

VIRTUAL PRIVATE CLOUD COMMUNICATION AND CONFIGURATION METHOD, AND RELATED APPARATUS

TECHNICAL FIELD

[0001] This application relates to the field of cloud technologies, and in particular, to a virtual
5 private cloud communication and configuration method and a related apparatus.

BACKGROUND

[0002] With development of cloud technologies, communication between two or more virtual
private clouds (Virtual Private Cloud, VPC) is required. However, due to reasons such as private
network address planning, if private network addresses of VPCs that need to communicate with
10 each other overlap, the VPCs cannot communicate with each other.

SUMMARY

[0003] To resolve a problem in the conventional technology, embodiments of the present
invention provide a virtual private cloud communication and configuration method and a related
apparatus, to effectively resolve a technical problem that VPCs on a cloud cannot communicate
15 with each other due to overlapping private network addresses.

[0004] According to a first aspect, this application provides a method for configuring virtual
private cloud VPC communication. In the method, a first virtual private cloud VPC and a second
VPC that have a same private network address segment communicate with each other by using a
third VPC. A private network address segment of the third VPC is different from the private
20 network address segment of the first VPC and the private network address segment of the second
VPC. The method includes the following steps: binding a private network address in the first VPC
with a first address, where the first address is an address that belongs to the private network address
segment of the third VPC; binding a private network address in the second VPC with a second
address, where the second address is an address that belongs to the private network address

segment of the third VPC, and the first address is different from the second address; configuring a source address of a packet sent by the first VPC to the second VPC, as the first address; and configuring a destination address the packet sent by the first VPC to the second VPC, as the second address.

5 **[0005]** Through bridging of the third VPC, the first VPC accesses the second VPC by accessing the second address bound with the second VPC, and the second VPC accesses the first VPC by accessing the first address bound with the first VPC. In this way, communication between the first VPC and the second VPC can be implemented when the private network address segment of the first VPC overlaps with the private network address segment of the second VPC.

10 **[0006]** According to a possible implementation of the first aspect, the configuration method further includes a step of configuring a routing rule on the third VPC. The routing rule on the third VPC includes: forwarding a packet whose destination address is the first address to the first VPC, and forwarding a packet whose destination address is the second address to the second VPC.

15 **[0007]** The routing rule is configured, so that the third VPC can forward a packet between the first VPC and the second VPC. In this way, bridging is implemented.

20 **[0008]** According to a possible implementation of the first aspect, the configuration method may further include the following steps: configuring a first gateway on the first VPC, and configuring a second gateway on the second VPC, where a private network address of the first gateway is configured as the first address, and a private network address of the second gateway is configured as the second address; configuring a first packet processing rule on the first gateway, where the first packet processing rule includes: converting a source address of an outbound packet from the address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and configuring a second packet processing rule on the second gateway, where the second packet processing rule includes:
25 converting a source address of the outbound packet from the address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC.

30 **[0009]** The packet processing rules are configured, so that the first gateway binds the address in the first VPC with the first address, and the second gateway binds the address in the second VPC with the second address. In this way, the first VPC accesses the second VPC by accessing the second address, and the second VPC accesses the first VPC by accessing the first address.

[0010] According to a possible implementation of the first aspect, the configuration method further includes a step of configuring a routing rule. Specifically, the routing rule is configured on a router of the first VPC, and the routing rule on the router of the first VPC includes: forwarding the packet whose destination address is the second address to the first gateway, and forwarding a packet whose destination address is the address in the first VPC to a subnet of the first VPC. A routing rule is configured on a router of the second VPC, and the routing rule on the router of the second VPC includes: forwarding the packet whose destination address is the first address to the second gateway, and forwarding a packet whose destination address is the address in the second VPC to the subnet of the first VPC.

[0011] The routing rules are configured, so that the router of the first VPC can forward the packet between the first gateway and the subnet of the first VPC, and the router of the second VPC can forward the packet between the second gateway and a subnet of the second VPC.

[0012] According to another possible implementation of the first aspect, the address in the first VPC includes an address for remotely accessing a subnet of a data center on premise center corresponding to the first VPC.

[0013] According to another possible implementation of the first aspect, the address in the first VPC includes an address in the subnet of the first VPC.

[0014] According to a second aspect, this application provides a method for configuring virtual private cloud VPC communication. The method is used for a first virtual private cloud VPC and a second VPC that have a same private network address segment to communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. The method includes the following steps: configuring a first gateway on the first VPC, and configuring a second gateway on the second VPC, where a first address is configured for the first gateway, a second address is configured for the second gateway, the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address; configuring a first packet processing rule on the first gateway, and configuring a second packet processing rule on the second gateway, where the first packet processing rule includes: converting a source address of an outbound packet from an address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and the second packet processing

rule includes: converting a source address of the outbound packet from an address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC; and configuring a first routing rule on a router of the first VPC, configuring a second routing rule on a router of the second VPC, and configuring a third routing rule on a router of the third VPC, where the first routing rule includes: routing a packet whose destination address is the second address to the first gateway; the second routing rule includes: routing a packet whose destination address is the first address to the second gateway; and the third routing rule includes: routing the packet whose destination address is the first address to the first gateway in the first VPC, and routing the packet whose destination address is the second address to the second gateway in the second VPC.

[0015] Through bridging of the third VPC, the first VPC accesses the second VPC by accessing the second address bound with the second VPC, and the second VPC accesses the first VPC by accessing the first address bound with the first VPC. In this way, communication between the first VPC and the second VPC can be implemented when the private network address segment of the first VPC overlaps with the private network address segment of the second VPC.

[0016] According to a possible implementation of the second aspect, the method further includes the following steps: configuring a connection relationship between the first VPC and the third VPC, and configuring a connection relationship between the second VPC and the third VPC.

[0017] Specifically, the first gateway in the first VPC may be configured to connect to the router of the third VPC, and the second gateway in the second VPC may be configured to connect to the router of the third VPC, so that the first VPC and the second VPC are separately connected to the third VPC. In addition, the third VPC performs forwarding on the first VPC by using the first address bound with the first VPC, and performs forwarding on the second VPC by using the second address bound with the second VPC.

[0018] According to a third aspect, this application provides a virtual private cloud VPC communication method. The method is used for a first virtual private cloud VPC and a second VPC that have a same private network address segment to communicate with each other by using a third VPC. A private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. The method includes the following steps: The first VPC sends a packet, where a source address of the packet is a first address, a destination address of the packet is a second address, both

the first address and the second address are addresses that belong to the private network address segment of the third VPC, a private network address in the first VPC is bound with the first address, and a private network address in the second VPC is bound with the second address. The third VPC receives the packet, and forwards the packet to the second VPC according to a preset routing rule, where a routing rule of the third VPC includes: forwarding a packet whose destination address is the second address to the second VPC.

[0019] Through bridging of the third VPC, the first VPC accesses the second VPC by accessing the second address bound with the second VPC, and the second VPC accesses the first VPC by accessing the first address bound with the first VPC. In this way, communication between the first VPC and the second VPC can be implemented when the private network address segment of the first VPC overlaps with the private network address segment of the second VPC.

[0020] According to a possible implementation of the third aspect, the routing rule further includes: forwarding a packet whose destination address is the first address to the first VPC. In this case, the method further includes the following steps: The second VPC sends a response packet, where a source address of the response packet is the second address, and a destination address of the response packet is the first address. The third VPC receives the response packet, and forwards the response packet to the first VPC according to the routing rule.

[0021] The routing rules are configured, so that a reply packet fed back by the second VPC can be forwarded to the first VPC by using the third VPC, to make a reply.

[0022] According to a fourth aspect, this application provides a virtual private cloud VPC communication method. A first VPC communicates with a second VPC by using a third VPC, the first VPC and the second VPC have a same private network address segment, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. A first gateway is configured on the first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway. Both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address. The method includes the following steps: A router of the first VPC receives a packet sent by a first device, where a source address of the packet is a private network address of the first device, and a destination address of the packet is the second address. The router of the first VPC forwards the packet to the first gateway according

to a first routing rule. The first gateway modifies the source address of the packet to the first address, and forwards a modified packet to a router of the third VPC. A third routing rule is configured on the router of the third VPC. The first routing rule is that a packet whose destination address belongs to the private network address segment of the third VPC needs to be forwarded to the first gateway. The third routing rule is that a packet whose destination address is the second address needs to be forwarded to the second gateway in the second VPC.

[0023] Through bridging of the third VPC, the first VPC accesses the second VPC by accessing the second address bound with the second VPC, and the second VPC accesses the first VPC by accessing the first address bound with the first VPC. In this way, communication between the first VPC and the second VPC can be implemented when the private network address segment of the first VPC overlaps with the private network address segment of the second VPC.

[0024] In a possible implementation of the fourth aspect, the first device may be a first virtual machine in a first subnet of the first VPC, or may be a physical machine or a virtual machine in a second subnet of a first data center on premise connected to the first VPC by using a remote communication tunnel. A second device may be a second virtual machine in a third subnet of the second VPC, or may be a physical machine or a virtual machine in a fourth subnet of a second data center on premise connected to the second VPC by using a remote communication tunnel.

[0025] In a possible implementation of the fourth aspect, the method further includes the following steps: The second gateway receives a packet forwarded by the router of the third VPC, modifies a destination address of the received packet to an address of the second device, and sends a modified packet to a router of the second VPC. The router of the second VPC forwards, according to a second routing rule, the received packet to a subnet in which the second device is located. The second routing rule is that the packet whose destination address belongs to the second address needs to be forwarded to the subnet in which the second device is located.

[0026] The packet is modified and forwarded by the second gateway; after being forwarded by the router of the second VPC, the packet may arrive at the subnet in which the second device is located. In this way, the second device can receive the packet.

[0027] According to a fifth aspect, embodiments of the present invention provide a virtual private cloud VPC communication configuration apparatus. A first virtual private cloud VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC. A private network address segment of the third VPC is different from the private

network address segment of the first VPC and the private network address segment of the second VPC. The apparatus includes the following modules: an address binding module, configured to: bind a private network address in the first VPC with a first address, where the first address is an address that belongs to the private network address segment of the third VPC; and bind a private network address in the second VPC with a second address, where the second address is an address that belongs to the private network address segment of the third VPC, and the first address is different from the second address; and an address configuration module, configured to: configure a source address of a packet sent by the first VPC to the second VPC, as the first address; configure a destination address of the packet sent by the first VPC to the second VPC, as the second address; configure a source address of a packet sent by the second VPC to the first VPC, as the second address; and configure a destination address of the packet sent by the second VPC to the first VPC, as the first address.

[0028] The fifth aspect or any implementation of the fifth aspect is an apparatus implementation corresponding to the first aspect or any implementation of the first aspect. Descriptions of the first aspect or any implementation of the first aspect are applicable to the fifth aspect or any implementation of the fifth aspect. Details are not described herein again.

