Enterprise Router

Service Overview

Issue	01
Date	2024-01-15

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
             Qianzhong Avenue
             Gui'an New District
             Gui Zhou 550029
             People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What's an Enterprise Router?

An enterprise router connects virtual private clouds (VPCs) and on-premises networks to build a central hub network. It has high specifications, provides high bandwidth, and delivers high performance. Enterprise routers use the Border Gateway Protocol (BGP) to learn, dynamically select, or switch between routes, thereby ensuring the service continuity and significantly improving network scalability and O&M efficiency.

Figure 1-1 and **Figure 1-2** show the networks with and without enterprise routers, respectively. **Table 1-1** compares the two networks.

Figure 1-1 A network without enterprise routers
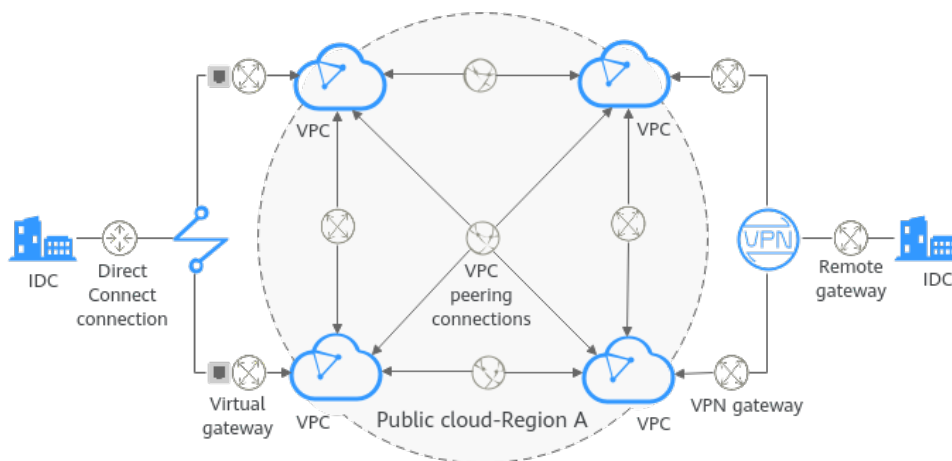
Figure 1-2 A network with enterprise routers
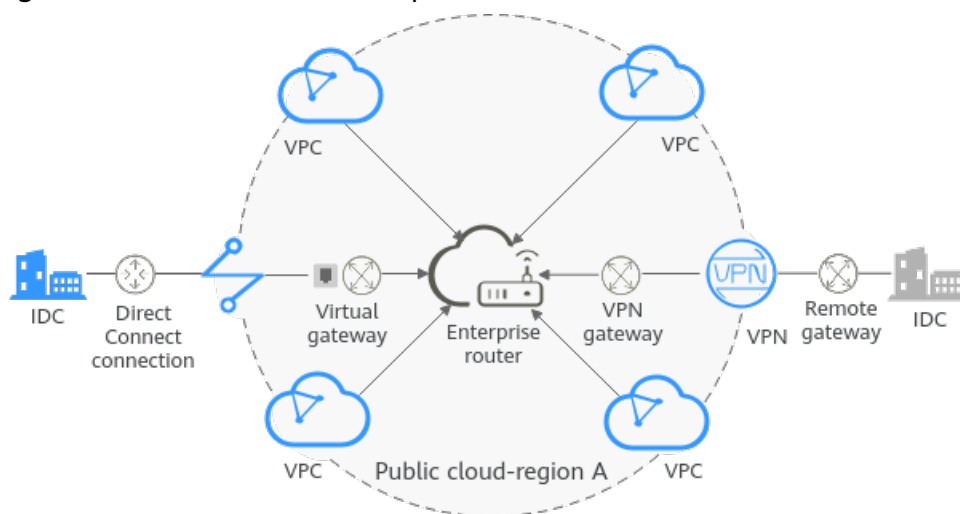
Table 1-1 Comparison between the networks with and without enterprise routers

Item	Without Enterprise Routers	With Enterprise Routers	Benefits of Using Enterprise Routers
Communications among VPCs in the same region	• Create six VPC peering connections between these four VPCs in the same region. • Add 12 routes, with three routes for each VPC to communicate with the other three VPCs.	• Attach the four VPCs to one enterprise router. This router can then handle the traffic from and to all the connected VPCs. • Add routes to the route tables of these four VPCs for routing traffic through the enterprise router. The enterprise router can automatically learn the VPC CIDR blocks and add them to its route table.	• There is no need to configure a large number of VPC peering connections. • Fewer routes need to be added, simplifying the maintenance.

