

# Alibaba Cloud Express Connect

## Best Practices

Issue: 20190401

## Legal disclaimer

---

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use








or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid <i>Instance_ID</i></code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

- Legal disclaimer..... I
- Generic conventions..... I
- 1 Access cloud services through physical connection.....1
- 2 Method for testing the network performance of the leased line..... 3
- 3 Multiple VPCs access Alibaba Cloud through the same physical connection.....13
- 4 Use Express Connect to connect your network to Alibaba Cloud.....21



# 1 Access cloud services through physical connection

---

## AnyTunnel VIP

AnyTunnel VIP belongs to 100.64.0.0/10 of each VPC. DNS, YUM, NTP, OSS, SLS, and other cloud services are all using IPs belonging to 100.64.0.0/10.

If you need to access these cloud services from the peer end of the leased line, namely your local data center, you must set the router interface pointing to VPC as the next hop of the route destined for 100.64.0.0/10 after you create the VBR. You also need to set the router interface pointing to Alibaba Cloud as the next hop of the route destined for 100.64.0.0/10 on the gateway device of the local data center.



### Note:

Because 100.64.0.0/10 is a reserved CIDR block of VPC, you need to split it into 100.64.0.0/11 and 100.96.0.0/11 and configure two route entries on the VBR.

## Configure the route on the VBR

1. Log on to the [Express Connect console](#).
2. In the left-side navigation pane, select Physical Connection > Virtual Border Router.
3. Click Manage in the Actions column of the target VBR.
4. On the VBR Details page, click Add Route Entry and configure the route entry. The following configurations are used in this tutorial:
  - Destination CIDR Block: Enter 100.64.0.0/11 and 100.96.0.0/11 respectively.
  - Next Hop Direction: To VPC
  - Next Hop: Select the exit for data packets. In this tutorial, select the router interface on the VBR.
5. Click OK to complete the configuration.

**Configure the route on the customer-side access device of the leased line**

**Add a static route pointing to Alibaba Cloud on the customer-side access device of the leased line:**

```
ip route 100 . 64 . 0 . 0 / 10 { Alibaba Cloud - side IP  
address }
```

## 2 Method for testing the network performance of the leased line

---

After completing the leased line access, you need to test the performance of the leased line to ensure that it can meet your service needs.

### Prerequisites

Before the test, ensure you have made the following preparations:

- Complete configurations regarding leased line access and routes. The local data center must be connected to the VPC through a leased line.
- Prepare a network access device for the local data center: The network access device is subjected to stress testing to test the packets per second (pps) of the local data center. It serves as the client or server in the Netperf or iperf3 test.

In this tutorial, the IP address of the local data center is 192.168.100.1.

- Prepare eight VPC ECS instances: The ECS instances serve as clients or servers in the Netperf or iperf3 test. They are connected to the network access device of the local data center to transmit test configurations and test results.

In this tutorial, eight ECS instances are used, of which the specification is ecs.se1.2xlarge, the image is centos\_7\_2\_64\_40G\_base\_20170222.vhd, and the IP address range is 172.16.0.2 – 172.16.0.9.

### Build the test environment

#### Install Netperf

Netperf is a tool for testing network performance and is based on TCP or UDP transmission.

Follow these steps to install Netperf on the network access device of the local data center and the eight ECS instances.

1. Run the following command to download netperf:

```
wget -c "https://codeload.github.com/HewlettPacker/netperf/tar.gz/netperf-2.5.0" -O netperf-2.5.0.tar.gz
```

2. Run the following command to install netperf:

```
tar -zxvf netperf-2.5.0.tar.gz
```

```
cd netperf - netperf - 2 . 5 . 0
./ configure
make
make install
```

3. Run the `netperf - h` and `netserver - h` commands to verify if the installation is successful.

### Install iperf3

Iperf3 is a tool for testing network performance and can test the maximum TCP or UDP bandwidth.

Follow these steps to install iperf3 on the network access device of the local data center and the eight ECS instances.

1. Run the following command to download iperf3:

```
yum install git - y
git clone https :// github . com / esnet / iperf
```

2. Run the following command to install iperf3:

```
cd iperf
./ configure && make && make install && cd ..
cd src
ADD_PATH ="$( pwd )"
PATH ="${ ADD_PATH }:${ PATH }"
export PATH
```

3. Run the `iperf3 - h` command to verify if the installation is successful.

### Enable the multiple queues feature

Run the following command on the network access device of the local data center to enable the multiple queue feature ( Assume the interface connected to the leased line is eth0.)

```
ethtool - L eth0 combined 4
echo " ff " > / sys / class / net / eth0 / queues / rx - 0 /
rps_cpus
echo " ff " > / sys / class / net / eth0 / queues / rx - 1 /
rps_cpus
echo " ff " > / sys / class / net / eth0 / queues / rx - 2 /
rps_cpus
echo " ff " > / sys / class / net / eth0 / queues / rx - 3 /
rps_cpus
```

Use netperf to test the packet forwarding performance of the leased line

After being installed, netperf creates two command line tools: netserver (server side) and netperf (client side). Main parameters of the two tools are shown in the following table.