[0029] According to a sixth aspect, this application provides a virtual private cloud VPC communication configuration apparatus. A first virtual private cloud VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. The apparatus includes: a gateway configuration module, configured to configure a first gateway on the first VPC, and configure a second gateway on the second VPC; an address configuration module, configured to: configure a first address for the first gateway; and configure a second address for the second gateway, where the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address; an address binding module, configured to: configure a first packet processing rule on the first gateway; and configure a second packet processing rule on the second gateway, where the first packet processing rule includes: converting a source address of an outbound packet from an address in the first VPC into the first address, sending a modified outbound packet to a router of the third VPC, converting a destination address of an inbound packet from the first address into

the address in the first VPC, and sending a modified inbound packet to a router of the first VPC; and the second packet processing rule includes: converting a source address of the outbound packet from an address in the second VPC into the second address, sending a modified outbound packet to the router of the third VPC, converting a destination address of the inbound packet from the second address into the address in the second VPC, and sending a modified inbound packet to a router of the second VPC; and a routing rule configuration module, configured to: configure a first routing rule on the router of the first VPC, configure a second routing rule on the router of the second VPC, and configure a third routing rule on the router of the third VPC, where the first routing rule includes: routing a packet whose destination address is the second address to the first gateway; the second routing rule includes: routing a packet whose destination address is the first address to the second gateway; and the third routing rule includes: routing the packet whose destination address is the first address to the first gateway in the first VPC, and routing the packet whose destination address is the second address to the second gateway in the second VPC.

[0030] The sixth aspect or any implementation of the sixth aspect is an apparatus implementation corresponding to the second aspect or any implementation of the second aspect. Descriptions of the second aspect or any implementation of the second aspect are applicable to the sixth aspect or any implementation of the sixth aspect. Details are not described herein again.

[0031] According to a seventh aspect, this application provides a virtual private cloud VPC communications system, including a first virtual private cloud VPC, a second VPC, and a third VPC. The first VPC and the second VPC have a same private network address segment, and the first VPC and the second VPC communicate with each other by using the third VPC. A private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. The first VPC is configured to send a packet. A source address of the packet is a first address, a destination address of the packet is a second address, both the first address and the second address are addresses that belong to the private network address segment of the third VPC, a private network address in the first VPC is bound with the first address, and a private network address in the second VPC is bound with the second address. The third VPC is configured to: receive the packet, and forward the packet to the second VPC according to a preset routing rule. A routing rule of the third VPC includes: forwarding a packet whose destination address is the second address to the second VPC.

[0032] The seventh aspect or any implementation of the seventh aspect is a system

implementation corresponding to the third aspect or any implementation of the third aspect. Descriptions of the third aspect or any implementation of the third aspect are applicable to the seventh aspect or any implementation of the seventh aspect. Details are not described herein again.

[0033] According to an eighth aspect, this application provides a virtual private cloud VPC

5 communications system, including a first virtual private cloud VPC, a second VPC, and a third VPC. The first VPC communicates with the second VPC by using the third VPC, and the first VPC and the second VPC have a same private network address segment. A private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC. A first gateway is configured on the
10 first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway. Both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address. A router of the first VPC is configured to receive a packet sent by a first device. A source address of the packet is a private network address of the
15 first device, and a destination address of the packet is the second address. The router of the first VPC is further configured to forward the packet to the first gateway according to a first routing rule. The first gateway is configured to: modify the source address of the packet to the first address, and forward a modified packet to a router of the third VPC. A third routing rule is configured on the router of the third VPC. The first routing rule is that a packet whose destination address belongs
20 to the private network address segment of the third VPC needs to be forwarded to the first gateway. The third routing rule is that a packet whose destination address is the second address needs to be forwarded to the second gateway in the second VPC.

[0034] The eighth aspect or any implementation of the eighth aspect is a system implementation corresponding to the fourth aspect or any implementation of the fourth aspect.

25 Descriptions in the fourth aspect or any implementation of the fourth aspect are applicable to the eighth aspect or any implementation of the eighth aspect. Details are not described herein again.

[0035] According to a ninth aspect, this application provides a virtual private cloud VPC

communications system, including a first virtual private cloud VPC, a second VPC, and a third VPC. The first VPC communicates with the second VPC by using the third VPC, and the first
30 VPC and the second VPC have a same private network address segment. A private network address segment of the third VPC is different from the private network address segment of the first VPC

and the private network address segment of the second VPC. A first gateway connected to the third VPC is configured on the first VPC, and a second gateway connected to the third VPC is configured on the second VPC. A first address is configured for the first gateway, and a second address is configured for the second gateway. Both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address. A first virtual machine in a first subnet of the first VPC is configured to send a packet to a switch of the first subnet. A source address of the packet is a private network address of the first virtual machine in the first subnet, and a destination address of the packet is the second address. The switch of the first subnet is configured to send the packet to a router of the first VPC. The router of the first VPC is configured to: receive the packet, and forward the packet to the first gateway. The first gateway is configured to: receive the packet, modify the destination address of the packet to the first address, and send a modified packet to a router of the third VPC. The router of the third VPC is configured to: receive the packet, and forward the packet to the second gateway. The second gateway is configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second virtual machine in a second subnet of the second VPC, in the second subnet, and send a modified packet to a router of the second VPC. The router of the second VPC is configured to: receive the packet, and forward the packet to a switch of the second subnet. The switch of the second subnet is configured to: receive the packet, and forward the packet to the second virtual machine.

[0036] According to a tenth aspect, this application provides a virtual private cloud VPC communications system, including a first virtual private cloud VPC, a second VPC, and a third VPC. The first VPC communicates with the second VPC by using the third VPC, and the first VPC and the second VPC have a same private network address segment, a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC, a first remote connection gateway remotely connected to a first data center on premise and a first gateway connected to the third VPC are configured on the first VPC, a second remote connection gateway remotely connected to a second data center on premise and a second gateway connected to the third VPC are configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway, both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second

address. The first remote connection gateway is configured to: receive a packet sent by a first device in a first subnet of the first data center on premise, and send the packet to a router of the first VPC. A source address of the packet is a private network address of the first device in the first subnet, and a destination address of the packet is the second address. The router of the first VPC is configured to: receive the packet, and forward the packet to the first gateway. The first gateway is configured to: receive the packet, modify the destination address of the packet to the first address, and forward a modified packet to a router of the third VPC. The router of the third VPC is configured to: receive the packet, and forward the packet to the second gateway. The second gateway is configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second device in a second subnet of the second data center on premise, in the second subnet, and send a modified packet to a router of the second VPC. The router of the second VPC is configured to: receive the packet, and forward the packet to the second remote connection gateway. The second remote connection gateway is configured to receive the packet, and send the packet to the second device in the second subnet of the second data center on premise.

[0037] According to an eleventh aspect, this application provides a virtual private cloud VPC communications system, including a first virtual private cloud VPC, a second VPC, and a third VPC. The first VPC communicates with the second VPC by using the third VPC, and the first VPC and the second VPC have a same private network address segment, a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC, a first gateway is configured on the first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway. Both the first address and the second address belong to the private network address segment of the third VPC, a router of the first VPC and a router of the second VPC are separately connected to a router of the third VPC, and the first address is different from the second address. A first virtual machine in a first subnet of the first VPC is configured to send a packet to a switch of the first subnet. A source address of the packet is a private network address of the first virtual machine in the first subnet, and a destination address of the packet is the second address. The switch of the first subnet is configured to send the packet to the first gateway. The first gateway is configured to: modify the source address of the packet to the first address, and send a modified packet to the router of the

first VPC. The router of the first VPC is configured to: receive the packet, and forward the packet to the router of the third VPC. The router of the third VPC is configured to: receive the packet, and forward the packet to the router of the second VPC. The router of the second VPC is configured to: receive the packet, and forward the packet to the second gateway. The second gateway is
5 configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second virtual machine in a second subnet of the second VPC, in the second subnet, and send a modified packet to a switch of the second subnet. The switch of the second subnet is configured to: receive the packet, and forward the packet to the second virtual machine.

[0038] According to a twelfth aspect, this application provides a computing device, including
10 at least one memory and at least one processor. The at least one memory is configured to store a program instruction, and the at least one processor executes the program instruction, to perform the method for implementing the first aspect and any possible implementation of the first aspect.

[0039] According to a thirteenth aspect, this application provides a computing device, including at least one memory and at least one processor. The at least one memory is configured
15 to store a program instruction, and the at least one processor executes the program instruction, to perform the method for implementing the second aspect and any possible implementation of the second aspect.

[0040] According to a fourteenth aspect, this application provides a non-transient readable storage medium. When the non-transient readable storage medium is executed by a computing
20 device, the computing device performs the method provided in any one of the first aspect or the possible implementations of the first aspect. The storage medium stores a program. The storage medium includes but is not limited to a volatile memory, for example, a random access memory or a non-volatile memory, for example, a flash memory, a hard disk drive (English: hard disk drive, HDD for short), or a solid-state drive (English: solid state drive, SSD for short).

[0041] According to a fifteenth aspect, this application provides a non-transient readable storage medium. When the non-transient readable storage medium is executed by a computing
25 device, the computing device performs the method provided in any one of the second aspect or the possible implementations of the second aspect. The storage medium stores a program. The storage medium includes but is not limited to a volatile memory, for example, a random access memory
30 or a non-volatile memory, for example, a flash memory, a hard disk drive (English: hard disk drive, HDD for short), or a solid-state drive (English: solid state drive, SSD for short).

[0042] According to a sixteenth aspect, this application provides a computing device program product. The computing device program product includes a computer instruction. When the computer instruction is executed by a computing device, the computing device performs the method provided in any one of the first aspect or the possible implementations of the first aspect.

5 The computer program product may be a software installation package. When the method provided in any one of the first aspect or the possible implementations of the first aspect needs to be used, the computer program product may be downloaded to and executed on the computing device.

[0043] According to a seventeenth aspect, this application provides another computing device program product. The computing device program product includes a computer instruction. When
10 the computer instruction is executed by a computing device, the computing device performs the method provided in any one of the second aspect or the possible implementations of the second aspect. The computer program product may be a software installation package. When the method provided in any one of the second aspect or the possible implementations of the second aspect needs to be used, the computer program product may be downloaded to and executed on the
15 computing device.

[0044] According to an eighteenth aspect, this application further provides a method for configuring virtual private cloud VPC communication. A first VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address
20 segment of the first VPC and the private network address segment of the second VPC. The method includes: providing a first configuration page for a user in the first VPC, where the first configuration page prompts the user in the first VPC to create a first gateway on the first VPC, and prompts the user in the first VPC to enter information about the third VPC to which the first gateway needs to be connected and a first address of the first gateway in the third VPC; providing
25 a second configuration page for a user in the second VPC, where the second configuration page prompts the user in the second VPC to create a second gateway on the second VPC, and prompts the user in the second VPC to enter the information about the third VPC to which the second gateway needs to be connected and a second address of the second gateway in the third VPC; and the first address and the second address belong to the private network address segment of the third
30 VPC, and the first address is different from the second address; creating the first gateway based on information about the first configuration page; and creating the second gateway based on

information about the second configuration page.

[0045] According to a possible implementation of the eighteenth aspect, the VPC communication configuration method further includes the following steps: configuring a first packet processing rule on the first gateway, and configuring a second packet processing rule on the second gateway, where the first packet processing rule includes: converting a source address of an outbound packet from an address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and the second packet processing rule includes: converting a source address of the outbound packet from an address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC; and configuring a first routing rule on a router of the first VPC, configuring a second routing rule on a router of the second VPC, and configuring a third routing rule on a router of the third VPC, where the first routing rule includes: routing a packet whose destination address is the second address to the first gateway; the second routing rule includes: routing a packet whose destination address is the first address to the second gateway; and the third routing rule includes: routing the packet whose destination address is the first address to the first gateway in the first VPC, and routing the packet whose destination address is the second address to the second gateway in the second VPC.