Item	Without Enterprise Routers	With Enterprise Routers	Benefits of Using Enterprise Routers
Communications between an on-premises data center and VPCs	Establish Direct Connect or VPN connections between each VPC and the data center.	Attach the Direct Connect or VPN connection to the enterprise router. These VPCs can then share the connection.	- Route propagation simplifies the route configuration and the O&M. - Multiple lines work in load-sharing or active/standby mode to achieve higher availability.

The comparison shows that the network with enterprise routers is simpler and highly scalable and is also easier to maintain.

2 Why Using Enterprise Routers

Enterprise routers have the following advantages:

High Performance

Enterprise routers use exclusive resources and are deployed in clusters to deliver the highest possible performance for workloads on large-scale networks.

High Availability

Enterprise routers can be deployed in multiple availability zones to work in active-active or multi-active mode, thereby ensuring service continuity and real-time seamless switchovers.

Simplified Management

Enterprise routers can connect to multiple VPCs, Direct Connect connections, or enterprise routers in different regions and route traffic among them. The network topology is simpler and the network is easier to manage and maintain.

- For cross-VPC communications, you only need to maintain the route tables on the VPCs without requiring so many VPC peering connections.

- For communications between VPCs and an on-premises data center, multiple VPCs can connect to an enterprise router and then communicate with the data center over one Direct Connect or VPN connection. You do not need to establish a Direct Connect or VPN connection between the data center and each of the VPCs.

- Enterprise routers can automatically learn, update, and synchronize routes, eliminating the need to manually configure or update routes whenever the network topology changes.

Seamless Failover Between Lines

Enterprise routers use the Border Gateway Protocol (BGP) to select the best path from multiple lines working in load-sharing or active/standby mode. If a single line fails, services can be failed over to another functioning line within seconds to ensure service continuity.

3 When to Use Enterprise Routers

You can use enterprise routers to build cloud, on-premises, or hybrid networks. Here are some typical application scenarios:

- **Scenario 1: Multiple VPCs communicating or not communicating with each other on the cloud, but communicating with the on-premises data center through a Direct Connect connection**
- **Scenario 2: Dynamic switchover between multiple Direct Connect connections**
- **Scenario 3: Active/Standby Direct Connect and VPN connections**

Scenario 1: Multiple VPCs communicating or not communicating with each other on the cloud, but communicating with the on-premises data center through a Direct Connect connection

