Cloud Connect Network

Product Introduction

Product Documentation

Contents

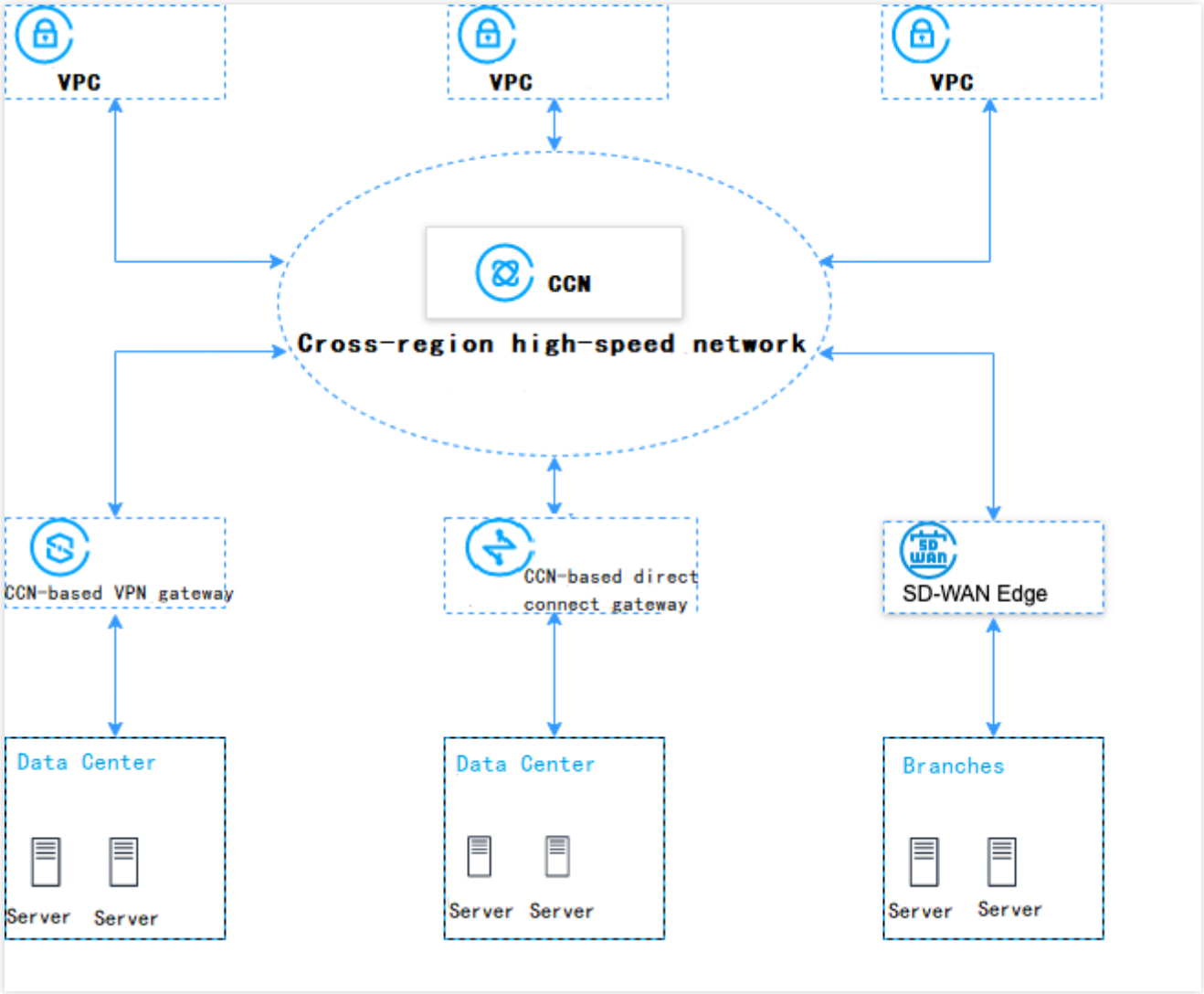
Product Introduction

Overview

Last updated：2024-01-10 14:41:59

What is Cloud Connect Network

Cloud Connect Network (CCN) can establish VPC–to-VPC connections and VPC-IDC connections. It provides you with public and private network multi-point interconnection, automatically synced routes, linkage prioritization, failure fast convergence, and other capabilities. With its presence in over 30 regions around the world, over 100 Gbps bandwidth and 99.99% high availability.



