Contents

1 Configuring VSU

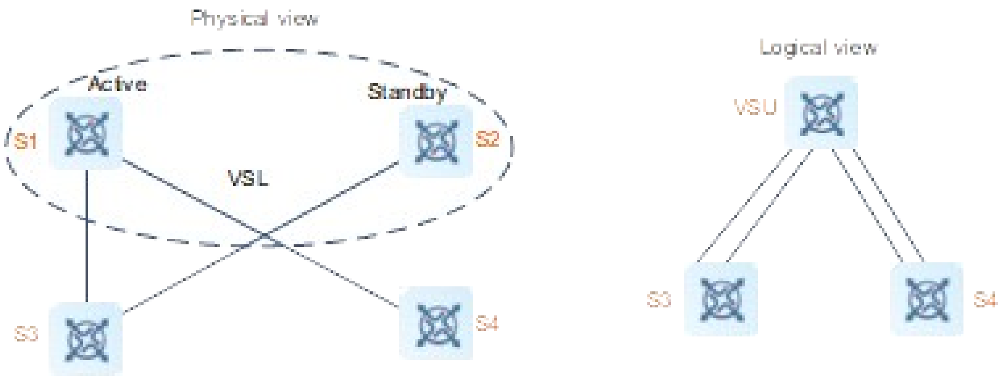
1.1 Introduction

Virtual Switching Unit (VSU) is an N:1 network device technology independently developed by Orion_B26Q. It simplifies the device operation & maintenance (O&M) and network topology by virtualizing multiple network devices into a single logical device for management and use. In addition, the VSU technology connects peripherals to different member devices in the VSU through aggregated links to achieve cross-device link redundancy and improve reliability and scalability of networks.

1.1.1 Basic Concepts

As shown in Figure 1-1, the left part shows the physical view of devices that form a VSU, which is equivalent to one logical device.

Figure 1-1Schematic Diagram of VSU



1. VSU

The VSU is a single logic entity composed of multiple redundant devices in a conventional network structure. The devices on the access layer, the distribution layer, and the core layer can form the VSU.

2. Domain ID

A domain ID is the unique identifier of a VSU and distinguishes different VSUs. Only two devices that share the same domain ID can compose a VSU.

3. Device ID

Each device in a VSU is called a member device, and each member device has a unique device ID, i.e. switch ID. This device ID is used to manage the member device and configure interfaces on the member device. When adding the device to a VSU, you need to configure an ID for a device and ensure that the ID is unique in the same VSU. If device IDs of member devices conflict in a VSU, only one device is retained according to rules.

4. Device priority

Priority is an attribute of a member device, and is used to elect a role. A higher priority indicates a higher probability of being elected as the active device. To elect a device as the active device, increase its priority. Member devices have two types of priorities.

- Configuration priority: priority stored in the configuration file, which is changed at any time, and takes effect after the configurations are saved and the VSU is restarted.
- Running priority: configuration priority stored in the configuration file at the startup, which does not change during VSU running.

5. Device role

Member devices are assigned with three roles based on their functions:

- Active device: Manages and controls the entire VSU. Only one active device exists in a VSU domain.
- Standby device: Serves as a backup of the active device and participates in data forwarding only. All received data packets are forwarded to the global active device for processing. When the active device is faulty, the standby device automatically switches to the active mode and takes over functions of the original active device.
- Candidate device: Serves as a backup of the standby device and participates in data forwarding only. When the standby device is faulty, the system automatically elects a new standby device from candidate devices to take over functions of the original standby device. When the active device is faulty and the standby device switches to the active mode, the system automatically elects a new standby device from candidate devices.

6. Role election

A VSU is composed of at least the active device and standby device. When it is composed of more than two devices, the other devices are candidate devices. Role election applies to the following scenarios:

- VSU setup
- Device fault or exit from a VSU
- VSU splitting
- VSU combination

Roles are elected based on the following rules:

- The active device is elected by priority. The device priorities are ranked as follows:

  Current active device (no active device exists upon startup) > Device with a higher priority > Device with a smaller ID > Device with a smaller MAC address
- A device directly connected to the active device is preferentially elected as the standby device to avoid dual active devices. The device priorities are ranked as follows:
  Device directly connected to the active device > Device with a higher priority > Device with a smaller MAC address

Note

- When a device joins an existing VSU in hot mode, the system does not switch between the active and standby roles, even if the device has a higher priority than the active and standby devices in the running VSU.

- The startup sequence of member devices may affect the election of the active device. A member device may not join the VSU in time due to slow startup (the current VSU directly converges if it does not discover a neighbor within 5 minutes). In this case, the member device joins the VSU in hot mode, and the system does not switch active/standby role even if the member device has a higher priority than the active device in the current VSU.
- A candidate device is elected as a standby device only.

7. Virtual switching link

The VSU is a network entity of multiple devices that need to share control information and data flows. Virtual Switching Link (VSL) is a special link used to transmit control information and data flows between the devices in the VSU. Figure 1-1 shows the locations of VSLs in the VSU.

A VSL usually exists in the form of aggregation port group, and a data flow transmitted by the VSL is load-balanced among the aggregation port members based on a traffic balancing algorithm.

- VSL traffic

Control flows transmitted by the VSL between devices are classified into the following two types:

- Protocol packets received by a member device, which are forwarded through the VSL to the global active device for processing.
- Protocol packets processed by the global active device, which are forwarded through the VSL to the interfaces of other member devices and then sent to the peer devices by these interfaces.

The data flows transmitted through the VSL between devices include:

- Flooding data flows in a VLAN
- Data flows that need to be forwarded across devices and transmitted through the VSL

A VSL also transmits internal management packets of the VSU, for example, protocol information of hot backup devices, and packets that carry configurations to be delivered from the active device to other member devices.

- CRC error detection of VSL port

When a VSL port has many consecutive Cyclic Redundancy Check (CRC) errors, disable this port and switch to another VSL port. CRC errors are handled according to the following rules:

- The VSL port is checked for CRC errors every 5 seconds by default. If the number of CRC errors incremented between one check and the latest check is greater than the threshold of CRC errors (the *error-number* parameter), one CRC error occurrence is counted.
- When the number of consecutive CRC errors exceeds the configured number (the *time-number* parameter), the port is abnormal.
- If there are multiple VSLs and CRC errors occur in only one link, VSL is switched. If there are multiple VSL links and CRC errors occur in the last normal VSL, the link is not switched to prevent topology splitting.
- The values of *error-number* and *time-number* vary with the scenario. The default values of *error-number* and *time-number* are **3** and **10** respectively. In scenarios with high tolerance for CRC errors, reduce the two recommended parameter values; otherwise, increase them.

- VSL recovery

By default, a device automatically restarts and joins the VSU again after a VSL fault is rectified. If the automatic restart function is disabled, you must enable this function or directly restart the device after the VSL fault is rectified to rebuild the VSU.

1.1.2 VSU Application

Compared with conventional networks, VSU has the following advantages:

- Low cost: lightweight and dynamic network capacity expansion for protecting the equipment investment in the existing network, and reducing the construction cost.
- Simple O&M: reduced management workload, simplified networking, and lowered O&M difficulty.
- High reliability: device and link redundancy mechanisms for improved network reliability.