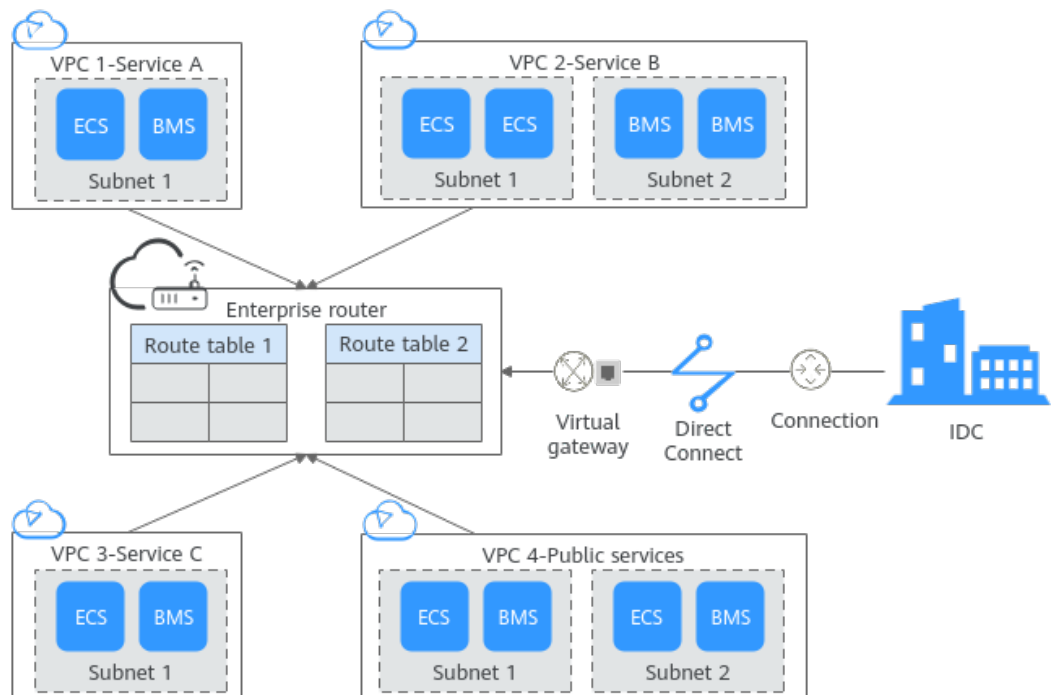**Figure 3-1** Diagram for scenario 1

Table 3-1 Using enterprise routers in scenario 1

Customer Requirements	Multiple service networks communicate or do not communicate with each other on the cloud but communicate with the on-premises data center. Suppose you require three VPCs for running the workloads on the public cloud, and the three VPCs (services A, B, and C) need to access public services in VPC 4 and your on-premises data center.
Pain Points	- VPC peering connections are required for communications among these VPCs, but they will complicate the network topology and make the network hard to manage. - VPC peering connections and routes are required for the public service VPC to communicate with each VPC. However, VPC peering connections do not fit in large-scale networks because of the following limitations: – A maximum of 50 VPC peering connections can be created in one region. – A VPC route table can have a maximum of 200 routes. - Direct Connect connections are required for each VPC to communicate with the on-premises data center, but they will incur high costs.
Benefits of Using Enterprise Routers	- VPCs can be associated with different route tables on the enterprise router to enable communication or isolation. The network topology is simple and easy to manage. - Enterprise routers can route traffic among all the connected VPCs without the need to configure a large number of VPC peering connections. – Each enterprise router can have a maximum of 2,000 routes in each route table, making it ideal for large-scale complex networks. - Multiple VPCs can access the on-premises data center over a Direct Connect connection, eliminating the need to configure multiple Direct Connect connections and reducing the costs.

Scenario 2: Dynamic switchover between multiple Direct Connect connections

Figure 3-2 Diagram for scenario 2
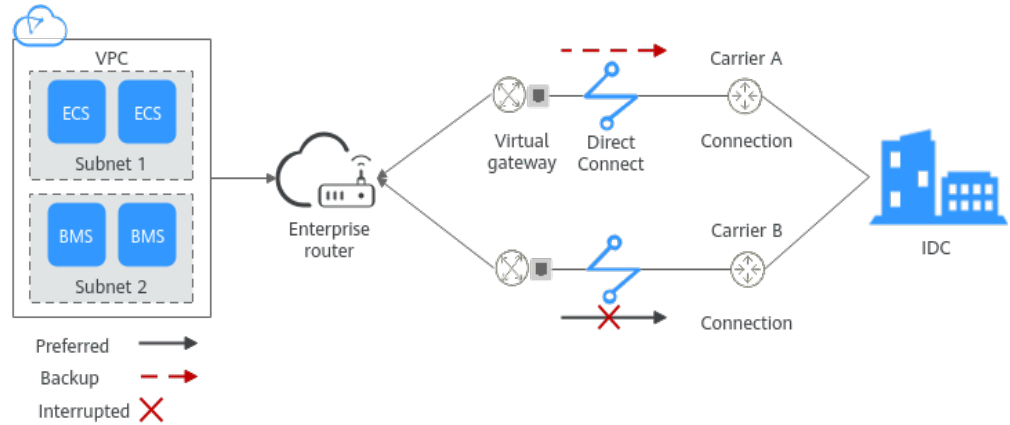
Table 3-2 Using enterprise routers in scenario 2

Customer Requirements	Some services run on the public cloud and some in the on-premises data center. Two independent high-bandwidth Direct Connect connections are deployed between the public cloud and the data center to enable communication between them.
Pain Points	Two Direct Connect connections are independent of each other and cannot work in load-sharing or active/standby mode.
Benefits of Using Enterprise Routers	Direct Connect connections are connected to the enterprise router. • Two Direct Connect connections can work in load-sharing mode to ensure high bandwidth and reliability. • Two Direct Connect connections can also work in active/standby mode. If one of the connections becomes unavailable, services are switched over to the other available connection within seconds, preventing service interruptions.

