

Cloud Connect Network

Product Introduction

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Product Introduction

Overview

Benefits

Use Cases

Use Limits

Product Introduction

Overview

Last updated : 2022-05-20 09:53:05

What is Cloud Connect Network

Cloud Connect Network (CCN) bridges between a Tencent Cloud [VPC](#) and another or between VPCs and local IDCs. 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 20 regions around the world, over 100 Gbps bandwidth and 99.99% high availability, it helps you easily build a fast, stable, secure, and flexible global network. CCN is typically used in:

- 1. High-quality private network connection between VPCs:** online education with real-time audio and video systems across regions, game acceleration using private network interconnection across regions, and cross-region disaster recovery.
- 2. Private network connection between VPCs and on-premises IDCs:** connect multiple VPCs through one [dedicated tunnel](#) for public and private network interconnection by a single access. Ideal for hybrid clouds.

Product Components

A CCN consists of:

- Associated network instances: network instances within the same CCN instance can communicate with each other. Instances including VPC, VPC (BM), direct connect gateway, and VPN gateway can be added to CCN. 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](#).

Features

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 interconnect multiple VPCs or your IDC with multiple VPCs, you need to establish one peering connection for each pair of VPCs and one dedicated tunnel between your IDC and each VPC. And then, you also need to make sure VPC and IDC IP ranges do not 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 the IDC to the CCN instance. After you add the instances to the CCN, it will 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	<ol style="list-style-type: none"> To interconnect n VPCs, you need to establish C_n^2 peering connections, where C_n^2 equals to $n * (n-1)/2$. Namely, six peering connections are required for interconnecting four VPCs. A single dedicated tunnel can only connect to one VPC. Peer connections cannot be established between VPCs with overlapping IP ranges. 	<ol style="list-style-type: none"> All instances added to the CCN instance are in a full mesh interconnection. Each dedicated tunnel can communicate with all VPCs and IDCs. CCN allows for network instances with overlapping CIDR blocks. This provides greater flexibility for interconnection.
Automatic route learning	<ol style="list-style-type: none"> Routes must be configured for every link. Manual updates are required for any link change. 	<ol style="list-style-type: none"> Routes are automatically learned and forwarded. Route tables are dynamically updated without manual maintenance.
Greater stability and reliability	Multi-cluster disaster recovery in a single zone.	Multi-zone hot backup disaster recovery with 99.99% high availability.
Lower costs	<ol style="list-style-type: none"> You pay for each link separately. You pay a higher unit price. 	<ol style="list-style-type: none"> You pay for all bandwidth in a region as a whole (similar to bandwidth packages), which evens out the price. Unit price is more competitive.
Lower 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.

Benefits

Last updated : 2020-09-10 11:07:49

Full-mesh Interconnection and Easy Management

CCN provides you with enterprise-grade network services for single-point access and full-mesh interconnection. Through the automatic forwarding and learning of full-mesh multi-node multi-level routing and second-level routing convergence, all network instances on CCN can be interconnected in one step for easy management with no cumbersome route configuration and management required.

Local Access and Intelligent Scheduling

Based on the multi-node and multi-link full-mesh interconnection, CCN helps you do away with cumbersome routing maintenance work. Its intelligent scheduling system is based on the unified detection of full-mesh multi-level network topology, routing and traffic and supports local access and shortest path routing for local businesses.

Ultra-low Latency and High-speed Transfer

Tencent Cloud operates interconnected Internet Data Centers (IDCs) in more than 30 regions around the globe. CCN enables the interconnection between any two associated network instances via the shortest path on the private network, without possible link congestion caused by public networks. This greatly reduces the network latency for global multi-point interconnections to ensure high-speed data transmission.

Reasonable Billing for Lower Costs

CCN is pay-per-use with a more reasonable monthly 95th percentile billing method, helping round off small fee amounts caused by network jitters. You only need to pay for the bandwidth resources actually used, avoiding the waste caused by prepayments.