Tool name	Main parameter	Parameter description
netserver (server side: receiving side tool)	-p	The port of the server.
netperf (client side: sending side tool)	-H	The IP address of the network access device of the local data center or the VPC server.
	-p	The port of the network access device of the local data center or the VPC server.
	-l	The running duration.
	-t	The protocol used for sending packets: TCP_STREAM or UDP_STREAM. We recommend using UDP_STREAM.
	-m	The data packet size.  <ul style="list-style-type: none"> <li>· We recommend that you set the value to 1 when testing pps.</li> <li>· We recommend that you set the value to 1400 when testing bps (bit per second).</li> </ul>

### Test the inbound direction

1. Start the netserver process on the network access device of the local data center and specify different ports:

```
netserver - p 11256
netserver - p 11257
netserver - p 11258
netserver - p 11259
netserver - p 11260
netserver - p 11261
netserver - p 11262
```

```
netserver -p 11263
```

2. Start the netperf process on the eight ECS instances in the VPC and specify different ports connecting to the network access device of the local data center.

```
netperf -H 192 . 168 . 100 . 1 -p 11256 -t UDP_STREAM
-l 300 -- -m 1 # first ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11257 -t UDP_STREAM
-l 300 -- -m 1 # second ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11258 -t UDP_STREAM
-l 300 -- -m 1 # third ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11259 -t UDP_STREAM
-l 300 -- -m 1 # fourth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11260 -t UDP_STREAM
-l 300 -- -m 1 # fifth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11261 -t UDP_STREAM
-l 300 -- -m 1 # sixth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11262 -t UDP_STREAM
-l 300 -- -m 1 # seventh ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11263 -t UDP_STREAM
-l 300 -- -m 1 # eighth ECS instance
```

3. If you want to test bps, change the preceding commands to:

```
netperf -H 192 . 168 . 100 . 1 -p 11256 -t UDP_STREAM
-l 300 -- -m 1400 # first ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11257 -t UDP_STREAM
-l 300 -- -m 1400 # second ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11258 -t UDP_STREAM
-l 300 -- -m 1400 # third ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11259 -t UDP_STREAM
-l 300 -- -m 1400 # fourth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11260 -t UDP_STREAM
-l 300 -- -m 1400 # fifth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11261 -t UDP_STREAM
-l 300 -- -m 1400 # sixth ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11262 -t UDP_STREAM
-l 300 -- -m 1400 # seventh ECS instance
netperf -H 192 . 168 . 100 . 1 -p 11263 -t UDP_STREAM
-l 300 -- -m 1400 # eighth ECS instance
```

### Test the outbound direction

1. Start the netserver process on the eight ECS instances in the VPC and specify the port as follows:

```
netserver -p 11256
```

2. Start eight netperf processes on the network access device of the local data center and specify different IP addresses.

```
netperf -H 172 . 16 . 0 . 2 -p 11256 -t UDP_STREAM -
-l 300 -- -m 1 # first ECS instance
netperf -H 172 . 16 . 0 . 3 -p 11256 -t UDP_STREAM -
-l 300 -- -m 1 # second ECS instance
netperf -H 172 . 16 . 0 . 4 -p 11256 -t UDP_STREAM -
-l 300 -- -m 1 # third ECS instance
```

```

netperf -H 172 . 16 . 0 . 5 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # fourth ECS instance
netperf -H 172 . 16 . 0 . 6 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # fifth ECS instance
netperf -H 172 . 16 . 0 . 7 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # sixth ECS instance
netperf -H 172 . 16 . 0 . 8 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # seventh ECS instance
netperf -H 172 . 16 . 0 . 9 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # eighth ECS instance

```

### 3. If you want to test bps, change the preceding commands to:

```

netperf -H 192 . 168 . 100 . 1 - p 11256 - t UDP_STREAM
- l 300 -- - m 1400 # first ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11257 - t UDP_STREAM
- l 300 -- - m 1400 # second ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11258 - t UDP_STREAM
- l 300 -- - m 1400 # third ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11259 - t UDP_STREAM
- l 300 -- - m 1400 # fourth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11260 - t UDP_STREAM
- l 300 -- - m 1400 # fifth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11261 - t UDP_STREAM
- l 300 -- - m 1400 # sixth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11262 - t UDP_STREAM
- l 300 -- - m 1400 # seventh ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11263 - t UDP_STREAM
- l 300 -- - m 1400 # eighth ECS instance

```

### Test the outbound direction

1. Start the netserver process on the eight ECS instances in the VPC and specify the port as follows:

```
netserver - p 11256
```

2. Start eight netperf processes on the network access device of the local data center and specify different IP addresses.

```

netperf -H 172 . 16 . 0 . 2 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # first ECS instance
netperf -H 172 . 16 . 0 . 3 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # second ECS instance
netperf -H 172 . 16 . 0 . 4 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # third ECS instance
netperf -H 172 . 16 . 0 . 5 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # fourth ECS instance
netperf -H 172 . 16 . 0 . 6 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # fifth ECS instance
netperf -H 172 . 16 . 0 . 7 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # sixth ECS instance
netperf -H 172 . 16 . 0 . 8 - p 11256 - t UDP_STREAM -
l 300 -- - m 1 # seventh ECS instance

```

```
netperf -H 172 . 16 . 0 . 9 - p 11256 - t UDP_STREAM -
-l 300 -- - m 1 # eighth ECS instance
```

**3. If you want to test bps, change the preceding commands to:**

```
netperf -H 192 . 168 . 100 . 1 - p 11256 - t UDP_STREAM
-l 300 -- - m 1400 # first ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11257 - t UDP_STREAM
-l 300 -- - m 1400 # second ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11258 - t UDP_STREAM
-l 300 -- - m 1400 # third ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11259 - t UDP_STREAM
-l 300 -- - m 1400 # fourth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11260 - t UDP_STREAM
-l 300 -- - m 1400 # fifth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11261 - t UDP_STREAM
-l 300 -- - m 1400 # sixth ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11262 - t UDP_STREAM
-l 300 -- - m 1400 # seventh ECS instance
netperf -H 192 . 168 . 100 . 1 - p 11263 - t UDP_STREAM
-l 300 -- - m 1400 # eighth ECS instance
```

