, protocol configuration information, and service configuration information;

an extraction module 502, configured to extract a plurality of knowledge graph triplets

a third obtaining module 507, configured to obtain a plurality of knowledge graph samples, where each knowledge graph sample is identified with all abnormal network entities that generate, when a fault occurs in a network to which the knowledge graph sample belongs, abnormal events in the network to which the knowledge graph sample belongs and a root-cause fault network entity; and

a second determining module 508, configured to determine the fault propagation relationship based on the plurality of knowledge graph samples.

[0082] Optionally, the network to which the knowledge graph sample belongs is the target network, or the network to which the knowledge graph sample belongs is another network of a same network type as the target network.

[0083] Optionally, the extraction module 502 is configured to:

extract the plurality of knowledge graph triplets from the network data based on an abstract service model corresponding to the network type of the target network, where the abstract service model is used to reflect the relationship between different network entities.

[0084] In conclusion, according to the data processing apparatus provided in this embodiment of this application, after obtaining the network data of the target network through the first obtaining module, the management device processes the network data, and generates the knowledge graph of the target network through the generation module. The knowledge graph of the target network can intuitively reflect the network entities in the target network and the relationship between different network entities, that is, can be used to visualize the network data. When needing to obtain the network information in the target network, the user only needs to view the knowledge graph of the target network without manually querying the command line. Therefore, the efficiency of obtaining the network information by the user is improved. In addition, after the fault occurs in the target network, the management device may further identify the abnormal network entities on the knowledge graph of the target network through the identification module, to intuitively reflect abnormal locations in the target network. Further, the management device may further determine the root-cause fault network entity in the abnormal network entities on the knowledge graph of the target network through the first determining module based on the fault propagation relationship between network entities, to implement automated inference and locating of a network fault root cause.

[0085] FIG. 9 is a block diagram of a data processing apparatus 90 according to an

embodiment of this application. The data processing apparatus 90 may be the management device in the application scenario shown in FIG. 1. As shown in FIG. 9, the data processing apparatus 90 includes a processor 901 and a memory 902.

[0086] The memory 902 is configured to store a computer program, where the computer program includes program instructions.

[0087] The processor 901 is configured to invoke the computer program to implement the data processing method shown in FIG. 2.

[0088] Optionally, the data processing apparatus 90 further includes a communication bus 903 and a communication interface 904.

[0089] The processor 901 includes one or more processing cores, and the processor 901 executes various function applications and data processing by running the computer program.

[0090] The memory 902 may be configured to store the computer program. Optionally, the memory may store an operating system and at least one application program unit required by a function. The operating system may be a real time operating system (RTX), Linux, UNIX, Windows, OS X, or the like.

[0091] There may be a plurality of communication interfaces 904, and the communication interface 904 is configured to communicate with another device, for example, communicate with a control device or a network device.

[0092] The memory 902 and the communication interface 904 are separately connected to the processor 901 via the communication bus 903.

[0093] FIG. 10 is a schematic diagram of a structure of a fault root cause locating apparatus 100 according to an embodiment of this application. The fault root cause locating apparatus 100 may be applied to the management device 101 in the application scenario shown in FIG. 1. As shown in FIG. 10, the apparatus 100 includes:

an obtaining module 1010, configured to obtain a first knowledge graph of a target network in which a fault occurs, where the first knowledge graph is identified with abnormal network entities that generate abnormal events in the target network, and a type of a network entity on the first knowledge graph is a network device, an interface, a protocol, or a service, where specifically, the first knowledge graph may be received from another apparatus, or may be generated by performing steps 203 to 205; and in a process of generating the first knowledge graph, an initial knowledge graph may be first generated or may be received from another apparatus, and

CLAIMS

What is claimed is:

1. A data processing method, comprising:

extracting a plurality of knowledge graph triplets from network data of a target network, wherein the network data comprises a network topology of the target network and device information of a plurality of network devices in the target network, and the device information comprises one or more of interface configuration information, protocol configuration information, and service configuration information, each knowledge graph triplet comprises two network entities and a relationship between the two network entities, and a type of the network entity is a network device, an interface, a protocol, or a service; and

generating a knowledge graph of the target network based on the plurality of knowledge graph triplets.

2. The method according to claim 1, wherein the device information further comprises a routing entry.

3. The method according to claim 1, wherein the relationship between the two network entities is a dependency relationship, a subordinate relationship, or an equivalence relationship.

4. The method according to claim 1, wherein after the generating a knowledge graph of the target network, the method further comprises:

when a fault occurs in the target network, obtaining abnormal events generated in the target network; and

identifying, on the knowledge graph of the target network, abnormal network entities that generate the abnormal events in the target network.

5. The method according to claim 4, wherein the abnormal event comprises one or more of an alarm log, a status change log, and an abnormal key performance indicator.

6. The method according to claim 4, wherein after the identifying, on the knowledge graph of the target network, abnormal network entities that generate the abnormal events in the target network, the method further comprises:

determining one or more root-cause fault network entities from all the abnormal network entities on the knowledge graph of the target network based on a fault propagation relationship between network entities; and

identifying the one or more root-cause fault network entities on the knowledge graph of the target network.