BRIEF DESCRIPTION OF DRAWINGS

[0046] FIG. 1 is a schematic diagram of a system structure of a VPC communications system;

[0047] FIG. 2 is a schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention;

[0048] FIG. 3A and FIG. 3B are another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention;

[0049] FIG. 4 is a flowchart of a method for configuring VPC communication according to an embodiment of the present invention;

[0050] FIG. 5a to FIG. 5g show VPC settings interfaces provided by a control platform;

[0051] FIG. 6A to FIG. 6C show a schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention;

[0052] FIG. 7A and FIG. 7B show another schematic diagram of a system structure of a VPC

communications system according to an embodiment of the present invention;

[0053] FIG. 8A to FIG. 8C show another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention;

[0054] FIG. 9A and FIG. 9B are another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention;

[0055] FIG. 10 is a schematic structural diagram of a configuration apparatus according to an embodiment of the present invention; and

[0056] FIG. 11 is a schematic structural diagram of a computing device according to an embodiment of the present invention.

DESCRIPTION OF EMBODIMENTS

[0057] Terms used in the embodiments of the present invention are first explained.

[0058] A cloud data center is a data center that provides a public cloud service.

[0059] A data center on premise is a data center that provides a non-public cloud service. If the data center on premise provides an on-premise service, the data center on premise includes a plurality of physical machines (physical machine). If the data center on premise provides a private cloud service, the data center on premise includes a plurality of virtual machines.

[0060] A public cloud service is infrastructure as a service (Infrastructure as a Service, IaaS). The public cloud service means that infrastructure provided by a public cloud service provider is externally provided as a service on the internet. In this service model, a user does not need to build a data center. Instead, the user rents infrastructure, such as a server, a storage, and a network, for use. The public cloud service is implemented by providing a virtual environment (such as a virtual machine). A core attribute of the public cloud is that a plurality of users share cloud infrastructure and the users are isolated from each other.

[0061] A non-public cloud service provides infrastructure dedicated to a single user, for example, a private cloud service and an on-premise service.

[0062] A private cloud (Private Clouds) service is that a single user owns and can fully control infrastructure, such as a server, a storage, and a network. The private cloud service is implemented by providing a virtual environment (such as a virtual machine). A core attribute of the private cloud service is that the single user exclusively uses the infrastructure.

[0063] An on-premise (On-premises) service is that a single user locally builds infrastructure, such as a server, a storage, and a network. The user exclusively uses the infrastructure. The on-premise service is implemented by using a physical machine.

[0064] A private network address is an IP address that cannot be forwarded on the internet but can be forwarded only on a local area network. The private network address is prohibited from being used on the internet.

[0065] The private network address is a reserved IP address. The following table lists classification of private network addresses, a network segment, and a quantity of private network addresses.

Classification of private network addresses	Network segment	Quantity of available private network addresses
Class A private network address	192.168.0.0/16	65,532
Class B private network address	172.16.0.0/12	1,048,572
Class C private network address	10.0.0.0/8	16,777,212

[0066] A virtual private cloud (Virtual Private Cloud, VPC) is configured on a public cloud, and the VPC is a virtual network of a user of a public cloud service in a cloud data center. Each VPC can separately form a network and is logically isolated from other VPCs. Therefore, private network address segments of subnets in different VPCs may be the same.

[0067] Specifically, each VPC has an independent tunnel number. Packets between virtual machines in a VPC have a same tunnel identifier and are sent to a physical network for transmission. Tunnel identifiers of virtual machines in the different VPCs are different, and the virtual machines are located on two different routing planes. Therefore, the virtual machines in the different VPCs cannot communicate with each other, naturally implementing logical isolation.

[0068] The tunnel identifier may be, for example, a virtual local area network identifier (Virtual Local Area Network Identification, VLAN ID) or a virtual network identifier (Virtual Network ID, VNI).

[0069] First, referring to FIG. 1, FIG. 1 is a schematic diagram of a system structure of a VPC communications system. As shown in FIG. 1, the VPC communications system includes a cloud data center 10 and a client 7, and the client 7 accesses the cloud data center 10 on the internet 8.

[0070] FIG. 1 is a logical schematic diagram of the cloud data center 10. The cloud data center

10 provides a VPC 1 and a VPC 2 to a public cloud user. The VPC 1 includes a router 1 and a subnet 1. A private network address segment of the VPC 1 is 192.168.0.0/16, and a private network address segment of the subnet 1 is 192.168.0.0/24. A virtual machine (virtual machine, VM) 1 and a VM 2 are configured in the subnet 1. A private network address of the VM 1 is 192.168.0.2, and
5 a private network address of the VM 2 is 192.168.0.3. The VM 1 and the VM 2 are connected to a switch 1, and the router 1 is connected to the switch 1.

[0071] It should be noted that the private network address segment of the subnet 1 is a subset of the private network address segment of the VPC 1. In addition to the subnet 1, the VPC 1 may further include other subnets, such as a subnet whose private network address segment is
10 192.168.1.0/24, or a subnet whose private network address segment is 192.168.2.0/24. The router 1 is configured to forward a packet for communication between different subnets.

[0072] In addition, the VPC 2 includes a router 2 and a subnet 2. The private network address segment of the VPC 2 is 192.168.0.0/16, and a private network address segment of the subnet 2 is 192.168.0.0/24. A VM 3 and a VM 4 are configured in the subnet 2. A private network address of
15 the VM 3 is 192.168.0.2, and a private network address of the VM 4 is 192.168.0.3. The VM 3 and the VM 4 are connected to a switch 2, and the router 2 is connected to the switch 2.

[0073] The subnet 1 and the subnet 2 have a same private network address segment. In other words, a private network address segment of the subnet 1 overlaps with a private network address segment of the subnet 2.

[0074] Similarly, the private network address segment of the subnet 2 is a subset of the private network address segment of the VPC 2. In addition to the subnet 2, the VPC 2 may further include other subnets, such as the subnet whose private network address segment is 192.168.1.0/24, or the subnet whose private network address segment is 192.168.2.0/24. The router 2 is configured to forward the packet for communication between different subnets.

[0075] The client 7 accesses a control platform 6 on the internet 8, and the control platform 6 provides a VPC configuration page. The client 7 accesses the VPC configuration interface on the internet 8, and enters configuration information of a VPC on the VPC configuration interface. The control platform 6 configures the VPC in the cloud data center 10 based on the configuration information. Specifically, each functional module in the VPC may be configured, for example, the
25 VPC may be created or deleted, a virtual machine may be created or deleted in the VPCs, and a routing rule of a router of the VPC may be configured. The control platform 6 may perform full
30

lifecycle management on the VPCs based on the configuration information. From a perspective of the client 7, the cloud data center 10 provides the VPC 1 and the VPC 2 that are logically isolated. The client 7 can log in to the VM 1 or the VM 2 of the VPC 1 by using a remote desktop. The client 7 also can log in to the VM 3 and the VM 4 in the VPC 2. The VPC 1 and the VPC 2 are logically isolated and do not interfere with each other.

[0076] The client 7 is a terminal device, for example, a mobile phone with a network access function, a personal computer, a personal digital assistant, or a thin client. A user uses virtual machines in the cloud data center 10 by using the client 7.

[0077] As shown in FIG. 1, the VM 1 and the VM 2 are configured in the subnet 1 of the VPC 1, the private network address 192.168.0.2 is set for the VM 1 in the subnet 1 of the VPC 1, the private network address 192.168.0.3 is set for the VM 2 in the subnet 1 of the VPC 1, and the VM 1 communicates with the VM 2 by using the switch 1. The VM 3 and the VM 4 are configured in the subnet 2 of the VPC 2, the private network address 192.168.0.2 is set for the VM 3 in the subnet 2 of the VPC 2, the private network address 192.168.0.3 is set for the VM 4 in the subnet 2 of the VPC 2, and the VM 3 communicates with the VM 4 by using the switch 2.

[0078] For example, the user uses the client 7 to log in to the VM 1, and enters an internet control message protocol (Internet Control Message Protocol, ICMP) command "ping 192.168.1.3" on the VM 1. The command is used to control the VM 1 to send an IP packet to the VM 2, to test whether the VM 1 and the VM 2 are interconnected. In this embodiment, because the VM 1 and the VM 2 are configured in the same VPC 1, the VM 1 obtains a reply from the VM 2.

[0079] However, as shown in FIG. 1, because the VPC 1 and the VPC 2 are logically isolated, the virtual machine in the VPC 1 cannot communicate with the virtual machine in the VPC 2. Specifically, the client 7 logs in to the VM 1, and may enter an ICMP command "ping 192.168.0.3" on the VM 1. The command is used to test whether the VM 1 and the VM 4 are interconnected. In this embodiment, because the VM 1 and the VM 4 are set in different VPCs, the VM 1 does not obtain a reply from the VM 4.

[0080] In an enterprise cloud application scenario, due to a need of service isolation between departments, VPCs can be used to isolate services. For example, the VPC 1 belongs to a research and development department, and the VPC 2 belongs to a finance department. In the logical architecture shown in FIG. 1, VMs in the research and development department can communicate

with each other, and VMs in the finance department can also communicate with each other. However, the VMs in the research and development department cannot communicate with the VMs in the finance department. VMs of different departments are configured in the different VPCs to effectively implement data isolation.

5 **[0081]** However, in a practical application, the VMs in the research and development department and the VMs in the finance department need to communicate with each other in some cases. For example, the VMs in the research and development department need to obtain financial data of the research and development department from the VMs in the finance department. If the VMs in the research and development department and the VMs in the finance department are
10 isolated from each other, the financial data cannot be obtained from the VMs in the finance department.

[0082] Therefore, in some implementations, the router 1 and the router 2 are connected, so that the VPC 1 and the VPC 2 can communicate with each other. However, in the scenario shown in FIG. 1, the private network address segment of the subnet 1 overlaps with the private network
15 address segment of the subnet 2. In this case, even if the router 1 and the router 2 are connected, the subnet 1 and the subnet 2 cannot communicate with each other. For example, the VM 1 communicates with the VM 3, the VM 1 constructs an IP packet whose source IP address and destination IP address are both 192.168.0.2. When the IP packet reaches the switch 1, the switch 1 intercepts the IP packet and sends the IP packet to the VM 1 based on the destination IP address
20 of the IP packet, an operating system of the VM 1 directly intercepts the IP packet. In this case, the IP packet cannot reach the subnet 2.

[0083] To resolve the foregoing technical problem, the embodiments of the present invention provide a VPC communications system. Referring to FIG. 2, FIG. 2 is a schematic diagram of a system structure of a VPC communications system according to an embodiment of the present
25 invention. As shown in FIG. 2, a VPC 1 and a VPC 2 that have a same private network address segment communicate with each other by using a VPC 3, and a private network address segment of the VPC 3 is different from the private network address segment of the VPC 1 and the private network address segment of the VPC 2. A private network address in the VPC 1 is bound with 10.0.0.9, and 10.0.0.9 is an address that belongs to the private network address segment of the
30 VPC 3. A private network address in the VPC 2 is bound with 10.0.0.10, and 10.0.0.10 is the address that belongs to the private network address segment of the VPC 3. A source address of a

packet sent by the VPC 1 to the VPC 2 is configured as 10.0.0.9, and a destination address of the packet sent by the VPC 1 to the VPC 2 is configured as 10.0.0.10. The packet is sent by the VPC 1 to the VPC 3, and forwarded by the VPC 3 to the VPC 2.