Product Components

Configuration of a CCN instance includes:
Associated network instances: Network instances added to the same CCN instance can communicate with each other. Supported resources include VPC, VPC (BM), direct connect gateways, and VPN gateways. For more information, see Associating Network Instances.
Note:
For CCN to automatically add the routes from the VPN gateway, the VPN gateway for CCN has the VPN tunnel created and SPD policy configured. For more information, see Connecting IDC to CCN Through VPN Gateway.
Route table: CCN automatically syncs routes of network instances added and presents them in its route table. For more information, see Viewing Routing Information.

Description

CCN has the following features:

Public and private network interconnection

CCN features multi-node multi-route-level automatic forwarding and syncing on the public and private network and route convergence in seconds, which allows you to interconnect all network instances with a simple step, and manage them easily.

Smart learning and scheduling

CCN frees you from the heavy route maintenance with its Full Mesh interconnection between multiple nodes and links in public and private networks. The smart scheduling system monitors the multi-layer network topology, routes, and traffic of the entire network to connect your local services to the nearest point and ensure interconnection using the shortest link.

Automatic route forwarding

CCN automatically syncs multi-level routes, and updates the routing table if your network topology changes. This simple management replaces your extra manual configuration or updates, which in turn, greatly improves the scalability and OPS efficiency of your network.

Feature Comparison

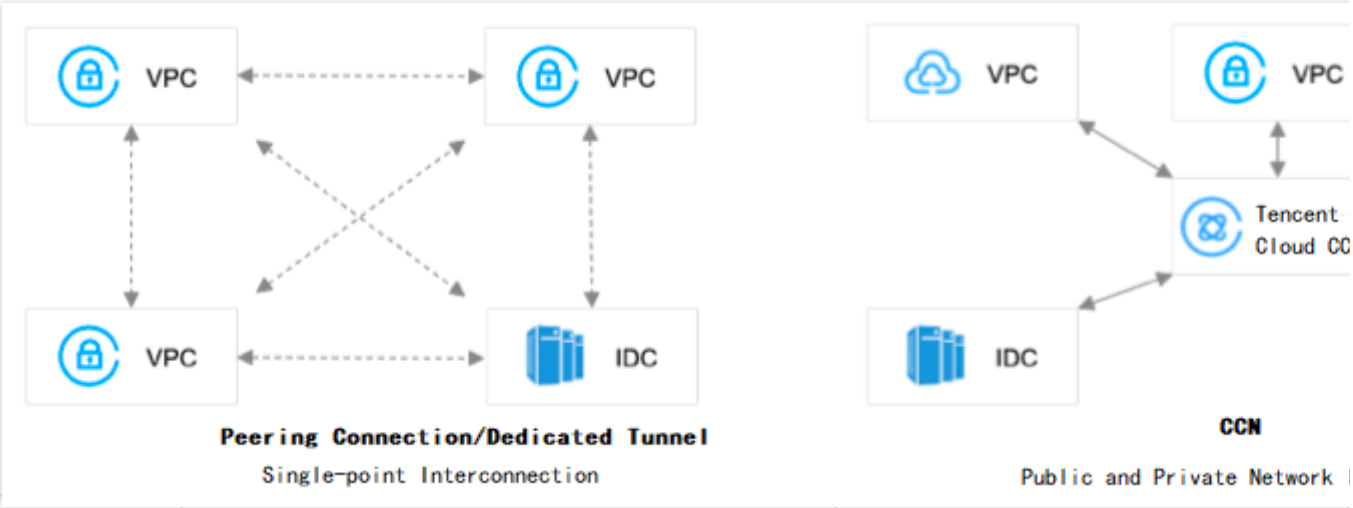
CCN vs. peering connection/dedicated tunnel