Scenario 3: Active/Standby Direct Connect and VPN connections

Figure 3-3 Diagram for scenario 3
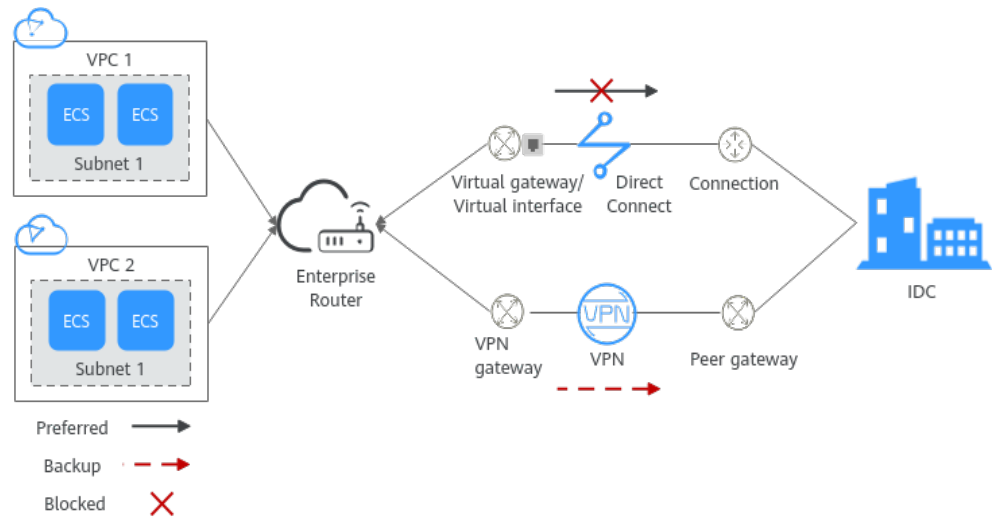
Table 3-3 Using enterprise routers in scenario 3

Customer Requirements	You are running workloads in your on-premises data center and on the public cloud. A single Direct Connect connection connects your on-premises data center to the cloud, which cannot ensure reliability.
Pain Points	You cannot afford another Direct Connect connection.
Benefits of Using Enterprise Routers	In this example, there are two connections, one Direct Connect connection and a VPN connection. Enterprise Router, Direct Connect, and VPC are used to build a hybrid cloud. When the Direct Connect connection becomes faulty, the VPN connection takes over to ensure that connectivity is not interrupted.

4 Functions

An enterprise router provides the functions listed in **Table 4-1**, allowing you to:

- Manage attachments, custom route tables, associations, propagations, and routes.
- Manage permissions, tags, and quota to improve service security.

Table 4-1 Functions of an enterprise router

Function	Description	Reference
Enterprise routers	An enterprise router is a high-performance centralized router that supports route learning. When creating an enterprise router, you can set parameters such as its region, AZ, and name. After an enterprise router is created, you can still change its parameters based on service requirements.	**Creating an Enterprise Router**
Attachments	You can add attachments to attach network instances to the enterprise router. Different network instances are attached through different consoles. • VPCs are attached through the Enterprise Router console. • Virtual gateways are attached through the Direct Connect console. • VPN gateways are attached through the VPN console.	**Attachment Overview**
Route tables	Route tables are used by enterprise routers to forward packets. Route tables contain associations, propagations, and routes. An enterprise router can have multiple route tables. You can associate attachments with different route tables to enable communication or isolation between network instances.	**Route Table Overview**

Function	Description	Reference
Associations	Associations are created manually or automatically to associate attachments with enterprise router route tables. ● Manually: Select a route table and create an association for an attachment in the route table. ● Automatically: You just need to enable **Default Route Table Association** and specify the default route table. The system automatically creates an association for an attachment in the default route table.	**Association Overview**
Propagations	A propagation is created manually or automatically to enable an enterprise router to learn the routes to an associated attachment. ● Manually: Select a route table and create a propagation for an attachment in the route table. ● Automatically: You just need to enable **Default Route Table Propagation** and specify the default route table. A propagation is automatically created for an attachment in the default propagation route table.	**Propagation Overview**
Routes	A route consists of information such as the destination address, next hop, and route type. There are two types of routes: ● Propagated routes ● Static routes	**Route Overview**
Sharing	You are the owner of the enterprise router, and other accounts are the users of your enterprise router. After you share your enterprise router with other accounts, these other users can attach their network instances to your enterprise router, so that their network instances can access your enterprise router. This allows VPCs in the same region but different accounts to be attached to the same enterprise router.	**Sharing Overview**

