Enterprise Switch

Getting Started

Issue 01

Date 2023-11-17

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

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 Preparations

Scenarios

Before you use Enterprise Switch, you need to make the following preparations:

- **Registering a HUAWEI ID and Enabling Huawei Cloud Services**
- **Topping Up Your Account**

Registering a HUAWEI ID and Enabling Huawei Cloud Services

If you already have a HUAWEI ID, skip this section. If you do not have one, proceed as follows:

1. **Register a HUAWEI ID and enable Huawei Cloud services**.
2. **Complete real-name authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For details about the pricing of enterprise switches, see **Pricing Details**.
- To top up an account, see **Topping Up an Account**.

2 Quick Start

Enterprise switches establish a Layer 2 network between on-premises data centers and VPCs based on the Layer 3 network established by VPN or Direct Connect. **Figure 2-1** shows the configuration process of enterprise switches.

Figure 2-1 Enterprise switch configuration flowchart
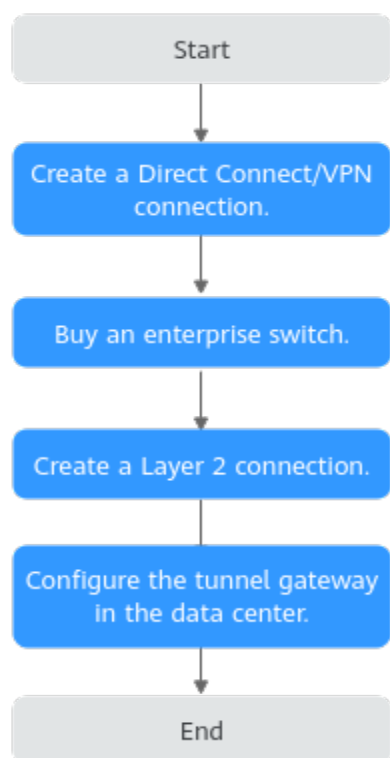
Table 2-1 Process description

No.	Step	Description
1	**Step 1: Use Direct Connect or VPN to Communicate at Layer 3**	An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC. This section describes how to create a Direct Connect or VPN connection between an on-premises data center and a VPC at Layer 3.
2	**Step 2: Buy an Enterprise Switch**	This section describes how to buy an enterprise switch. An enterprise switch allows Layer 2 communication between an on-premises data center and a VPC based on VPN or Direct Connect.
3	**Step 3: Create a Layer 2 Connection**	After an enterprise switch is created, you need to create a Layer 2 connection to enable the local Layer 2 connection subnet and the remote VXLAN switch to communicate at Layer 2.
4	**Step 4: Configure a Tunnel Gateway in Your Data Center**	This section describes how to configure the tunnel gateway on a VXLAN tunnel switch of an on-premises data center.

3 Step 1: Use Direct Connect or VPN to Communicate at Layer 3

Scenarios

An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC. This section describes how to create a Direct Connect or VPN connection between an on-premises data center and a VPC at Layer 3.

Prerequisites

You have planned the resources required both on the cloud and on premises. For details about resource planning, see **How Enterprise Switches Work**.

Procedure

1. Create a Direct Connect or VPN connection.

    For details, see **Direct Connect User Guide** or **Virtual Private Network User Guide**.

    📖 **NOTE**

    Only classic VPNs can be used together with enterprise switches.

2. **Submit a service ticket** to check whether your Direct Connect or VPN connection supports VXLAN interconnection with an enterprise switch. If your connection does not support this, contact customer service.

4 Step 2: Buy an Enterprise Switch

Scenarios

This section describes how to buy an enterprise switch. An enterprise switch allows Layer 2 communication between an on-premises data center and a VPC based on VPN or Direct Connect.

Prerequisites

- You have planned the resources required both on the cloud and on premises. For details about resource planning, see **How Enterprise Switches Work**.

- An enterprise switch establishes a Layer 2 network based on a Layer 3 network between an on-premises data center and a VPC created by Direct Connect or VPN. You need to create a Direct Connect or VPN connection first by referring to **Use Direct Connect or VPN to Communicate at Layer 3**.