Without CCN, if you want to connect multiple VPCs with your cloud IDC, or connect to your cloud IDC via a direct connection, you need set up peering connections between each pair of VPC endpoints, and create dedicated channels and gateways between of each VPCs and the direct connection. At the same time, the VPC and IDC IP ranges cannot overlap. After establishing the connection, you must manage the route tables of instances and manually add routing policies to make it all work.

On the other hand, doing the same with CCN would only require a CCN instance and adding all VPCs and direct connect gateway to the CCN instance. Only one DC channel and gateway are required for one direct connection. CCN can automatically forward and sync all routes, saving you the hassle of manually configuring and managing the route tables of the instances.

Note:

For more information on how to migrate existing applications to CCN, see Best Practices.



CCN Benefit	Peering Connection/Dedicated Tunnel	CCN
Full-mesh links	1. To interconnect n VPCs, you need to establish Cn2 peering connections, where Cn2 equals to n * (n-1)/2. Namely, six peering connections are required for interconnecting four VPCs. 2. A single dedicated tunnel can only connect to one VPC. 3. Peer connections cannot be established between VPCs with overlapping IP ranges.	1. All instances added to the CCN instance are in a full mesh interconnection. 2. Each dedicated tunnel can communicate with all VPCs and IDCs. 3. CCN allows for network instances with overlapping CIDR blocks. This provides greater flexibility for interconnection.
Routing	1. Routes must be configured for every link. 2. Manual updates are required for any link change.	1. Routes are automatically learned and forwarded. 2. Route tables are dynamically updated without manual maintenance.

Stability and reliability	Multi-cluster disaster recovery in a single zone.	Multi-zone hot backup disaster recovery with 99.99% high availability.
Costs	1. Pay for each link separately. 2. Relatively higher unit price.	1. Pay for all bandwidth in a region as a whole (similar to bandwidth packages), which evens out the price. 2. Lower unit price.
Latency	Connections are established using lines randomly selected among multiple underlying lines. The latency difference can be 10 ms or more and the latency fluctuates.	Select the optimal line.

Strengths

Last updated：2024-01-10 14:41:59

Full-mesh

Tencent Cloud Connect Network (CCN) provides enterprise-level network services that support single-point access and full-mesh interconnection. CCN features multi-node multi-route-level automatic forwarding and syncing on the public and private network and route convergence in seconds, which allows you to interconnect all network instances with a simple step.

Smart scheduling

CCN frees you from the heavy route maintenance with its Full Mesh interconnection between multiple nodes and links in public and private networks. The smart scheduling system monitors the multi-layer network topology, routes, and traffic of the entire network to connect your local services to the nearest point and ensure interconnection using the shortest link.

Fast transmission

Tencent Cloud operates interconnected IDCs in more than 30 regions around the globe. Any two network instances associated with the CCN are interconnected via the shortest path on the private network. Therefore, there is no need to worry about bypassing public networks or possible link congestion. This greatly reduces the network latency for global multi-point interconnections to ensure high-speed data transmission.

Cost effective

CCN supports monthly 95th percentile billing on a pay-as-you-go basis.

Secure and reliable

Network is isolated and encrypted at multiple layers based on the MPLS-VPN technology, and user networks are isolated from each other.

Bandwidth monitoring and flexible adjustment

CCN provides single-region outbound bandwidth monitoring, speed limiting, and alarming features, helping you better manage businesses with various monitoring metrics. You can also adjust the bandwidth cap in each region at any time based on your business needs to control network connectivity easily.