Multiple-layer Encryption for Security and Reliability

Based on MPLS-VPN technology, CCN isolates tenant networks from one another by encrypting the network at multiple layers. All data communications of the network instances in CCN do not pass through the Internet, which

provides better communication quality and network availability and results in low latency and low packet loss. Further, CCN makes your data more secure and stable by guaranteeing communication quality through multi-level linkage redundancy.

Bandwidth Monitoring for Flexible Adjustment

CCN has single-region egress bandwidth monitoring, speed limiting and alarming functions. Multi-metric monitoring can help you better manage your business. The upper bandwidth limit in each region can be adjusted at any time according to your business growth needs for easier controlling of the network.

Use Cases

Last updated : 2020-09-11 10:50:37

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.

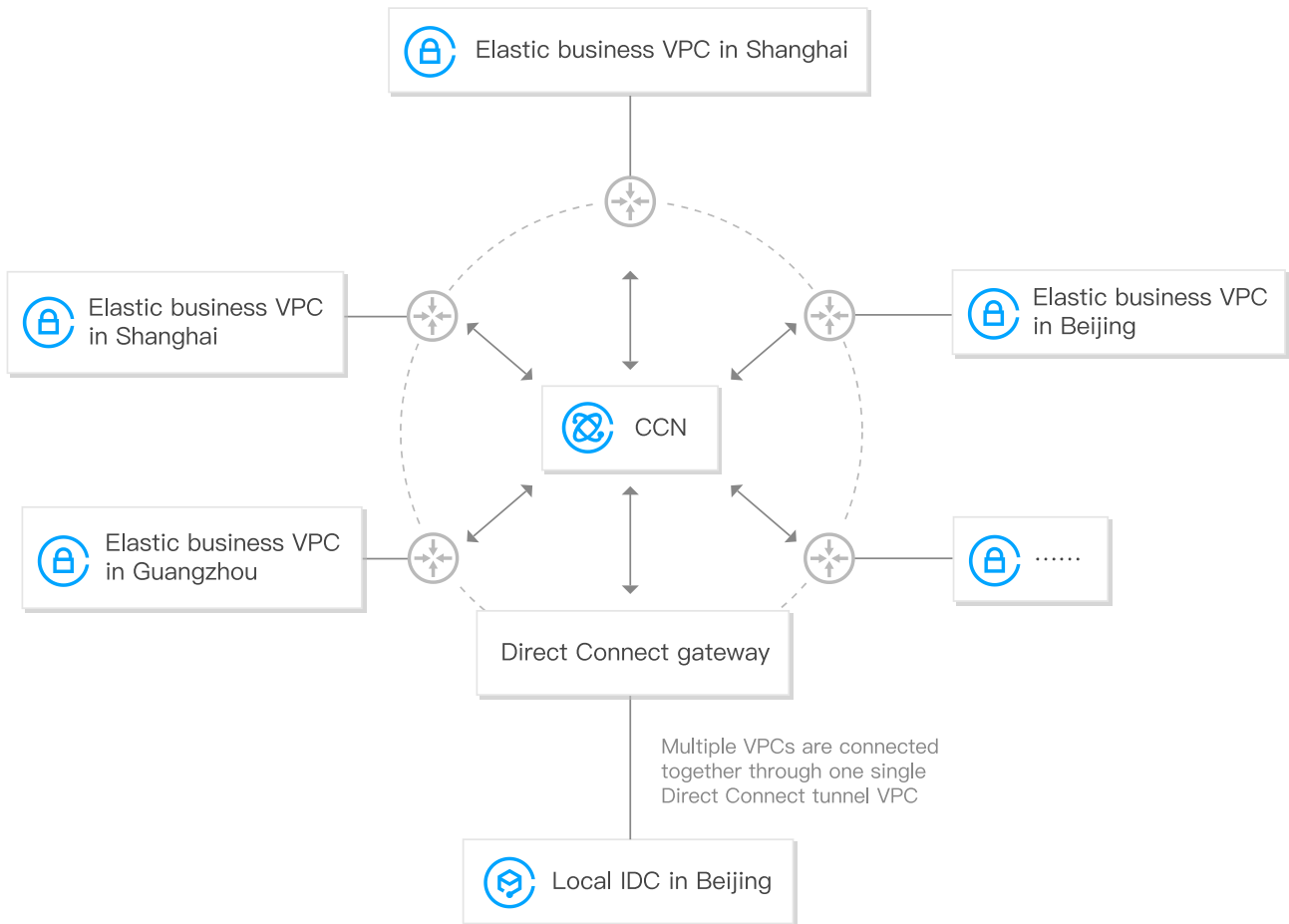
Solution

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

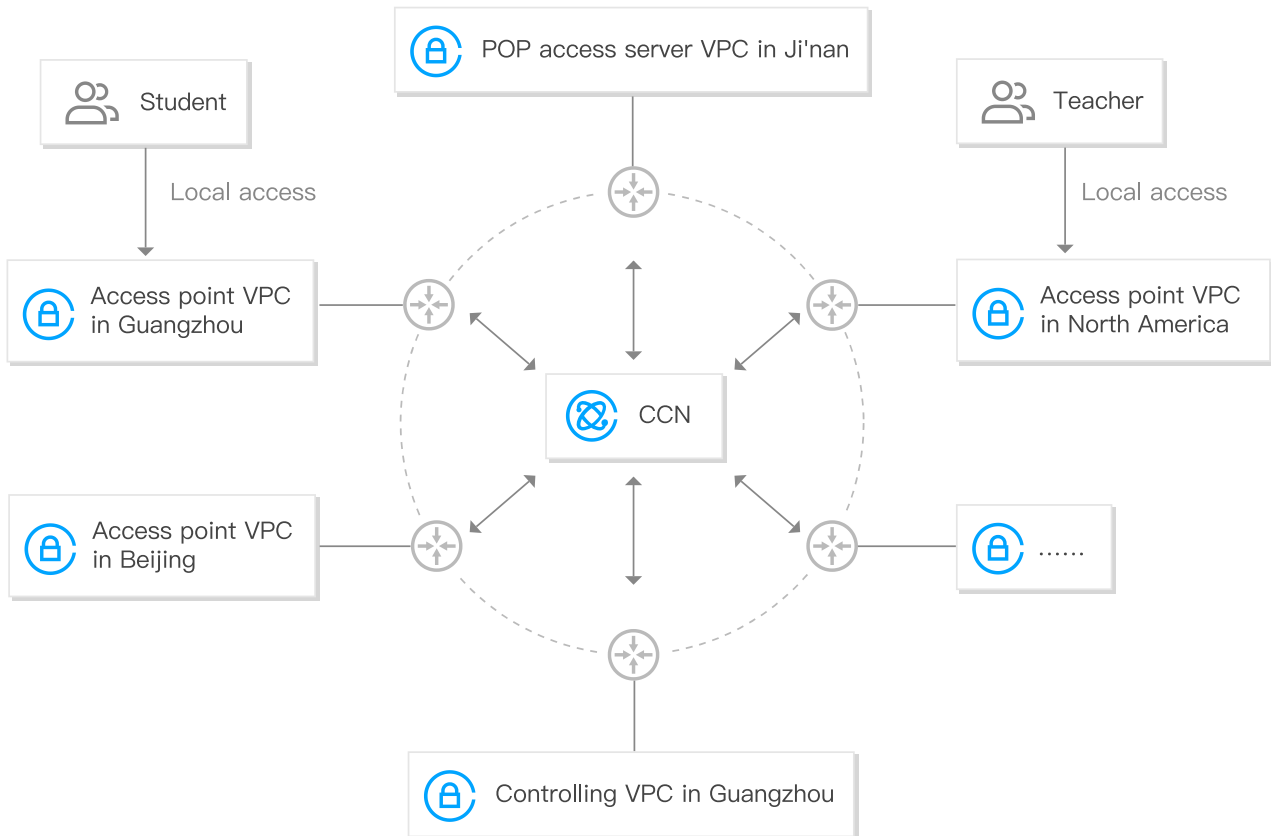
Teachers and students are located in different geographic locations for distance learning, making multiple VPCs and connections necessary for the interconnection if peering connection is used. High-quality interconnection across different regions is also required for live streaming platforms so as to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