1. Flexible expansion

Capacity expansion applies to the following scenarios:

- Port expansion: The port density of the existing access switch cannot meet the requirement of increasing access users, as shown in Figure 1-1.
- Forwarding capacity expansion: The forwarding capacity of the existing core switch cannot meet the requirement of increasing services, as shown in Figure 1-2.
- Bandwidth expansion: The uplink bandwidth cannot meet the demand in peak hours, as shown in Figure 1-3.

The above problems are solved by adding a switch to form a VSU with the original switch. Physically, the two switches seem to be one, and the original switch backs up and sends the current configurations in batches to the new switch. Therefore, this change has little impact on network planning and configuration. The VSU features the following:

- Higher port density: The VSU forwards data as a whole, and the new switch is equivalent to a port expansion card of the original switch to increase port density.
- Higher forwarding capacity: If one switch has a forwarding capacity of 14,400 Mpps, the entire VSU has a forwarding capacity of 28800 Mpps after one switch is added.
- Larger bandwidth: If a 1000 M switch needs to perform 10 G uplink connection but provides only two 10G ports, up to 20 Gbps uplink bandwidth is supported. By adding one switch of the same type to set up a VSU, you can configure four 10 G ports into one aggregation group to increase the uplink bandwidth to 40 Gbps.

Figure 1-1Port Expansion over VSU

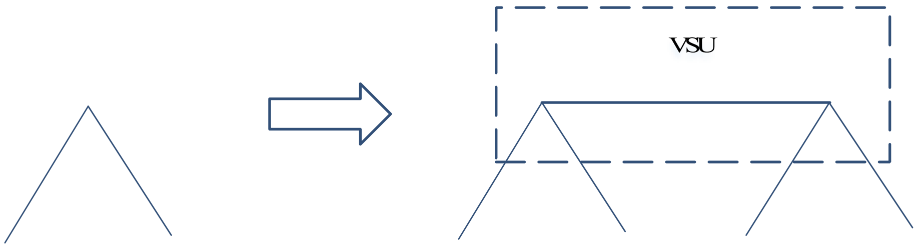


Figure 1-2Forwarding Capacity Expansion over VSU

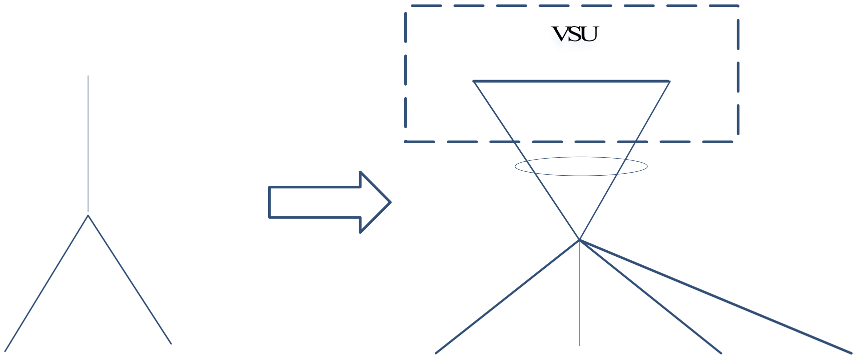
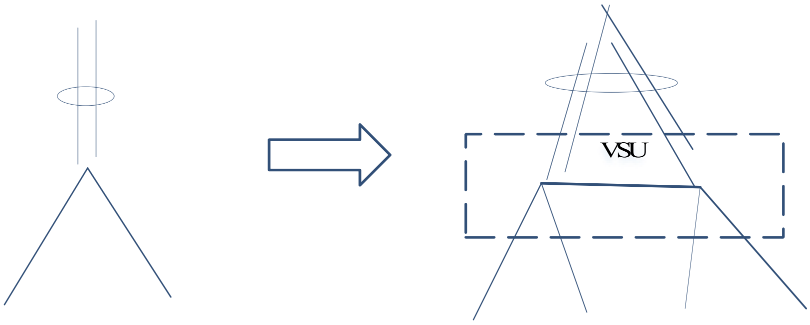


Figure 1-3Bandwidth Expansion over VSU

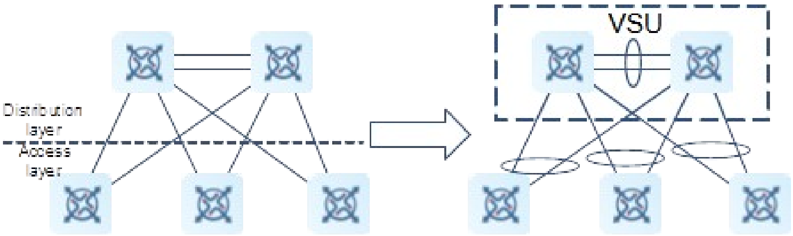


2. Simplified management

Simplified management is reflected in the following aspects:

- Device: After multiple devices form a VSU, an administrator can manage them together, without connecting to them for separate configuration and management. If a VSU is deployed between two floors/buildings, only one distribution device is needed between the floors/buildings, and this reduces the management and O&M costs.
- Networking: Figure 1-1 shows a common networking mode. Typically, each access switch is connected to two distribution switches to improve network reliability. The entire network topology is complex and has a loop. You also have to enable protocols such as Multiple Spanning Tree Protocol (MSTP) and Virtual Router Redundancy Protocol (VRRP) to eliminate the loop and support gateway backup. To meet the traffic balancing requirement, multi-loop network technologies such as Ethernet ring protection switching (ERPS) also need to be enabled. As a result, the configuration is complex, and the maintenance is difficult and prone to errors. After a VSU is formed, MSTP, VRRP, and ERPS are not required. Only the common link aggregation function can balance traffic , eliminate loops, and provide cross-device link redundancy, thus simplifying the topology and making deployment easier.

Figure 1-1**Simplified Networking over VSU**



3. Hot backup

As shown in Figure 1-1, two switches form a VSU to provide the following redundancy to adapt to high reliability scenarios:

- Device redundancy: redundancy between member devices in the VSU. Failure of the standby device does not affect the entire system, but failure of the active device makes the system switch to the standby device. This switching is similar to the dual-engine switching of a standalone device. Such switching is completed within milliseconds, without interrupting services (TCP flows rely on the retransmission mechanism to ensure service continuity).
- Link redundancy: A switch connects to surrounding devices through aggregated links, which provides cross-device link redundancy, implements load balancing, and fully utilizes all bandwidth. If one member link fails, the system switches to another member link within milliseconds.