Notes and Constraints

- The switch in an on-premises data center must support VXLAN because the enterprise switch needs to establish a VXLAN tunnel to the data center at Layer 2.

- The local tunnel subnet must have three IP addresses reserved for the enterprise switch.

Procedure

1. Log in to the management console.

2. Click in the upper left corner and select the desired region and project.

3. On the console homepage, choose **Networking** > **Enterprise Switch**.

   The **Enterprise Switch** page is displayed.

4. In the upper right corner of the page, click **Buy**.

   The page for buying an enterprise switch is displayed.

5. Configure parameters as prompted. For details, see **Table 4-1**.

Table 4-1 Parameter descriptions

Parameter	Description	Example Value
Billing Mode	Mandatory Enterprise switches can be billed on a yearly/monthly or pay-per-use basis. ● If you buy a yearly/monthly enterprise switch, you need to make a one-off payment for the enterprise switch in your selected period. ● If you buy a pay-per-use enterprise switch, your enterprise switch is billed by the second, and settled by the hour. If the usage is less than an hour, you are billed based on the actual duration consumed. **NOTE** The yearly/monthly billing mode is available only in regions **LA-Santiago** and **AF-Johannesburg**.	Pay-per-use
Region	Mandatory Select the region nearest to you to ensure the lowest latency possible.	LA-Santiago
Active AZ	Mandatory Enterprise switches are deployed in active/standby mode. Select the AZ where the active node is deployed. An active AZ carries traffic. You can set the AZ to the one where your ECSs that need to communicate with an on-premises data center are deployed to ensure quick and uninterrupted access to ECSs.	AZ1
Standby AZ	Mandatory Enterprise switches are deployed in active/standby mode. Select the AZ where the standby node is deployed. A standby AZ is used for backup and disaster recovery. Set the standby AZ to be different from the active AZ.	AZ2

Parameter	Description	Example Value

Specifications	Mandatory
	
	Currently, the following enterprise switch specifications are supported:
	
	● Basic
	  – Maximum Bandwidth: 3 Gbit/s
	  – Maximum PPS: 500,000
	  – Connected Subnets: 1
	● Standard
	  – Maximum Bandwidth: 5 Gbit/s
	  – Maximum PPS: 1,000,000
	  – Connected Subnets: 3
	● Enhanced
	  – Maximum Bandwidth: 10 Gbit/s
	  – Maximum PPS: 2,000,000
	  – Connected Subnets: 6
	
	The specifications cannot be changed after the enterprise switch is created.
		Enhanced

VPC	Mandatory VPC that the enterprise switch belongs to. If **Tunnel Connection** is set to **Direct Connect** or **VPN**, the VPC is set to the one that the Direct Connect virtual gateway or VPN gateway belongs to by default.	vpc-01
Tunnel Subnet	Mandatory Subnet of the VPC that the enterprise switch belongs to. It is the local tunnel subnet. Local and remote tunnel subnets communicate with each other at Layer 3 over Direct Connect or VPN. Enterprise switches allow communications between cloud and on-premises networks at Layer 2 based on the Layer 3 network between tunnel subnets.	subnet-01

Parameter	Description	Example Value
Local Tunnel IP Address	Mandatory IP address in the local tunnel subnet, which can be automatically assigned or manually specified. If an enterprise switch establishes a VXLAN tunnel with an on-premises data center at Layer 2, each end of the VXLAN tunnel requires a tunnel IP address, that is the local and remote tunnel IP addresses. The two IP addresses must be different.	Automatically assign IP address
Name	Mandatory Enter the name of the enterprise switch. The name: ● Must contain 1 to 64 characters. ● Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	esw-01
Description	Optional Enter the description of the enterprise switch in the text box as required.	-

6. Click **Next**.

7. Confirm the enterprise switch information and click **Submit**.

   This operation takes 3 to 6 minutes to complete. If the status is **Running**, the enterprise switch is created.

Follow-Up Operations

After an enterprise switch is created, you need to create a Layer 2 connection and configure a remote tunnel gateway. For details, see **Getting Started**.