**Analyze test results**

The following results are displayed when netperf processes on the client side are completed.

```
Socket      Message      Elapsed      Messages
Size        Size         Time         Okay         Errors        Throughput
bytes       bytes        secs        # #         10 ^ 6bits / sec
124928     1           10 . 00     4532554     0           3 . 63
212992     10 . 00     1099999     0 . 88
```

Descriptions of fields in the test results are shown in the following table:

Field	Description
Socket Size	Buffer size
Message Size	Packet size (Byte)
Elapsed Time	The duration of test (s)
Message Okay	The number of packets successfully sent out
Message Errors	The number of packets fail to be sent out
Throughput	Network throughput (Mbit/s)

You can obtain the pps of the tested link if you divide the number of packets successfully sent out by the duration of test. That is, pps = the number of packets successfully sent out / the duration of test.



## Use iperf3 to test the bandwidth of the leased line

Main parameters of iperf3 are shown in the following table.

Tool name	Main parameter	Description
iPerf3	-s	Indicates receiving packets as the server.
	-i	Interval between every two reports, in seconds.
	-p	The listening port of the server.
	-u	Indicates using the UDP protocol to send packets . If this parameter is not specified, the TCP protocol is used.
	-l	Indicates the length of the read-write buffer . We recommend that you set the value to 16 when testing the packet forwarding performance and to 1400 when testing the bandwidth.
	-b	The bandwidth used by the UDP mode, in bits/s.
	-t	Set the duration of transmission. In the specified time period, iperf repeatedly sends packets of specified length. The default value is 10 seconds.
	-A	CPU affinity. You can bind an iperf3 process to the logic CPU of the corresponding number to avoid cross-CPU scheduling of the iperf3 process.

### Test the inbound direction

1. Start the iperf3 process in the server mode on the network access device of the local data center and specify different ports as follows:

```
iPerf3 -s -i 1 -p 16001
iPerf3 -s -i 1 -p 16002
iPerf3 -s -i 1 -p 16003
iPerf3 -s -i 1 -p 16004
iPerf3 -s -i 1 -p 16005
iPerf3 -s -i 1 -p 16006
iPerf3 -s -i 1 -p 16007
iPerf3 -s -i 1 -p 16008
```

2. Start the iperf3 process in the client mode on the eight ECS instances in the VPC and specify different ports connecting to the network access device of the local data center.

```
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16001 -A 1
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16002 -A 2
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16003 -A 3
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16004 -A 4
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16005 -A 5
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16006 -A 6
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16007 -A 7
iPerf3 -u -l 16 -b 100m -t 120 -c 192 . 168 .
100 . 1 -i 1 -p 16008 -A 8
```

### Test the outbound direction

1. Start the iperf3 process in the server mode on each ECS instance in the VPC and specify the port:

```
iPerf3 -s -i 1 -p 16001
```

2. Start eight iperf3 processes in the client mode on the network access device of the local data center and the value of `-c` is the IP address of each ECS instance.

```
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
2 -i 1 -p 16001 -A 1
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
3 -i 1 -p 16001 -A 2
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
4 -i 1 -p 16001 -A 3
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
5 -i 1 -p 16001 -A 4
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
6 -i 1 -p 16001 -A 5
iPerf3 -u -l 16 -b 100m -t 120 -c 172 . 16 . 0 .
7 -i 1 -p 16001 -A 6
```

```

iPerf3 -u -l 16 -b 100m -t 120 -c 172.16.0.8
8 -i 1 -p 16001 -A 7
iPerf3 -u -l 16 -b 100m -t 120 -c 172.16.0.9
9 -i 1 -p 16001 -A 8

```

## Analyze test results

The following results are displayed when iperf3 processes on the client side are completed.

```

[ ID ] Interval Transfer Bandwidth Jitter Lost / Total
Datagrams
[ 4 ] 0.00 - 10.00 sec 237 MBytes 199 Mbits / sec 0
.027 ms 500 / 30352 (1.6%)
[ 4 ] Sent 30352 datagrams

```

Descriptions of fields in the rest results are shown in the following table:

Field	Definition
Transfer	The total number of data transmitted
Bandwidth	Bandwidth
Jitter	Jitter
Lost/Total Datagrams	The number of dropped packets / The total number of packets (packet loss)

PPS = The number of packets received by the peer end/Duration



### Note:

We recommend that you run the `sar` command on the server side to count the packets actually received and use the obtained value as the actual result, such as

```
sar -n DEV 1 320 .
```

## Alibaba Cloud side speed limit

In addition to limits on the leased line, the following are limits on the communication between the VPC and the local data center:

- The maximum read-write speed of OSS is 5 Gbit/s.
- To improve the reliability, the speed of a single hash stream from the VPC to the VBR is limited to “Express Connect bandwidth / 12”. For example, if the

bandwidth from the VBR to the VPC is large1, namely 1 Gbps, the maximum bandwidth of a single hash stream is 83 Mbps.

**Hash stream:** The data stream that is defined by the combination of the source IP address, source port, transport layer protocol, destination IP address, and destination port. For example, “192.168.1.1 10000 TCP 121.14.88.76 80” forms a hash stream. A terminal whose IP address is 192.168.1.1 is connected to port 80 of a terminal whose IP address is 121.14.88.76 through port 10000 by using the TCP protocol.

