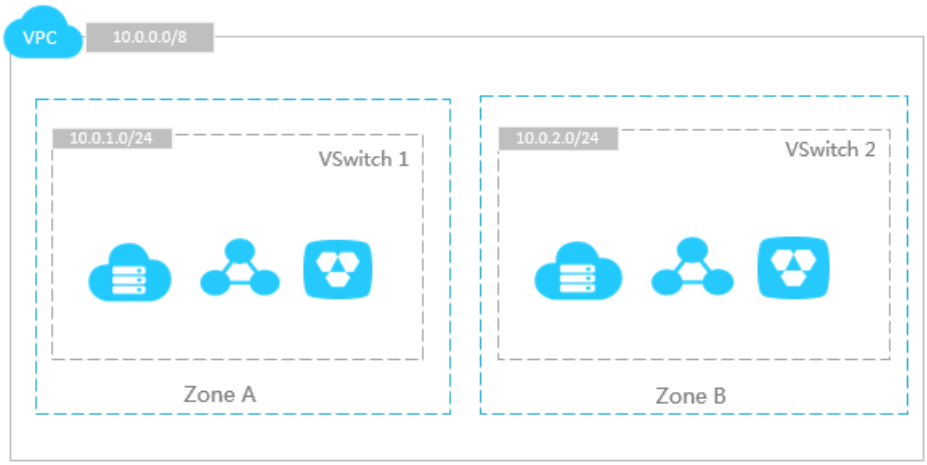
Virtual Private Cloud

VPC Product Introduction

VPC Product Introduction

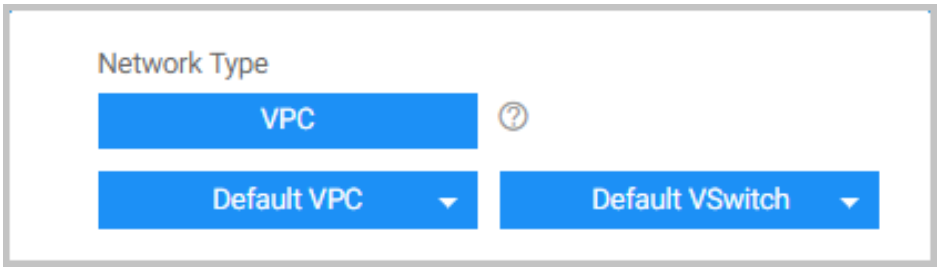
The Virtual Private Cloud (VPC) is a private network established in Alibaba Cloud. VPCs are logically isolated from other virtual networks in Alibaba Cloud. VPCs allow you to launch and use Alibaba Cloud resources in your VPC.

You have full control over your Alibaba Cloud VPC. For example, you can select its IP address range, further segment your VPC into subnets, as well as configure route tables and network gateways. Additionally, you can connect VPCs with an on-premises network using a physical connection or VPN to form an on-demand customizable network environment. This allows you to smoothly migrate applications to Alibaba Cloud with little effort.



Default VPC and VSwitch

Alibaba Cloud provides a default VPC and VSwitch in the situation that you do not have any existing VPC and VSwitch to use when creating a cloud product instance. A default VPC and VSwitch will be created with the creation of an instance.



Default VPC and VSwitch feature list

Default VPC	Default VSwitch

The default VPC in each region is unique.	The default VSwitch in each Availability Zone is unique.
The netmask for a default VPC is /16, such as 172.31.0.0/16, providing up to 65536 private IP addresses.	The netmask for a default VSwitch is /20, such as 172.31.0.0/20, providing up to 4096 private IP addresses.
Default VPCs do not count in the allocated VPC quota.	Default VSwitches do not count in the allocated VSwitch quota.
Default VPCs are created by the system, all self-created VPCs are non-default VPCs.	Default VSwitches are created by the system, all self-created VSwitches are non-default VSwitches.
Operations and restrictions for default and non-default VPCs are the same.	Operations and restrictions for default and non-default VSwitches are the same.