7. The method according to claim 6, wherein the method further comprises:

obtaining a plurality of knowledge graph samples, wherein each knowledge graph sample is identified with all abnormal network entities that generate, when a fault occurs in a network to which the knowledge graph sample belongs, abnormal events in the network to which the knowledge graph sample belongs and a root-cause fault network entity; and

determining the fault propagation relationship based on the plurality of knowledge graph samples.

8. The method according to claim 7, wherein the network to which the knowledge graph sample belongs is the target network, or the network to which the knowledge graph sample belongs is another network of a same network type as the target network.

9. The method according to claim 1, wherein the extracting a plurality of knowledge graph triplets from the network data comprises:

extracting the plurality of knowledge graph triplets from the network data based on an abstract service model corresponding to the network type of the target network, wherein the abstract service model is used to reflect a relationship between different network entities.

10. A data processing apparatus, wherein the apparatus comprises:

a processor; and

a memory, coupled to the processor and configured to store instructions that when executed by the processor cause the apparatus to:

extract a plurality of knowledge graph triplets from network data of a target network, wherein the network data comprises a network topology of the target network and device information of a plurality of network devices in the target network, and the device information comprises one or more of interface configuration information, protocol configuration information, and service configuration information, each knowledge graph triplet comprises two network entities and a relationship between the two network entities, and a type of the network entity is a network device, an interface, a protocol, or a service; and

generate a knowledge graph of the target network based on the plurality of knowledge graph triplets.

11. The apparatus according to claim 10, wherein the device information further comprises a

routing entry.

12. The apparatus according to claim 10, wherein the relationship between the two network entities is a dependency relationship, a subordinate relationship, or an equivalence relationship.

13. The apparatus according to claim 10, wherein when executed by the processor, the instructions further cause the apparatus to:

when a fault occurs in the target network, obtain abnormal events generated in the target network; and

identify, on the knowledge graph of the target network, abnormal network entities that generate the abnormal events in the target network.

14. The apparatus according to claim 13, wherein the abnormal event comprises one or more of an alarm log, a status change log, and an abnormal key performance indicator.

15. The apparatus according to claim 13, wherein when executed by the processor, the instructions further cause the apparatus to:

determine one or more root-cause fault network entities from all the abnormal network entities on the knowledge graph of the target network based on a fault propagation relationship between network entities; and

identify the one or more root-cause fault network entities on the knowledge graph of the target network.

16. The apparatus according to claim 15, wherein when executed by the processor, the instructions further cause the apparatus to:

obtain a plurality of knowledge graph samples, wherein each knowledge graph sample is identified with all abnormal network entities that generate, when a fault occurs in a network to which the knowledge graph sample belongs, abnormal events in the network to which the knowledge graph sample belongs and a root-cause fault network entity; and

determine the fault propagation relationship based on the plurality of knowledge graph samples.

17. A fault root cause locating method, comprising:

obtaining a first knowledge graph of a target network in which a fault occurs, wherein the first knowledge graph is identified with abnormal network entities that generate abnormal events in the target network, and a type of a network entity on the first knowledge graph is a network device, an interface, a protocol, or a service; and

determining one or more root-cause fault network entities from all the abnormal network entities on the first knowledge graph of the target network based on a fault propagation relationship between network entities.

18. The method according to claim 17, wherein the obtaining a first knowledge graph of a target network in which a fault occurs comprises:

when the fault occurs in the target network, obtaining the abnormal events generated in the target network; and

identifying, on an initial knowledge graph of the target network, the abnormal network entities that generate the abnormal events in the target network, to obtain the first knowledge graph, wherein the initial knowledge graph is generated based on network data of the target network, the network data comprises a network topology of the target network and device information of a plurality of network devices in the target network, and the device information comprises one or more of interface configuration information, protocol configuration information, and service configuration information.

19. A fault root cause locating apparatus, wherein the apparatus comprises:

a processor; and

a memory, coupled to the processor and configured to store instructions that when executed by the processor cause the data processing apparatus to:

obtain a first knowledge graph of a target network in which a fault occurs, wherein the first knowledge graph is identified with abnormal network entities that generate abnormal events in the target network, and a type of a network entity on the first knowledge graph is a network device, an interface, a protocol, or a service; and

determine one or more root-cause fault network entities from all the abnormal network entities on the first knowledge graph of the target network based on a fault propagation relationship between network entities.

20. The apparatus according to claim 19, wherein when executed by the processor, the instructions further cause the apparatus to:

when the fault occurs in the target network, obtain the abnormal events generated in the target network; and

identify, on an initial knowledge graph of the target network, the abnormal network entities that generate the abnormal events in the target network, to obtain the first knowledge graph,

wherein the initial knowledge graph is generated based on network data of the target network, the network data comprises a network topology of the target network and device information of a plurality of network devices in the target network, and the device information comprises one or more of interface configuration information, protocol configuration information, and service configuration information.