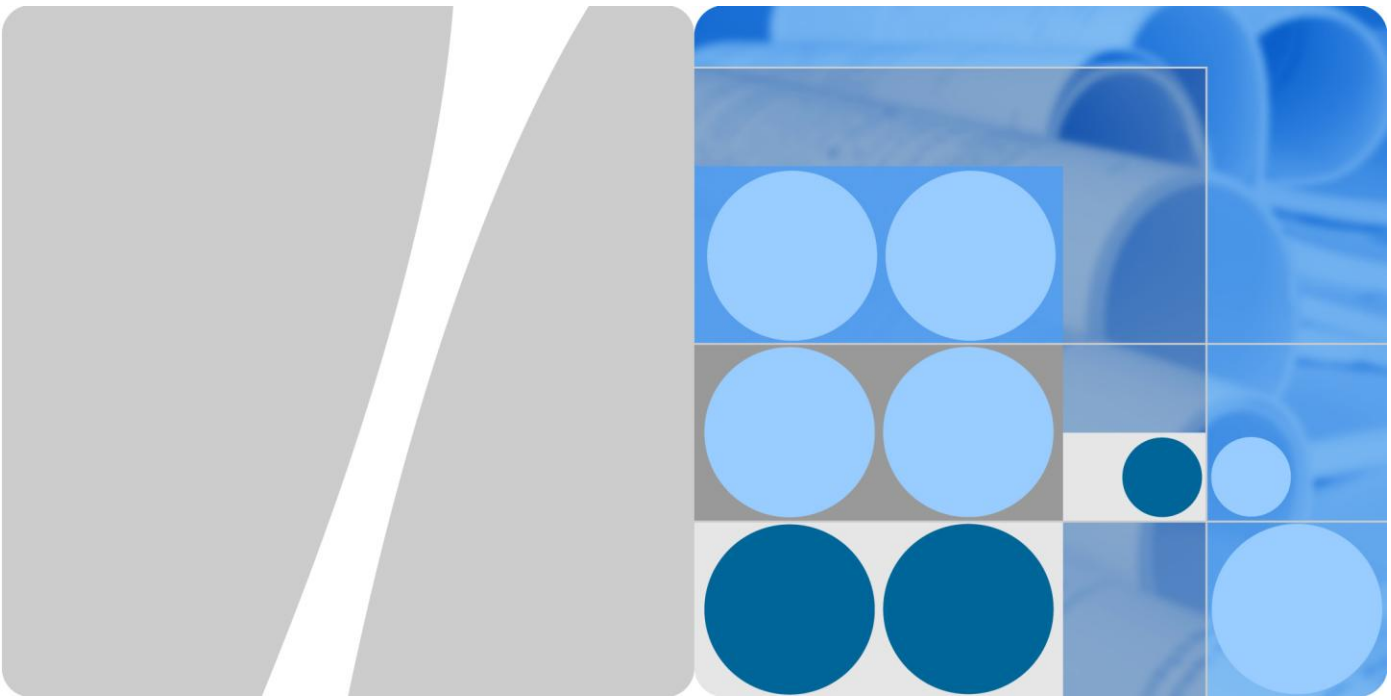


CloudEngine 8800&7800&6800&5800 Series Switches

iStack Technology White Paper

Issue 03

Date 2016-01-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

Contents

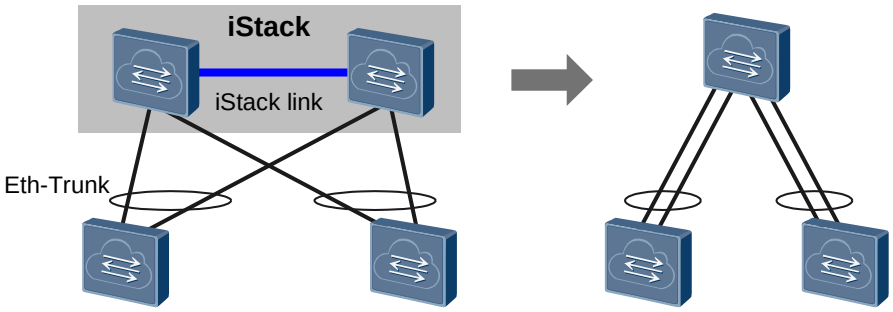
1 Stack Overview

This section describes the definition of a stack and purpose of setting up a stack.

Definition

Intelligent stack (iStack) technology combines multiple switches into a virtual switching device, as shown in Figure 1-1.

Figure 1-1 Schematic diagram of a stack



Purpose

Stacking technology provides high network reliability and scalability, while simplifying network management.

- High reliability: Member switches in a stack work in redundancy mode. Inter-device Eth-Trunk links can also be set up between the member switches to implement link redundancy.
- High scalability: By combining physical switches into a stack, you can easily increase the number of ports, bandwidth, and processing capability without changing the network topology.
- Simple configuration and management: You can log in to a stack from any member switch to manage and configure all the member switches in the stack. In addition, complicated Layer 2 ring protection protocols (such as MSTP) or Layer 3 protection switching protocols (such as VRRP) are not required after switches set up a stack; therefore, the network configuration is much simpler.

2 Principles

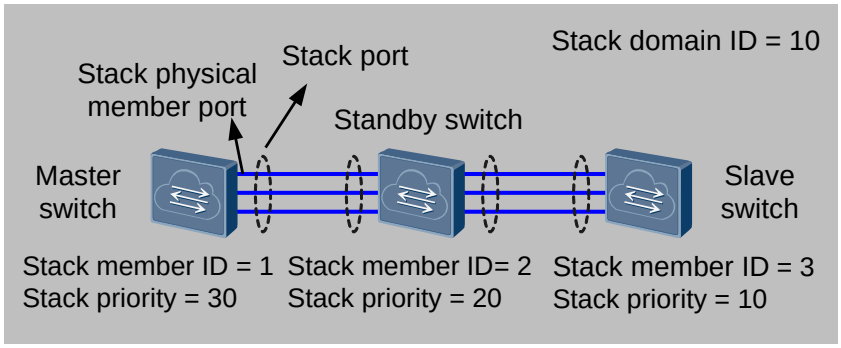
About This Chapter

This section describes concepts and mechanisms of stacking technology.