Background information

With the continuous development of cloud computing, the requirements of the virtual network are getting higher and higher, such as scalability, security, reliability, privacy, and higher requirements of connection performance. This gives rise to a variety of network virtualization technologies.

The earlier solution is to combine the virtual machine’ s network with the physical network to form a flat network architecture, such as the large Layer-2 network. With the increase in the scale of virtual networks, the problems such as ARP spoofing, broadcast storms, host scanning, and other issues are getting more and more serious for the earlier solutions. Various network isolation technologies emerge to resolve these problems by completely isolating the physical networks from the virtual networks. One of these technologies is to isolate users with VLAN. But a VLAN only supports a maximum of 4096 nodes, it cannot support the huge amount of users in the cloud.

Principle description

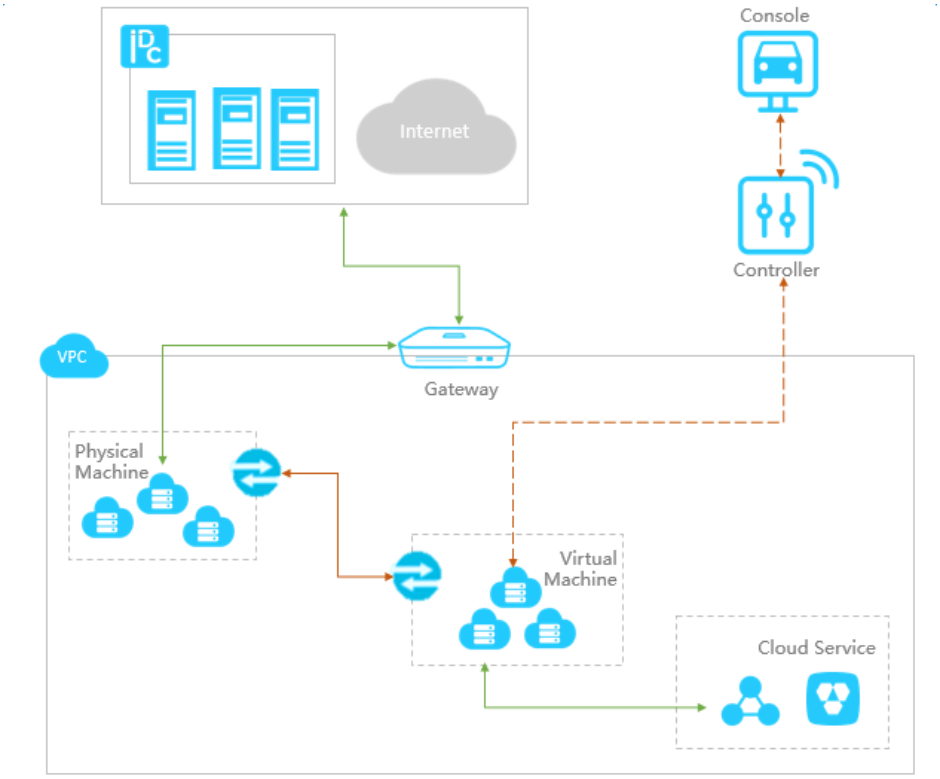
Based on the mainstream tunneling technologies, a Virtual Private Cloud (VPC) isolates the virtual networks. Each VPC has a unique tunnel ID, and a tunnel ID corresponds to only one VPC. A tunnel encapsulation that carries a unique tunnel ID is added to each data packet transmitted between the ECS instances within a VPC. Then the data packet is transmitted over the physical network. Because the tunnel IDs for the ECS instances in different VPCs are different and they are located on two different routing planes, the ECS instances from different VPCs cannot communicate with each other and are isolated by nature.

Based on the tunneling technologies, the Alibaba Cloud research and development team has developed the VSwitch, Software Defined Network (SDN) technology and hardware gateway, which are the basis for the team to successfully design and develop the VPC.