Figure 1-1**Hot Backup over VSU**

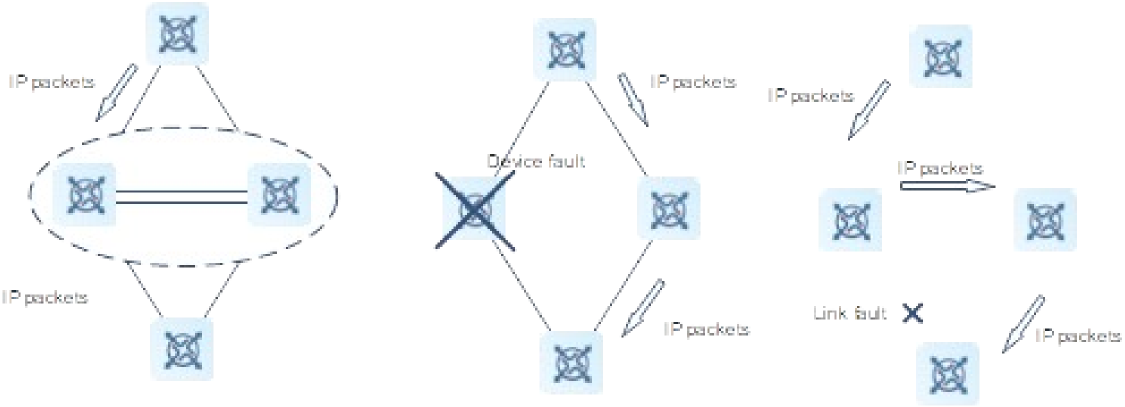
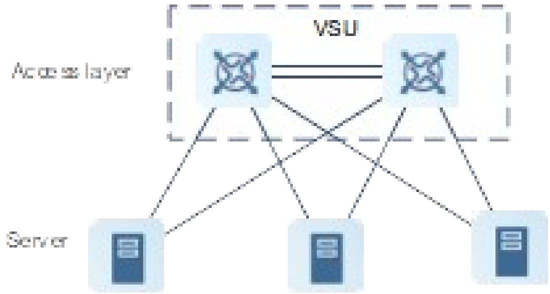


Figure 1-2 shows the typical application scenarios. Access servers with high availability requirements are connected with devices on the access layer by binding multiple network interface cards of a single server into an aggregation port. As the aggregation port allows access to only one access device, the risk of failure of the single device increases. In this case, setting up a VSU enables the server to connect to member devices in the VSU over the aggregation port. This deployment prevents network interruption caused by the single point of failure of the access device or the failure of a single link, and improves network reliability of services carried by the server.

Figure 1-2**Server Access Link Redundancy**



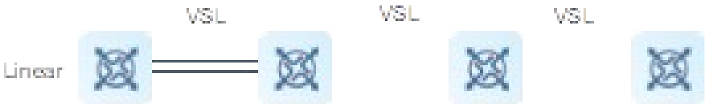
1.1.3 VSU Topology

A VSU supports linear topology and ring topology.

1. Linear topology

As shown in Figure 1-1, devices are connected through a VSL to form a line, and this topology is therefore called linear topology. The linear topology is simple. It uses a few ports and cables. Two devices are connected with a communication link only. Therefore, the VSL is less reliable.

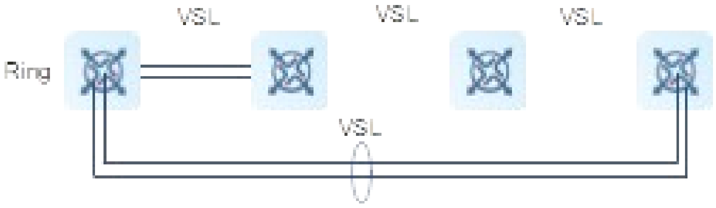
Figure 1-1Linear Topology



2. Ring topology

In the ring topology shown in Figure 1-1, the two communication links backed up by each other form link redundancy, which improves the reliability of the VSU.

Figure 1-1Ring Topology



Note

- The ring topology is recommended for the VSU, to ensure that the failure of any single device or any single VSL link does not affect the normal operation of the entire VSU.
- Besides, you are advised to configure multiple VSLs to improve reliability. You are advised to configure at least two VSLs.

3. Topology convergence

During setup of the VSU, the management scope is determined through topology convergence. The process is as follows:

(1) The member devices discover their neighbors through a topology discovery protocol to determine the list of devices included in the VSU.

(2) The global active device is elected to manage the entire VSU.

(3) The global standby device is elected as the backup for the active device.

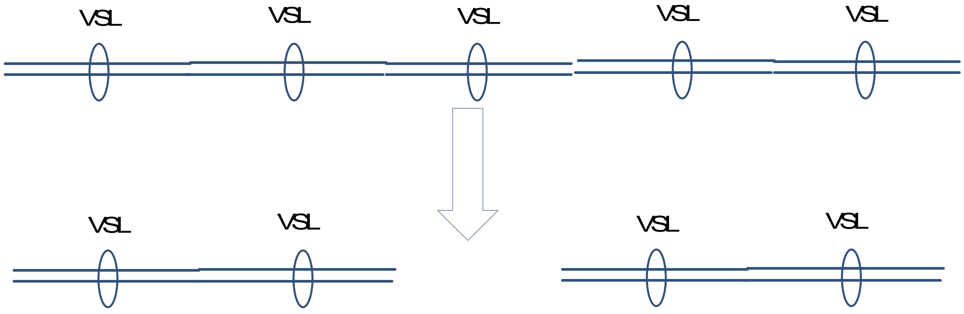
Note

The startup time varies with a device, and the first topology convergence time is different accordingly.

4. Topology splitting

The linear topology is split if the Virtual Switching Link-aggregation port (VSL-AP) link is disconnected. As shown in Figure 1-1, the VSU is split into two groups. In this case, there are two devices with the same configurations on the network, causing the network to malfunction. This topology splitting is resolved by deploying the dual-active detection (DAD) function (see section 1.1.4 DAD).

Figure 1-1Topology Splitting



5. Topology combination

Topologies are combined when two VSUs with the same VSU domain ID are connected through a VSL-AP link. During topology combination, one of the VSUs automatically restarts in an attempt to join the other VSU, as shown in Figure 1-1.

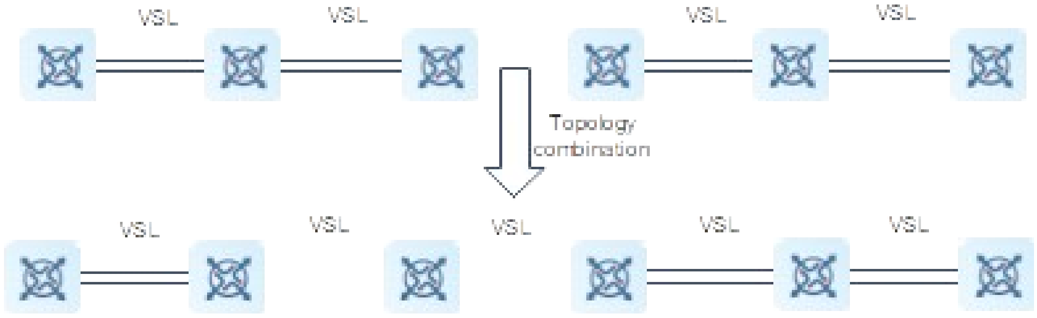
Topologies are combined based on the principle of minimizing the service impact caused by topology combination. The topology combination rules are as follows (topology combination starts from the first rule; if the optimal topology is not selected according to the first rule, the system goes on with the next rule for judgment):

(1) The user configurations are superior to other configurations. A VSU member device with the highest priority prevails.

(2) If the active device cannot be determined according to the preceding rule, a device with a smaller device ID prevails (in a case with two global active devices).

(3) If the active device cannot be determined according to the preceding rule, a device with a smaller MAC address prevails (in a case with two global active devices).