2.1 Concepts

Figure 2-1 shows the roles and related concepts in a stack.

Figure 2-1 Roles and concepts in a stack



- Roles

  Switches that have joined a stack are member switches. Each member switch in a stack plays one of the following roles:

  - Master switch

    The master switch manages the entire stack. A stack has only one master switch.

  - Standby switch

    The standby switch is a backup of the master switch. When the master switch fails, the standby switch takes over all services from the master switch. A stack has only one standby switch.

  - Slave switch

    A slave switch forwards service traffic. The more slave switches in a stack, the higher forwarding performance the stack can provide. Apart from the master and standby switches, all the other switches in a stack are slave switches.

- Stack domain

  After switches are connected using stack links and set up a stack, they form a stack domain. Multiple stacks can be deployed on a network to support various applications. These stacks are identified by their domain IDs.

- Stack member ID

  Stack member IDs are used to identify and manage member switches in a stack. Each member switch in a stack has a unique member ID.

- Stack priority

  The stack priority of a member switch determines the role of the member switch in role election. A larger value indicates a higher priority and higher probability that the member switch is elected as the master switch.

- Physical member port

  After the mode of a physical port is set to stack, the port becomes a physical member port. Physical member ports are used to connect stack member switches.

- Stack port

  A stack port is a logical port exclusively used for stacking and includes several physical stack ports. Multiple physical member ports can be added to a stack port to improve stack link bandwidth and reliability.

  Each switch supports two stack ports, named Stack-Port*n*/1 and Stack-Port*n*/2, where *n* is the stack member ID of the switch.

2.2 Stack Setup

A stack is set up after the following stages:

1. Physical connection setup: When multiple switches are connected in a specific topology according to network requirements, a stack network is established.
2. Master election: Member switches exchange stack competition packets and elect a master switch according to master election rules.
3. Topology collection: The master switch collects information about all the member switches and calculates the topology. If some member switches have the same stack member ID, the master switch reassigns stack member IDs to the member switches.
4. Running: The master switch synchronizes the topology of the entire stack to all the member switches and selects a standby switch.

Physical Connection Setup

Two stack topologies are available: chain topology and ring topology, as shown in Figure 2-2. Table 2-1 compares the two stack topologies in terms of reliability, link bandwidth utilization, and convenience of cable connections.

Figure 2-2 Stack topologies

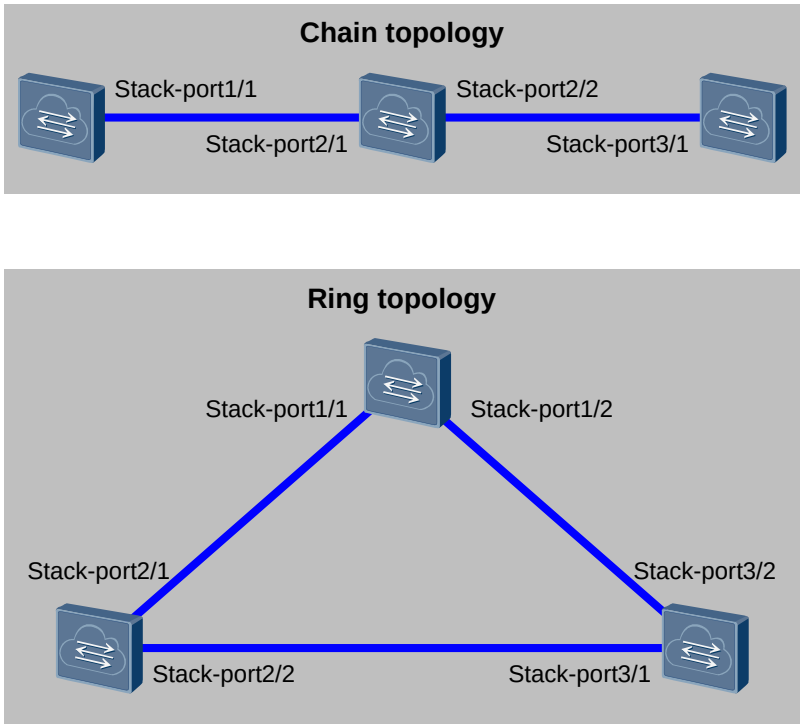


Table 2-1 Comparison between stack topologies

Topology	Advantage	Disadvantage	Usage Scenario
Chain topology	Supports long-distance stacking because the first and last member switches do not need to be connected by a physical link.	• Low reliability: If any stack link fails, the stack splits. • Low stack link bandwidth efficiency: The entire stack relies on a single path.	A chain topology is recommended when member devices are far from one another and a ring topology is difficult to deploy.
Ring topology	• High reliability: If a stack link fails, the topology changes from ring to chain, and the stack can still function	The first and last member switches need to be connected by a physical link, so this topology is not appropriate for long-distance stacking.	A ring topology is recommended when member switches are located near one another, because this topology has higher reliability and link utilization.

Topology	Advantage	Disadvantage	Usage Scenario
	normally. • High link bandwidth efficiency: Data can be forwarded along the shortest path.		

Role Election

After a stack is set up, member switches exchange stack competition packets to elect a master switch. The member switches compare the following items in the listed order to elect the master switch (the election ends when a winning switch is found):

1. Running status: The switch that starts first becomes the master switch.
2. Stack priority: The switch with the highest stack priority becomes the master switch.
3. Software version: The switch running the latest software version becomes the master switch.
4. Bridge MAC address: The switch with the smallest bridge MAC address becomes the master switch.

   During the delivery of a device, 16 MAC addresses are allocated to the device, among which the smallest MAC address becomes the bridge MAC address.

Topology Collection

After a master switch is elected, it collects information about all the member switches and calculates the topology. If some member switches have the same stack member ID, the master switch reassigns stack member IDs to the member switches.

Stable Running

After the master switch completes topology calculation, it synchronizes the topology of the entire stack to all the member switches and selects a standby switch. The master switch compares the following items of member switches in the listed order to select the standby switch (the election ends when a winning switch is found):

1. Stack priority: The switch with the highest stack priority becomes the standby switch.
2. MAC address: The switch with the smallest MAC address becomes the standby switch.

Software Version Synchronization

A stack supports software version synchronization among the member switches. The member switches do not have to run the same software version, and they can set up a stack as long as their software versions are compatible with each another. If software version running on a member switch is different from that on the master switch, the member switch downloads the system software from the master switch, restarts with the new system software, and rejoins the stack.