Function	Description	Reference
Flow logs	The flow log function records traffic logs of attachments on enterprise routers in real time. The logs allow you to monitor the network traffic of attachments and analyze network attacks, helping you achieve efficient O&M. Flow logs can capture traffic of the following types of attachments: ● VPC ● Virtual gateway ● VPN gateway	**Flow Log Overview**
Monitoring	You can use Cloud Eye to monitor the network status of enterprise routers and their attachments.	**Supported Metrics**
Auditing	You can use Cloud Trace Service (CTS) to record operations associated with your enterprise routers for future query, audit, and backtracking.	**Key Operations Recorded by CTS**
Permissions	You can use Identity and Access Management (IAM) to set different permissions for employees in your enterprise to control their access to enterprise routers.	**Creating a User and Granting Permissions**
Tags	Tags are used to identify cloud resources. You can add tags to enterprise routers and route tables.	**Tag Overview**
Quotas	Quotas can limit the number or amount of resources available to users, for example, how many enterprise routers can be created, how many attachments can be created for each enterprise router, and how many routes can be added to each route table.	**Quotas**

5 How Enterprise Routers Work

You can attach your network connections to an enterprise router to quickly construct diversified networks and meet various service requirements. **Figure 5-1** shows the process of using an enterprise router, including creating an enterprise router, adding attachments to the enterprise router, and configure routes.

Currently, enterprise routers support the following attachments:

- **VPC attachment**: Attach VPCs from the same region as that of an enterprise router to the router.
- **Virtual gateway attachment**: Attach Direct Connect virtual gateways from the same region as that of an enterprise router to the router.
- **VPN gateway attachment**: Attach VPN gateways from the same region as that of an enterprise router to the router.

Figure 5-1 Processing of using an enterprise router
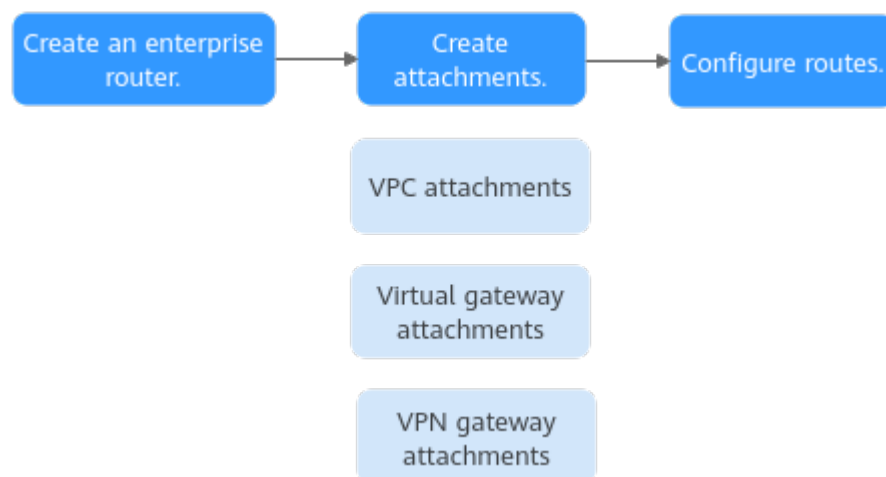
Figure 5-2 shows how an enterprise router works. **Table 5-2** describes the traffic flows in detail if an enterprise router is used for networking.

Figure 5-2 How an enterprise router works
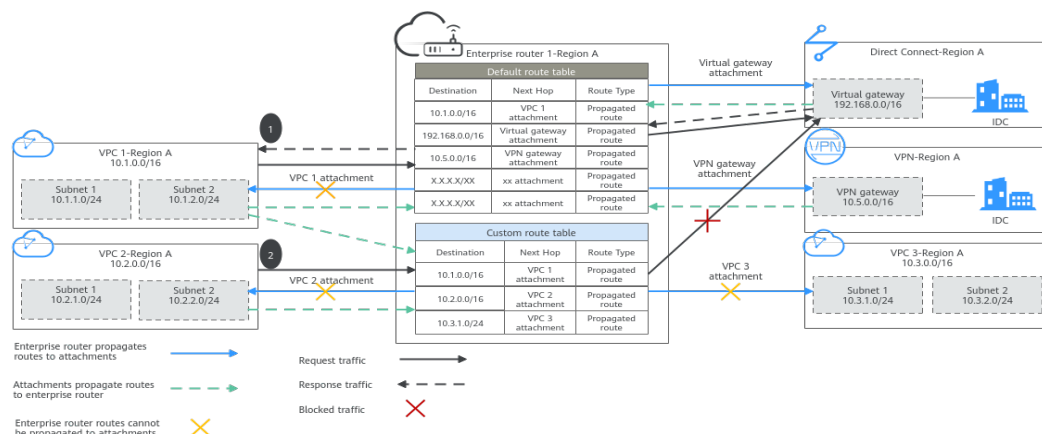
Table 5-1 Network traffic flows

No.	Route	Description
1	Request from VPC 1 to Direct Connect virtual gateway	After receiving requests from VPC 1 to the virtual gateway, enterprise router 1 searches the default route table for the route to the virtual gateway and forwards the requests through this route.
	Response from Direct Connect virtual gateway to VPC 1	After receiving responses from the virtual gateway to VPC 1, enterprise router 1 searches the default route table for the route to VPC 1 and forwards the responses through this route.
2	Request from VPC 2 to Direct Connect virtual gateway	Enterprise router 1 cannot forward requests from VPC 2 to the virtual gateway because the custom route table of enterprise router 1 that is associated with VPC 2 does not contain the route to this virtual gateway.