5 Step 3: Create a Layer 2 Connection

Scenarios

After an enterprise switch is created, you need to create a Layer 2 connection to enable the local Layer 2 connection subnet and the remote VXLAN switch to communicate at Layer 2.

Notes and Constraints

- Each Layer 2 connection connects a local and a remote Layer 2 connection subnet. Each enterprise switch supports a maximum of six Layer 2 connections.

- The Layer 2 connections of an enterprise switch can share a tunnel IP address, but their tunnel VNIs must be unique. A tunnel VNI is the identifier of a tunnel.

- If a Layer 2 connection connects a local Layer 2 connection subnet to an enterprise switch, the local Layer 2 connection subnet must have two IP addresses reserved as active and standby interface IP addresses. The two IP addresses cannot be used by any local resources and must be different from the IP addresses in the remote Layer 2 connection subnet.

Procedure

1. Log in to the management console.

2. Click ⊚ in the upper left corner and select the desired region and project.

3. On the console homepage, choose **Networking** > **Enterprise Switch**.

   The **Enterprise Switch** page is displayed.

4. Click the name of the target enterprise switch.

   The enterprise switch details page is displayed.

5. In the lower right part of the enterprise switch details page, click **Create Connection**.

   The page for creating a Layer 2 connection is displayed.

6. Configure the parameters as prompted. For details, see **Table 5-1**.

Table 5-1 Parameter descriptions

Parameter	Description	Example Value
Enterprise Switch	Name of the enterprise switch. You do not need to set this parameter.	l2cg-01
VPC	VPC that is associated with the enterprise switch, that is, the VPC that the local tunnel subnet belongs to. You do not need to set this parameter.	vpc-01
Layer 2 Connection Subnet	Mandatory Select the layer 2 connection subnet in the VPC. This Layer 2 connection subnet is used to communicate with the Layer 2 connection subnet in an on-premises data center at Layer 2. ● The local and remote Layer 2 connection subnets can overlap, but the IP addresses of the servers that need to communicate in the local and remote subnets must be different. Otherwise, the communication fails. ● A VPC subnet that has been used a Layer 2 connection cannot be used by any other Layer 2 connections or enterprise switches.	subnet-01
Interface IP Address	Mandatory IP addresses in the VPC subnet that are connected to the enterprise switch, including active and standby interface IP addresses. The IP addresses can be automatically assigned or manually specified.	Automatically assign
Remote Access Information > Tunnel VNI	Mandatory Network identifier of the VXLAN tunnel used by an on-premises data center to connect to an enterprise switch, which is used to uniquely identify the VXLAN. For the same VXLAN tunnel, the on-premises data center and the cloud must use the same tunnel VNI.	10001
Remote Access Information > Tunnel IP Address	Mandatory IP address of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch.	-

Paramete r	Description	Example Value
Remote Access Informatio n > Tunnel Port	Port number of the VXLAN tunnel used by the on-premises data center to connect to the enterprise switch. Port **4789** is used by default. You do not need to set this parameter.	4789
Name	Mandatory Enter the name of the Layer 2 connection. The name: ● Must contain 1 to 64 characters. ● Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	l2conn-01

7. Click **Create**.

   This operation takes 20 to 60 seconds to complete. If the status is **Not connected** or **Connected**, the Layer 2 connection is created.

6 Step 4: Configure a Tunnel Gateway in Your Data Center

Scenarios

This section describes how to configure the tunnel gateway on a VXLAN tunnel switch of an on-premises data center.

The following uses Huawei CE6850, Ruijie RG-S6250, and H3C S6520 series switches as examples. To check more configurations, see the product documentation of the corresponding switch.

- **Procedure (Huawei CE6850 Switches)**
- **Procedure (Ruijie RG-S6250 Switches)**
- **Procedure (H3C S6520 Switches)**

Notes and Constraints

If you use an enterprise switch to connect your on-premises data center to the cloud, the switches of your data center must support the VXLAN function. If high reliability is required, the VXLAN switches need to be deployed in disaster recovery mode.

