

Alibaba Cloud Express Connect

Best Practices

Issue: 20180930

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.	 Danger: 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.	 Warning: 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.	 Note: 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.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
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 Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	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....	2
3 Multi-VPC physical connection.....	11
4 Use Express Connect to achieve nearby access and one-point access to global resources.....	18

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 bar, 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/HewlettPackard/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.

Tool name	Main parameter	Parameter description
	-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"> We recommend that you set the value to 1 when testing pps. We recommend that you set the value to 1400 when testing bps (bit per second).

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, $\text{pps} = \frac{\text{the number of packets successfully sent out}}{\text{the duration of test}}$.

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.

Tool name	Main parameter	Description
	-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 -i 1 -p 16001 -A 7
iPerf3 -u -l 16 -b 100m -t 120 -c 172.16.0.9 -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 test 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 Multi-VPC physical connection

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

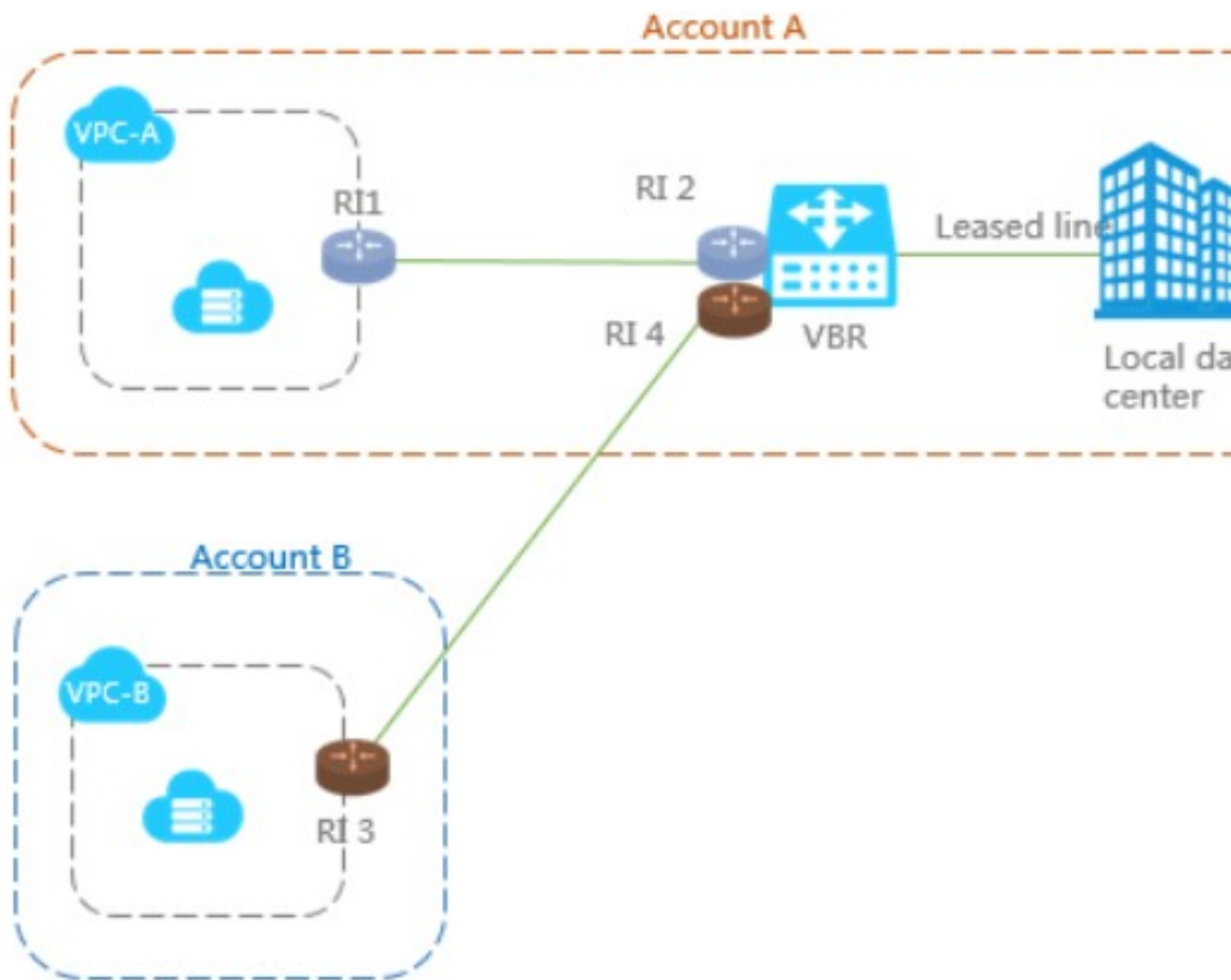
**Note:**

Now a leased line can be connected to 5 VPCs at most. You can open a ticket to increase the quota.