## 3 Multiple VPCs access Alibaba Cloud through the same physical connection

---

You can use a physical connection that is already connected to an access point of Alibaba Cloud to connect multiple VPCs.



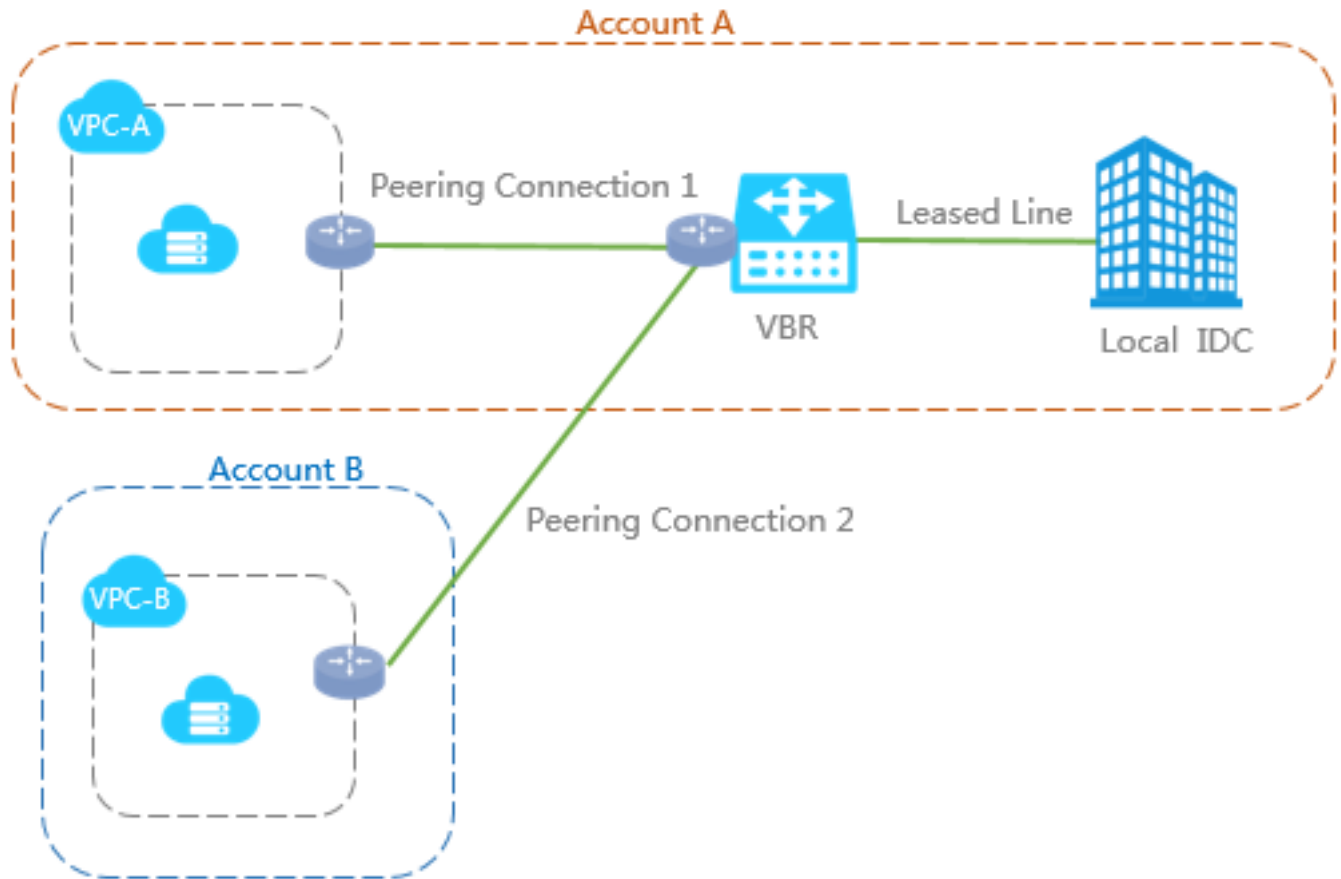
Note:

Currently, a physical connection can be used by five VPCs at most. You can open a ticket to increase the quota.

### Background information

A company has opened account A on Alibaba Cloud and created VPC-A. The company has already opened a physical connection under account A to connect the local data center (172.16.0.0/12) of the company to VPC-A. A subsidiary of the company has open account B on Alibaba Cloud and VPC-B is under account B. The subsidiary wants to connect VPC-B to the local data center.

Because the company has purchased a physical connection under account A and connected the local data center to an access point of Alibaba Cloud, account B of the subsidiary can also use this physical connection to connect the VPC under account B to the local data center.



In this tutorial, the VPC and physical connection configurations are as follows:

Account A	Account B
Account ID: 12345678	Account ID: 87654321
<b>VPC</b> <ul style="list-style-type: none"> <li>• Name: VPC-A</li> <li>• Region: China (Beijing)</li> <li>• VPC ID: vpc-12345678</li> <li>• CIDR block: 10.10.0.0/16</li> </ul>	<b>VPC</b> <ul style="list-style-type: none"> <li>• Name: VPC-B</li> <li>• Region: China (Hangzhou)</li> <li>• VPC ID: vpc-87654321</li> <li>• CIDR block: 192.168.0.0/16</li> </ul>
<b>Physical connection</b> <ul style="list-style-type: none"> <li>• VBR name: VPC-Beijing</li> <li>• VBR ID: vbr-12345678</li> <li>• Physical connection ID: pc-AAA</li> <li>• VLAN ID: 1000</li> </ul>	N/A

### Prerequisites

Make sure that you have completed the following configurations:

- You have accessed through the physical connection and route configurations are completed. The local data center has been connected to the VPC in Alibaba Cloud. For more information, see [Connect an on-premises IDC to a VPC through a physical connection](#).