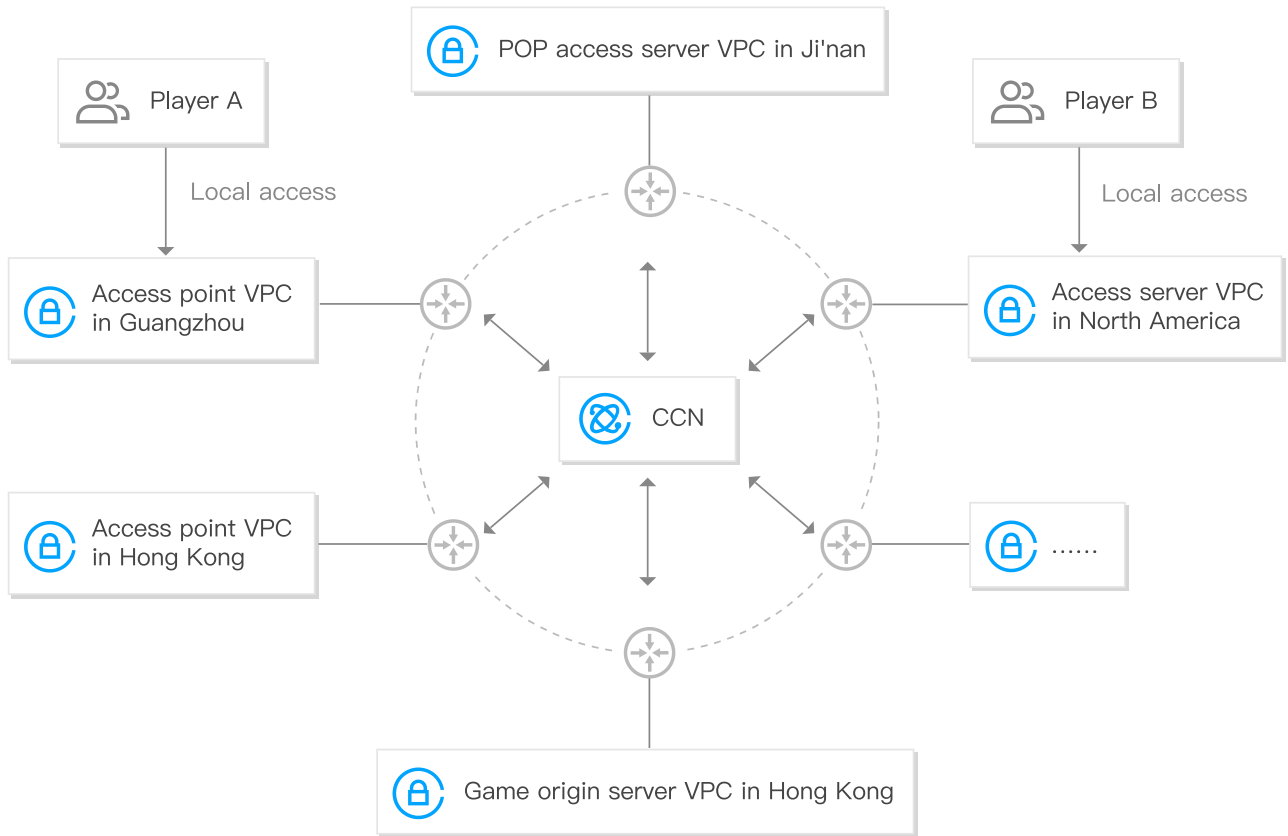
Online games have players around the world and is latency-sensitive. Multiple servers need to be deployed in different regions in order to meet the requirements of local access and cross-server PvP battles.