[0084] Through bridging of the VPC 3, the VPC 1 can access the VPC 2 by accessing 10.0.0.10 that is bound with the VPC 2. In this way, communication between the VPC 1 and the VPC 2 may be implemented when the private network address segment of the VPC 1 overlaps with the private network address segment of the VPC 2.

[0085] For further clear description, refer to FIG. 3A and FIG. 3B in the following. FIG. 3A and FIG. 3B are another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention. FIG. 3A and FIG. 3B are a specific implementation of FIG. 2. In this embodiment, a VPC 3 is configured between a VPC 1 and a VPC 2 by using a control platform 6, and a private network address segment that does not overlap a private network address of the VPC 1 and a private network address of the VPC 2 is set for the VPC 3. In addition, a gateway 1 connected to the VPC 3 is disposed in the VPC 1. A first private network address of the VPC 3 is set on the gateway 1. A gateway 2 connected to the VPC 3 is disposed in the VPC 2. A second private network address of the VPC 3 is set on the gateway 2. A VM 1 in the VPC 1 is bound with the gateway 1, and a VM 3 in the VPC 2 is bound with the gateway 2, by setting routing rules of routers of the VPC 1, the VPC 2, and the VPC 3 and packet processing rules of the gateway 1 and the gateway 2. In this way, the VM 1 communicates with the VM 3 by accessing the second private network address of the VPC 3, and the VM 3 communicates with the VM 1 by accessing the first private network address of the VPC 3.

[0086] The control platform 6 may perform the foregoing gateway creation and rule configuration in a cloud data center 10 based on configuration information, and the configuration information is entered by a client 7 into a VPC configuration interface provided by the control platform 6.

[0087] In another embodiment, the control platform 6 may also automatically generate the foregoing configuration information, and perform the foregoing configuration.

[0088] Details are as follows:

[0089] The control platform 6 may allocate a private network address 10.0.0.9 of the private network address segment (for example, 10.0.0.0/24) of the VPC 3 to the gateway 1 based on the configuration information, and allocate another private network address 10.0.0.10 of the private

network address segment (for example, 10.0.0.0/24) of the VPC 3 to the gateway 2. In addition, the gateway 1 is configured to connect to a router 3 of the VPC 3, and the gateway 2 is configured to connect to the router 3 of the VPC 3. The control platform 6 separately configures the routers and the gateways.

5 **[0090]** A router 1 is provided with:

 a routing rule 1: When a destination IP address of a packet received by the router 1 is the private network address segment 10.0.0.0/24 of the VPC 3, the router 1 forwards the IP packet to the gateway 1; and

 a routing rule 2: When the destination IP address of the packet received by the router 1
10 is a private network address segment 192.168.0.0/24 of a subnet 1, the router 1 forwards the packet to the subnet 1.

[0091] The gateway 1 is provided with:

 a packet processing rule 1: When a source IP address of an outbound packet received by the gateway 1 is a private network address 192.168.0.2 of the VM 1 in the subnet 1, the gateway
15 1 converts 192.168.0.2 into the private network address 10.0.0.9 of the gateway 1 in the VPC 3, and sends a modified outbound packet to the router 3 of the VPC 3; and

 a packet processing rule 2: When a destination IP address of an inbound packet received by the gateway 1 is the private network address 10.0.0.9 of the gateway 1 in the VPC 3, the gateway
20 1 converts 10.0.0.9 into the private network address 192.168.0.2 of the VM 1 in the subnet 1, and sends a modified inbound packet to the router 1 of the VPC 1.

[0092] The outbound packet is a packet received by the gateway 1 from the router 1, and the inbound packet is a packet received by the gateway 1 from the router 3.

[0093] The router 3 is provided with:

 a routing rule 5: When a destination IP address of a packet received by the router 3 is
25 the private network address 10.0.0.10 of the gateway 2 in the VPC 3, the router 3 forwards the IP packet to the gateway 2; and

 a routing rule 6: When the destination IP address of the packet received by the router 3 is the private network address 10.0.0.9 of the gateway 1 in the VPC 3, the router 3 forwards the packet to the gateway 1.

30 **[0094]** The gateway 2 is provided with:

 a packet processing rule 3: When a destination IP address of an inbound packet received

by the gateway 2 is the private network address 10.0.0.10 of the gateway 2 in the VPC 3, the gateway 2 converts 10.0.0.10 into a private network address 192.168.0.2 of the VM 3 in a subnet 2, and sends a modified inbound packet to a router 2; and

a packet processing rule 4: When a source IP address of an outbound packet received by the gateway 2 is the private network address 192.168.0.2 of the VM 3 in the subnet 2, the gateway 2 converts 192.168.0.2 into the private network address 10.0.0.10 of the gateway 2 of the VPC 3.

[0095] The outbound packet is a packet received by the gateway 2 from the router 2, and the inbound packet is a packet received by the gateway 2 from the router 3.

[0096] A router 2 is provided with:

a routing rule 3: When a destination IP address of a packet received by the router 2 is the private network address segment 10.0.0.0/24 of the VPC 3, the router 2 forwards the packet to the gateway 2; and

a routing rule 4: When the destination IP address of the packet received by the router 2 is a private network address segment 192.168.0.0/24 of the subnet 2, the router 2 forwards the packet to the subnet 2.

[0097] It should be noted that the gateway 1 may have two private network addresses. One private network address belongs to the VPC 1, and is used for internal setting and management of the gateway disposed in the VPC 1. The other address belongs to the VPC 3 (for example, 10.0.0.9), and is used for external communication. This patent application relates to external communication. Therefore, unless otherwise specified, the private network address of the gateway 1 in this patent application is a private network address of the gateway 1 that belongs to the VPC 3. Similarly, the gateway 2 may also have two private network addresses, and details are not described herein.

[0098] The following specifically describes a method for setting the foregoing corresponding rules of the gateway and the router with reference to FIG. 4. FIG. 4 is a flowchart of a method for configuring VPC communication according to an embodiment of the present invention. The method is performed by a control platform 6, and the method includes the following steps.

[0099] Step S101: Create a gateway 1 in a VPC 1.

[00100] Specifically, refer to FIG. 5a. FIG. 5a shows a settings interface 1 of the VPC 1. In the interface, a user needs to enter a gateway name (the gateway 1), a VPC (the VPC 1) in which the gateway is located, a VPC (a VPC 3) to which the gateway is to connect, and a private network

address 10.0.0.9 of the VPC to which the gateway is to connect.

[00101] Step S102: Configure a packet processing rule of the gateway 1.

[00102] With reference to FIG. 5b, FIG. 5b shows a settings interface 2 of the VPC 1. In the interface, the user enters a packet processing rule of the created gateway 1. The packet processing rule shown in FIG. 5b is the packet processing rule 1 and the packet processing rule 2 of the gateway 1 that are shown in FIG. 3.

[00103] The packet processing rule 1 includes a source network address translation (Source network address translation, SNAT) rule, and the packet processing rule 2 includes a destination network address translation (Destination net address translation, DNAT) rule.

10 **[00104]** Step S103: Configure a routing rule of the VPC 1.

[00105] With reference to FIG. 5c, FIG. 5c shows a settings interface 3 of the VPC 1. In the interface, the user enters a routing rule of a router 1, to be specific, the packet processing rule 1 and the packet processing rule 2 that are shown in FIG. 2.

[00106] Step S104: Create a gateway 2 in a VPC 2.

15 **[00107]** Specifically, refer to FIG. 5d. FIG. 5d shows a settings interface 1 of the VPC 2. In the interface, the user needs to enter a gateway name (the gateway 2), a VPC (the VPC 2) in which the gateway is located, the VPC (the VPC 3) to which the gateway is to connect, and a private network address 10.0.0.10 of the VPC to which the gateway is to connect.

[00108] Step S105: Configure a packet processing rule of the gateway 2.

20 **[00109]** With reference to FIG. 5e, FIG. 5e shows a settings interface 2 of the VPC 2. In the interface, the user enters a packet processing rule of the created gateway 2. The packet processing rule shown in FIG. 5e is the packet processing rule 3 and the packet processing rule 4 of the gateway 2 that are shown in FIG. 2.

[00110] Step S106: Configure a routing rule of the VPC 2.

25 **[00111]** With reference to FIG. 5f, FIG. 5f shows a settings interface 3 of the VPC 2. In the interface, the user enters a routing rule of a router 2, to be specific, the packet processing rule 3 and the packet processing rule 4 that are shown in FIG. 2.

[00112] Step S107: Configure a routing rule of the VPC 3.

30 **[00113]** With reference to FIG. 5g, FIG. 5g shows a settings interface of the VPC 3. In the interface, the user enters a routing rule of a router 3, to be specific, the packet processing rule 5 and the packet processing rule 6 that are shown in FIG. 2.

[00114] A sequence of steps S101 to S107 may be adjusted as required. For example, the step of creating a gateway 2 may be first performed, and then the step of creating a gateway 1 is performed. This is not limited in this embodiment of the present invention.

[00115] It should be noted that the foregoing configuration information is entered, by using a client 7, by the user to a VPC configuration interface provided by the control platform 6, and the configuration information is sent by the control platform 6 to the control platform 6. The control platform 6 configures the VPC 1 and the VPC 2 based on the configuration information.

[00116] After the control platform 6 performs the foregoing configuration method, the VPC communications system shown in FIG. 3 may be implemented in a cloud data center 10.

[00117] Further, referring to FIG. 6A to FIG. 6C, FIG. 6A to FIG. 6C are a data interaction diagram of a VPC communication method according to an embodiment of the present invention. The method is based on the VPC communications system shown in FIG. 3A and FIG. 3B, and specifically shows a packet flow direction when a VM 1 accesses a VM 3 across VPCs.

[00118] As shown in FIG. 6A to FIG. 6C, the VPC communication method according to this embodiment of the present invention includes the following steps.

[00119] Step 1: The VM 1 constructs an IP packet 1 and sends the IP packet 1 to a switch 1.

[00120] A source IP address of an IP header of the IP packet 1 is a private network address 192.168.0.2 of the VM 1 in a subnet 1, a destination IP address of the IP header of the IP packet 1 is a private network address 10.0.0.10 of a gateway 2 in a subnet 3, and a data part of the IP packet 1 carries request information.

[00121] It should be noted that the VM 1 may query for a correspondence between 10.0.0.10 and the VM 3 in advance based on a service requirement. For example, the VM 1 may query a VPC 2 for the correspondence between 10.0.0.10 and the VM 3, and may also query a control platform 6 for the correspondence between 10.0.0.10 and the VM 3.

[00122] Step 2: The switch 1 forwards the IP packet 1 to a router 1.

[00123] After receiving the IP packet 1, the switch 1 determines that the destination IP address of the IP packet 1 does not belong to the subnet 1, and sends the IP packet 1 to the router 1 to perform cross-network-segment packet transmission.

[00124] Step 3: The router 1 forwards the IP packet 1 according to a routing rule 1.

[00125] After receiving the IP packet 1, the router 1 matches the routing rule 1 based on the destination IP address (10.0.0.10) of the IP packet 1, and sends the IP packet 1 to a gateway 1

according to the routing rule 1.