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vbr-zze06ya5g r-zze06ya5g	Beijing-Daxing-A	vpc-b01aey9ec r-bp1mrtuawm	China (Hangzhou)	No	2Mbps	Pay-As-You-Go Created at Jan 16, 2019, 18:48:04 Connected at Jan 16, 2019, 19:22:56	<span style="color: green;">●</span> Initiator: Activated <span style="color: green;">●</span> Acceptor: Activated	

- Obtain the ID of the account to which the other VPC belongs.

### Step 1: Create a VBR for account B

To create a VBR for account B on the existing physical connection, follow these steps:

1. Use account A to log on to the [Express Connect console](#).
2. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).
3. On the Virtual Border Routers (VBRs) page, click Create VBR.
4. Configure the VBR.

The configurations in this tutorial are as follows. For more information, see [Create a virtual border router](#).

- **Account:** Select Another Account.



#### Note:

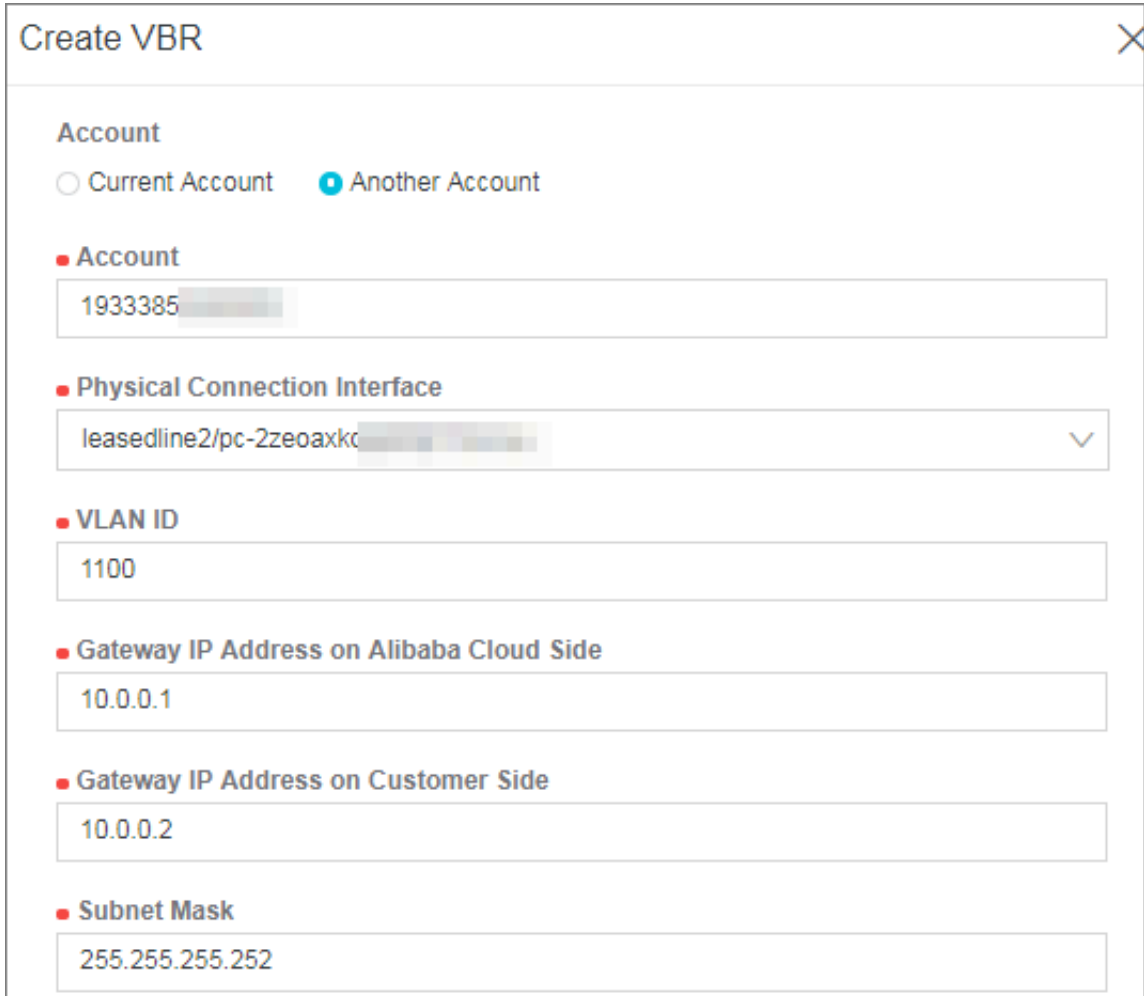
If the VPC you want to connect to the cloud and the physical connection belong to the same account, select Current Account.

- **Account:** Enter the account ID of the VPC to access.
- **Physical Connection Interface:** Select the applied physical connection interface.
- **VLAN ID:** Enter a VLAN ID. In this tutorial, enter 1100.
- **Gateway IP Address on Alibaba Cloud Side:** Enter the gateway address used by the VPC to access the local data center.
- **Gateway IP Address on Customer Side:** Enter the gateway address used by the local data center to access the VPC.
- **Subnet Mask:** Enter 255.255.255.252.