The following lists some switches that support the VXLAN function.

- Huawei switches: Huawei CE58, CE68, CE78, and CE88 series switches, such as CE6870, CE6875, CE6881, CE6863, and CE12800 switches
- Switches of other vendors: Cisco Nexus 9300, Ruijie RG-S6250, and H3C S6520 series switches

Networking Example

In this example, the Layer 2 subnet gateway and the VXLAN tunnel are on different switches.

The tunnel IP address on the cloud is 10.0.6.3, the tunnel IP address of the tunnel switch on the on-premises data center is 2.2.2.2, and the tunnel VNI is 5010.

Figure 6-1 Layer 2 subnet gateway and VXLAN tunnel on different switches
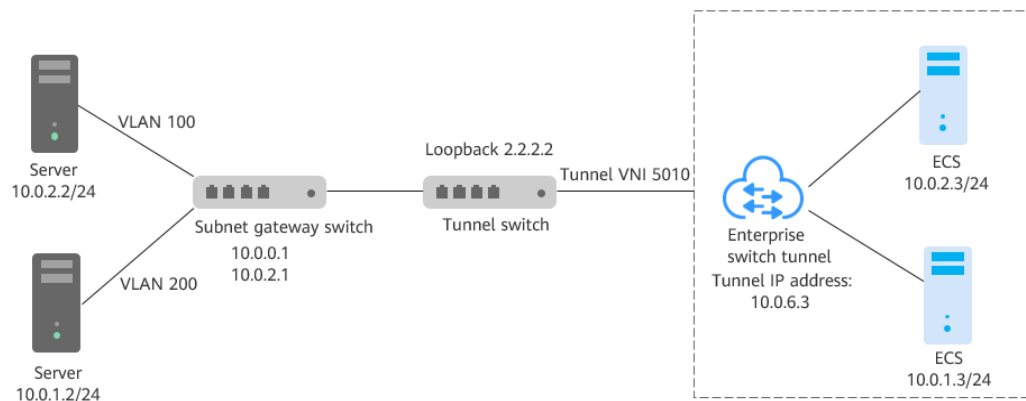
Procedure (Huawei CE6850 Switches)

Configure the tunnel switch of your data center to divert the traffic of the VLAN corresponding to the Layer 2 subnet to the tunnel.

> **NOTICE**
>
> Currently, most CE series switches do not support forwarding of encapsulated VXLAN packets through Layer 3 sub-interfaces. Layer 3 sub-interfaces cannot be used by VXLAN uplinks (connected to enterprise switches). Instead, VLAN interfaces can be used.

1. Log in to the tunnel switch and run the **system-view** command to switch to the system view.

2. Switch to the loopback 0 interface view and configure the tunnel IP address.

   Example:

   interface loopback 0

   ip address 2.2.2.2 255.255.255.255

3. Use the **quit** command to exit the interface view and return to the system view.

4. Switch to the bridge domain (BD) view and configure the VXLAN VNI for the BD.

   Example:

   bridge-domain 10

   vxlan vni 5010

5. Use the **quit** command to exit the BD view and return to the system view.

6. Create a Layer 2 sub-interface and use the sub-interface to divert traffic from the VLAN at Layer 2 to the tunnel.

   Example:

   interface 10ge 1/0/2.1 mode l2

   encapsulation dot1q vid 100

   bridge-domain 10

7. Use the **interface nve** command to create an NVE interface, switch to the NVE interface view, and configure the IP address (2.2.2.2) for the source VTEP of the VXLAN tunnel.

    Example:

    interface nve1

    source 2.2.2.2

8. Use the **vni** command in the NVE interface view to configure an ingress replication list for VNI 5010.

    Example:

    vni 5010 head-end peer-list 10.0.6.3

9. Check the VXLAN configuration status in the system view:

    display vxlan vni 5010 verbose

    Figure 6-2 VXLAN configuration status


    ```
    [~B0706-172.30.192.3-core-new-gateway]display vxlan vni 5010 verbose
        BD ID                 : 10
        State                 : up
        NVE                   : 1
        Source Address        : 2.2.2.2
        Source IPv6 Address   : -
        UDP Port              : 4789
        BUM Mode              : head-end
        Group Address         : -
        Peer List             : 10.0.6.3
        IPv6 Peer List        : -
    ```

    If the value of **State** is **up**, the tunnel status is normal.