Logical architecture

As shown in the following figure, the VPC architecture contains three main components: VSwitches, a gateway and a controller.

> The VSwitches and gateways form the key data path. A controller uses the self-developed protocol to forward the forwarding table to the gateway and the VSwitches, which completes the key configuration path. In the overall architecture, the configuration path and data path are separated from each other.
>
> The VSwitches are distributed nodes, the gateway and controller are deployed in clusters, and all the links have redundant disaster recovery. This improves the overall availability of the VPC.
>
> The performance of Alibaba Cloud VSwitch and gateway are in a leading position of the field. The self-developed SDN protocol and controllers can easily control thousands of tons of VPCs in the cloud.



In addition to an isolated private network, Alibaba Cloud provides each VPC with a separated VRouter and VSwitches, giving you the capability to design your VPC network in a rich set of ways.

If you have intranet security requirements, you can use the security group function to do the access control and isolation in a finer granularity. By default, a VPC ECS instance can only communicate with

other ECS instances or other cloud services in the same VPC. You can use the VPC related products such as EIP and Express Connect to connect your VPC with the Internet, other VPCs and your on-premises data centers.

VPCs allow you to establish an isolated network environment in Alibaba Cloud. Alibaba Cloud also provides each VPC with an independent VRouter and VSwitch. You have full control over your private virtual network, such as the private IP address range, VSwitch CIDR, the route table, and so on.

VPC

You can create and manage cloud product instances in your VPC, such as ECS, SLB, and RDS.

When creating a VPC, you must specify the private IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. For more details, refer to Classless Inter-Domain Routing.

You can use the following standard CIDR block and the subset as the IP address range of your VPC.

CIDR block	Number of available IP addresses	Notes
192.168.0.0/16	65,532	Exclude system reserved addresses
172.16.0.0/12	1,048,572	Exclude system reserved addresses
10.0.0.0/8	16,777,212	Exclude system reserved addresses

The CIDR block cannot be changed once a VPC is created. Therefore, we recommend to use a larger sized CIDR block to avoid IP expansion. The system does not create the system route based on the VPC CIDR block. That is, using a relatively large CIDR block will not impact your business application.

VSwitch

A VSwitch is a basic network device for a VPC and is designed to connect the cloud product instances in the VPC. You can further segment your VPC into subnets by adding VSwitches. A VPC must contain at least 1 VSwitch and can contain up to 24 VSwitches.

> Note：VSwitch does not support multicast or broadcast.

When creating a VSwitch in a VPC, you need to specify the private IP address range in the form of a Classless Inter-Domain Routing (CIDR) block. The allowed block size for a VSwitch is between a /16 netmask and /29 netmask.

Default VPC and VSwitch

To simplify the creation process of VPC-type cloud product instances, Alibaba Cloud VPC provides the default VPC and VSwitch function. With the default VPC and VSwitch, you do not need to create a VPC and VSwitch ahead of time when creating a VPC-type cloud product instance.

> Note: If you do not want to use the default VPC and VSwitch, select the non-default VPC and VSwitch when creating VPC-type cloud product instance. Otherwise, the cloud product instance will be created in the default VPC and VSwitch.

IP addresses

IP addresses allow the VPC resources to communicate with each other and resources on the Internet. In a VPC, you may need to use the following IP addresses:

Private IP

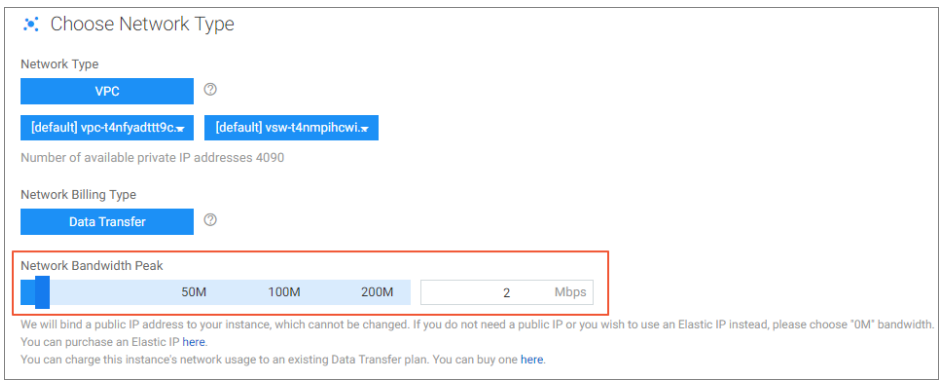
The system allocates a private IP address to each VPC cloud product instance, such as ECS instance, SLB instance, and RDS instance. The private IP address can be used for the intranet access among the VPC cloud product instances， but cannot be used for the external Internet access.

The private IP address is unique in the VPC, which is allocated based on the VSwitch CIDR block.

Public IP

A public IP address is allocated to the VPC-type ECS instance. You can use this IP address to access the Internet or provide public services.

> Note: If you set a value larger than 0 for the network bandwidth peak, a public IP address is not allocated to a VPC ECS instance by default.



Elastic IP

Elastic IP addresses (EIPs) are public IP address resources that you can purchase and possess separately. EIPs can be dynamically bound to a VPC ECS instance. With an EIP, ECS instances can communicate with the Internet.

An EIP address is a NAT IP. It is located in the public network gateway of the Alibaba Cloud and mapped to the private network interface card (NIC) of the bound ECS instance by NAT. Therefore, the ECS instance that has bound an EIP can communicate with the Internet without disclosing its EIP in the NIC.

VRouter

A VRouter is a hub in the VPC connecting all VSwitches in the VPC and serves as a gateway device connecting the VPC with other networks.

The VRouter supports static routing, load sharing, EMCP, standby routing, and other configuration methods in the scenario that a leased line is connected to a VPC.

A VRouter and route table are automatically created after you create a VPC. You cannot create or delete them directly. They will be deleted automatically with the deletion of the VPC. You can add route entries to the route table to route network traffic.

Each entry in the route table is a route entry determining where network traffic is directed. There are two types of route entries: system route entries and custom route entries.

System route entry

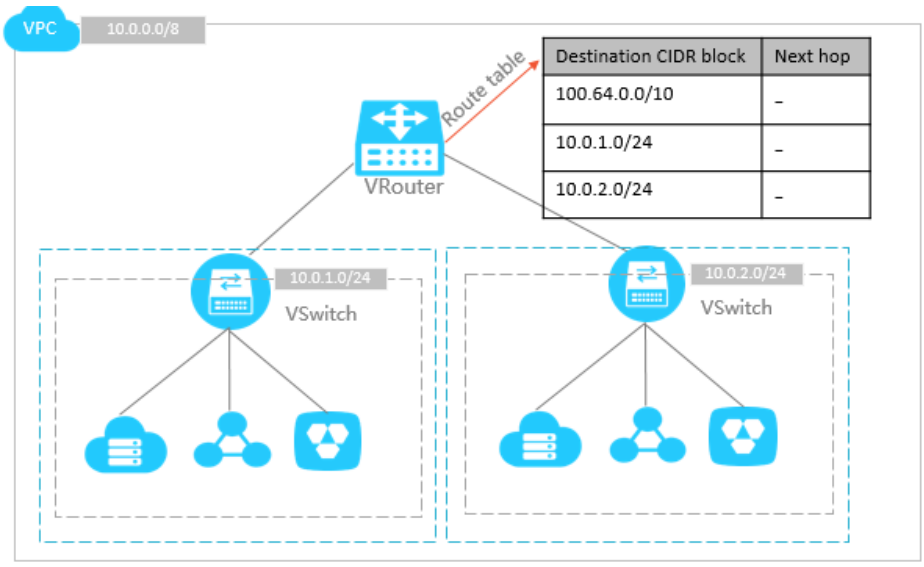
A route entry with the destination CIDR block 100.64.0.0/10 is added by the system when you create a VPC. This allows for communication between cloud product instances in the VPC.