Scenario

A company has opened account A on Alibaba Cloud and created VPC-A. Account A already opened a leased line that connects the local data center 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 there is already a leased line under account A that connects the local data center to the access point of Alibaba Cloud, VPC-B under account B of the subsidiary can reuse the leased line and VBR of account A. The company only needs to create a router interface for the VBR under account A and the VPC under account B respectively and connect the two interfaces, as shown in the following figure.



In this tutorial, VPC and leased line configurations are as follows:

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

Account A	Account B
<ul style="list-style-type: none"> VLAN ID: 1000 	

Step 1: Create router interfaces

Create a router interface on the VBR under account A and the VPC under account B respectively, so that the VRouter of the VPC and the VBR can send messages to each other through the router interfaces. For more information, see Router interfaces.



Note:

The router interface on the VBR must act as the initiator.

Create the initiator router interface

Follow these steps to create a router interface for the VBR:

1. Log on to the [Express Connect console](#).
2. In the left-side navigation pane, select **Router Interface**. Click **Create Router Interface**.
3. Configure the router interface. This tutorial uses the following configurations.
 - Scenario: Physical Access.
 - Router Creation: Create Initiator.
 - Router Type: VRouter
 - Local Region: China (Beijing).
 - Access Point: Beijing-Daxing-A.
 - VBR ID: vbr-12345678.
 - Peer Region: China (Hangzhou).
 - Peer Router Type: VRouter.
 - Specification: Large.1(1Gb).
4. Click **Buy Now** to complete the creation.

Go back to the **Router Interface** page after about one minute and select the target region.

Then you can see the newly created router interface under account A. In this tutorial, the ID of the router interface under account A is ri-AAA.

Create the receiver router interface

Follow these steps to create the receiver router interface:

1. Use account B to log on to the [Express Connect console](#).

2. In the left-side navigation pane, select **Router Interface**. Click **Create Router Interface**.

3. Configure the router interface. This tutorial uses the following configurations.

- Billing Method: Pay-As-You-Go.
- Scenario: Physical Access.
- Router Creation: Create Receiver.
- Router Type: VRouter
- Local Region: China (Hangzhou).
- VPC ID: vpc-87654321.
- Peer Region: China (Beijing).
- Peer Access Point: Beijing-Daxing-A.
- Peer Router Type: VRouter

4. Click **Buy Now**.

Go back to the **Router Interface** page after about one minute and select the target region.

Then you can see the newly created router interface under account B. In this tutorial, the ID of the router interface under account B is ri-BBB.

Step 2: Initiate a connection

After creating router interfaces, you need to add peer router interfaces and initiate a connection.

Only the initiator router interface can initiate a connection.

Add peer router interface for the VPC under account B

Follow these steps to create a router interface for the VPC of account B:

1. Use account B to log on to the [Express Connect console](#).
2. In the left-side navigation pane, select **Router Interface**.
3. Select the region where the target router interface is located and find the target router interface.
4. Click **Add** in the **Peer Router Interface** column or click **More > Edit Peer Interface**.
5. In the displayed dialog box, select **Other Account** and enter the account ID (12345678), VBR ID (vbr-AAA), and router interface ID (ri-AAA) of account A.

Add information of the peer router interface

Account : ☐ Current Account ☒ Other Account

Peer VRouter Type : **VBR**

* Peer Account ID :

* Peer VRouter ID :

* Peer Router Interface ID :

OK Cancel

Add peer router interface for the router interface on the VBR under account A and initiate a connection

Follow these steps to add peer router interface for the router interface on the VBR under account A and initiate a connection:

1. Use account A to log on to the [Express Connect console](#).
2. In the left-side navigation pane, select **Router Interface**.
3. Click the region where the target router interface is located and find the target router interface.
4. Click **Add** in the **Peer Router Interface** column or click **More > Edit Peer Interface**.
5. In the displayed dialog box, select **Other Account** and enter the account ID (87654321), VBR ID (vbr-BBB), and router interface ID (ri-BBB) of account B.