Procedure (Ruijie RG-S6250 Switches)

Establish a VXLAN tunnel between a VXLAN switch and an enterprise switch, so that Layer 2 packets from an on-premises server can be encapsulated into IP packets and then sent to the enterprise switch. Configure VXLAN and VLAN encapsulation rules on downlink Layer 2 sub-interfaces of the VXLAN switch to identify the VXLAN of packets.

1. Enter the global configuration mode.

    Example:

    Ruijie#**configure**

2. Create a VXLAN.

    Example:

    Ruijie(config)#**vxlan 5010**

    NOTICE

    VXLAN ID 5010 in this step must be the same as the tunnel VNI in remote access information configured during Layer 2 connection creation in **Table 5-1**.

    ---

3. Switch to the loopback interface view and configure the tunnel IP address.

    Example:

    Ruijie(config)#**interface loopback 0**

    Ruijie(config-if-Loopback 0)#**ip address 2.2.2.2 255.255.255.255**

    Ruijie(config-if-Loopback 0)# **exi**

    NOTICE

    For a new interface IP address (including the loopback interface IP address) of the VXLAN switch, check whether there is a route to direct traffic from the IP address to the tunnel subnet of the enterprise switch. If there is no such a route, configure one on the VXLAN switch. The VXLAN switch can be an aggregation switch or a core switch. Select a switch based on the network plan.

    ---

4. Create a VXLAN tunnel.

    a. Create an OverlayTunnel1 interface. This interface is used to statically create an overlay tunnel.

        Example:

        Ruijie(config)#**interface overlayTunnel 1**

    b. Specify the source IP address of the overlay tunnel. This will be the loopback interface IP address.

        Example:

        Ruijie(config-if-OverlayTunnel 1)#**tunnel source 2.2.2.2**

    c. Specify the destination IP address of the overlay tunnel. This will be the tunnel IP address of the enterprise switch.

        Example:

        Ruijie(config-if-OverlayTunnel 1)#**tunnel destination 10.0.6.3**

        Ruijie(config-if-OverlayTunnel 1)#**exit**

5. Associate the VXLAN instance with the OverlayTunnel interface.

    Example:

    Ruijie(config)#**vxlan 5010**

    Ruijie(config-vxlan)#**tunnel-interface OverlayTunnel 1**

    Ruijie(config-vxlan)#**exit**

> **NOTICE**
>
> - A maximum of six Layer 2 connections can be created on an enterprise switch. Each connection corresponds to a VXLAN. Multiple VXLAN instances can be associated with the same OverlayTunnel interface, for example, OverlayTunnel1.
> - A VXLAN switch can connect to multiple enterprise switches. In this case, you can associate multiple OverlayTunnel interfaces, for example, OverlayTunnel1 and OverlayTunnel2, with the same VXLAN.
> - Due to chip limitations, Ruijie RG-S6250 switches do not allow multiple VXLAN tunnels to use the same physical egress, and each VXLAN tunnel needs to encapsulate its unique DMAC and VID information. For details, contact Ruijie technical support.

6. Create a Layer 2 sub-interface and configure VXLAN and VLAN encapsulation rules.

   Create the sub-interface (AggregatePort 1.100) on the link aggregation interface (AggregatePort1) to receive data packets of VLAN 100, encapsulate the packets into VXLAN 5010, and forward them through the VXLAN tunnel.

   Example:

   Ruijie(config)#**interface AggregatePort 1.100**

   Ruijie(config-subif-AggregatePort 1.100)#**encapsulation dot1q s-vid 100**

   Ruijie(config-subif-AggregatePort 1.100)#**encapsulation vxlan 5010**

   Ruijie(config-subif-AggregatePort 1.100)#**exit**

> **NOTICE**
>
> The method for creating Ethernet service instances on physical Ethernet interfaces of switches is similar.