Table 5-2 Working principles of an enterprise router

No.	Action	Description
1	Add **attachments** to the enterprise router.	Attach network instances to enterprise router 1 in region A. ● Network instances from the same region 　– **VPC attachments**: VPC 1, VPC 2, and VPC 3 　– **Virtual gateway attachment**: Virtual gateway 　– **VPN gateway attachment**: VPN gateway

No.	Action	Description
2	Associate the **attachments** with the **route tables** of the enterprise router. Each attachment can only be associated with one route table.	• Associate VPC 1 with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from VPC 1 attachment to the default route table and custom route table of enterprise router 1. • Associate VPC 2 with the custom route table of enterprise router 1 and create a propagation to propagate the routes learned from VPC 2 to the custom route table.
3	Create **propagation** for the attachments to propagate the **routes** to the enterprise router's **route tables**. You can create multiple propagation records for the same attachment.	• Associate VPC 3 with the custom route table of enterprise router 1, and add static routes for VPC 3 to this custom route table. • Associate the Direct Connect virtual gateway with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from the virtual gateway attachment to the default route table. • Associate the VPN gateway with the default route table of enterprise router 1 and create a propagation to propagate the routes learned from the VPN gateway attachment to the default route table.

Attachments

If you want to attach a network instance to an enterprise router, you need to add an attachment of a specific type to the enterprise router. The attachment type varies according to the network instance, as listed in **Table 5-3**.

Table 5-3 Attachments

Attachment Type	Network Instance
VPC attachment	VPC
Virtual gateway attachment	Virtual gateway of Direct Connect
VPN gateway attachment	VPN gateway

Route Tables

Route tables are used by enterprise routers to forward packets. Route tables contain associations, propagations, and routes. Route tables are classified into custom and default route tables, as detailed in **Table 5-4**.

Table 5-4 Route tables

Route Table	Description
Custom route table	You can create multiple custom route tables on an enterprise router and use different routes for flexible communication and isolation between network instances.
Default route table	If you enable **Default Route Table Association** and **Default Route Table Propagation**, the system then automatically associates and propagates new attachments with the default route table. You can specify a custom route table as the default route table. If you do not specify any route table as the default route table, the system automatically creates a default route table.

Associations

Each attachment can be associated with one route table for:

- Packet forwarding: Packets from the attachment are forwarded through the routes specified in the associated route table.
- Route propagation: The routes in the associated route tables are automatically propagated to the route table of the attachment.

Not all attachments can propagate routes. For details, see **Table 5-5**.

Table 5-5 Associations

Attachment	Route Learning
VPC	Not supported
Virtual gateway	Supported
VPN gateway	Supported

Route Propagation

You can create a propagation for each attachment to propagate routes to one or more route tables on an enterprise router.

For VPC attachments, their CIDR blocks are propagated to the enterprise router. For other attachments, all routes are propagated to the enterprise router. For details, see **Table 5-6**.

Table 5-6 Propagation

Attachment	Propagated Routes to Enterprise Router
VPC	VPC CIDR blocks
Virtual gateway	All routes
VPN gateway	All routes

Routes

Routes are used to forward packets. A route contains information such as the destination, next hop, and route type. **Table 5-7** describes the routes of different types.

Table 5-7 Routes

Route Type	Description	Attachment
Propagated routes	Propagated routes are automatically learned through propagation and cannot be modified or deleted.	• VPC • Virtual gateway • VPN gateway
Static routes	Static routes are manually created and can be modified or deleted.	• VPC

6 Billing

Enterprise routers are free of charge. If you create attachments to an enterprise router, you will be charged for attachments and the amount of traffic flowing through the attachments. For details, see **Table 6-1**.

You can use an enterprise router to connect different types of attachments, including VPC, virtual gateway, and VPN gateway. In addition, an enterprise router can connect attachments from different accounts.