Use Cases

Last updated：2024-01-10 14:41:59

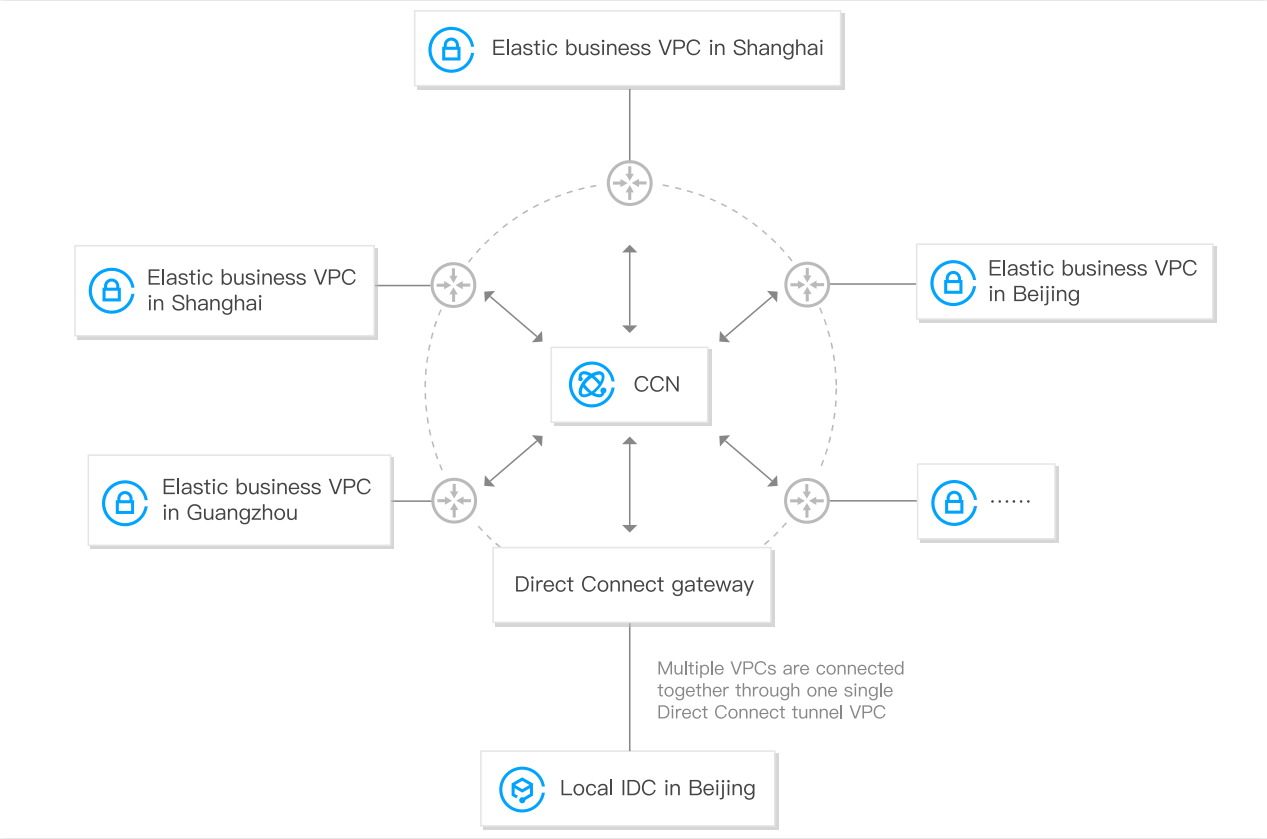
Use Case 1. Building a Hybrid Cloud

Background

You have deployed a business VPC and a disaster recovery VPC on Tencent Cloud, and own an on-premise IDC off the cloud. You want to implement resource interconnection between your VPCs and the on-premise IDC.