Figure 1-1Topology Combination



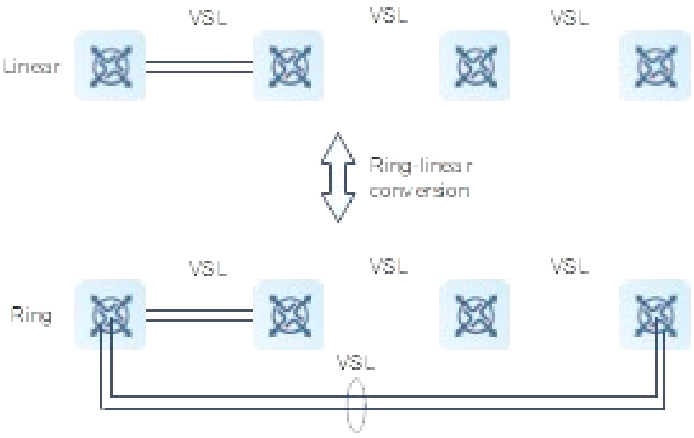
Note

During topology combination of two VSUs, they must be elected. The VSU that fails the election automatically restarts and joins the other VSU in hot mode.

6. Topology conversion

As shown in Figure 1-1, when one VSL-AP link is disconnected, the ring topology is converted into a linear one. The whole VSU can still run normally without network disconnection. However, to avoid the failure of other VSL-AP links or nodes, troubleshoot the VSL fault in time for VSL recovery. After the VSL-AP link is recovered, the linear topology is converted back into a ring one.

Figure 1-1Conversion Between the Ring Topology and Linear Topology



1.1.4 DAD

When the VSL is disconnected, the standby device becomes the active device. If the original active device is still running, two active devices are main roles and an IP address conflict and other problems occur in the LAN due to their same configurations. In this case, the VSU must detect dual device devices, and take recovery measures. The VSU supports DAD in two ways:

- Bidirectional forwarding detection-based (BFD-based) DAD
- AP-based DAD

1. Detection rules

Determine the desired active device according to the following rules one by one:

(1) The healthier device prevails. (A greater sum of bandwidths of up physical ports excluding the administration port and VSL port indicates a healthier device).

(2) The global active device with a higher priority prevails.

(3) The global active device in the VSU with more physical devices prevails.

(4) The global active device with the smaller ID prevails.

(5) The global active device with the smaller MAC address prevails.

(6) The global active device with the longer startup time prevails.

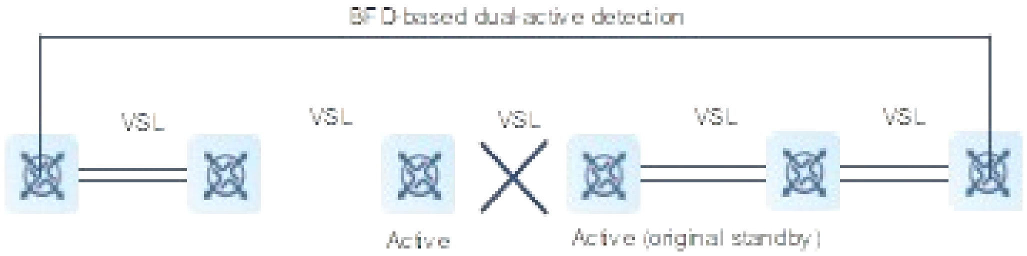
Caution

If DAD is not configured, the network is interrupted after the topology is split.

2. BFD-based DAD

The VSU supports the BFD-based DAD function. Figure 1-1 shows the connection topology. A dedicated link for DAD is added between two edge devices. When the VSL between the global active and standby devices is disconnected, two active devices coexist. If the BFD-based DAD function is configured, the two active devices send BFD-based DAD packets to each other through the BFD link, and find two identical active devices. Finally, the VSU including one of the active devices is shut down based on rules (see "Topology combination" for details) to enter the Recovery mode to avoid network exceptions.

Figure 1-1BFD-based DAD



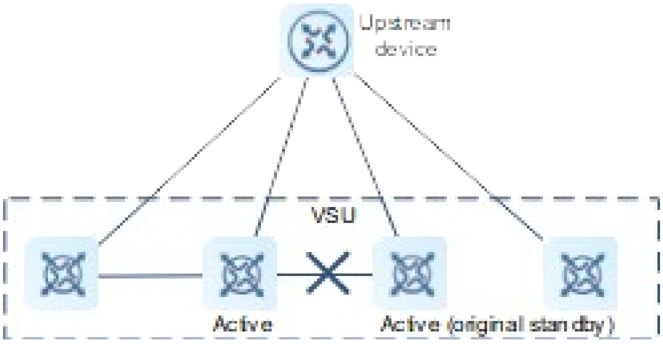
Caution

- When there is only one pair of BFD links, you are advised to deploy them at both ends of the topology.
- Extended BFD is used for the BFD-based detection, and the DAD ports cannot be configured by the existing BFD configurations and display commands.

3. AP-based DAD

The VSU also supports the AP-based DAD mechanism. Figure 1-1 shows the connection topology. The VSU and the upstream device must support the AP-based DAD function. When the VSL port is disconnected, dual active devices coexist and send detection packets to each AP member port. The upstream device forwards the detection packets from one active device to the other. The AP is composed of four member ports, which are connected to different devices in the VSU. When the topology is split, the four member ports all send and receive detection packets, and find two identical active devices. Finally, the VSU including one of the active devices is shut down based on rules (see "Topology combination" for details) to enter the Recovery mode to avoid network exceptions.

Figure 1-1AP-based DAD



✓ **Specification**

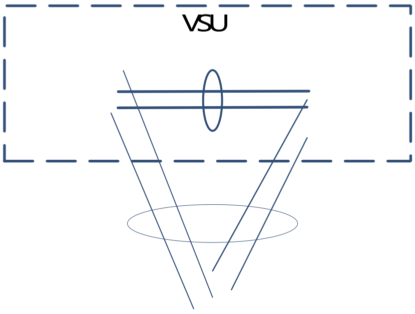
In the preceding topology, the upstream device must be a Orion_B26Q device and can forward detection packets.

1.1.5 Traffic Forwarding

1. Cross-device Aggregation

An AP binds multiple physical links to form a logical link. The VSU supports an AP across member devices. As shown in Figure 1-1, two devices form a VSU and switch A is connected to the VSU as an AP. For switch A, the AP connections shown in the figure are equivalent to those of a common AP group.

Figure 1-1Cross-device AP



A peripheral device is physically connected to each device in the VSU when a cross-device AP is configured. The advantages are as follows:

- Reserved bandwidth for the VSL: For cross-device AP traffic, the AP member of the same device is preferentially selected as the traffic egress, to avoid unnecessary traffic from being transmitted over the VSL.

- Improved network reliability: If a chassis fails, a member port on a normal device still works properly.

Table 1-1 lists the possible cross-device AP faults and their impact:

Table 1-1Cross-device AP Faults and Principle Description

Fault Scenario		Principle Description
Link fault	A single link of the AP is faulty.	● The cross-device AP redistributes traffic among the remaining normal links. ● A VSL is needed to forward traffic whose egress port is a port on the device with the faulty link.
	All links of the AP are faulty.	● The AP state changes to link down just as a common AP is disconnected.
Device fault	The active device is faulty.	● The original standby device is switched to the active device. ● Member ports on other member devices continue to work properly ● The cross-device AP redistributes traffic among the remaining normal links.
	The standby/candidate device is faulty.	● The AP member ink connected to the member device is disconnected but other member links still work properly. ● The cross-device AP redistributes traffic among the remaining normal links.