Table 6-1 Enterprise router billing items

Billing Item	Attachment Type	Description
Attachment	- VPC - Virtual gateway - VPN gateway	Hourly billing starts when an attachment is created and stops when the attachment is deleted. If an attachment is created to a shared enterprise router, hourly billing starts when the enterprise router owner accepts the attachment. An attachment of an enterprise router is billed hourly and only in full hours. If the usage duration is less than one hour, the attachment is still billed for a full hour. The following uses a VPC attachment as an example. - Scenario 1: You added a VPC attachment to an enterprise router at 12:36 on July 6, 2022 and deleted the attachment at 12:57 on July 6, 2022. In this case, you need to pay for a full hour. - Scenario 2: You added a VPC attachment to an enterprise router at 12:59 on July 6, 2022 and deleted the attachment at 13:01 on July 6, 2022. In this case, your usage spanned 2 clock hours, so you need to pay for 2 full hours. The price of different types of attachments is subject to that displayed on the console.
Traffic	- VPC - Virtual gateway - VPN gateway	The amount of traffic flows from an attachment to an enterprise router (inbound traffic) is billed. The price of traffic per GB is subject to that displayed on the console.

An attachment creator pays for its attachment and used traffic.

For example, if a shared enterprise router has VPC attachments from its owner and other accounts. If the owner creates attachments to the enterprise router, the owner pays for the attachments and used traffic. If the other accounts create attachments to the enterprise router, these accounts pay for the attachments and used traffic.

◻ NOTE

Only VPC attachments can be added to shared enterprise routers.

7 Permissions

If you need to assign different permissions to employees in your enterprise to control their access to your cloud resources, you can use the Identity and Access Management (IAM) for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control.

On the IAM console, you can create IAM users and assign permissions to control their access to specific resources. For example, you can create IAM users for software developers and assign permissions to allow them to use enterprise router resources but disallow them from performing any high-risk operations such as deleting such resources.

IAM is free of charge.

For more information, see **IAM Service Overview**.

Enterprise Router Permissions

By default, new IAM users do not have any permissions assigned. You need to add them to one or more groups and attach policies or roles to these groups so that these users can inherit permissions from the groups and perform specified operations on cloud services.

An enterprise router is a project-level service deployed in a specific region. You need to select a project for which the permissions will be granted. If you select **All projects**, the permissions will be granted for all the projects. You need to switch to the authorized region before accessing an enterprise router.

Table 7-1 lists all the system-defined policies on enterprise routers.

Table 7-1 System-defined policies on enterprise routers

System Policy	Description	Type	Dependency
ER FullAccess	Administrator permissions for enterprise routers. Users with such permissions can operate and use all resources on enterprise routers.	System policy	None

System Policy	Description	Type	Dependency
ER ReadOnlyAccess	Read-only permissions for enterprise routers. Users with such permissions can only view data on enterprise routers.	System policy	None

Table 7-2 lists the common operations supported by each system-defined policy. You can select a proper one as required.

Table 7-2 Common operations supported by each system policy

Operation	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
Creating an enterprise router	√	x	√	x
Modifying an enterprise router	√	x	√	x
Viewing an enterprise router	√	√	√	√
Deleting an enterprise router	√	x	√	x
Adding a Virtual Private Cloud (VPC) to an enterprise router	√	x	√	x
Deleting a VPC attachment	√	x	√	x
Viewing attachments of all types	√	√	√	√
Creating a route table	√	x	√	x
Renaming a route table	√	x	√	x
Viewing a route table	√	√	√	√
Deleting a route table	√	x	√	x

Operation	Tenant Administrator	Tenant Guest	ER FullAccess	ER ReadOnlyAccess
Creating an association for an attachment in a route table	√	x	√	x
Viewing associations in a route table	√	√	√	√
Deleting an association from a route table	√	x	√	x
Creating a propagation for an attachment in the route table	√	x	√	x
Viewing a propagation in a route table	√	√	√	√
Deleting a propagation from a route table	√	x	√	x
Creating a static route	√	x	√	x
Modifying a static route	√	x	√	x
Viewing a route	√	√	√	√
Deleting a static route	√	x	√	x
Creating a flow log	√	x	√	x
Viewing a VPC flow log	√	√	√	√
Disabling a flow log	√	x	√	x
Enabling a flow log	√	x	√	x
Deleting a flow log	√	x	√	x
Adding a resource tag	√	x	√	x
Modifying a resource tag	√	x	√	x

Operation	Tenant Administrat or	Tenant Guest	ER FullAccess	ER ReadOnlyAc cess
Viewing a resource tag	√	√	√	√
Deleting a resource tag	√	x	√	x

Related Links

- **What Is IAM?**
- **Creating a User and Granting Permissions**

8 Notes and Constraints

Quotas

Table 8-1 lists the quotas about enterprise router resources. Some default quotas can be increased.