7. Check the VXLAN configuration status in the system view:

   show vxlan 5010

   VXLAN configuration status
   ```
   VXLAN 5010
   Symmetric property  : FALSE
   Router Interface    : -
   Extend VLAN         : -
   VTEP Adjacency Count: 1
   VTEP Adjacency List :
   Interface           Source IP      Destination IP  Type
   --------------------- -------------- -------------- -------
   OverlayTunnel 1     2.2.2.2   10.0.6.3     static
   ```

Procedure (H3C S6520 Switches)

Establish a VXLAN tunnel between a VXLAN switch and an enterprise switch, associate the VXLAN tunnel with a VXLAN, so that Layer 2 packets from VMs can be encapsulated into IP packets and then sent to the enterprise switch. Configure Ethernet service instances and matching rules on downlink interfaces of a VXLAN switch to identify the VXLAN that packets belong to.

1. Configure the switch to work in VXLAN mode.

   Save the configuration, and restart the switch. (Skip this step if the switch is already working in VXLAN mode.)

   Example:

   <SwitchA> **system-view**

   [SwitchA] **switch-mode 1**

   ```
   Reboot device to make the configuration take effect.
   ```

   [SwitchA] **quit**

   <SwitchA> **reboot**

   ```
   Start to check configuration with next startup configuration file, please wait..
   .......DONE!
   Current configuration may be lost after the reboot, save current configuration?
   [Y/N]:y
   This command will reboot the device. Continue? [Y/N]:y
   ```

2. Create a tunnel interface and configure an IP address for the interface.

   Create a loopback interface and configure an IP address for the loopback interface as the remote IP address of the VXLAN tunnel.

   Example:

   [SwitchA] **interface loopback 0**

   [SwitchA-LoopBack0] **ip address 2.2.2.2 32**

   NOTICE

   For a new interface IP address (including the loopback interface IP address) of the VXLAN switch, check whether there is a route to direct traffic from the IP address to the tunnel subnet of the enterprise switch. If there is no such a route, configure one on the VXLAN switch. The VXLAN switch can be an aggregation switch or a core switch. Select a switch based on the network plan.

   ---

3. Create a VXLAN.

   a. Enable L2VPN.

      Example:

      <SwitchA> **system-view**

      [SwitchA] **l2vpn enable**

   b. Enable Layer 2 forwarding for the VXLAN tunnel.

      Example:

      [SwitchA] **undo vxlan ip-forwarding**

   c. Create the VSI **vpna** and VXLAN 5010.

      Example:

      [SwitchA] **vsi vpna**

      [SwitchA-vsi-vpna] **vxlan 5010**

      [SwitchA-vsi-vpna-vxlan5010] **quit**

      [SwitchA-vsi-vpna] **quit**

> **NOTICE**
>
> The VXLAN ID must be the same as the tunnel VNI in remote access
> information configured during Layer 2 connection creation in **Table 5-1**.

4. Create a VXLAN tunnel.

   Create a VXLAN tunnel (Tunnel1) to the enterprise switch.

   Example:

   [SwitchA] **interface tunnel 1 mode vxlan**

   [SwitchA-Tunnel1] **source 2.2.2.2**

   [SwitchA-Tunnel1] **destination 10.0.6.3**

   [SwitchA-Tunnel1] **quit**

5. Associate the VXLAN with the VXLAN tunnel.

   On the VXLAN switch, associate the VXLAN tunnel (Tunnel1) with VXLAN
   5010.

   Example:

   [SwitchA] **vsi vpna**

   [SwitchA-vsi-vpna] **vxlan 5010**

   [SwitchA-vsi-vpna-vxlan5010] **tunnel 1**

   [SwitchA-vsi-vpna-vxlan5010] **quit**

   [SwitchA-vsi-vpna] **quit**

> **NOTICE**
>
> ● A maximum of six Layer 2 connections can be created on an enterprise
>   switch. Each connection corresponds to a VXLAN. Multiple VXLANs can be
>   associated with the same VXLAN tunnel, such as, Tunnel1.
> ● A VXLAN switch can connect to multiple enterprise switches. In this case,
>   you can associate multiple VXLAN tunnels, for example, Tunnel1 and
>   Tunnel2, with the same VXLAN.