[00126] Step 4: The gateway 1 modifies the source IP address of the IP packet 1 according to a packet processing rule 1, and sends a modified IP packet 1 to a router 3.

5 **[00127]** After the gateway 1 receives the IP packet 1 from the router 1, because the IP packet 1 is from the router 1, the gateway 1 determines that the IP packet 1 is an outbound packet, matches the packet processing rule 1 based on the source IP address of the IP packet 1, modifies the source IP address of the IP packet 1 from 192.168.0.2 to 10.0.0.9, and sends a modified IP packet 1 to the router 3.

10 **[00128]** Step 5: The router 3 forwards the IP packet 1 to the gateway 2 according to a routing rule 5.

[00129] After receiving the IP packet 1, the router 3 matches the routing rule 5 based on the destination IP address (10.0.0.10) of the IP packet 1, and forwards the IP packet 1 to the gateway 2.

15 **[00130]** Step 6: The gateway 2 modifies the destination IP address of the IP packet 1 according to a packet processing rule 3, and sends a modified IP packet 1 to a router 2.

20 **[00131]** After the gateway 2 receives the IP packet 1 from the router 3, because the IP packet 1 is from the router 3, the gateway 2 determines that the IP packet 1 is an inbound packet, matches the packet processing rule 3 based on the destination address of the IP packet 1, modifies the destination IP address of the IP packet 1 from 10.0.0.10 to 192.168.0.2, and sends a modified IP packet 1 to the router 2.

[00132] Step 7: The router 2 forwards the modified IP packet 1 to a switch 2 according to a routing rule 4.

25 **[00133]** The router 2 matches the routing rule 4 based on the destination IP address 192.168.0.2 of the IP packet 1, and sends the IP packet 1 to a subnet 2. The switch 2 is disposed in a subnet 2, to be specific, the switch 2 that sends the IP packet 1 to the switch 2 in the subnet 2.

[00134] Step 8: The switch 2 sends the IP packet 1 to the VM 3.

[00135] The switch 2 sends the IP packet 1 to the VM 3 based on the destination IP address 192.168.0.2 of the IP packet 1.

[00136] Step 9: The VM 3 constructs an IP packet 2 and sends the IP packet 2 to the switch 2.

30 **[00137]** The IP packet 2 is a reply packet of the IP packet 1.

[00138] After receiving the IP packet 1, the VM 3 obtains the request information from the data

part of the IP packet 1, generates reply information based on the request information, and constructs the IP packet 2. Specifically, the VM 3 sets the source IP address 10.0.0.9 of the IP packet 1 to a destination IP address of the IP packet 2, and sets the destination IP address 192.168.0.2 of the IP packet 1 to a source IP address of the IP packet 2, sets the reply information in a data part of the IP packet 2, and sends the IP packet 2 to the switch 2.

[00139] Step 10: The switch 2 forwards the IP packet 2 to the router 2.

[00140] After receiving the IP packet 2, the switch 2 determines that the destination IP address 10.0.0.9 of the IP packet 2 does not belong to the subnet 1 (192.168.0.0/24), and sends the IP packet 2 to the router 2 to perform cross-network-segment packet transmission.

[00141] Step 11: The router 2 forwards the IP packet 2 according to a routing rule 3.

[00142] After receiving the IP packet 2, the router 2 matches the routing rule 3 based on the destination IP address (10.0.0.9) of the IP packet 2, and sends the IP packet 2 to the gateway 2 according to the routing rule 3.

[00143] Step 12: The gateway 2 modifies the source IP address of the IP packet 2 according to a packet processing rule 4, and sends a modified IP packet 2 to the router 3.

[00144] After the gateway 2 receives the IP packet 2 from the router 2, because the IP packet 2 is from the router 2, the gateway 2 determines that the IP packet 2 is an outbound packet, matches the packet processing rule 4 based on the source IP address of the IP packet 2, modifies the source IP address of the IP packet 2 from 192.168.0.2 to 10.0.0.10, and sends a modified IP packet 2 to the router 3.

[00145] Step 13: The router 3 forwards the IP packet 2 to the gateway 1 according to a routing rule 6.

[00146] After receiving the IP packet 2, the router 3 matches the routing rule 6 based on the destination IP address (10.0.0.9) of the IP packet 2, and forwards the IP packet 2 to the gateway 1.

[00147] Step 14: The gateway 1 modifies the destination IP address of the IP packet 2 according to a packet processing rule 2, and sends a modified IP packet 2 to the router 1.

[00148] After the gateway 1 receives the IP packet 2 from the router 3, because the IP packet 2 is from the router 3, the gateway 1 determines that the IP packet 2 is an inbound packet, matches the packet processing rule 2 based on the destination address of the IP packet 2, modifies the destination IP address of the IP packet 2 from 10.0.0.9 to 192.168.0.2, and sends a modified IP packet 2 to the router 1.

[00149] Step 15: The router 1 forwards the modified IP packet 2 to the switch 1 according to a routing rule 2.

[00150] The router 1 matches the routing rule 2 based on the destination IP address 192.168.0.2 of the IP packet 2, and sends the IP packet 2 to the subnet 1. The switch 1 is disposed in the subnet 1, to be specific, the switch 1 that sends the IP packet 2 to the switch 1 in the subnet 1.

[00151] Step 16: The switch 1 sends the IP packet 2 to the VM 1.

[00152] The switch 1 sends the IP packet 2 to the VM 1 based on the destination IP address 192.168.0.2 of the IP packet 2.

[00153] After receiving the IP packet 2, the VM 1 determines that the IP packet 2 is the reply packet of the IP packet 1 based on the source IP address 10.0.0.10 and the destination IP address 192.168.0.2 of the IP packet 2 (because the source IP address and the destination IP address of the IP packet 2 are inverted compared with those of the IP packet 1). The VM 1 obtains the reply information from the data part of the IP packet 2 to complete a communication process between the VM 1 and the VM 2.

[00154] To sum up, the gateway 1, the gateway 2 and a VPC 3 are configured in a cloud data center 10, and the routers of a VPC 1, the VPC 2, and the VPC 3, and the gateway 1 and the gateway 2 are configured, so that the VM 1 and the VM 3 can communicate with each other when the VM 1 and the VM 3 have the same private network address.

[00155] For example, this embodiment of the present invention is applicable to the following scenario: The VPC 3 is used as a large internal network of an enterprise, and the VPC 1 and the VPC 2 are used as small internal networks of the enterprise. For example, the VPC 1 is a virtual network of a finance department, the VPC 2 is a virtual network of a research and development department, and the VPC 3 is a virtual network of an IT management department of the enterprise. When private network addresses of the VPC 1 and the VPC 2 overlap with each other, a private network address of the VPC 3 may be applied for from the control platform 6. For example, the VPC 1 applies for a private network address 1 of the VPC 3, and the VPC 2 applies for a private network address 2 of the VPC 3. A virtual machine in the VPC 1 is bound with the private network address 1 by using a gateway, and a virtual machine in the VPC 2 is bound with the private network address 2 by using a gateway. The virtual machine in the VPC 1 can access the virtual machine in the VPC 2 by accessing the private network address 2, and the virtual machine in the VPC 2 can access the virtual machine in the VPC 1 by accessing the private network address 1. In this way, a

technical problem that different VPCs of the enterprise cannot communicate with each other due to overlapping private network addresses is resolved.

[00156] It should be noted that the VPC 1, the VPC 2, and the VPC 3 may belong to different users, and the different users log in to their VPCs by using their own accounts. When the VPC 1 needs to connect to the VPC 3, a user of the VPC 1 may enter an account of a user of the VPC 3 on the control platform. The control platform sends a request to a settings interface of the VPC 3 based on the account of the user of the VPC 3, and the user of the VPC 3 can confirm whether to accept the request on the settings interface of the VPC 3. If the request is accepted, the control platform establishes a connection between the VPC 1 and the VPC 3. The VPC 2 and the VPC 3 are connected in a similar way.

[00157] In another embodiment, when the VPC 1, the VPC 2, and the VPC 3 belong to a same user, the user may log in to the VPC 1, the VPC 2, and the VPC 3 by using one account. In this case, the control platform does not need to send a request.

[00158] The user can register an account on the control platform and use the account to purchase a VPC on a payment page provided by the control platform.

[00159] Referring to FIG. 7A and FIG. 7B, FIG. 7A and FIG. 7B show another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention. In this embodiment, with respect to the embodiment shown in FIG. 2, a gateway 1 may also be bound with a VM in another subnet of the VPC 1, and a gateway 2 may also be bound with a VM in another subnet of the VPC 2. As shown in FIG. 7A and FIG. 7B, a subnet 3 (192.168.1.0/24) is further configured in the VPC 1, and a VM 5 is configured in the subnet 3. A private network address of the VM 5 is 192.168.1.2. A subnet 4 (192.168.1.0/24) is further configured in the VPC 2, and a VM 6 is configured in the subnet 4. A private network address of the VM 6 is 192.168.1.2.

[00160] In this case, if the VM 5 needs to communicate with the VM 6, a routing rule 7 may be configured for a router 1: A packet whose destination IP address belongs to 192.168.1.0/24 is forwarded to the subnet 3; a routing rule 8 is added to a router 2: The packet whose destination IP address belongs to 192.168.1.0/24 is forwarded to the subnet 4, and a private network address (for example, 10.0.0.11) of a VPC 3 is allocated to the gateway 1; a packet processing rule 5 is set for the gateway 1: When a source IP address of an outbound packet is 192.168.1.2, the source IP address is modified to 10.0.0.11. A packet processing rule 6 is set for the gateway 1: When a

destination IP address of an inbound packet is 10.0.0.11, the destination IP address is modified to 192.168.1.2.

[00161] A private network address (for example, 10.0.0.12) of the VPC 3 is allocated to the gateway 2, and a packet processing rule 7 is set for the gateway 2: When the source IP address of the outbound packet is 192.168.1.2, the source IP address of the outbound packet is modified to 10.0.0.12, and a modified outbound packet is sent to a router 3. A packet processing rule 8 is set for the gateway 2: When the destination IP address of the inbound packet is 10.0.0.12, the destination IP address of the inbound packet is modified to 192.168.1.2.

[00162] A routing rule 9 is set for the router 3: When a destination IP address of a packet is 10.0.0.12, the packet is sent to the gateway 2. A routing rule 10 is set for the router 3: When a destination IP address of a packet is 10.0.0.11, the packet is sent to the gateway 1.

[00163] Based on the foregoing configuration, the VM 5 may construct an IP packet whose source IP address is 192.168.1.2 and whose destination IP address is 10.0.0.12, and send the IP packet to the VM 6 in a communication manner similar to that in the foregoing embodiments by using the router 1, the gateway 1, the router 3, the gateway 2, and the router 2. In addition, an IP packet that is returned by the VM 6 and that is used for reply may also be sent to the VM 1 by using the router 2, the gateway 2, the router 3, the gateway 1, and the router 1.

[00164] Therefore, in this embodiment of the present invention, different rules are set for the gateways and the routers, so that different subnets that are in the VPC 1 and the VPC 2 and that have a same private network address segment can communicate with each other.

[00165] Further, the embodiments of the present invention may also implement communication between data centers on premise when private network addresses overlap with each other. Referring to FIG. 8A to FIG. 8C, FIG. 8A to FIG. 8C show another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention.