Configuration File Synchronization

A stack uses a strict configuration file synchronization mechanism to ensure that the member switches work like one device.

- When a stack is set up, each member switch starts with its own configuration file. After switches start, the standby and slave switches combine their stack configurations into the configuration file of the master switch to form the configuration file of the stack system.
- When the stack is running normally, the master switch manages the entire stack, and synchronizes configurations made by users to the other switches in real time to maintain configuration consistency on all the member switches.

The configuration file synchronization mechanism ensures that the member switches save the same configuration file. If the master switch fails, other member switches can provide services using the same configuration file.

Configuration Combination and Conflict Detection

Configuration Combination

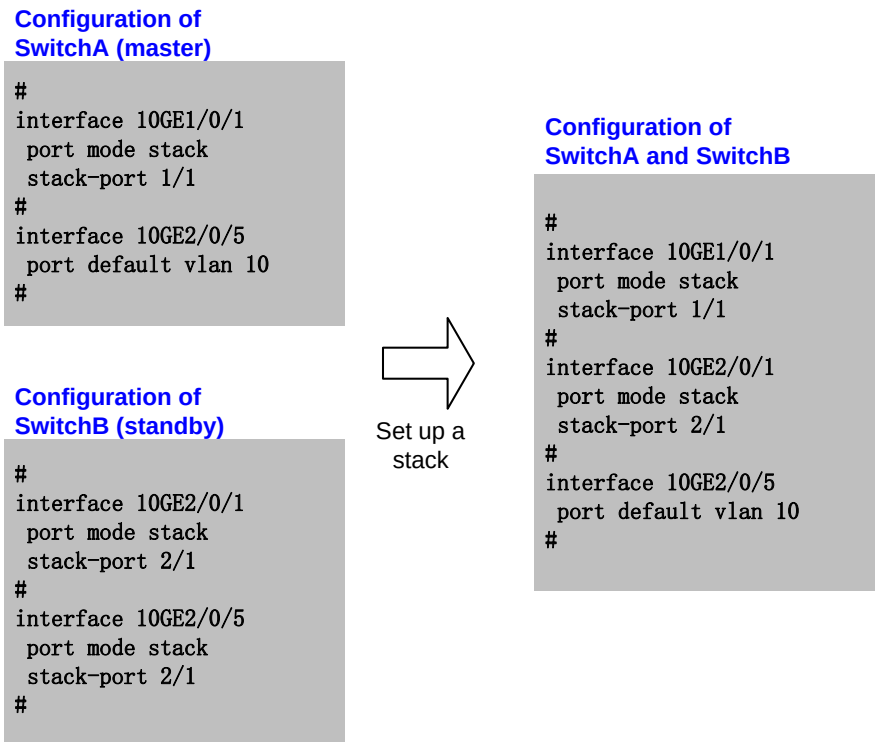
Stack configuration on a switch is saved in the configuration file. When a stack is set up, the standby and slave switches combine their own stack configurations with that of the master switch. The configuration combination rules are as follows:

- The standby and slave switches combine their stack configurations with that of the master switch, including the stack attribute configuration, stack port configuration, and 40GE port split configuration. If the master switch has the offline stack configurations of the standby and slave switches, the stack configuration of the master switch takes effect.

  As shown in Figure 2-3, SwitchA and SwitchB in a stack combine their port configurations. Port 10GE2/0/5 on SwitchA is configured with common services and the configuration conflicts with the port configuration of SwitchB. Because SwitchA is the master switch, the port configuration of SwitchA takes effect.
- After a stack is set up, the standby and slave switches synchronize their configuration files with the configuration file of the master switch to keep the same configuration with the master switch.

  As shown in Figure 2-3, SwitchB synchronizes its configuration file with that of SwitchA after the stack is set up.

Figure 2-3 Port configuration combination



Configuration Conflict Detection

A configuration conflict may occur if the master switch has offline configurations made for the standby and slave switches, which may cause a stack setup failure. A configuration conflict occurs in the following situations:

- When member switches combine their physical member port configurations, the number of physical member ports in a stack port exceeds the limit.
- All physical member ports on the standby and slave switches have the Shutdown configuration on the master switch or have configuration conflicts with the stack system.
- Stack ports of the standby or slave switch have the shutdown configuration or the configuration that conflicts with the stack on the master switch.
- A stack contains physical member ports of different types.
- All physical member ports are added to different stack ports.

When any of the preceding conflicts occurs, the standby and slave switches cannot set up a stack with the master switch. In this case, modify the configuration of the master switch or the standby and slave switches to avoid configuration conflicts, and then restart the switches.

2.3 Stack Management

After a stack is set up, the member switches are virtualized into one device on the network. The management, login, and access methods are all different from those used on a single switch.

2.3.1 Member Switch Management

Member switches in a stack are managed on a per-slot basis and are identified by stack member IDs. When using commands to configure and manage the member switches in a stack, you must specify their stack member IDs. For example, you can run **display device slot 2** to view information about a member switch in a stack. Here, **2** is the stack member ID of this switch.

In a stack, interface numbers contain stack member IDs, in the *stack member ID/subcard ID/port number* format. For example, after a switch joins a stack and is assigned stack member ID 2, the first interface on the switch is numbered 10GE2/0/1.

2.3.2 Stack Login

After a stack is set up, the member switches are virtualized into one device on the network, and all resources on the member switches are managed by the master switch. You can log in to the stack from any member switch to manage and maintain the entire stack. When you log in to a stack, you actually log in to the master switch, regardless of what login method you use and which member switch you have logged in to.

You can log in to a stack using the following methods:

- Local login: Log in through the console interface of any member switch.
- Remote login: Log in through the management interface or another Layer 3 interface of any member switch, using remote login protocols such as Telnet and STelnet.

NOTE

- After a stack is set up, the configuration file of the master switch takes effect in the stack. Therefore, you must specify the IP address of the master switch when logging in to the stack remotely.
- If multiple management interfaces are available in a stack, only one management interface takes effect.

2.3.3 File System Access

To access the file system on a switch, you need to specify the root directory of the flash storage. The flash storage name on a standalone switch without the stacking function is different from that on a stack member switch.