2. Traffic balancing

In a VSU, traffic may have multiple egresses. The AP and Equal-cost Multi-path Routing (ECMP) have respective traffic balancing algorithms, for example, traffic is balanced based on the source and destination MAC addresses. For details, see the description about the link AP module in the interface configuration guide. In this configuration guide, packets received by the local device are preferentially forwarded by the local device. In this way, packets are forwarded to other devices not through a VSL.

1.1.6 System Management

1. Console access

The console of the VSU active device manages multiple devices in the system. The consoles of the standby and candidate devices do not support command line input. However, you can configure VSU-related commands on the active device for a specified member device, or log in to the console of the active device through the serial port of the standby device. You can also redirect to the master supervisor module of a device by running the **session** command.

2. Interface naming

In VSU mode, the same slot ID may appear on multiple devices. Therefore, device ID (switch ID) is added to an interface name. For example, interface GigabitEthernet 1/1/1 indicates GE port 1 in slot 0 of a device with the ID of 1; interface GigabitEthernet 2/1/2 indicates GE port 2 in slot 0 of a device with the ID of 2.

3. Access to the file system

In VSU mode, you can access to the file systems on other member devices from the active device. The detailed access method is the same as that of the local file system. The only difference lies in URL prefixes.

4. Log management

All member devices of the VSU can display syslogs. Syslogs generated by the active device are displayed on the console of the active device, and their format is identical to that of syslogs displayed in standalone mode. Syslogs of other member devices are also displayed on the console of the active device, but their format is different from that of syslogs in standalone mode, because the device ID is added to the syslogs. For example, a syslog generated in standalone mode is "%VSU-5-DTM_TOPO_CVG: Node discovery done. Topology converged." Accordingly, a syslog generated by a member device with the device ID of 3 is "%VSU-5-DTM_TOPO_CVG:(3) Node discovery done. Topology converged."

1.1.7 System Upgrade

Usually, the main program versions of member devices in the VSU need to be consistent. But if such numerous member devices are upgraded one by one in standalone mode, this consumes much time and effort, and easily causes errors. The VSU offers a comprehensive system upgrade solution below:

- Check the main program versions of all member devices to determine whether the versions are consistent.
- If inconsistency is identified, the VSU synchronizes the main program of the active device to all member devices via Trivial File Transfer Protocol.

1.1.8 Quick Blinking Location

In the network cabling environment, the equipment room and the operating console are often in different places. If there are many devices in the environment, network administrators are hard to locate specific devices. Quick blinking location provides network administrators with a method for locating devices by quick blinking. By enabling this function for a device on the console, you easily find the corresponding device in the equipment room.

Note

A state of the original Status indicator is not displayed when quick blinking location is enabled, and is displayed only when it is disabled.

1.2 Restrictions and Guidelines

- A VSU can be set up by different products of the same series, but not by products of different series.
- Use 10G ports or above as the VSL ports.
- When the Switched Port Analyzer (SPAN) function is configured, a VSL port is used as neither the source

port nor the destination port of SPAN.

1.3 Configuration Task Summary

The VSU configuration includes the following tasks:

(1) Setting Up a VSU

(2) Configuring BFD-based DAD

(3)

(4) Configuring the VSL

(5) (Optional) Configuring VSU Attributes

All the following configuration tasks are optional and may be selected as needed.

- Configuring Basic VSU Attributes
- Configuring Traffic Balancing
- Switching to Standalone Mode
- Configuring Recovery Method for Recovery Mode

(6) (Optional) Configuring Quick Blinking Location

1.4 Setting Up a VSU

1.4.1 Overview

Devices start up in standalone mode by default. You need to configure the same domain ID on all devices used to set up a VSU, and assign a unique virtual machine ID for each device.

1.4.2 Restrictions and Guidelines

- If the current device works in VSU mode and cannot directly switch to another VSU domain, first switch to standalone mode and then to another VSU.
- The VSU configurations are applicable to a single physical device, and the configurations are stored in the special configuration file **config_vsu.dat**. Therefore, the **show running config** command does not display the VSU configurations. You can display the current VSU configurations by running the **show switch virtual config** command only.
- In standalone mode, the VSU running information is blank. When you run the **show switch virtual**, a prompt is displayed, indicating that the device works in standalone mode and there is no VSU running information.

1.4.3 Prerequisites

The VSL between VSU devices is normal.

1.4.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the VSU domain ID and enter the config-vs-domain configuration mode.

switch virtual domain *domain-id*

The default domain ID is 100.

Only devices with the same domain ID can form a VSU.

(4) Configure the device ID of the VSU.

switch *switch-id*

The default device ID is 1.

(5) (Optional) Configure the device priority.

switch *switch-id* **priority** *priority-number*

The default device priority is 100. A larger value indicates a higher priority.

(6) (Optional) Configure the device alias.

switch *switch-id* **description** *device-name*

No device alias is configured by default.

(7) (Optional) Specify the manner of saving the VSU configuration file of a device.

switch cfg_mode { **normal** | **single** }

normal is selected by default. That is, the VSU configurations are separately saved in **config_vsu.dat**.

(8) Return to the global configuration mode.

exit

(9) Enter the VSL port configuration mode.

vsl-port

(10) Add the member ports to the VSL.

port-member interface *interface-type interface-number*

No member port is configured by default.

The VSL member port is a two-dimensional port in standalone mode. The port must be a 10G port or above.

(11) Return to the privileged EXEC mode.

end

(12) Switch the device from the standalone mode to the VSU mode.

switch convert mode virtual

A device works in standalone mode by default.

1.5 Configuring BFD-based DAD

1.5.1 Overview

The BFD-based DAD is configured to prevent coexistence of two active devices.

1.5.2 Restrictions and Guidelines

- BFD detection ports must be direct physical routed ports in different devices.
- The configured port type is unlimited. DAD links are used to transmit only BFD packets and thus need less traffic. Therefore, you are advised to configure a 1000M or 100M port as the DAD port.
- After a layer-3 (L3) routed port configured for DAD is switched to a layer-2 (L2) switching port (by running the **switchport** command on the port), the BFD DAD configuration is automatically cleared.
- You are advised to directly connect only the active and standby devices in BFD mode.
- When the VSUs detect a dual-active conflict and one VSU enters the **Recovery** mode, you can rectify the fault by eliminating the VSL failure rather than by directly resetting the VSU in the **Recovery** mode. Otherwise, a dual-active conflict may be incurred in the network.
- Excluded ports in **Recovery** mode must be routed ports rather than VSL ports. After an excluded port is switched from a routed port to a switching port (by running the **switchport** command on the port), the excluded port configuration associated with this port is automatically cleared.
- When dual active devices are detected, one of them must enter the **Recovery** mode. In **Recovery** mode, all service ports of the device must be disabled. To ensure normal use of certain special ports (for example, management ports for remote login to devices), you can configure excluded ports that are not disabled in Recovery mode.

1.5.3 Prerequisites

A VSU has been set up.

1.5.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the BFD detection port configuration mode.

interface *interface-type interface-number*

(4) Configure the BFD detection port as a routed port.

no switchport

A port is an L2 switching port by default.