In FIG. 8A to FIG. 8C, a data center on premise 21 and a data center on premise 22 are added based on the embodiment shown in FIG. 3A and FIG. 3B. The data center on premise 21 includes a subnet 5, and a physical machine (Physical machine, PM) 1 and a PM 2 are disposed in the subnet 5. The data center on premise 22 includes a subnet 6, and a physical machine (Physical machine, PM) 3 and a PM 4 are disposed in the subnet 6. The subnet 5 accesses a remote connection gateway 1 in a VPC 1 by using a remote connection gateway 3, and the subnet 6 accesses a remote connection gateway 2 in a VPC 2 by using a remote connection gateway 4. A remote

communication tunnel is formed between the remote connection gateway 3 and the remote connection gateway 1, and a remote communication tunnel is formed between the remote connection gateway 4 and the remote connection gateway 2. An IP packet may be transmitted in the remote communication tunnel, and the IP packet remains unchanged in a transmission process.

5 **[00166]** It should be noted that the remote connection gateway 1 in the VPC 1 and the remote connection gateway 2 in the VPC 2 may be configured by a control platform 6 based on configuration information, and the configuration information is entered by a user to the control platform 6 by using a client 7.

10 **[00167]** For example, the remote communication gateway may be a virtual private network (Virtual private network, VPN) gateway or a manual gateway.

15 **[00168]** As shown in FIG. 8, a private network address of the subnet 5 overlaps with a private network address of the subnet 6, the PM 1 needs to communicate with the PM 3, a routing rule 11 may be added to a router 1: A packet whose destination IP address belongs to 192.168.2.0/24 is forwarded to the remote connection gateway 1; a routing rule 12 is added to a router 2: The packet
20 whose destination IP address belongs to 192.168.2.0/24 is forwarded to the remote connection gateway 2, and a private network address (for example, 10.0.0.13) of a VPC 3 is allocated to a gateway 1; a packet processing rule 9 is set for the gateway 1: When a source IP address of an outbound packet is 192.168.2.2, the source IP address is modified to 10.0.0.13; a packet processing rule 10 is set for the gateway 1: When a destination IP address of an inbound packet is 10.0.0.13,
25 the destination IP address is modified to 192.168.2.2.

30 **[00169]** A private network address (for example, 10.0.0.14) of the VPC 3 is allocated to a gateway 2, a packet processing rule 11 is set for the gateway 2: When the source IP address of the outbound packet is 192.168.2.2, the source IP address is modified to 10.0.0.14, and a modified outbound packet is sent to a router 3. A packet processing rule 12 is set for the gateway 2: When
the destination IP address of the inbound packet is 10.0.0.14, the destination IP address is modified to 192.168.2.2, and a modified inbound packet is sent to the router 2.

[00170] A routing rule 13 is set for the router 3: When a destination IP address of a packet is 10.0.0.14, the packet is sent to the gateway 2. A routing rule 14 is set for the router 3: When a destination IP address of a packet is 10.0.0.13, the packet is sent to the gateway 1.

30 **[00171]** Based on the foregoing configuration, the PM 1 may construct an IP packet whose source IP address is 192.168.2.2 and whose destination IP address is 10.0.0.14. The packet is

forwarded by a switch 5 to the remote connection gateway 3, is sent to the remote connection gateway 1 by using the remote communication tunnel, and is sent by the remote connection gateway 1 to the router 1. Then, the IP packet is sent to the remote connection gateway 2 by using the router 1, the gateway 1, the router 3, the gateway 2, and the router 2 in a communication manner similar to that in the foregoing embodiments, and is sent to the remote connection gateway 4 by using the remote communication tunnel, to arrive at the PM 3 in the subnet 6. Similarly, an IP packet that is returned by the PM 3 and that is used for reply may also be sent to the PM 1.

[00172] It should be noted that a PM in a data center on premise may alternatively be replaced by a VM. This is not limited in this embodiment of the present invention.

[00173] Therefore, in another embodiment of the present invention, different rules are set for the gateways and the routers, so that different subnets in a data center on premise that have a same private network address segment can communicate with each other by using the data center on premise.

[00174] Referring to FIG. 9A and FIG. 9B, FIG. 9A and FIG. 9B are another schematic diagram of a system structure of a VPC communications system according to an embodiment of the present invention. Compared with the embodiment shown in FIG. 3A and FIG. 3B, in this embodiment, a gateway 1 is disposed in a subnet 1, and a gateway 2 is disposed in a subnet 2. In this case, the gateway 1 and the gateway 2 can support only communication with the subnet 1 and the subnet 2.

[00175] Specifically, a control platform 6 may allocate a private network address 10.0.0.9 of a private network address segment of the VPC 3 (for example, 10.0.0.0/24) to the gateway 1 based on configuration information, and allocate another private network address 10.0.0.10 of the private network address segment of the VPC 3 (for example, 10.0.0.0/24) to the gateway 2. In addition, a router 1 is configured to connect to a router 3, and a router 2 is configured to connect to the router 3.

[00176] A router 1 is provided with:

a routing rule 1': When a destination IP address of a packet received by the router 1 is 10.0.0.10, the router 1 forwards the packet to the VPC 3; and

a routing rule 2': When the destination IP address of the packet received by the router 1 is 10.0.0.9, the router 1 forwards the packet to the gateway 1.

[00177] The gateway 1 is provided with:

a packet processing rule 1': When a source IP address of an outbound packet received

by the gateway 1 is a private network address 192.168.0.2 of a VM 1 in the subnet 1, the gateway 1 converts 192.168.0.2 into the private network address 10.0.0.9 of the gateway 1 in the VPC 3, and sends a modified outbound packet to the router 1; and

5 a packet processing rule 2': When a destination IP address of an inbound packet received by the gateway 1 is the private network address 10.0.0.9 of the gateway 1 of the VPC 3, the gateway 1 converts 10.0.0.9 into the private network address 192.168.0.2 of the VM 1 in the subnet 1, and sends a modified inbound packet to the gateway 1.

[00178] The outbound packet is a packet received by the gateway 1 from a switch 1, and the inbound packet is a packet received by the gateway 1 from the router 1.

10 **[00179]** The router 2 is provided with:

a routing rule 5': When a destination IP address of a packet received by the router 2 is 10.0.0.9, the router 2 forwards the packet to the VPC 3.

a routing rule 6': When the destination IP address of the packet received by the router 2 is 10.0.0.10, the router 2 forwards the packet to the gateway 2.

15 **[00180]** The gateway 2 is provided with:

a packet processing rule 3': When a destination IP address of an inbound packet received by the gateway 2 is 10.0.0.10, the gateway 2 converts 10.0.0.10 into 192.168.0.2, and sends a modified inbound packet to the router 2; and

20 a packet processing rule 4': When a source IP address of an outbound packet received by the gateway 2 is 192.168.0.2, the gateway 2 converts 192.168.0.2 into 10.0.0.10, and sends a modified outbound packet to the router 1.

[00181] The outbound packet is a packet received by the gateway 2 from a switch 2, and the inbound packet is a packet received by the gateway 1 from the router 2.

[00182] A router 3 is provided with:

25 a routing rule 3': When a destination IP address of a packet received by the router 3 is 10.0.0.10, the router 2 forwards the packet to the router 2.

a routing rule 4': When the destination IP address of the packet received by the router 2 is 10.0.0.9, the router 2 forwards the packet to the router 1.

[00183] When the VM 1 needs to access a VM 3 across VPCs, the VM 1 constructs an IP packet 1'. A source IP address of the IP packet 1' is the private network address 192.168.0.2 of the VM 1 in the subnet 1, and a destination IP address of the IP packet 1' is the private network address

30

10.0.0.10 of the gateway 2 in a subnet 3. A data part of the IP packet 1' carries request information.

[00184] The VM 1 sends the IP packet 1' to the switch 1. The switch 1 determines that the destination IP address of the IP packet 1' does not belong to the subnet 1, and sends the IP packet 1' to the gateway 1. The gateway 1 matches the packet processing rule 1' for the IP packet 1',
5 converts the source IP address of the IP packet 1 from 192.168.0.2 to 10.0.0.9, and sends a modified IP packet 1' to the router 1. The router 1 matches the routing rule 2' for the IP packet 1', and forwards the IP packet 1' to the router 3 of the VPC 3.

[00185] The router 3 receives the IP packet 1', matches the routing rule 3 for the IP packet 1', and forwards the IP packet 1' to the router 2 of a VPC 2.

10 **[00186]** The router 2 receives the IP packet 1', matches the routing rule 6 for the IP packet 1', and forwards the IP packet 1' to the gateway 2.

[00187] The gateway 2 receives the IP packet 1', matches the packet processing rule 3' for the IP packet 1', converts the destination IP address of the IP packet 1' from 10.0.0.10 to 192.168.0.2, and sends the IP packet 1' to the switch 2. The switch 2 sends the IP packet 1' to the VM 3.

15 **[00188]** The VM 3 generates reply information based on the request information carried in the data part of the IP packet 1', and constructs an IP packet 2'. The IP packet 2' is a reply packet of the IP packet 1', a source IP address of the IP packet 2' is the destination IP address 192.168.0.2 of the IP packet 1', and a destination IP address of the IP packet 2' is the source IP address 10.0.0.9 of the IP packet 1'. A data part of the IP packet 2' carries reply information.

20 **[00189]** The VM 3 sends the IP packet 2' to the switch 2. The switch 2 determines that the destination IP address of the IP packet 2' does not belong to the subnet 2, and sends the IP packet 2' to the gateway 2.

[00190] The gateway 2 matches the packet processing rule 4' for the IP packet 2', converts the source IP address of the IP packet 2' from 192.168.0.2 to 10.0.0.10, and sends the IP packet 2' to
25 the router 2.

[00191] The router 2 matches the routing rule 5' for the IP packet 2', and forwards the IP packet 2' to the router 3 of the VPC 3.

[00192] The router 3 receives the IP packet 2', matches the routing rule 4' for the IP packet 2', and forwards the IP packet 2' to the router 1 of a VPC 1.

30 **[00193]** The router 1 receives the IP packet 2', matches the routing rule 2' for the IP packet 2', and forwards the IP packet 2' to the gateway 1.

[00194] The gateway 1 receives the IP packet 2', matches the packet processing rule 2' for the IP packet 2', converts the destination IP address of the IP packet 2' from 10.0.0.9 to 192.168.0.2, and sends the IP packet 2' to the switch 1. The switch 1 sends the IP packet 2 to the VM 1.

[00195] The VM 1 obtains the reply information carried in the IP packet 2'. For the VM 1, the IP packet 6 is from 10.0.0.10, and the IP packet 6 is the reply packet of the IP packet 1'.

[00196] In conclusion, in this embodiment, although the VM 1 and a VM 2 have the same private network address, the VM 1 and the VM 2 can access each other through bridging of the VPC 3.

[00197] Further, referring to FIG. 10, FIG. 10 is a schematic structural diagram of a configuration apparatus according to an embodiment of the present invention. As shown in FIG. 10, a configuration apparatus 60 includes a first configuration module 601 and a second configuration module 602. The first configuration module 601 is configured to perform an action of creating a gateway in the foregoing embodiment, and the second configuration module 602 is configured to perform an action of setting rules for the gateways and routers in the foregoing embodiment.

[00198] The configuration apparatus 60 may be disposed on a control platform 6.