- On a standalone switch without the stacking function:

  flash: indicates the root directory of the flash storage on the switch.
- In a stack:
  - **flash**: indicates the root directory of the flash storage on the master switch.
  - **Stack member ID#flash**: indicates the root directory of the flash storage on the standby switch or a slave switch. For example, **2#flash** indicates the root directory of the flash storage on the member switch with stack member ID 2.

For more information about the file system, see section "File System Overview" in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Basic Configurations*.

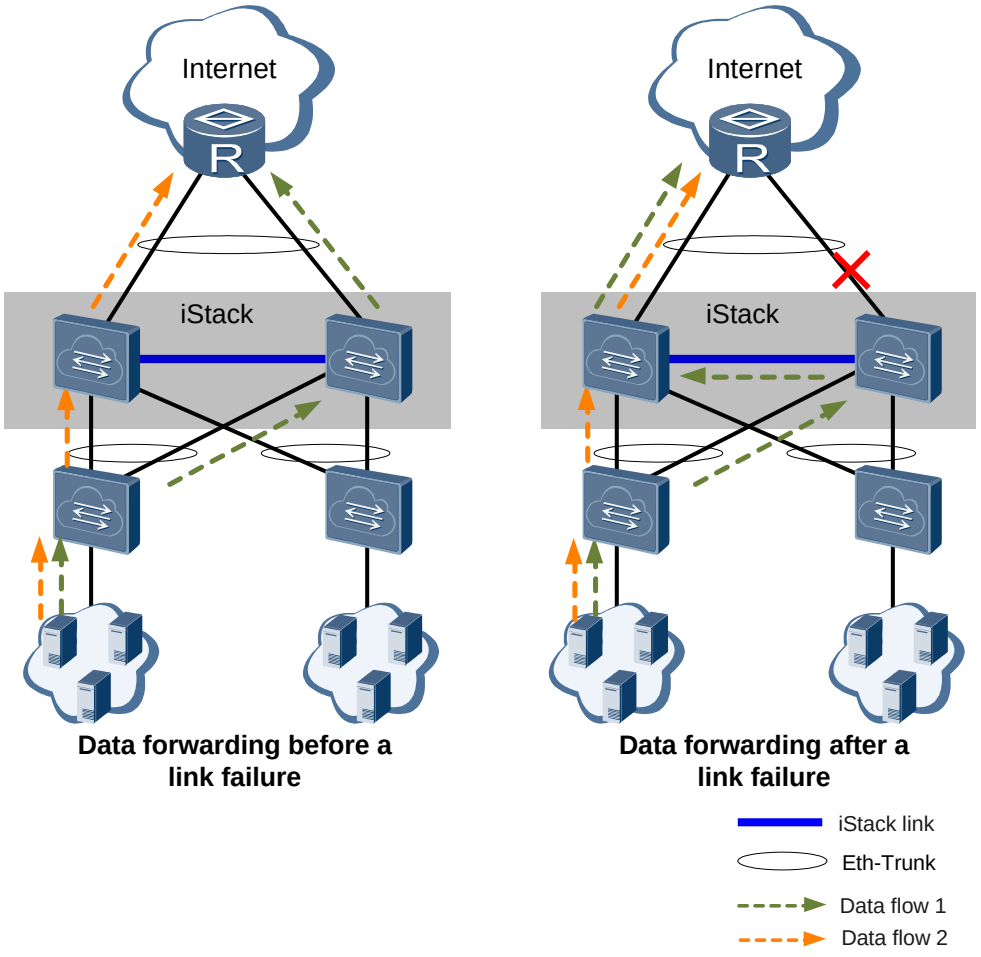
2.4 Inter-Device Link Aggregation and Local Preferential Forwarding

Inter-Device Link Aggregation

A stack supports inter-device link aggregation (Eth-Trunk). That is, Ethernet ports on different member switches can be bound to one Eth-Trunk. The Eth-Trunk link still works when a member switch or a member link in the Eth-Trunk fails, ensuring reliable data transmission. Inter-device link aggregation prevents single-point failures in a stack and greatly improves network reliability.

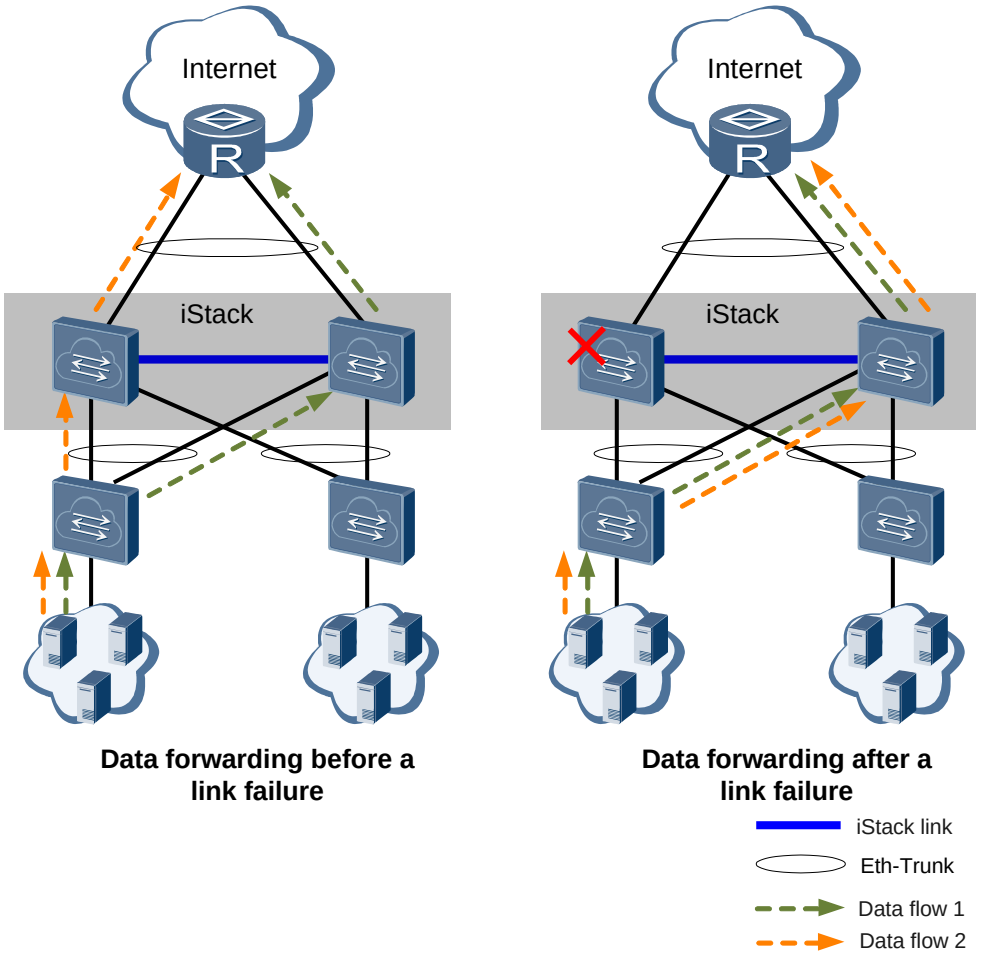
As shown in Figure 2-4, traffic sent to the core device on the network is equally distributed to member links of an Eth-Trunk set up between the stack member switches. When an Eth-Trunk member link fails, traffic on this link is distributed to the other link. This link backup mechanism improves network reliability.