Solution

Launch a cloud-based environment on Tencent Cloud, and connect it to the local IDC using Direct Connect. In this way, data is stored on cloud for disaster recovery, and elastic services can be deployed locally and on-cloud, creating a hybrid cloud solution.
After creating a CCN instance, you only need to integrate the direct connect gateway connected with the IDC, elastic business VPC and backup data centers into the instance. You do not need to create multiple peering connections and Direct Connect tunnels. The routes are generated automatically, which greatly simplifies the configuration workload.
Outcomes:
Add VPCs to CCN to implement automatic routing, eliminating the need to create multiple peering connections.
Add a direct connect gateway to CCN and connect multiple VPCs through one dedicated tunnel, achieving interconnection between your on-premise and on-cloud environments.



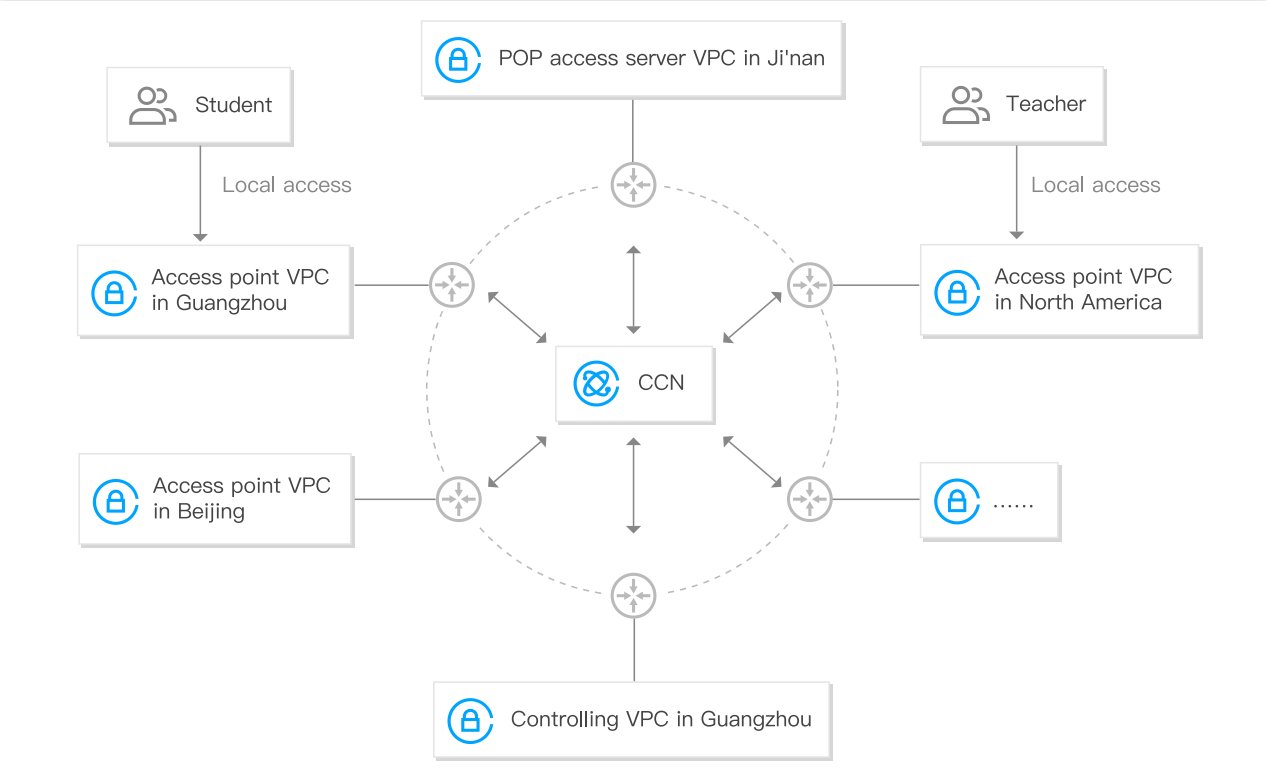
Use Case 2. Online Education

Background

Teachers and students are located in different geographic locations for distance learning, making multiple VPCs and connections necessary for the interconnection if peering connection is used. High-quality interconnection across different regions is also required for live streaming platforms so as to ensure clear audio and video communications.