[00199] Referring to FIG. 11, FIG. 11 is a schematic structural diagram of a computing device according to an embodiment of the present invention. As shown in FIG. 11, the computing device may include a processing unit 421 and a communications interface 422. The processing unit 421 is configured to implement functions defined by an operating system running on a physical server and various software programs, for example, to implement a function of the control platform 6. The communications interface 422 is configured to communicate and interact with another computing node. Another device may be another physical server. Specifically, the communications interface 422 may be a network adapter. Optionally, the physical server may further include an input/output interface 423. The input/output interface 423 is connected to an input/output device, to receive input information and output an operation result. The input/output interface 423 may be a mouse, a keyboard, a display, a CD-ROM drive, or the like. Optionally, the physical server may further include a secondary memory 424. The secondary memory 424 is generally referred to as an external memory. A storage medium of the secondary memory 424 may be a magnetic medium (for example, a floppy disk, a hard disk, or a magnetic tape), an optical medium (for example, an optical disc), a semiconductor medium (for example, a solid-state drive), or the like. The

processing unit 421 may have a plurality of specific implementation forms. For example, the processing unit 421 may include a processor 4212 and a memory 4211. The processor 4212 performs related operations of the control platform 6 in the foregoing embodiments based on a program instruction stored in the memory 4211. The processor 4212 may be a central processing unit (CPU) or a graphics processing unit (English: graphics processing unit, GPU). The processor 4212 may be a single-core processor or a multi-core processor. The processing unit 421 may alternatively be independently implemented by using a logic device with built-in processing logic, for example, a field programmable gate array (English full name: Field Programmable Gate Array, FPGA for short) or a digital signal processor (English: digital signal processor, DSP).

[00200] It may be clearly understood by a person skilled in the art that, for a convenient and brief description, for a detailed working process of the foregoing system, apparatus, and unit, refer to a corresponding process in the foregoing method embodiments, and details are not described herein again.

[00201] Further, in another embodiment of the present invention, a container may alternatively be used to replace a virtual machine. This is not limited in this embodiment of the present invention.

[00202] An embodiment of the present invention further provides a computer program product for implementing a function of the foregoing control platform. The computer program product includes a computer-readable storage medium that stores program code, and an instruction included in the program code is used to perform the method procedure described in any one of the foregoing method embodiments. A person of ordinary skill in the art may understand that the foregoing storage medium may include any non-transitory (non-transitory) machine-readable medium capable of storing program code, such as a USB flash drive, a removable hard disk, a magnetic disk, an optical disc, a random access memory (Random-Access Memory, RAM), a solid-state disk (Solid State Disk, SSD), or a non-volatile memory (non-volatile memory).

[00203] It should be noted that any apparatus embodiment described above is merely an example. The units described as separate parts may or may not be physically separate, and parts displayed as units may or may not be physical units, that is, may be located in one place, or may be distributed onto a plurality of network units. Some or all of the processes may be selected based on an actual requirement to achieve an objective of solutions of the embodiments. In addition, in the accompanying drawings of the apparatus embodiments provided by the present invention, connection relationships between processes indicate that there are communication connections

between the processes, which may be specifically implemented as one or more communications buses or signal cables. A person of ordinary skill in the art may understand and implement the embodiments of the present invention without creative efforts.

[00204] Based on the description of the foregoing implementations, a person skilled in the art may clearly understand that the present invention may be implemented by software in addition to necessary universal hardware, or by dedicated hardware, including a dedicated integrated circuit, a dedicated CPU, a dedicated memory, a dedicated component, and the like. Generally, any function that can be implemented by a computer program can be easily implemented by corresponding hardware. Moreover, a specific hardware structure used to implement a same function may be in various forms, for example, in a form of an analog circuit, a digital circuit, a dedicated circuit, or the like. However, for the present invention, software program implementation is a better implementation in most cases. Based on such an understanding, technical solutions of the present invention essentially or the part contributing to the conventional technology may be implemented in a form of a software product. The software product is stored in a readable storage medium, such as a floppy disk of a computer, a USB flash drive, a removable hard disk, a read-only memory (Read-Only Memory, ROM), a random access memory (Random Access Memory, RAM), a magnetic disk, or an optical disc, and includes several instructions for instructing a computer device (which may be a personal computer, a host, a network device, and the like) to perform the methods described in the embodiments of the present invention.

[00205] It may be clearly understood by a person skilled in the art that, for the detailed working process of the foregoing system, apparatus, and unit, refer to the corresponding process in the foregoing method embodiments, and details are not described herein again.

[00206] The foregoing descriptions are merely specific implementations of the present invention, but are not intended to limit the protection scope of the present invention. Any variation or replacement readily figured out by the person skilled in the art within the technical scope disclosed in the present invention shall fall within the protection scope of the present invention. Therefore, the protection scope of the present invention shall be subject to the protection scope of the claims.

CLAIMS

What is claimed is:

1. A method for configuring virtual private cloud VPC communication, wherein a first VPC and a second VPC that have a same private network address segment communicate with each other
5 by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; and the method comprises:

binding a private network address in the first VPC with a first address, wherein the first address is an address that belongs to the private network address segment of the third VPC;

10 binding a private network address in the second VPC with a second address, wherein the second address is an address that belongs to the private network address segment of the third VPC, and the first address is different from the second address; and

configuring a source address of a packet sent by the first VPC to the second VPC, as the first address, and configuring a destination address of the packet sent by the first VPC to the second
15 VPC, as the second address.

2. The method according to claim 1, further comprising:

configuring a routing rule on the third VPC, wherein the routing rule on the third VPC comprises: forwarding a packet whose destination address is the first address to the first VPC, and forwarding a packet whose destination address is the second address to the second VPC.

20 3. The method according to claim 1 or 2, further comprising:

configuring a first gateway on the first VPC, and configuring a second gateway on the second VPC, wherein a private network address of the first gateway is configured as the first address, and a private network address of the second gateway is configured as the second address;

the binding a private network address in the first VPC with a first address comprises:
25 configuring a first packet processing rule on the first gateway, wherein the first packet processing rule comprises: converting a source address of an outbound packet from the address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and

the binding a private network address in the second VPC with a second address comprises:
30 configuring a second packet processing rule on the second gateway, wherein the second packet

processing rule comprises: converting a source address of the outbound packet from the address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC.

4. The method according to claim 3, further comprising:

5 configuring a routing rule on a router of the first VPC, wherein the routing rule on the router of the first VPC comprises: forwarding the packet whose destination address is the second address to the first gateway, and forwarding a packet whose destination address is the address in the first VPC to a subnet of the first VPC; and

10 configuring a routing rule on a router of the second VPC, wherein the routing rule on the router of the second VPC comprises: forwarding the packet whose destination address is the first address to the second gateway, and forwarding a packet whose destination address is the address in the second VPC to the subnet of the first VPC.

5. A method for configuring virtual private cloud VPC communication, wherein a first VPC and a second VPC that have a same private network address segment communicate with each other
15 by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; and the method comprises:

20 configuring a first gateway on the first VPC, and configuring a second gateway on the second VPC, wherein a first address is configured for the first gateway, a second address is configured for the second gateway, the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address;

25 configuring a first packet processing rule on the first gateway, and configuring a second packet processing rule on the second gateway, wherein the first packet processing rule comprises: converting a source address of an outbound packet from an address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and the second packet processing rule comprises: converting a source address of the outbound packet from an address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC; and

30 configuring a first routing rule on a router of the first VPC, configuring a second routing rule on a router of the second VPC, and configuring a third routing rule on a router of the third VPC,

wherein the first routing rule comprises: routing a packet whose destination address is the second address to the first gateway; the second routing rule comprises: routing a packet whose destination address is the first address to the second gateway; and the third routing rule comprises: routing the packet whose destination address is the first address to the first gateway in the first VPC, and
5 routing the packet whose destination address is the second address to the second gateway in the second VPC.

6. The method according to claim 5, further comprising: configuring a connection relationship between the first VPC and the third VPC, and configuring a connection relationship between the second VPC and the third VPC.

10 7. A virtual private cloud VPC communication method, wherein a first VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; and the method comprises:

15 sending, by the first VPC, a packet, wherein a source address of the packet is a first address, a destination address of the packet is a second address, both the first address and the second address are addresses that belong to the private network address segment of the third VPC, a private network address in the first VPC is bound with the first address, and a private network address in the second VPC is bound with the second address; and

20 receiving, by the third VPC, the packet, and forwarding the packet to the second VPC according to a preset routing rule, wherein a routing rule of the third VPC comprises: forwarding a packet whose destination address is the second address to the second VPC.

8. The method according to claim 7, wherein the routing rule further comprises: forwarding a packet whose destination address is the first address to the first VPC; and

25 the method further comprises:

sending, by the second VPC, a response packet, wherein a source address of the response packet is the second address, and a destination address of the response packet is the first address; and

receiving, by the third VPC, the response packet, and forwarding the response packet to the
30 first VPC according to the routing rule.

9. A virtual private cloud VPC communication method, wherein a first VPC communicates

with a second VPC by using a third VPC, the first VPC and the second VPC have a same private network address segment, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; a first gateway is configured on the first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway; both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address; and the method comprises:

receiving, by a router of the first VPC, a packet sent by a first device, wherein a source address of the packet is a private network address of the first device, and a destination address of the packet is the second address;

forwarding, by the router of the first VPC, the packet to the first gateway according to a first routing rule; and

modifying, by the first gateway, the source address of the packet to the first address, and forwarding a modified packet to a router of the third VPC, wherein a third routing rule is configured on the router of the third VPC, the first routing rule is that a packet whose destination address belongs to the private network address segment of the third VPC needs to be forwarded to the first gateway, and the third routing rule is that a packet whose destination address is the second address needs to be forwarded to the second gateway in the second VPC.

10. The method according to claim 9, further comprising:

receiving, by the second gateway, a packet forwarded by the router of the third VPC, modifying a destination address of the received packet to an address of a second device, and sending a modified packet to a router of the second VPC; and

forwarding, by the router of the second VPC according to a second routing rule, the received packet to a subnet in which the second device is located, wherein the second routing rule is that the packet whose destination address is the second address needs to be forwarded to the subnet in which the second device is located.

11. A virtual private cloud VPC communication configuration apparatus, wherein a first virtual private cloud VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private

network address segment of the second VPC; and the apparatus comprises:

a first configuration module, configured to: bind a private network address in the first VPC with a first address, wherein the first address is an address that belongs to the private network address segment of the third VPC; and bind a private network address in the second VPC with a second address, wherein the second address is an address that belongs to the private network address segment of the third VPC, and the first address is different from the second address; and

a second configuration module, configured to: configure a source address of a packet sent by the first VPC to the second VPC, as the first address; configure a destination address of the packet sent by the first VPC to the second VPC, as the second address; configure a source address of a packet sent by the second VPC to the first VPC, as the second address; and configure a destination address of the packet sent by the second VPC to the first VPC, as the first address.

12. The apparatus according to claim 11, wherein

the second configuration module is configured to configure a routing rule on the third VPC, wherein the routing rule on the third VPC comprises: forwarding a packet whose destination address is the first address to the first VPC, and forwarding a packet whose destination address is the second address to the second VPC.