Figure 2-4 Link backup through inter-device link aggregation



As shown in Figure 2-5, when a member switch in the stack fails, traffic is switched to the Eth-Trunk member link on the other member switch. This device backup mechanism improves network reliability.

Figure 2-5 Device backup through inter-device link aggregation



Local Preferential Forwarding

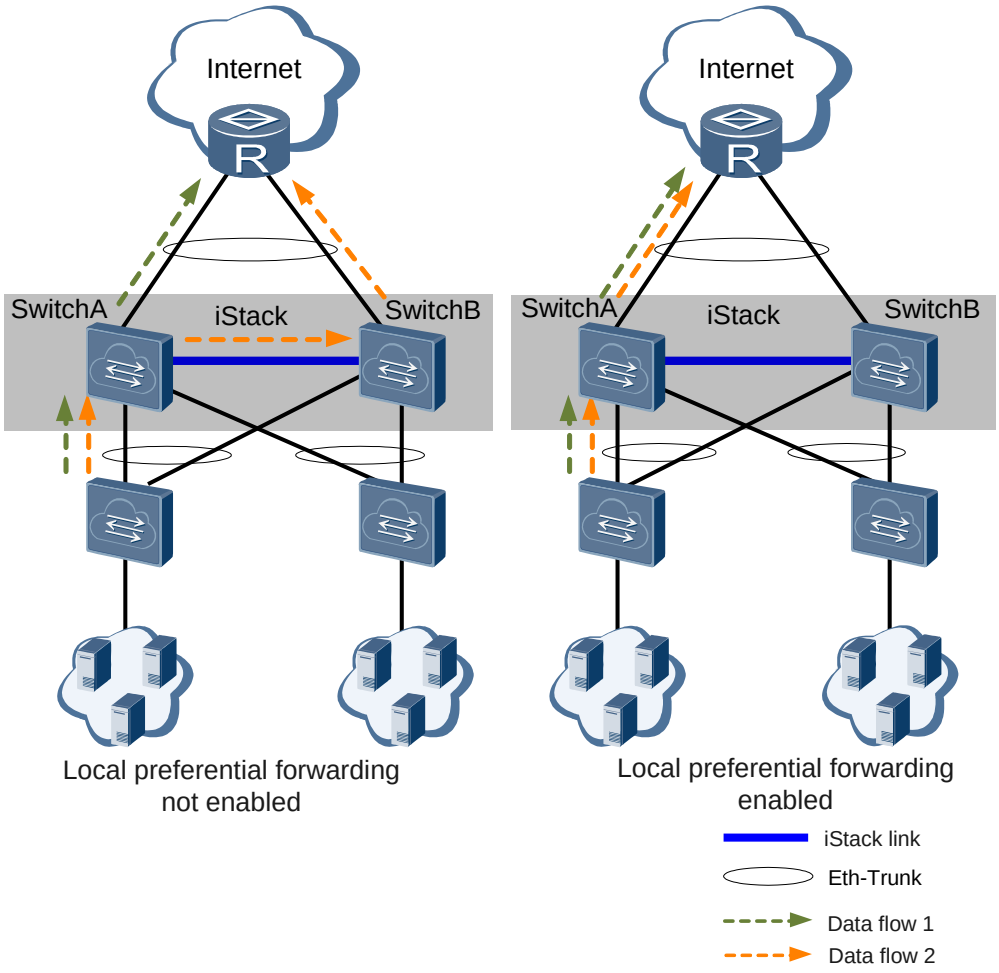
When an inter-device Eth-Trunk is configured in a stack, the stack uses the hash algorithm to select outbound interfaces in the Eth-Trunk. Therefore, traffic received on a member switch may be forwarded through the other member switch. Inter-device forwarding consumes bandwidth on stack links. As bandwidth provided by a stack cable is limited, this forwarding mode increases loads on stack cables and reduces forwarding efficiency. Local preferential forwarding can solve this problem. This feature ensures that traffic reaching the local switch is preferentially forwarded through a local interface. If the local outbound interface fails, traffic is forwarded through an interface on the other member switch.

As shown in Figure 2-6, SwitchA and SwitchB set up a stack, and their uplink and downlink interfaces are bundled to Eth-Trunk interfaces. Without the local preferential forwarding feature, traffic reaching SwitchA is load balanced between the Eth-Trunk member links. Some of traffic is forwarded through the stack cables and sent out from a physical interface on SwitchB. If local preferential forwarding is enabled, traffic reaching SwitchA is forwarded through a local physical interface.

NOTE

This function is only valid for known unicast packets, and is invalid for unknown unicast packets, broadcast packets, and multicast packets.