Solution

Based on Tencent Cloud's coverage in over 20 regions around the globe and intelligent full-mesh scheduling algorithm, any two points can be interconnected through the shortest path on the private network with no public network bypassing and link congestion, providing global multi-point interconnection with reduced latency.
Outcomes:
Teachers and students have local access to online services with high transfer quality and low latency.
VPCs in different regions can interconnect with all other instances once connected to CCN.



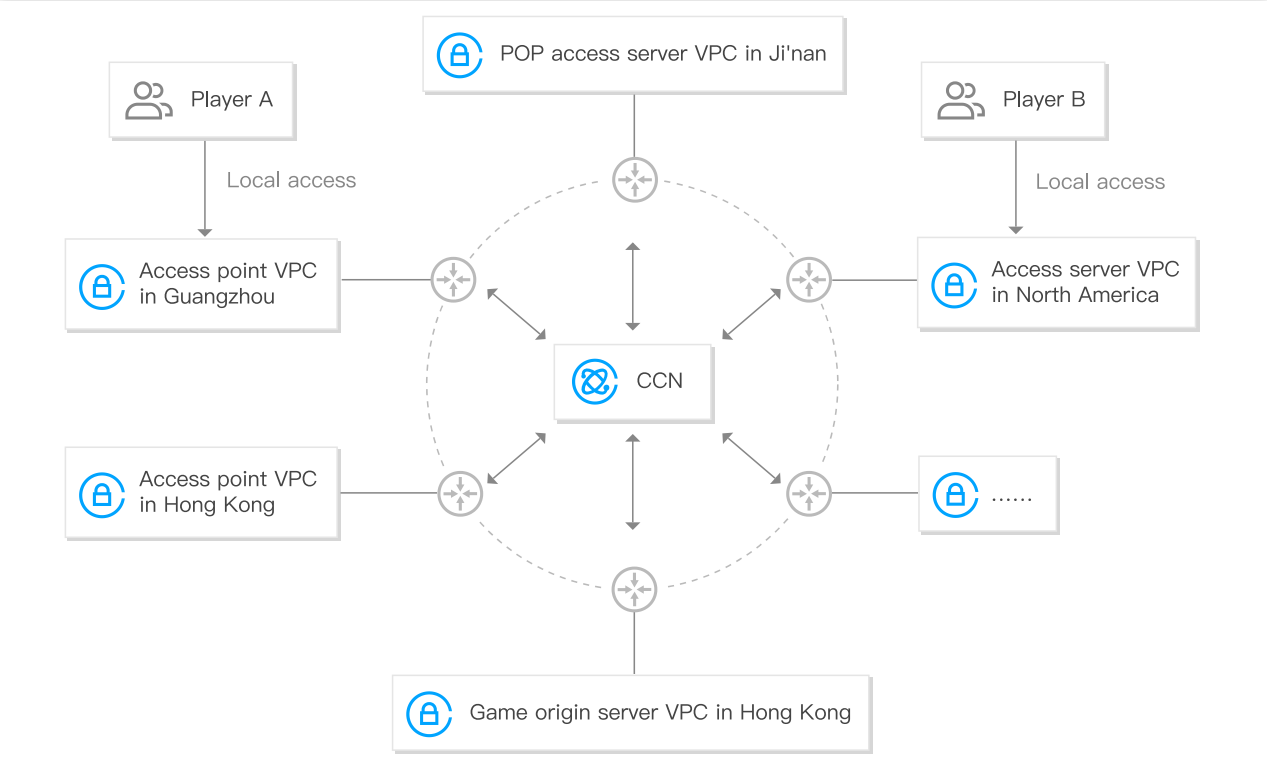
Use Case 3. Gaming Acceleration

Background

Online games have players around the world and is latency-sensitive. Multiple servers need to be deployed in different regions in order to meet the requirements of local access and cross-server PvP battles.