You can log in to the console to view default quotas. For details, see **Viewing Quotas**.

Table 8-1 Enterprise router resource quotas

Item	Adjustable
Maximum number of enterprise routers that can concurrently connect to a VPC	No
Maximum number of VPCs that can be attached to an enterprise router	**Yes**
Maximum number of virtual gateways that can be attached to an enterprise router	**Yes**
Maximum number of VPN gateways that can be attached to an enterprise router	**Yes**
Maximum number of route tables allowed on each enterprise router	No
Maximum number of routes allowed on each enterprise router	No
Maximum number of static routes allowed in each route table	**Yes**
Maximum number of flow logs that can be created by each account	No

Specifications

Table 8-2 lists the specifications of the enterprise router.

Table 8-2 Enterprise router specifications

Item	Default Setting	Adjustable
Maximum number of enterprise routers that can be created by each account	1	Contact customer service.
Maximum forwarding capability supported by each enterprise router	100 Gbit/s	Contact customer service.

Constraints

There are some constraints on using enterprise routers, as described in **Table 8-3**. You can follow our suggestions to handle these issues.

Table 8-3 Constraints on enterprise routers

Constraint	Suggestion
If a service VPC is being used by ELB, VPC Endpoint, NAT Gateway (private NAT gateway), Distributed Cache Service (DCS), or hybrid DNS, this VPC cannot be attached to an enterprise router. **NOTICE** If you attach a service VPC to an enterprise router when Elastic Load Balance (ELB), VPC Endpoint, or DCS is being used together with Enterprise Router, persistent connections may be intermittently interrupted during service reliability assurance, such as a DR switchover, an upgrade, or elastic scaling. Ensure that the clients are capable of automatic reconnection in case of intermittent disconnection.	Contact customer service to confirm the service compatibility and preferentially use a transit VPC for networking. For details, see scheme 2 in **Selecting a Network Scheme**.

Constraint	Suggestion
Traffic cannot be forwarded from a VPC to the enterprise router that it attached to if you set the destination of a route whose next hop is the enterprise router to 0.0.0.0/0 in the VPC route table and if: ● An ECS in the VPC has an EIP bound. ● The VPC is being used by ELB, NAT Gateway, VPC Endpoint, or DCS.	● Suggestion 1: Change the destination address of the route. For details, see **Why Traffic Can't Be Forwarded from a VPC with a Route Destination of 0.0.0.0/0 to Its Enterprise Router?** ● Suggestion 2: Use a transit VPC for networking. For details, see scheme 2 in **Selecting a Networking Scheme**.
If a VPC attached to an enterprise router has a NAT gateway associated and **Scenario** of the SNAT or DNAT rules is set to **Direct Connect**, the network from the on-premises data center to the VPC is disconnected.	Use a transit VPC for networking. For details, see scheme 2 in **Selecting a Networking Scheme**.

9 Enterprise Router and Other Services

Table 9-1 Interactions between an enterprise router and other cloud services

Service	Interaction
Virtual Private Cloud (VPC)	You can attach VPCs to an enterprise router to enable communication between multiple VPCs without configuring a large number of VPC peering connections.
Direct Connect	You can attach a Direct Connect virtual gateway to an enterprise router to connect VPCs to an on-premises data center through one Direct Connect connection.
Virtual Private Network (VPN)	You can attach a VPN gateway to an enterprise router to connect VPCs to an on-premises data center through a shared VPN connection.
Identity and Access Management (IAM)	You can use IAM to assign different permissions to different users to control their access to enterprise router resources.
Cloud Eye	You can use Cloud Eye to monitor the network status of enterprise routers and their attachments, and report alarms when exceptions occur, ensuring smooth service running.
Cloud Trace Service (CTS)	You can use CTS to record operations associated with your enterprise routers for future query, audit, and backtracking.
Tag Management Service (TMS)	You can use tags to identify enterprise routers and route tables.

10 Region and AZ

Concept

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified into universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides specific services for specific tenants.

- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. to support high-availability systems.

Selecting a Region

If your target users are in Europe, select the **EU-Dublin** region.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.

- For lower network latency, deploy resources in the same AZ.

A Change History

Released On	Description
2024-01-15	This issue is the first official release.