Figure 2-6 Local preferential forwarding



2.5 Joining and Leaving a Stack

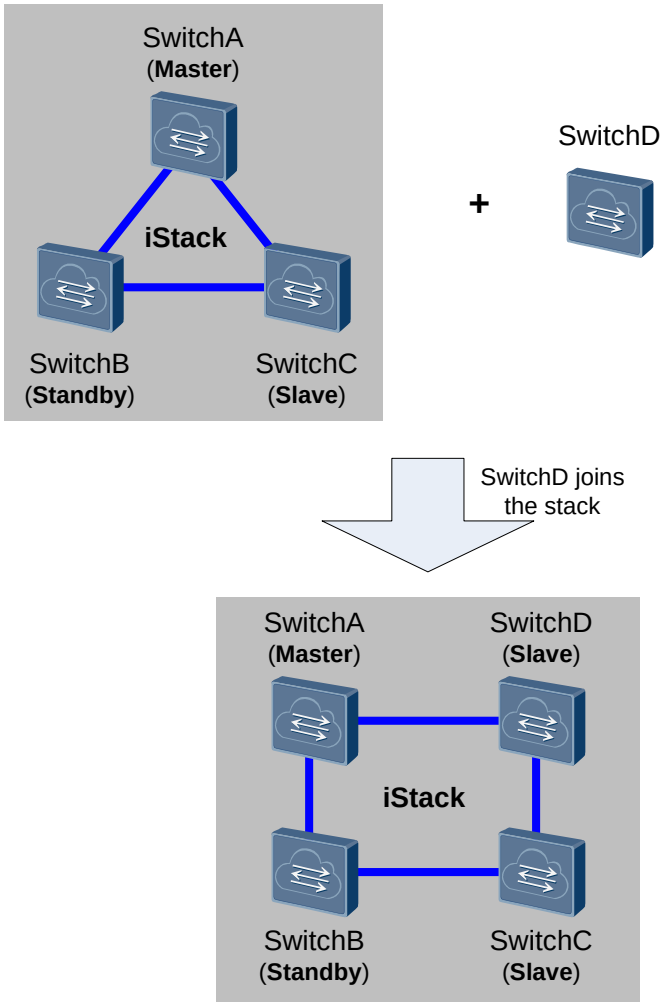
Joining a Stack

Figure 2-7 illustrates how a new switch joins a running stack.

NOTE

- A switch can be added to a stack while it is powered on or off. This section describes how a member switch joins a stack after being powered off. For details on how a member switch joins a stack after being powered on, see 2.6 Stack Merging.
- It is not recommended to add a member switch to a stack while the power is on.

Figure 2-7 A new member joins a stack



To add a switch to a stack, perform the following steps:

1. Examine the physical connections between the current stack member switches and determine where to connect the new member switch.
   - If the stack has a chain topology, add the new switch to either end of the chain to minimize the impact on running services.
   - If the stack has a ring topology, tear down a physical link to change the ring topology to a chain topology, and add the new switch to either end of the chain. Then connect the switches on both end to restore the ring topology.
2. Complete stack configuration on the stack and new member switch and save the configuration.
3. Power off the new member switch, connect it to the stack using stack cables, and power it on.

The new member switch joins the stack as a slave switch, and the original master and standby switches retain their roles. If the stack member ID of the new member switch conflicts with another member switch in the stack, the master switch assigns a new stack member ID to the new member switch. The member switch then updates the stack topology and synchronizes the stack topology to all the member switches.

Leaving a Stack

A member switch leaves a stack after it is disconnected from the stack. Depending on the role of the switch that has left the stack, the stack is affected in the following ways:

- When the master switch leaves the stack, the standby switch becomes the new master switch. It then recalculates the topology, synchronizes updated the topology to the other member switches, and selects a new standby switch. Then the stack enters the running state.
- When the standby switch leaves the stack, the master switch selects a new standby switch, recalculates the topology, and synchronizes the updated topology to the other member switches. Then the stack enters the running state.
- When a slave switch leaves the stack, the master switch recalculates the topology and synchronizes the updated topology to the other member switches. Then the stack enters the running state.

A member switch leaves a stack after you disconnect its stack cables and remove it from the stack.

- After removing a member switch from a ring stack topology, use a stack cable to connect the two ports originally connected to this member switch to ensure network reliability.
- In a chain topology, removing an intermediate switch causes the stack to split. Therefore, analyze services before removing a member switch from the stack to minimize the impact on services.

2.6 Stack Merging

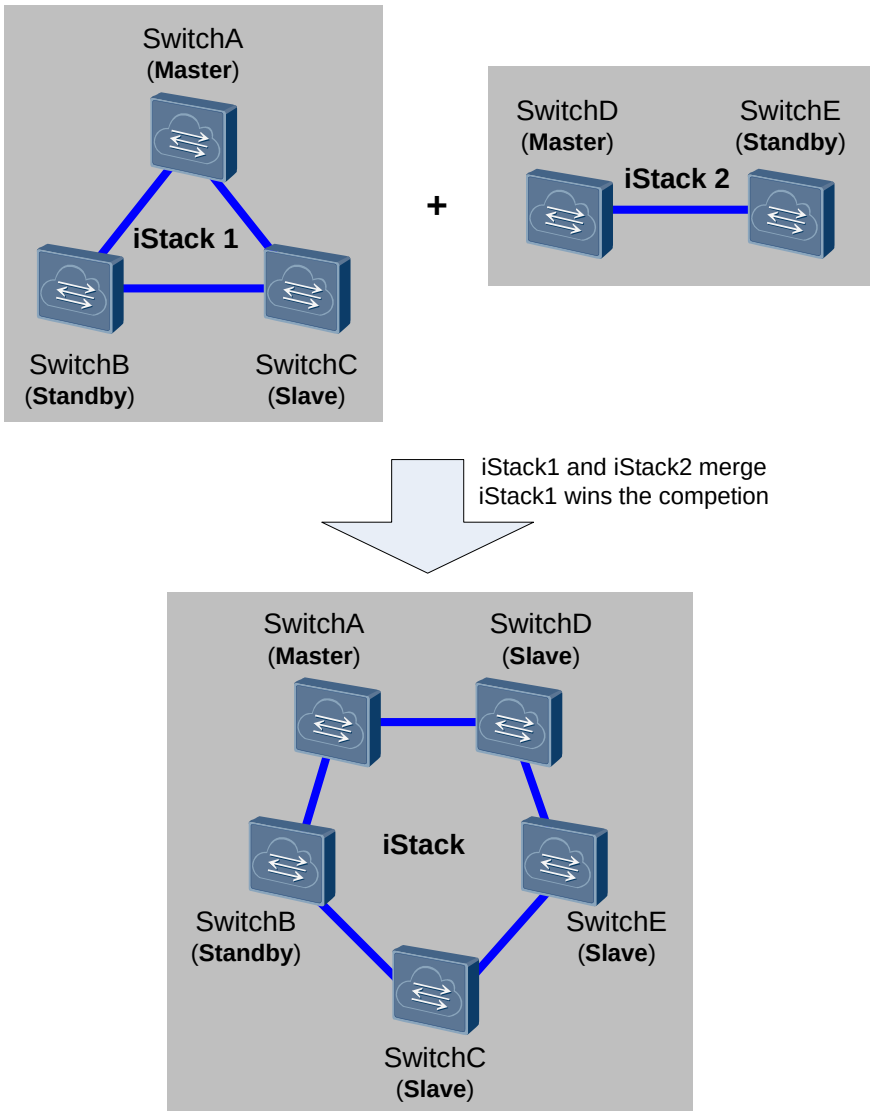
As shown in Figure 2-8, two stacks in the running state can merge into one stack. After two stacks merge, the master switches of the two stacks compete to be the master switch of the new stack. The two switches compare the following items in the listed order to elect the master switch (the election ends when a winning switch is found):