(5) Return to the global configuration mode.

exit

(6) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(7) Enable the DAD function and specify the BFD-based detection method.

dual-active detection bfd

The DAD function is disabled by default.

(8) Configure a BFD detection port.

dual-active bfd interface *interface-type interface-number*

No BFD detection port is configured by default.

(9) (Optional) Configure the list of excluded ports for Recovery mode.

dual-active exclude interface *interface-type interface-number*

No excluded port is configured by default.

1.6 Configuring AP-based DAD

1.6.1 Overview

The AP-based DAD method is configured to prevent coexistence of two active devices.

1.6.2 Restrictions and Guidelines

- When the VSUs detect a dual-active conflict and one VSU enters the **Recovery** mode, you can rectify the fault by eliminating the VSL failure rather than by directly resetting the VSU in the **Recovery** mode. Otherwise, a dual-active conflict may be incurred in the network.
- Excluded ports for the **Recovery** mode must be routed ports rather than VSL ports. After an excluded port is switched from a routed port to a switching port (by running the **switchport** command on the port), the excluded port configuration associated with this port is automatically cleared.

1.6.3 Prerequisites

A VSU has been set up.

1.6.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Enable the DAD function and specify the AP-based detection method.

dual-active detection aggregateport

The DAD function is disabled by default.

(5) Configure an AP-based detection port.

dual-active interface *interface-type interface-number* [**vlan** *vlan-id*]

No AP-based detection port is configured by default.

When the AP is a trunk port and the native VLAN is beyond the VLAN range allowed by the AP-based detection port, configure a detection VLAN for the AP-based detection port. The configured VLAN must fall in the VLAN range allowed by the trunk port, and be created on the device in advance.

(6) In AP mode of the upstream and downstream devices, enable the function of forwarding AP-based DAD packets.

dad relay enable

The DAD packets are not forwarded by default.

(7) (Optional) Configure the list of excluded ports for Recovery mode.

dual-active exclude interface *interface-type interface-number*

No excluded port is configured by default.

When dual active devices are detected, one of them must enter the **Recovery** mode. In **Recovery** mode, all service ports of the device must be disabled. To ensure normal use of certain special ports (for example, management ports for remote login to devices), you can configure excluded ports that are not disabled in **Recovery** mode.

1.7 Configuring the VSL

1.7.1 Overview

To modify a VSL member port (switch to or back from a common port, or add or delete a VSL) during setup or running of a VSU, you can log in to the VSU console through a serial port or Telnet.

1.7.2 Restrictions and Guidelines

- In practice, dynamic negotiation is used by the VSL AP to prevent link connection faults. A VSL port pool is first configured, and all VSL ports of the same member device are added to the same AP after negotiation. Ports connected to the same device are in the same AP.
- During VSU running, configured VSL member links take effect immediately. VSL ports need to be configured on all devices.
- Chassis-type devices allow 10G SFP ports or ports with higher bandwidth to act as VSL ports. Box-type devices depend on the actual product version.
- Do not set member ports (four 10G ports) of a 40G port as VSL member ports.
- To prevent a loop from being instantaneously generated when a VSL member port exits the VSL AP, the system automatically sets the member port to the **shutdown** state when you run the configuration command. After the VSL member port exits the VSL AP, you can reconnect the link and run the **no shutdown** command to enable the port again. When you configure the VSL port, the system runs the **shutdown** command to shut down the port first. If the configuration fails and you need to continue using the port as a common port, you can run the **no shutdown** command to enable the port again. An added member port ID must be three-dimensional.
- If a port is configured as an NLB reflex port, this port can be switched to a VSL member port only after the NLB reflex port configuration is deleted.
- If the VSU topology is split when a VSL port is switched to a common port, the VSL port must not be deleted. You can disconnect the physical port before deleting the VSL port.

1.7.3 Prerequisites

A VSU has been set up.

1.7.4 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSL port configuration mode.

vsl-port

(4) Add the member ports for the VSL.

port-member interface *interface-type interface-number*

No VSL member port is configured by default.

The VSL member port must be a 10G port.

1.8 Configuring VSU Attributes

1.8.1 Overview

In VSU mode, you can configure enhancements to increase the reliability and usability of the VSU.

1.8.2 Configuration Tasks

The VSU attribute configuration includes the following tasks:

All the following configuration tasks are optional and may be selected as needed.

- Configuring Basic VSU Attributes
- Configuring the VSL
- Configuring Traffic Balancing
- Switching to Standalone Mode
- Configuring Recovery Method for Recovery Mode

1.8.3 Configuring Basic VSU Attributes

1. Overview

During VSU setup or running, you can log in to the console of the active or standby device of the VSU to modify some parameters.

2. Restrictions and Guidelines

All configuration commands take effect only after the device is restarted, except the device alias modification command, which takes effect immediately.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Configure the basic VSU attributes as required.

- Modify the VSU domain ID of a specified device.

  switch *switch-id* **domain** *new-domain-id*

  The default VSU domain ID is 100.

- Modify the ID of the specified device.

  switch *switch-id* **renumber** *new-switch-id* [**force**]

  The default device ID is 1.

- Modify the priority of the specified device.

  switch *switch-id* **priority** *priority-number*

  The default device priority is 100.

- Modify the alias of the specified device.

  switch *switch-id* **description** *device-name*

  No device alias is configured by default.

- Set the CRC error parameter.

  switch crc errors *error-number* **times** *time-number*

  By default, one CRC error occurrence is recorded if the number of CRC errors incremented between two checks is 3 or more. If 10 consecutive CRC error occurrences is recorded, the port is considered abnormal.

- Specify the manner of saving the VSU configuration file of a device.

  switch cfg_mode { **normal** | **single** }

  normal is selected by default. That is, the VSU configurations are separately saved in **config_vsu.dat**.

1.8.4 Configuring Traffic Balancing

1. Overview

In the VSU, if egresses are distributed on multiple devices, traffic balancing allows forwarding traffic preferentially on the local device.

2. Restrictions and Guidelines

- By default, AP-based and ECMP-based Local Forward First (LFF) are enabled.
- In VSU mode, the cross-device AP-based LFF and ECMP-based LFF over routed ports are enabled by default. To set up a VSU with L3 switches, you are advised to configure the AP-based load balancing based on IP addresses (**src-ip**, **dst-ip**, and **src-dst-ip**).

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Disable the AP-based LFF.

no switch virtual aggregateport-lff enable

In VSU mode, the AP-based LFF is enabled by default.

(5) Disable the ECMP-based LFF.

no switch virtual ecmp-lff enable

In VSU mode, the ECMP-based LFF is enabled by default.

1.8.5 Switching to Standalone Mode

1. Overview

This function switches devices in a VSU to the standalone mode.

2. Restrictions and Guidelines

You can switch devices in a VSU to the standalone mode by using a saved standalone configuration file, or by clearing the VSU configuration.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Switch a device to the standalone mode.

switch convert mode standalone [*switch-id*]

A device works in standalone mode by default.

1.8.6 Configuring Recovery Method for Recovery Mode

1. Overview

This function disables the automatic restart function for the Recovery mode.

2. Restrictions and Guidelines

If the automatic restart function is disabled, you must enable this function again or manually restart the device to recover the device in recovery mode.

3. Prerequisites

A VSU has been set up.

4. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the VSU domain configuration mode.

switch virtual domain *domain-id*

(4) Disable the automatic restart function for the **Recovery** mode.

no recovery auto-restart enable

By default, the automatic restart function is enabled for the Recovery mode after the link fault is rectified.

1.9 Configuring Quick Blinking Location

1.9.1 Overview

When quick blinking location is enabled, the device status indicator blinks quickly.

1.9.2 Restrictions and Guidelines

- Quick blinking location is automatically disabled 30 minutes after it is started.
- The configuration takes effect immediately and cannot be saved. If you restart the device or perform an active/standby switch, quick blinking location is disabled.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enable/Disable quick blinking location.

led-blink { **enable** | **disable** } [**device** *switch-id*]

Quick blinking location is disabled by default. If no device ID is specified, the command applies to all devices in the VSU domain.

1.10 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Table 1-1VSU Monitoring

Command	Purpose
show switch virtual [**topology** | **config** | **role balance**]	Views the topology, configurations, roles, and forwarding and balancing policies of the running VSU.
show switch virtual dual-active { **bfd** | **aggregateport** | **summary** }	Displays the information about the current DAD.
show switch virtual link [**port**]	Displays the information about the current VSL.
show switch id	Displays the ID of the current device.

1.11 Configuration Examples

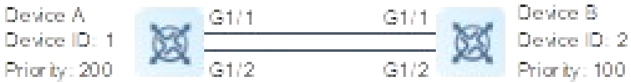
1.11.1 Setting Up a VSU

1. Requirements

As shown in Figure 1-1, connect Device A to Device B through two 10G cables to form a VSU with basic configurations.

2. Topology

Figure 1-1**Topology of the VSU**



3. Notes

- Configure the domain ID, device ID, device priority, device name, and VSL ports for the VSU.
- Configure the VSU switching mode.

4. Procedure

(1) On Device A, set the domain ID to 100, device ID to 1, device priority to 200, VSU device name to Device A, and VSL ports to tenGigabitEthernet 1/1 and tenGigabitEthernet 1/2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# switch virtual domain 100
DeviceA(config-vs-domain)# switch 1
DeviceA(config-vs-domain)# switch 1 priority 200
DeviceA(config-vs-domain)# switch 1 description DeviceA
DeviceA(config-vs-domain)# switch crc errors 10 times 20
DeviceA(config-vs-domain))# exit
DeviceA(config)# vsl-port
DeviceA(config-vsl-port)# port-member interface tengigabitethernet 1/1
DeviceA(config-vsl-port)# port-member interface tengigabitethernet 1/2
DeviceA(config)# exit
DeviceA# switch convert mode virtual
```

(2) On Device B, set the domain ID to 100, device ID to 2, device priority to 100, VSU device name to Device B, and VSL ports to tenGigabitEthernet 1/1 and tenGigabitEthernet 1/2.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# switch virtual domain 100
DeviceB(config-vs-domain)# switch 2
DeviceB(config-vs-domain)# switch 2 priority 100
DeviceB(config-vs-domain)# switch 2 description DeviceB
DeviceB(config-vs-domain)# switch crc errors 10 times 20
DeviceB(config-vs-domain))# exit
DeviceB(config)# vsl-port
DeviceB(config-vsl-port)# port-member interface Tengigabitethernet 1/1
DeviceB(config-vsl-port)# port-member interface Tengigabitethernet 1/2
DeviceB(config-vsl-port)# exit
DeviceB# switch convert mode virtual
```

5. Verification

(1) Run the **show switch virtual role** command to verify whether the role of Device A is **Active** and that of Device B is **Standby**. If yes, the VSU is set up; if not, the VSU fails to be set up.

```
DeviceA# show switch virtual role
Switch_id     Domain_id     Priority     Position     Status     Role
Description
1(1)          100(100)      200(200)     LOCAL        OK         ACTIVE
DeviceA
2(2)          100(100)      100(100)     REMOTE       OK         STANDBY
DeviceB
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
switch virtual domain 100
!
switch 1
switch 1 priority 200
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!
end
```

- Device B configuration file

```
hostname DeviceB
!
switch virtual domain 100
!
switch 2
switch 2 priority 100
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!
end
```

7. Common Errors

- Different domain IDs (**domain-id**) are configured.
- The VSL ports are not up.

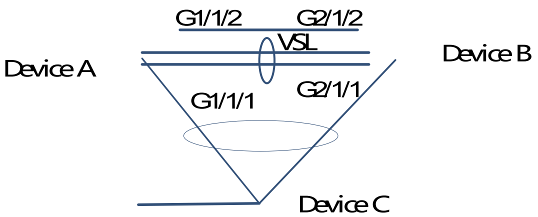
1.11.2 Configuring BFD-based DAD

1. Requirements

As shown in Figure 1-1, form a VSU with Device A and Device B. To prevent an IP address conflict in the LAN caused by two identical active devices in case of VSL disconnection, configure the BFD-based detection mechanism to quickly detect two active devices and to actively switch one of them to the Recovery mode (the service forwarding function is disabled).

2. Topology

Figure 1-1**Topology for BFD-based DAD**



3. Notes

- Enable the BFD-based DAD.
- Designate a BFD detection port, which must be configured as a routed port.

Note

As Device A and Device B form the VSU, the preceding configuration can be performed on either Device A or Device B. Device A is used as an example.

4. Procedure

On Device A, configure GigabitEthernet 1/1/2 and GigabitEthernet 2/1/2 as routed ports, enable the BFD-based DAD, and set the BFD-based detection ports to GigabitEthernet 1/1/2 and GigabitEthernet 2/1/2.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface GigabitEthernet 1/1/2
DeviceA(config-if-GigabitEthernet 1/1/2)# no switchport
DeviceA(config)# interface GigabitEthernet 2/1/2
DeviceA(config-if-GigabitEthernet 2/1/2)# no switchport
DeviceA(config-if)# switch virtual domain 1
DeviceA(c config-vs-domain)# dual-active detection bfd
DeviceA(config-vs-domain)# dual-active bfd interface GigabitEthernet 1/1/2
DeviceA(config-vs-domain)# dual-active bfd interface GigabitEthernet 2/1/2
```

5. Verification

Disconnect all VSLs, log in to the console of Device A , and run the **show switch virtual** command to check whether **Status** is set to **OK** (Device A runs normally when dual active devices are detected).

```
VSU# show switch virtual
Switch_id     Domain_id     Priority     Position     Status     Role
Description
---------------------------------------------------------------------------------
---------
1(1)          1(1)          100(100)     LOCAL        OK         ACTIVE
DeviceA
```

Log in to the console of Device A, and run the **show switch virtual dual-active bfd** command to check whether the BFD enabling status is **Yes** and the status of the BFD-based detection port GigabitEthernet 2/1/2 of Device B is **Down**.

```
VSU-RECOVERY-2# show switch virtual dual-active bfd
BFD dual-active detection enabled: Yes
BFD dual-active interface configured:
  GigabitEthernet 1/1/2: UP
  GigabitEthernet 2/1/2: DOWN
```

Log in to the console of Device B, and run the **show switch virtual** command to check whether the value of **Status** changes to **Recovery** and the device name is suffixed with **-RECOVERY-2**.