13. The apparatus according to claim 11 or 12, wherein the second configuration module is configured to:

configure a first gateway on the first VPC, and configure a second gateway on the second VPC, wherein a private network address of the first gateway is configured as the first address, and a private network address of the second gateway is configured as the second address;

configure a first packet processing rule on the first gateway, wherein the first packet processing rule comprises: converting a source address of an outbound packet from the address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and

configure a second packet processing rule on the second gateway, wherein the second packet processing rule comprises: converting a source address of the outbound packet from the address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC.

14. The apparatus according to claim 13, wherein the second configuration module is further configured to:

configure a routing rule on a router of the first VPC, wherein the routing rule on the router of the first VPC comprises: forwarding the packet whose destination address is the second address to the first gateway, and forwarding a packet whose destination address is the address in the first VPC to a subnet in which the address in the first VPC is located; and

5 configure a routing rule on a router of the second VPC, wherein the routing rule on the router of the second VPC comprises: forwarding the packet whose destination address is the first address to the second gateway, and forwarding a packet whose destination address is the address in the second VPC to the subnet in which the address in the first VPC is located.

15. A virtual private cloud VPC communication configuration apparatus, wherein a first VPC
10 and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; and the apparatus comprises:

a first configuration module, configured to: configure a first gateway on the first VPC;
15 configure a second gateway on the second VPC; configure a first address for the first gateway; configure a second address for the second gateway, wherein the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address; configure a first packet processing rule on the first gateway; and configure a second packet processing rule on the second gateway, wherein the first packet
20 processing rule comprises: converting a source address of an outbound packet from an address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and the second packet processing rule comprises: converting a source address of the outbound packet from an address in the second VPC into the second address, and converting a destination address of the inbound packet from the second
25 address into the address in the second VPC; and

a second configuration module, configured to: configure a first routing rule on a router of the first VPC, configure a second routing rule on a router of the second VPC, and configure a third routing rule on a router of the third VPC, wherein the first routing rule comprises: routing a packet whose destination address is the second address to the first gateway; the second routing rule
30 comprises: routing a packet whose destination address is the first address to the second gateway; and the third routing rule comprises: routing the packet whose destination address is the first

address to the first gateway in the first VPC, and routing the packet whose destination address is the second address to the second gateway in the second VPC.

16. The apparatus according to claim 15, wherein

the second configuration module is further configured to configure a connection relationship
5 between the first VPC and the third VPC, and configure a connection relationship between the second VPC and the third VPC.

17. A virtual private cloud VPC communications system, comprising a first VPC, a second VPC, and a third VPC, wherein the first VPC and the second VPC have a same private network address segment, the first VPC and the second VPC communicate with each other by using the
10 third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC;

the first VPC is configured to send a packet, wherein a source address of the packet is a first address, a destination address of the packet is a second address, both the first address and the
15 second address are addresses that belong to the private network address segment of the third VPC, a private network address in the first VPC is bound with the first address, and a private network address in the second VPC is bound with the second address; and

the third VPC is configured to: receive the packet, and forward the packet to the second VPC according to a preset routing rule, wherein a routing rule of the third VPC comprises: forwarding
20 a packet whose destination address is the second address to the second VPC.

18. The system according to claim 17, wherein the routing rule further comprises: forwarding a packet whose destination address is the first address to the first VPC;

the second VPC is further configured to send a response packet, wherein a source address of the response packet is the second address, and a destination address of the response packet is the
25 first address; and

the third VPC is further configured to: receive the response packet, and forward the response packet to the first VPC according to the routing rule.

19. A virtual private cloud VPC communications system, comprising a first VPC, a second VPC, and a third VPC, wherein the first VPC communicates with the second VPC by using the
30 third VPC, the first VPC and the second VPC have a same private network address segment, and a private network address segment of the third VPC is different from the private network address

segment of the first VPC and the private network address segment of the second VPC; a first gateway is configured on the first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway; and both the first address and the second address belong to the private network address
5 segment of the third VPC, and the first address is different from the second address, wherein

a router of the first VPC is configured to receive a packet sent by a first device, wherein a source address of the packet is a private network address of the first device, and a destination address of the packet is the second address;

the router of the first VPC is further configured to forward the packet to the first gateway
10 according to a first routing rule; and

the first gateway is configured to: modify the source address of the packet to the first address, and forward a modified packet to a router of the third VPC, wherein a third routing rule is configured on the router of the third VPC, the first routing rule is that a packet whose destination address belongs to the private network address segment of the third VPC needs to be forwarded to
15 the first gateway, and the third routing rule is that a packet whose destination address is the second address needs to be forwarded to the second gateway in the second VPC.

20. The system according to claim 19, wherein

the second gateway is configured to: receive a packet forwarded by the router of the third VPC, modify a destination address of the received packet to an address of a second device, and
20 send a modified packet to a router of the second VPC; and

the router of the second VPC is configured to forward, according to a second routing rule, the received packet to a subnet in which the second device is located, where the second routing rule is that the packet whose destination address belongs to the second address needs to be forwarded to the subnet in which the second device is located.

25 21. A virtual private cloud VPC communications system, comprising a first VPC, a second VPC, and a third VPC, wherein the first VPC communicates with the second VPC by using the third VPC, the first VPC and the second VPC have a same private network address segment, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; a first
30 gateway connected to the third VPC is configured on the first VPC, a second gateway connected to the third VPC is configured on the second VPC, a first address is configured for the first gateway,

and a second address is configured for the second gateway; and both the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address, wherein

a first virtual machine in a first subnet of the first VPC is configured to send a packet to a switch of the first subnet, wherein a source address of the packet is a private network address of the first virtual machine in the first subnet, and a destination address of the packet is the second address;

the switch of the first subnet is configured to send the packet to a router of the first VPC;

the router of the first VPC is configured to: receive the packet, and forward the packet to the first gateway;

the first gateway is configured to: receive the packet, modify the destination address of the packet to the first address, and send a modified packet to a router of the third VPC;

the router of the third VPC is configured to: receive the packet, and forward the packet to the second gateway;

the second gateway is configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second virtual machine in a second subnet of the second VPC, in the second subnet, and send a modified packet to a router of the second VPC;

the router of the second VPC is configured to: receive the packet, and forward the packet to a switch of the second subnet; and

the switch of the second subnet is configured to: receive the packet, and forward the packet to the second virtual machine.

22. A virtual private cloud VPC communications system, comprising a first VPC, a second VPC, and a third VPC, wherein the first VPC communicates with the second VPC by using the third VPC, the first VPC and the second VPC have a same private network address segment, a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC, a first remote connection gateway remotely connected to a first data center on premise and a first gateway connected to the third VPC are configured on the first VPC, a second remote connection gateway remotely connected to a second data center on premise and a second gateway connected to the third VPC are configured on the second VPC, a first address is configured for the first gateway, a second address is configured for the second gateway, both the first address and the second address

belong to the private network address segment of the third VPC, and the first address is different from the second address, wherein

the first remote connection gateway is configured to: receive a packet sent by a first device in a first subnet of the first data center on premise, and send the packet to a router of the first VPC, wherein a source address of the packet is a private network address of the first device in the first subnet, and a destination address of the packet is the second address;

the router of the first VPC is configured to: receive the packet, and forward the packet to the first gateway;

the first gateway is configured to: receive the packet, modify the destination address of the packet to the first address, and send a modified packet to a router of the third VPC;

the router of the third VPC is configured to: receive the packet, and forward the packet to the second gateway;

the second gateway is configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second device in a second subnet of the second data center on premise, in the second subnet, and send a modified packet to a router of the second VPC;

the router of the second VPC is configured to: receive the packet, and forward the packet to the second remote connection gateway; and

the second remote connection gateway is configured to receive the packet, and send the packet to the second device in the second subnet of the second data center on premise.

23. A virtual private cloud VPC communications system, comprising a first VPC, a second VPC, and a third VPC, wherein the first VPC communicates with the second VPC by using the third VPC, the first VPC and the second VPC have a same private network address segment, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; a first gateway is configured on the first VPC, a second gateway is configured on the second VPC, a first address is configured for the first gateway, and a second address is configured for the second gateway; and both the first address and the second address belong to the private network address segment of the third VPC, a router of the first VPC and a router of the second VPC are separately connected to a router of the third VPC, and the first address is different from the second address, wherein

a first virtual machine in a first subnet of the first VPC is configured to send a packet to a switch of the first subnet, wherein a source address of the packet is a private network address of the first virtual machine in the first subnet, and a destination address of the packet is the second address;

5 the switch of the first subnet is configured to send the packet to the first gateway;

 the first gateway is configured to: modify the source address of the packet to the first address, and send a modified packet to the router of the first VPC;

 the router of the first VPC is configured to: receive the packet, and forward the packet to the router of the third VPC;

10 the router of the third VPC is configured to: receive the packet, and forward the packet to the router of the second VPC;

 the router of the second VPC is configured to: receive the packet, and forward the packet to the second gateway;

 the second gateway is configured to: receive the packet, modify the destination address of the received packet to a private network address, of a second virtual machine in a second subnet of the second VPC, in the second subnet, and send a modified packet to a switch of the second subnet; and

 the switch of the second subnet is configured to: receive the packet, and forward the packet to the second virtual machine.

20 24. A method for configuring virtual private cloud VPC communication, wherein a first VPC and a second VPC that have a same private network address segment communicate with each other by using a third VPC, and a private network address segment of the third VPC is different from the private network address segment of the first VPC and the private network address segment of the second VPC; and the method comprises:

25 providing a first configuration page to a user in the first VPC, wherein the first configuration page prompts the user in the first VPC to create a first gateway on the first VPC, and prompts the user in the first VPC to enter information about the third VPC to which the first gateway needs to be connected and a first address of the first gateway in the third VPC;

 providing a second configuration page to a user in the second VPC, wherein the second configuration page prompts the user in the second VPC to create a second gateway on the second VPC, and prompts the user in the second VPC to enter the information about the third VPC to

which the second gateway needs to be connected and a second address of the second gateway in the third VPC; and the first address and the second address belong to the private network address segment of the third VPC, and the first address is different from the second address;

creating the first gateway based on information about the first configuration page; and

5 creating the second gateway based on information about the second configuration page.

25. The method according to claim 24, further comprising:

configuring a first packet processing rule on the first gateway, and configuring a second packet processing rule on the second gateway, wherein the first packet processing rule comprises: converting a source address of an outbound packet from an address in the first VPC into the first address, and converting a destination address of an inbound packet from the first address into the address in the first VPC; and the second packet processing rule comprises: converting a source address of the outbound packet from an address in the second VPC into the second address, and converting a destination address of the inbound packet from the second address into the address in the second VPC; and

15 configuring a first routing rule on a router of the first VPC, configuring a second routing rule on a router of the second VPC, and configuring a third routing rule on a router of the third VPC, wherein the first routing rule comprises: routing a packet whose destination address is the second address to the first gateway; the second routing rule comprises: routing a packet whose destination address is the first address to the second gateway; and the third routing rule comprises: routing the packet whose destination address is the first address to the first gateway in the first VPC, and routing the packet whose destination address is the second address to the second gateway in the second VPC.

26. A computing device, comprising at least one memory and at least one processor, wherein the at least one memory is configured to store a program instruction, and the at least one processor executes the program instruction to perform the method according to any one of claims 1 to 4.

27. A computing device, comprising at least one memory and at least one processor, wherein the at least one memory is configured to store a program instruction, and the at least one processor executes the program instruction to perform the method according to any one of claims 5 to 8.