#### Note:

Ensure that the gateway addresses are in the same CIDR block and do not conflict with the CIDR blocks of the VPC and the local data center.



The screenshot shows a 'Create VBR' form with the following fields and values:

- Account:**  Current Account  Another Account
- Account:** 1933385
- Physical Connection Interface:** leasedline2/pc-2zeoaxk
- VLAN ID:** 1100
- Gateway IP Address on Alibaba Cloud Side:** 10.0.0.1
- Gateway IP Address on Customer Side:** 10.0.0.2
- Subnet Mask:** 255.255.255.252

## Step 2: Create a peering connection

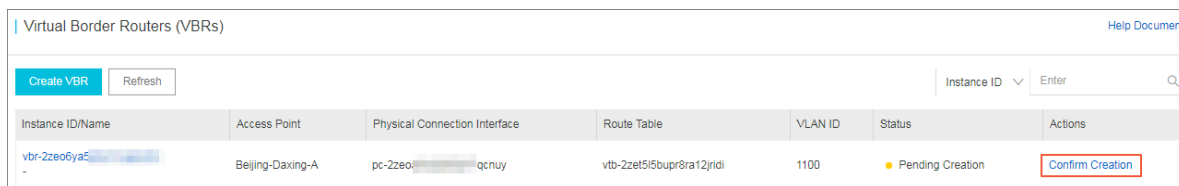
After you use account A to create a VBR for account B on the existing physical connection, you can use account B to build a peering connection between the VBR and the VPC.

To create a peering connection, follow these steps:

1. Use account B to log on to the [Express Connect console](#).
2. In the left-side navigation pane, click Physical Connections > Virtual Border Routers (VBRs).



3. Locate the VBR that you created, click Confirm Creation. View the configure information and click OK.

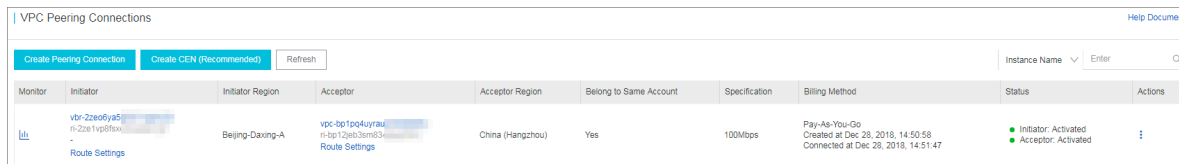


4. Click the VBR ID. On the VBR Details page, click Peering Connections.
5. Click Create Peering Connection.
6. Create a peering connection between the created VBR and the VPC you want to connect to the cloud.

The configurations in this tutorial are as follows. For more information, see [Interconnect a VPC and a VBR](#).

- **Account:** Select Same as Peer.
- **Connection Type:** Select VBR-to-VPC.
- **Routers to Create:** Select Initiator and Acceptor.
- **Local Region:** Select China (Beijing).
- **Local Access Point:** Select the access point of the physical connection.
- **Local VBR ID:** Select the created VBR.
- **Peer Region:** Select the region to which the target VPC belongs. In this tutorial, China (Hangzhou) is selected.
- **Peer VPC ID:** Select the VPC to connect.
- **Bandwidth:** Select a bandwidth for the intranet communication. In this tutorial, select 2 Mb.

The connection is successfully established if the status of both the acceptor and the initiator is activated.



### Step 3: Configure routes

After establishing the peering connection, you must configure routes in the VPC, VBR, and local data center.

**1. To configure routes for a VBR:**

a. On the VBR details page, click the Routes tab page, and then click Add Route.

**b. Add a route directing to the VPC:**

- **Destination Subnet:** Enter the CIDR block of the VPC. In this example, enter 192.168.0.0/16.
- **Next Hop Type:** Select VPC.
- **Next Hop:** Select the VPC.