```
VSU-RECOVERY-2#show switch virtual
Switch_id     Domain_id     Priority     Position     Status     Role
Description
---------------------------------------------------------------------------------
----------
2(2)          1(1)            90(90)     LOCAL        Recovery   ACTIVE
DeviceB
```

Log in to the console of Device B, and run the **show switch virtual dual-active summary** command to check whether the value of **In dual-active recovery mode** is **Yes** (Device B works in recovery mode).

```
VSU-RECOVERY-2# show switch virtual dual-active summary
BFD dual-active detection enabled: Yes
Aggregateport dual-active detection enabled: No
Interfaces excluded from shutdown in recovery mode:
```

```
In dual-active recovery mode: Yes
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 1/1/2
 no switchport
!
interface GigabitEthernet 2/1/2
 no switchport
!
switch virtual domain 1
dual-active detection bfd
dual-active bfd interface GigabitEthernet 1/1/2
dual-active bfd interface GigabitEthernet 2/1/2
!
switch 1
switch 1 priority 100
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 1/1/2
 no switchport
!
interface GigabitEthernet 2/1/2
 no switchport
!
switch virtual domain 1
dual-active detection bfd
dual-active bfd interface GigabitEthernet 1/1/2
dual-active bfd interface GigabitEthernet 2/1/2
!
switch 2
switch 2 priority 90
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

7. Common Errors

- The BFD-based detection port is not configured as a routed port.
- Either BFD-based or AP-based DAD is selected.

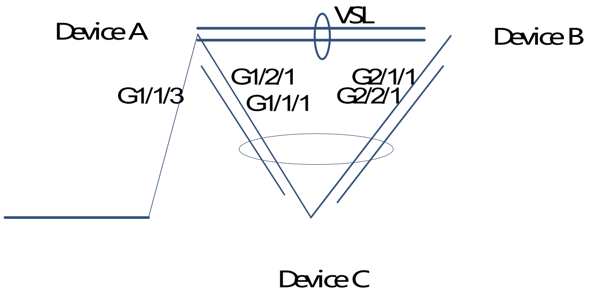
1.11.3 Configuring AP-based DAD

1. Requirements

As shown in Figure 1-1, form a VSU with Device A and Device B, and connect Device C to Device A and Device B separately over an AP. To prevent an IP address conflict in the LAN caused by two identical active devices in case of VSL disconnection, configure the AP-based detection mechanism to quickly detect two active devices and to actively switch one of them to the Recovery mode (the service forwarding function is disabled).

2. Topology

Figure 1-1**Topology for AP-based DAD**



3. Notes

- Configure the ports connecting Device C to Device A and Device C to Device B as the same AP group.
- Enable the AP-based DAD.
- Configure the AP-based detection port.
- Configure the ports connecting Device C to Device A and Device B as the same AP group. Enable the function of forwarding AP-based DAD packets of this port group.

Note

As Device A and Device B form the VSU, the preceding configuration can be performed on either Device A or Device B. Device A is used as an example.

4. Procedure

On Device A, add GigabitEthernet 1/1/1, GigabitEthernet 1/2/1, GigabitEthernet 2/1/1, and GigabitEthernet 2/2/1 to the AP group port-group 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# interface range GigabitEthernet 1/1/1-2
DeviceA(config-if-range)# port-group 1
DeviceA(config-if-range)# interface range GigabitEthernet 2/1/1-2
DeviceA(config-if-range)# port-group 1
```

On Device A, enable the AP-based DAD, and set the detection port to aggregatePort 1.

```
DeviceA> enable
DeviceA# configure
DeviceA(config)# switch virtual domain 1
DeviceA(config-vs-domain)# dual-active detection aggregateport
DeviceA(config-vs-domain)# dual-active interface aggregatePort 1
```

On Device C, add GigabitEthernet 0/1, GigabitEthernet 0/2, GigabitEthernet 0/3, and GigabitEthernet 0/4 to the AP group port-group 1.

```
DeviceC> enable
DeviceC# configure
DeviceC(config)# interface range GigabitEthernet 0/1-4
DeviceC(config-if-range)# port-group 1
```

On Device C, configure the function of forwarding DAD packets.

```
DeviceC> enable
DeviceC# interface aggregatePort 1
DeviceC(config-if-AggregatePort 1)# dad relay enable
```

5. Verification

Run the **show switch virtual dual-active summary** and **show switch virtual dual-active aggregateport** commands to check whether the configurations are correct.

```
DeviceA# show switch virtual dual-active summary
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: NO
DeviceA# show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
  AggregatePort 1: UP
     GigabitEthernet 1/1/1: UP
```

```
    GigabitEthernet 1/2/1: UP
    GigabitEthernet 2/1/1: UP
    GigabitEthernet 2/2/1: UP
```

```
S57H3_206_VSU-RECOVERY-2#sh switch virtual dual-active su
BFD dual-active detection enabled: No
Aggregateport dual-active detection enabled: Yes
Interfaces excluded from shutdown in recovery mode:
In dual-active recovery mode: Yes
S57H3_206_VSU-RECOVERY-2#sh switch virtual
Switch_id     Domain_id     Priority     Position     Status     Role
Description
--------------------------------------------------------------------------------
---------
2(2)          100(100)      100(100)     LOCAL        Recovery   ACTIVE
S57H4-207
S57H3_206_VSU-RECOVERY-2#show switch virtual dual-active aggregateport
Aggregateport dual-active detection enabled: Yes
Aggregateport dual-active interface configured:
  AggregatePort 7: DOWN
    GigabitEthernet 1/0/1: DOWN
    GigabitEthernet 2/0/1: DOWN
```

6. Configuration Files

- Device A configuration file

```
hostname DeviceA
!
interface GigabitEthernet 1/1/1
 port-group 1
!
interface GigabitEthernet 1/1/2
 port-group 1
!
interface GigabitEthernet 2/1/1
 port-group 1
!
interface GigabitEthernet 2/1/2
 port-group 1
!
switch virtual domain 1
dual-active detection aggregateport
dual-active interface aggregatePort 1
!
switch 1
switch 1 priority 100
switch 1 description DeviceA
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device B configuration file

```
hostname DeviceB
!
interface GigabitEthernet 1/1/1
 port-group 1
!
interface GigabitEthernet 1/1/2
 port-group 1
!
interface GigabitEthernet 2/1/1
 port-group 1
!
interface GigabitEthernet 2/1/2
 port-group 1
!
switch virtual domain 1
dual-active detection aggregateport
dual-active interface aggregatePort 1
!
switch 2
switch 2 priority 90
switch 2 description DeviceB
switch crc errors 10 times 20
!
port-member interface TenGigabitEthernet 0/1
port-member interface TenGigabitEthernet 0/2
!
switch convert mode virtual
!

end
```

- Device C configuration file

```
hostname DeviceC
!
interface GigabitEthernet 0/1
```

```
 port-group 1
!
interface GigabitEthernet 0/2
 port-group 1
!
interface GigabitEthernet 0/3
 port-group 1
!
interface GigabitEthernet 0/4
 port-group 1
!
interface AggregatePort 1
 dad relay enable
!

end
```

7. Common Errors

- The AP detection port must be an AP.
- Either AP-based or BFD-based DAD is selected.

1.12 Common Misconfigurations

- The VSL port type is not supported.
- Different domain IDs (**domain-id**) are configured.