Solution

With coverage in over 20 regions around the globe and based on full-mesh network topology and monitoring of routing and real-time bandwidth, CCN uses an intelligent scheduling system to achieve low-latency interconnection, allowing global players to battle on the same servers for an ultimate gaming experience.
Outcomes:
Players have local access to the service VPCs with low latency.
CCN uses a full-mesh topology to support multi-region VPC connection for a global network.



Use Limits

Last updated：2024-01-10 14:41:59

Limits on the Multi-Route Table Feature in Beta Test

CCN's multi-route table and route table selection policy features (hereinafter referred to as the multi-route table feature) are currently in beta test. Relevant documents are available only to beta users for reference. Users that are not included in the beta test need to wait until the feature is officially commercialized.
Currently, the multi-route table feature is available only in some test regions. It also has the following limits:
The multi-route table feature can be tested by CCN instance. You can submit the ID of a CCN instance to Tencent Cloud for evaluation. After the CCN instance passes the evaluation, we will contact you to start testing.
The multi-route table feature cannot be tested on CCN instances bound with SD-WAN access service Edge devices.
Route table selection policies take effect only for CCN's cross-region traffic and direct connect gateway-based traffic.

Resource Limits

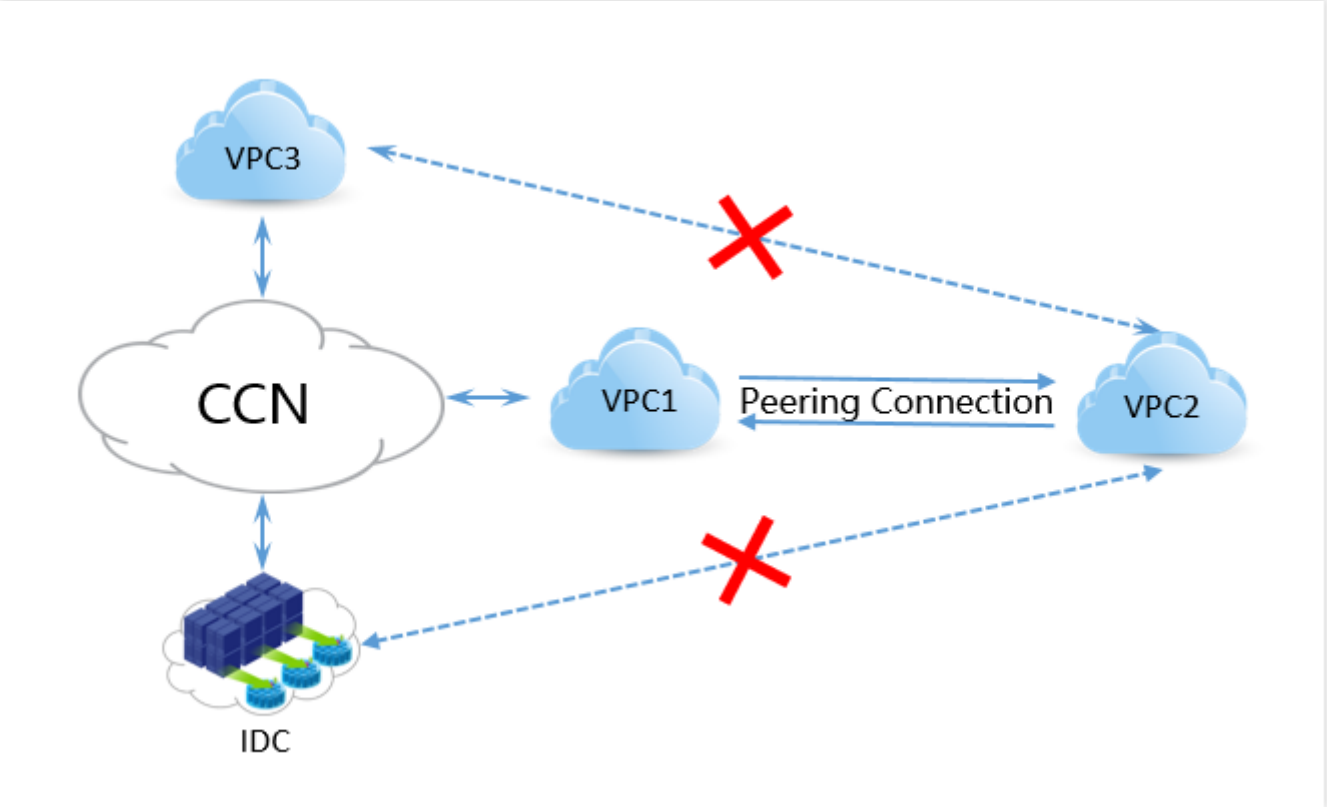
The following table lists the limits on the supported CCN resources. For limits on other Virtual Private Cloud (VPC) products, see Quota Limit.