- Stack priority: The switch with a higher stack priority becomes the master switch.
- Software version: The switch running a later software version becomes the master switch.
- Bridge MAC address: The switch with a smaller bridge MAC address becomes the master switch.

  During the delivery of a device, 16 MAC addresses are allocated to the device, among which the smallest MAC address becomes the bridge MAC address.

After the new master switch is elected, the member switches originally belonging to the same stack as this new master switch retain their roles and configurations, and their services are unaffected. Switches in the other stack restart and join the new stack as slave switches, and services on these switches are interrupted.

Figure 2-8 Two stacks merge



Stack merging occurs in either of the following situations:

- A switch is configured with the stacking function and is connected to a running stack using a stack cable while the power is on.
- A stack splits because a stack link or member switch fails. After the stack link or member switch recovers, the two stacks merge into one again.

The stack merging process is similar to the process when a new member switch joins a stack. For details, see 2.5 Joining and Leaving a Stack. The master competition rules used in a stack merging process are the same as the master election rules used in a stack.

2.7 Stack Split and Dual-Active Detection

Stack Split

If you remove some member switches from a running stack without powering off the switches or if multiple stack cables fail, the stack splits into multiple stacks.

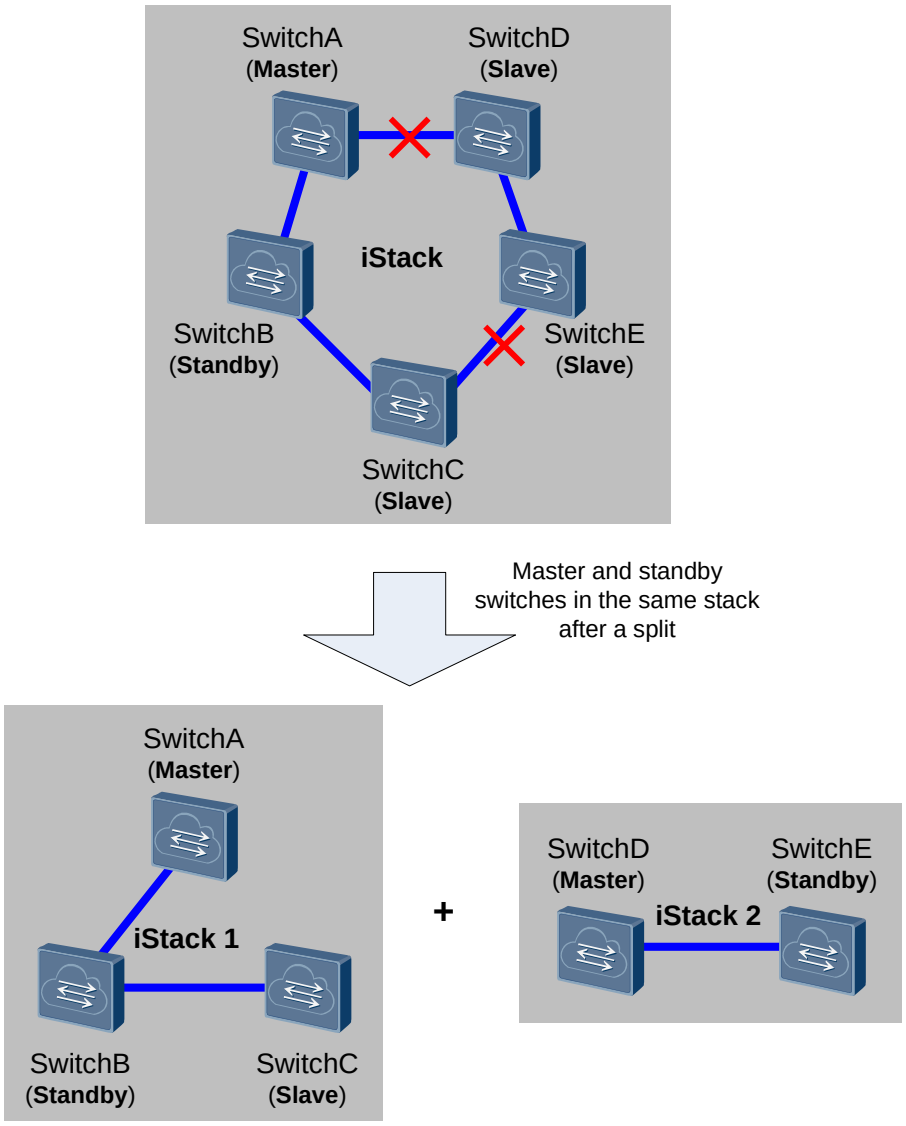
Depending on the locations of the master and standby switches after a split, either of the following situations occurs:

- The original master and standby switches are in the same stack after the split.

  The original master switch recalculates the stack topology, deletes topology information of the removed member switches, and synchronizes new topology information to the other member switches in the new stack. The removed switches restart, set up a new stack, and elect a new master switch.

  As shown in Figure 2-9, the original master switch (SwitchA) and standby switch (SwitchB) are in the same stack after the split. SwitchA deletes topology information related to SwitchD and SwitchE and synchronizes new topology information to SwitchB and SwitchC. After SwitchD and SwitchE restart, they set up a new stack.