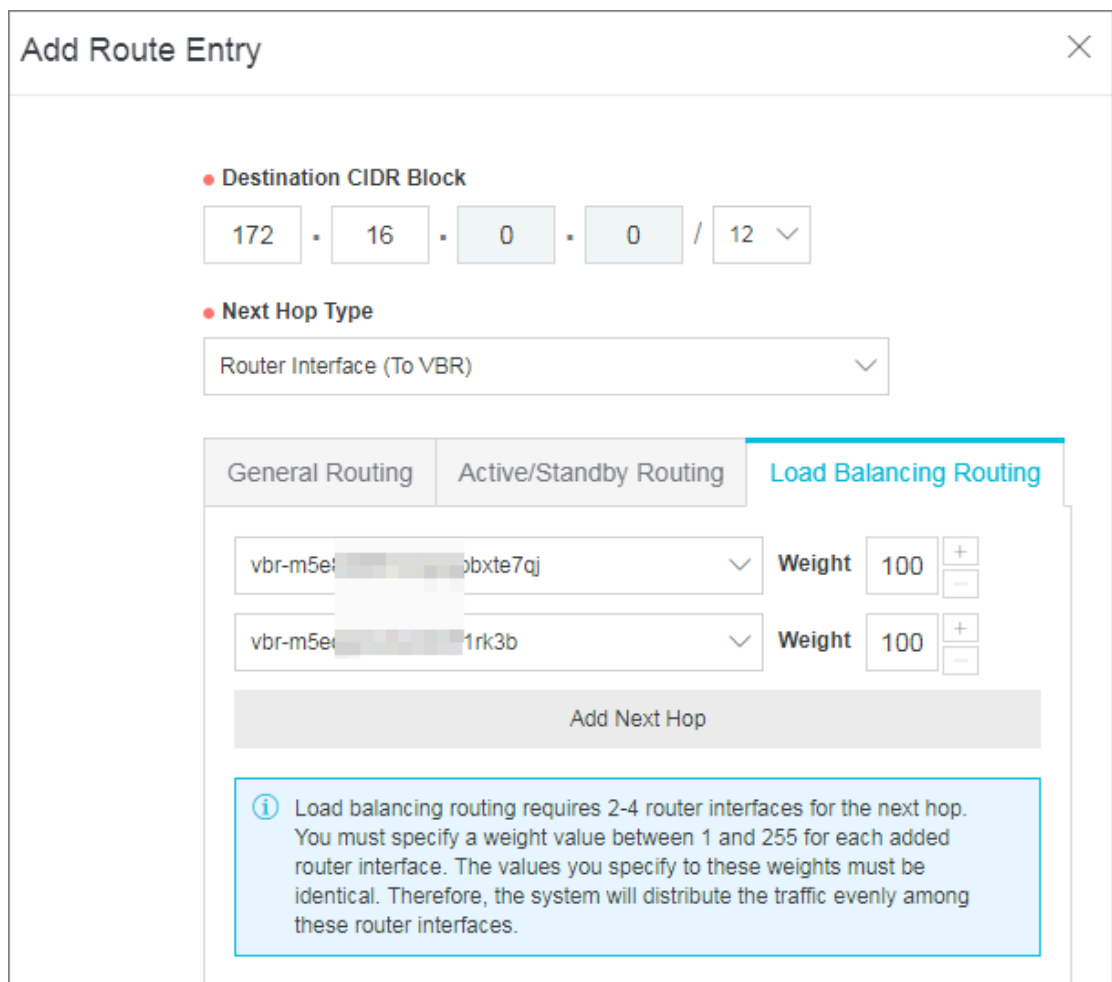
**c. Add a route pointing to the physical connection:**

- **Destination Subnet:** Enter the CIDR block of the on-premises IDC. In this example, enter 172.16.0.0/12.
- **Next Hop Type:** Select Physical Connection Interface.
- **Next Hop:** Select the physical connection interface.

d. Repeat the preceding steps to configure routes for the other VBR.

## 2. To configure a route for the VPC:

- a. On the VPC Peering Connections page, find the created peering connection, and click the VPC ID of the acceptor to open the VPC Details page. Here, you can view the ID of the route table.
- b. On the [Route Tables](#) page, click the target route table ID, and then click Add Route Entry.
- c. Configure a route:
  - Destination CIDR Block: Enter the CIDR block of the on-premises IDC. In this example, enter 172.16.0.0/12.
  - Next Hop Type: Select Router Interface (To VBR).
  - Next Hop: Select Load Balancing Routing, and then select the created VBR.



**Add Route Entry** ✕

• Destination CIDR Block

172 . 16 . 0 . 0 / 12 v

• Next Hop Type

Router Interface (To VBR) v

General Routing   Active/Standby Routing   **Load Balancing Routing**

vbr-m5e...obxte7qj v   Weight 100 + -

vbr-m5e...1rk3b v   Weight 100 + -

Add Next Hop

i Load balancing routing requires 2-4 router interfaces for the next hop. You must specify a weight value between 1 and 255 for each added router interface. The values you specify to these weights must be identical. Therefore, the system will distribute the traffic evenly among these router interfaces.

### d. Configure a route for the on-premises IDC.

You can configure a static route or BGP dynamic routing to forward data between the on-premises IDC to VBR:

- **Static route**

**Example:**

```
ip route 192 . 168 . 0 . 0 / 16 10 . 100 . 0 . 1
```

- **Dynamic routes**

You can also use BGP to forward data between the on-premises IDC and the VBR. For more information, see [Configure BGP](#).

**Note:**

The advertised CIDR block must be the CIDR block of the VPC that will be used to communicate with the on-premises IDC. In this example, enter 192.168.0.0/16.

**Step 4: Test the access**

After the VPC is connected to the local data center, test the speed of the physical connections to ensure that service needs are met. For more information, see [Test the network performance of a physical connection](#).

## 4 Use Express Connect to connect your network to Alibaba Cloud

---

### Overview

Express Connect allows you to implement a highly reliable intranet communication between your on-premises data center and Alibaba Cloud VPC, and between VPCs that are based in different regions. Specifically, Express Connect provides the following two key features:

- VPC-to-VPC connection

Express Connect supports intranet communication between two VPCs regardless of the regions they are based or the accounts under which they are billed. The connection between two VPCs that are based in the same region is provided free of charge, whereas the connection between two VPCs that are based in different regions incurs fees

To implement a connection between VPCs, Alibaba Cloud creates a Router Interface (RI) on the VRouter of each of the two VPCs, and uses its own backbone transmission network to achieve secure, reliable, and fast communication between the two VPCs. For more information, see [VPC interconnection](#).

- Physical connection

You can use a leased line to physically connect your on-premises data center to Alibaba Cloud. After that, you can create a VBR and RIs to achieve communication between the on-premises data center and a VPC in Alibaba Cloud. For more information, see [Connect an on-premises data center to a VPC through a physical connection](#).

### Access points

If you use a leased line to connect an on-premises data center to an Alibaba Cloud VPC, you only need to select an access point that is closest in geographic proximity to your on-premises data center. You do not need to build a physical connection between your on-premises data center and Alibaba Cloud VPC.

Access points include Alibaba Cloud access points and access points provided by Alibaba Cloud partners.