Resource	Limit
Number of CCN instances per account	5
Number of network instances that can be associated with one CCN instance	25

Feature Limits

Non-transitivity of peering connections
A peering connection does not affect the interconnection between a CCN instance and VPC instances associated with it. A CCN instance distributes routes only to the network instances associated with it for interconnection.
For example, as shown in the following figure, a peering connection has been established between VPC1 and VPC2. After VPC1 is associated with a CCN instance, only VPC1 can interconnect with network instances VPC3 and IDC

associated with the CCN instance, while VPC2 can only interconnect with VPC1 through the peering connection, but not other instances associated with the CCN instance.



Route Limits

To ensure that network instances in CCN are interconnected, CCN restricts the CIDR blocks of the network instances.

Limits on VPC CIDR blocks

CCN restricts CIDR blocks at the subnet level: Two subnets with identical CIDR blocks in different VPCs cannot interconnect with each other (see "Rules for CIDR overlapping conflicts" below). Accordingly, even if the CIDR blocks of two VPCs overlap, as long as their subnets have different CIDR blocks, you can still associate them with a CCN instance for interconnection.

Rules for CIDR overlapping conflicts

1. If the CIDR blocks of network instances overlap, only the route of the network instance that is first associated with the CCN instance will take effect.
2. For a network instance already in a CCN instance, if a route conflict occurs due to operations such as subnet creation, the new route will not take effect, and the existing valid route will remain valid.

Solution:

Evaluate the network condition, disable/delete the conflicting route, and enable the route needed.
Change the IP range to ensure that there is no IP range overlapping between the subnets that need to interconnect with each other through a CCN instance. For example, you can change the CVM instance network to another subnet or VPC with a non-conflicting IP range and then use a CCN instance for interconnection. For more information, see Changing Instance Subnet and Switching to VPC.

Rules for CIDR inclusive conflicts

If the CIDR blocks of multiple network instances have an inclusive conflict, only the route of the network instance that is first associated with the CCN instance will take effect.
Solution:
You can enable invalid routes in the route table, which, once enabled, will forward data based on the longest mask matching rule.
Change the IP range to ensure that there is no inclusive conflict between the subnets that need to interconnect with each other through a CCN instance. For example, you can change the CVM instance network to another subnet or VPC with a non-conflicting IP range and then use a CCN instance for interconnection. For more information, see Changing Instance Subnet and Switching to VPC.

Example of an inclusive conflict

Assume that VPC1 is first associated with CCN instance A, the CIDR block of its subnet A is `10.0.1.0/20`, and VPC1 can interconnect with other instances in CCN instance A. Then, VPC2 is associated with CCN instance A, and the CIDR block of its subnet B is `10.0.1.0/24`, which is included in the CIDR block of subnet A in VPC1. In this case, a CIDR block inclusive conflict occurs. As a result, the routing policy of subnet B in VPC2 will become invalid by default, and VPC2 cannot interconnect with other network instances in CCN instance A.
However, you can enable this invalid route in the CCN route table, which can forward data according to the longest mask matching rule. If the destination IP address of the routing policy is `10.0.1.0/24`, the data will be forwarded to subnet B in VPC2 based on the rule.