Additionally, a route entry is added for each VSwitch by the system when you create a VSwitch. The destination CIDR block of this system route entry is the CIDR block of the VSwtich.

Custom route entry

You are allowed to add customized route entries for your VPC. For details, refer to Manage a route table.

The following figure indicates how VRouter works.



Security isolation

- The cloud servers of different users are located in different VPCs.
- Different VPCs are isolated by tunnel IDs. Using VSwitches and VRouters, you can segment your VPC into subnets as you would in the traditional network environment. Different cloud servers in the same subnet use the VSwitch to communicate with each other, while cloud servers in different subnets within a VPC use VRouters to communicate with each other.
- The intranet between different VPCs is completely isolated and can only be interconnected by external mapping of IP (Elastic IP and NAT IP).
- Because the IP packets of cloud servers are encapsulated with the tunneling ID, the data link layer (two-layer MAC address) of the cloud server will not transfer to the physical network. Therefore, the two-layer network of different cloud servers is isolated. That is, the two-layer networks between different VPCs are isolated.
- ECS instances within a VPC use a security group firewall to control the network access. This is the third layer isolation.

Access control

- Security groups provide flexible access control rules.
- Compliant with security isolation rules of government and financial users.

Software Defined Network (SDN)

- SDN provides customized network configurations.
- Management operations take effect in real time.

Various network connection methods

- Software VPNs are supported.

- Lease line connection is supported.

Terms	Descriptions
Virtual Private Cloud (VPC)	VPC is a private network established in Alibaba Cloud. It is logically isolated from other virtual networks in Alibaba Cloud. Alibaba Cloud VPC enables you to launch and use the Alibaba Cloud resources in your own VPC.
VSwitch	A VSwitch is a basic network device of a VPC and used to connect different cloud product instances. When creating a cloud product instance in a VPC, you must specify the VSwitch that the instance is located.
VRouter	A VRouter is a hub in the VPC that connects all VSwitches in the VPC and serves as a gateway device that connects the VPC to other networks. VRouter routes the network traffic according to the configurations of route entries.
Route Table	A route table is a list of route entries in a VRouter.
Route Entry	Each entry in a route table is a route entry. A route entry specifies the next hop address for the network traffic destined to a CIDR block. It has two type of entries: system route entry and custom route entry.

VPC

Items	Limitations	Ticket submission permits exemption
Available CIDR blocks	192.168.0.0/16，172.16.0.0/12，10.0.0.0/8, and their subsets	Supported
Maximum number of VPCs for an account	5	Supported
Maximum number of VRouters in a VPC	1	Unsupported
Maximum number of VSwitches in a VPC	24	Unsupported
Maximum number of route tables in a VPC	1	Unsupported
Maximum number of route entries in a route table	48	Supported
Maximum number of cloud product instances that can run in a VPC	10,000	Unsupported

VRouter and VSwitch

Items	Limitations
VRouter	- Each VPC can have only one VRouter. - VRouter does not support dynamic route protocols, such as BGP or OSPF. - Each VRouter has only one route table. - Route entries in a route table affect all the cloud product instances in the VPC. Currently, the source IP routing rules are not supported by VSwitches and cloud product instances.
VSwitch	- VSwitches are a layer-3 switch, therefore the layer-2 broadcast and multicast are not supported. - The number of instances that a VSwitch can have = 10,000 - the number of existing instances in the VPC. - The CIDR block cannot be modified.

Release Date	Changes
August 4, 2015	Alibaba Cloud fully launched, providing the Virtual Private Cloud (VPC), VRouter, route table, and VSwitch services.
December 28, 2015	Resource Access Management (RAM) was supported.
March 29, 2016	VPC documentation was updated.
March 30, 2016	The default VPC function was released.