6. Configure an Ethernet service instance to match frames and associate the
   instance with the VSI.

   Create Ethernet service instance 1000 on Bridge-Aggregation1 of the VXLAN
   switch to match frames of VLAN 100 and associate the instance with VSI
   vpna (VXLAN 5010).

   Example:

   [SwitchA] **Bridge-Aggregation 1**

   [SwitchA-Bridge-Aggregation1] **port link-type trunk**

   [SwitchA-Bridge-Aggregation1] **service-instance 1000**

   [SwitchA-Bridge-Aggregation1-srv1000] **encapsulation s-vid 100**

   [SwitchA-Bridge-Aggregation1-srv1000] **xconnect vsi vpna**

   [SwitchA-Bridge-Aggregation1-srv1000] **quit**

   [SwitchA-Bridge-Aggregation1] **quit**

> **NOTICE**
>
> The method for creating Ethernet service instances on physical Ethernet interfaces of switches is similar.

7. Check the status of the VXLAN tunnel interface.

   – The status of the VXLAN tunnel interface is **Up**.

   Example:

   [SwitchA]**display interface Tunnel 1**

   ```
   Tunnel1
   Current state: UP
   Line protocol state: UP
   Description: Tunnel1 Interface
   Bandwidth: 64 kbps
   Maximum transmission unit: 1464
   Internet protocol processing: Disabled
   Last clearing of counters: 17:19:44 Fri 01/18/2013
   Tunnel source 2.2.2.2, destination 10.0.6.3
   Tunnel protocol/transport UDP_VXLAN/IP
   Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
   Input: 0 packets, 0 bytes, 4 drops
   Output: 0 packets, 0 bytes, 0 drops
   ```

   – Check the VSI information. The VXLAN tunnel associated with the VXLAN and the Ethernet service instance associated with the VSI are in **Up** status.

   Example:

   [SwitchA]**display l2vpn vsi verbose**

   ```
   VSI Name: vnpa
   VSI Index          : 1
   VSI State          : Up
   MTU                : 1500
   Bandwidth          : -
   Broadcast Restrain     : -
   Multicast Restrain     : -
   Unknown Unicast Restrain: -
   MAC Learning          : Enabled
   MAC Table Limit       : -
   MAC Learning rate      : -
   Drop Unknown          : -
   Flooding          : Enabled
   Statistics          : Disabled
   VXLAN ID          : 5010
   Tunnels:
   Tunnel Name       Link ID    State    Type        Flood proxy
   Tunnel1           0x5000001  UP       Manual      Disabled
   ACs:
   AC            Link ID    State    Type
   BAGG1 srv1000     0          Up       Manual
   ```

A Change History

Released on	Description
2023-11-17	This issue is the eighth official release. Modified the following content: Added support for the yearly/monthly billing mode in **Step 2: Buy an Enterprise Switch**.
2023-02-27	This issue is the seventh official release. Modified the following content: Added basic enterprise switches in **Step 2: Buy an Enterprise Switch**.
2022-12-02	This issue is the fifth official release. Modified the following content: Added parameters related to enterprise switch specifications in **Step 2: Buy an Enterprise Switch**.
2022-11-08	This issue is the fourth official release. Modified the following content: Modified procedure for using Direct Connect or VPN to communicate at Layer 3 in **Step 1: Use Direct Connect or VPN to Communicate at Layer 3**.
2022-07-22	This issue is the third official release. Modified the following content: Added standard enterprise switches in **Step 2: Buy an Enterprise Switch**.
2022-06-09	This issue is the second official release. Modified the following content: Added the configuration guide for Ruijie RG-S6250 and H3C S6520 series switches in **Step 4: Configure a Tunnel Gateway in Your Data Center**.
2022-04-20	This issue is the first official release.