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 : 2022-06-22 18:57:20

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

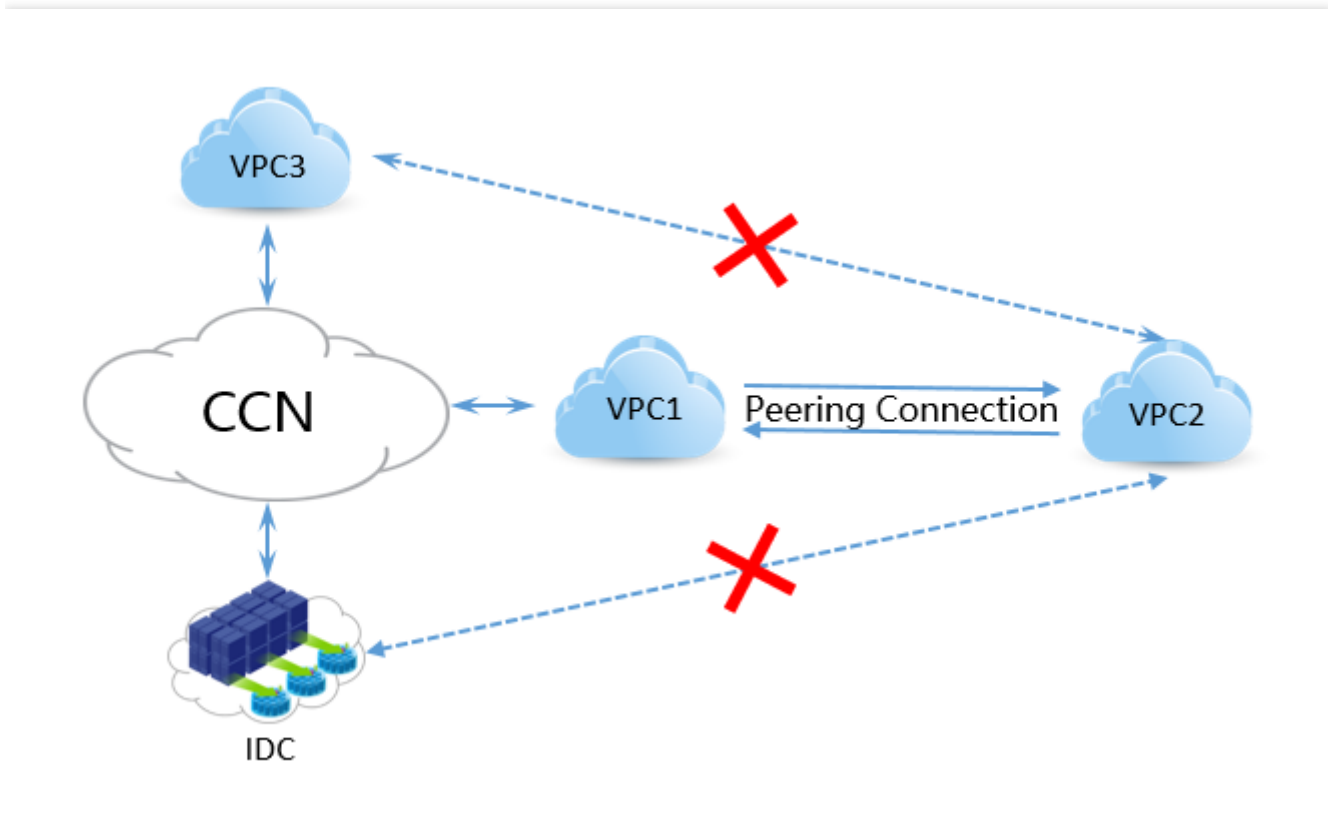
Feature Limits

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.