- **Alibaba Cloud access points**

You can view all [access points](#) of Alibaba Cloud in the Express Connect console. If an access point is available in the city where your on-premises data center is located, you can directly select this access point for the leased line connection.

Region	China North 1 (Qingdao)	China North 2 (Beijing)	China North 3 (Zhangjiakou)	China North 5 (Hohhot)	<b>China East 1 (Hangzhou)</b>
	China East 2 (Shanghai)	China South 1 (Shenzhen)	Hong Kong	Singapore	Australia (Sydney)
	Malaysia (Kuala Lumpur)	Indonesia (Jakarta)	Japan (Tokyo)	India (Mumbai)	US (Silicon Valley)
	US (Virginia)	Germany (Frankfurt)	UK(London)	UAE (Dubai)	
SP	<b>China Unicom</b>	China Telecom	China Mobile	Others	
Access Point	<b>Hangzhou-Yuhang-A- Ali</b>	Hangzhou-Linan-A- HuatongCloud	Hangzhou-Xiaoshan- A-CU	Hangzhou-Jiangan- B-21vianet	Hangzhou-Deqing-A- CU
Port Specification	<b>1G and below</b>	10G	The fee charged for renting resources changes based on the specification of a port. Apply for a port as required.		
Port Type	100Base-T	<b>1000Base-LX</b>			
Redundant Connection ID	<b>None</b> ▼				

- **Access points of Alibaba Cloud partners**

Some access points are also provided by Alibaba Cloud partners, and are connected with Alibaba Cloud through dedicated physical lines. This means that if no Alibaba Cloud access point is available, you can select an access point provided by one of our partners. To obtain the information about your selected physical connection, contact the Alibaba Cloud partner.

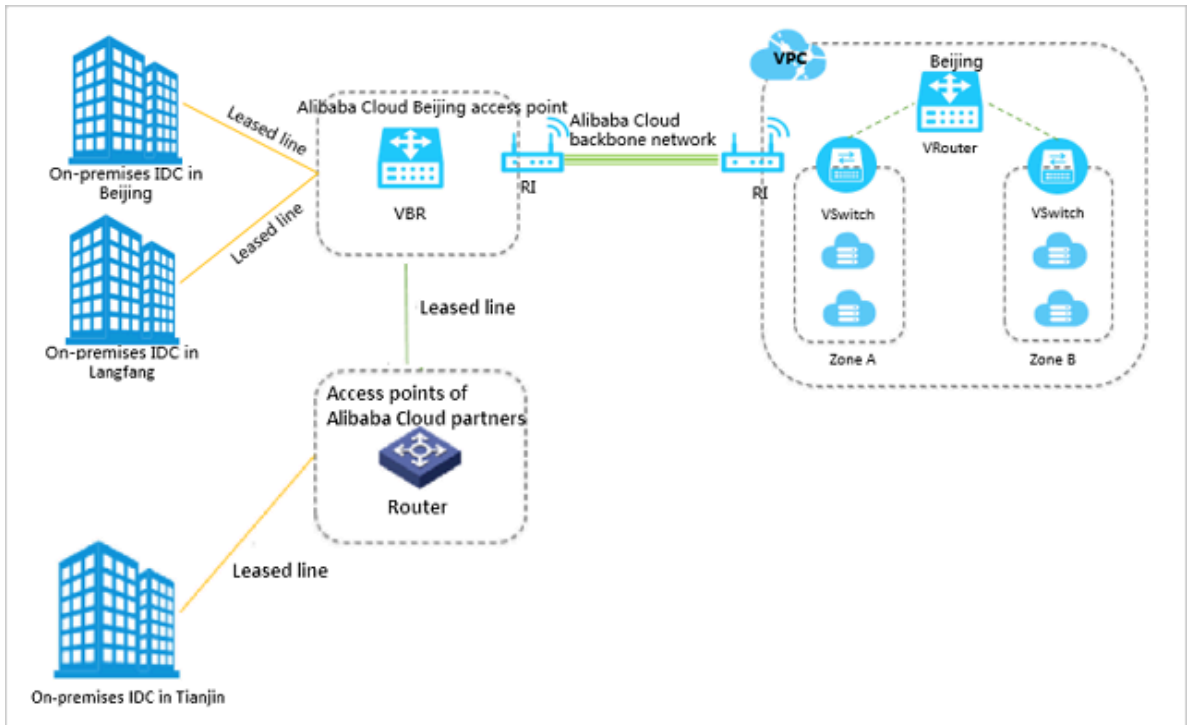
As a best practice, if no Alibaba Cloud access point or access point provided by an Alibaba Cloud partner is available directly in the city where your on-premises data center is located, we recommend that you select an access point that is nearest to the city where your on-premises data center is based.

For example, the following figure shows two on-premises data center centers (one in Beijing, one in Langfang) connected to an Alibaba Cloud access point based

in Beijing. Additionally, the figure shows an on-premises data center located in Tianjin that is connected to Alibaba Cloud VPC through a leased line connected to the access point of an Alibaba Cloud partner. Note that the lines in yellow are leased lines that need to be installed by your service provider.



Note:



### Access global resources from one point

By connecting to any one access point, you can connect your resources to Alibaba Cloud VPCs around the globe through the access point.

For example, you want to connect an on-premises data center in Beijing to a VPC in Beijing and a VPC in Shenzhen through physical connection. To implement that, you only need to use a leased line to connect the on-premises data center to an Alibaba Cloud Beijing access point, and create two RIs respectively connecting to the two VPCs on the VBR.



Note:

In the following figure, only the lines in yellow need to be installed by your service provider.