路由器接口ID

请输入路由器接口ID进行精确查询

搜索

ID/名称	监控	路由器ID/类型(所有)	本端位置	对端路由器接口	对端位置	连接角色	规格	状态(所有)	付费类型	操作
ri- <div></div>	<div></div>	<div>vrt-2zepuy8qbrq6yhdje53t6</div> <div>VPC路由器</div>	华北 2	ri- <div></div>	北京-大兴-A	接收端	Negative	已激活	按量付费 2018-01-04 21:35:32 连接	<div>路由配置</div> <div>冻结</div> <div>更多</div>

6. Find the router interface of the VBR, and click **Initiate a Connection**.

The connection is established successfully when the status of the router interfaces ri-AAA and ri-BBB changes to **Active**.

Step 3: Configure routes

After creating the router interfaces, you need to configure routes so that the local data center can communicate with the VPC.

Configure routes on the VBR

Follow these steps to forward the traffic, destined for the on-premises IDC (CIDR block: 172.16.0.0/12), from the VBR to the leased line:

1. Use account A to log on to the [Express Connect console](#).
2. In the left-side navigation pane, click **Virtual Border Router**.
3. Find the target VBR and click **Manage**. Then click **Add Route Entry** on the page of VBR details.
4. Configure the route. In this tutorial, the route configurations are as follows:
 - **Destination CIDR Block:** The CIDR block of the local data center. In this tutorial, enter 172.16.0.0/12.
 - **Next Hop Direction:** Select To VPC and then select the existing leased line.

Follow these steps to forward the traffic, destined for the VPC (CIDR block: 192.168.0.0/16), from the VBR to the VPC:

1. Use account A to log on to the [Express Connect console](#).
2. In the left-side navigation pane, click **Virtual Border Router**.
3. Find the target VBR and click **Manage**. Then click **Add Route Entry** on the page of VBR details.
4. Configure a route. In this tutorial, the route configurations are as follows:
 - **Destination CIDR Block:** The CIDR block of the peer VPC. In this tutorial, enter 192.168.0.0/16.
 - **Next Hop Direction:** Select To VPC.
 - **Next Hop:** Select the router interface of the VBR. In this tutorial, select ri-BBB.

Configure the route on the VPC

Follow these steps to forward the traffic, destined for the local data center (CIDR block: 172.16.0.0/12), from the VPC to the VBR:

1. Use account B to log on to the [Express Connect console](#).

2. In the left-side navigation pane, click **Router Interface**. Find the target router interface and click **Router Configuration**.

3. Configure the route. In this tutorial, the route configurations are as follows:

- **Destination CIDR Block:** The CIDR block of the local data center. In this tutorial, enter 172.16.0.0/12.
- **Next Hop Type:** Select Router Interface.
- **Router Interface:** Select the router interface of VPC-B. In this tutorial, select ri-AAA.

Configure the route on the local data center

Till now, the route configuration on Alibaba Cloud has been completed. You still need to add a route entry for the VPC CIDR block in the physical access device of the customer. The destination CIDR block is the Alibaba Cloud-side IP address. For example:

```
ip route 192.168.0.0/16 10.100.0.1
```

You can also configure BGP dynamic routing to point traffic to the border router:

1. Create BGP peer groups. For more information, see [Manage BGP peer groups](#).
2. Add BGP peers to the BGP groups, see [Manage BGP peers](#).
3. Advertise BGP network, see [Advertise BGP network](#).



Note:

Make sure the destination CIDR block of the BGP routing is the same as that of the static route. In this tutorial, it is 192.168.0.0/16.

Till now, all configurations have been completed.

Step 5: Performance test

After the two networks are connected with each other, test the speed of the leased line to ensure it can meet service needs. For more information, see [Test the network performance of a physical connection](#).

4 Use Express Connect to achieve nearby access and one-point access to global resources

Overview

Express Connect helps you build high-quality and high-reliability intranet communication between local data centers and VPCs in different regions of Alibaba Cloud. Express Connect has the following key features:

- VPC interconnection

Express Connect supports intranet communication between two VPCs regardless of their regions and accounts. Same-region VPC interconnection is free of charge.

Alibaba Cloud creates a [Router Interface](#) on each VRouter of the two VPCs, respectively, to achieve secure, reliable, fast, and convenient communication between the two VPCs. For more information, see [VPC interconnection](#).

- Physical access

You can use a leased line to physically connect your local data center to Alibaba Cloud, and create a VBR and router interfaces to achieve communication between the local data center and a VPC in Alibaba Cloud. For more information, see [Physical access](#).

Nearby access

When using a leased line to connect a local data center to a VPC, you only need to select an access point nearest to the local data center, and do not need to build a physical line between the local data center and the VPC. 其中接入点分为阿里云自有接入点和合作伙伴接入点。

阿里云自有接入点

You can obtain information about access points through [The map about Express Connect](#) or [Leased line access points](#) on the Express Connect console. If there is an access point in the city where the local data center is located, you can directly apply for leased line access to the access point.

合作伙伴接入点

合作伙伴的接入点已经提前和阿里云建立了专线连接，您只需要在本地IDC和合作伙伴接入点间建立专线连接就可以实现本地IDC和云上VPC间的内网互连。您可以参考高速通道控制台的#####，并联系阿里云合作伙伴获取专线接入的相关信息。

If there is no access point in the city where your local data center is located, you can select a nearby access point and establish connection between the local data center and the access point.

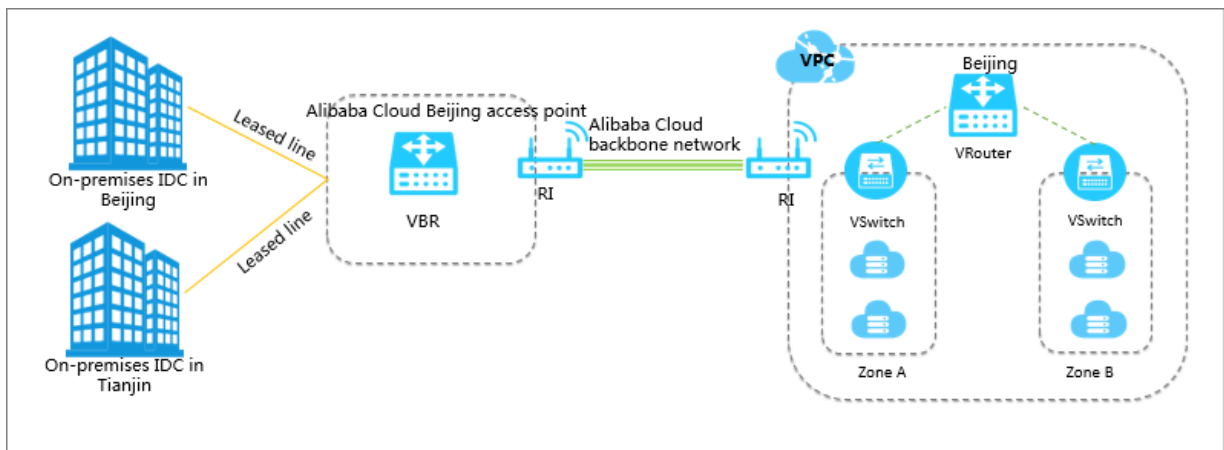
For example, a user has a local data center in Beijing and a local data center in Tianjin, respectively, the user can achieve physical access through the following methods:

- Because there is an access point in Beijing, the user only needs to connect the local data center in Beijing to the Alibaba Cloud Beijing access point.
- Because there is no access point in Tianjin, but the local data center is near to the Alibaba Cloud Beijing access point, the user can use a leased line to connect the local data center in Tianjin to the Alibaba Cloud Beijing access point.
- 廊坊既没有阿里云的自有接入点，也没有合作伙伴接入点，由于位于廊坊的IDC距离阿里云北京接入点距离较近，该用户可以使用专线把位于廊坊的IDC和阿里云北京接入点连接。



Note:

In the following figure, only the lines in orange need to be constructed by a carrier.



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, a user wants to connect a local data center in Beijing to a VPC in Beijing and a VPC in Shenzhen through physical access. The user only need to use a leased line to connect the local

data center to the Alibaba Cloud Beijing access point, and create two router interfaces respectively connecting to the two VPCs on the VBR.

**Note:**

In the following figure, only the lines in orange need to be constructed by a carrier.