Figure 2-9 Original master and standby switches in the same stack after a split

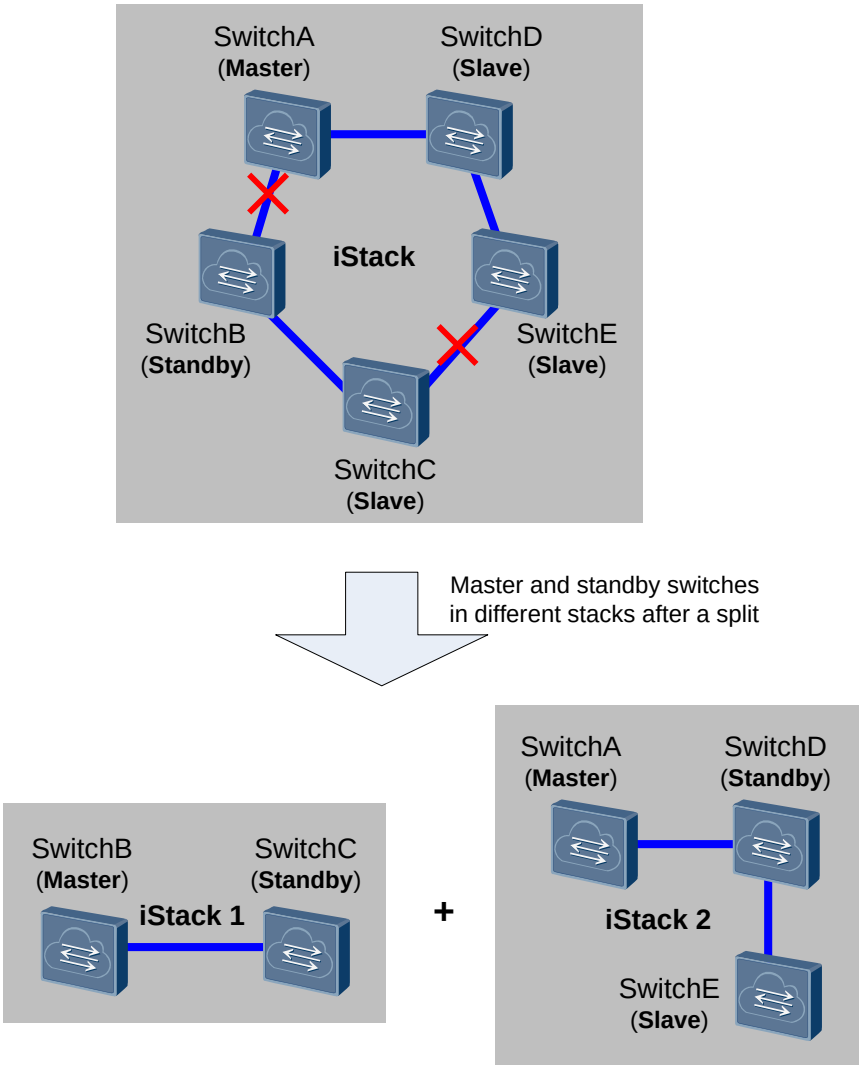


- The original master and standby switches are in different stacks after the split.

  The original master switch specifies a new standby switch in its stack, recalculates the topology, and synchronizes topology information to the other member switches in the stack. The original standby switch becomes the master switch in its stack. It then recalculates the topology, synchronizes topology information to the other member switches in the stack, and specifies a new standby switch.

  As shown in Figure 2-10, the original master switch (SwitchA) and standby switch (SwitchB) are in different stacks after the split. SwitchA specifies SwitchD as the new standby switch, recalculates the stack topology, and synchronizes new topology information to SwitchD and SwitchE. In the other stack, SwitchB becomes the master switch. It then recalculates the topology, synchronizes topology information to SwitchC, and specifies SwitchC as the new standby switch.

Figure 2-10 Original master and standby switches in different stacks after a split



Dual-Active Detection

Dual-active detection (DAD) is a protocol that can detect stack split and dual-active situations and take recovery actions to minimize impact of a stack split on services.

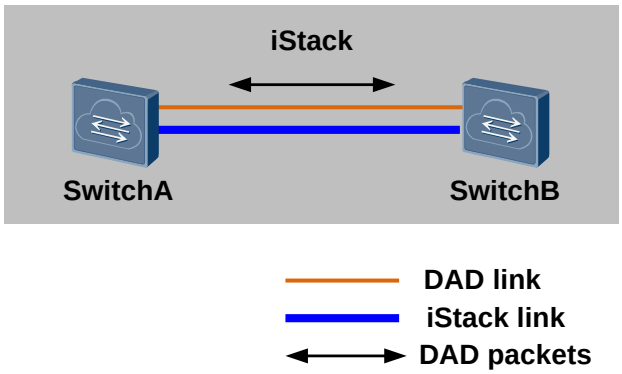
DAD Detection Modes

DAD can be implemented in the following modes:

- **Direct mode through service ports**

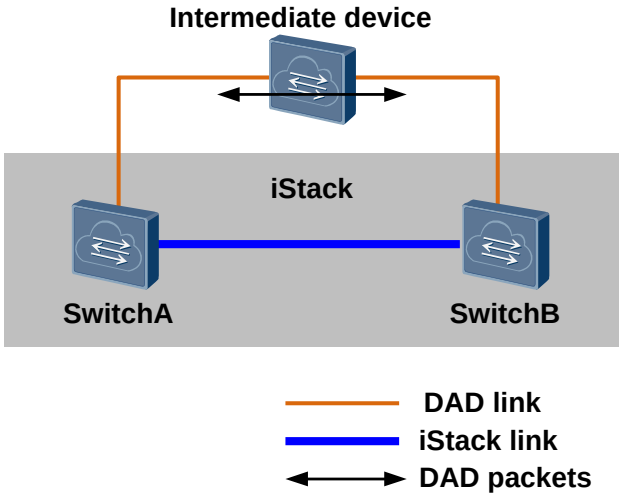
  In this mode, DAD is performed through dedicated direct links between member switches, as shown in Figure 2-11.

Figure 2-11 DAD in direct mode



The direct detection links can also be connected through an intermediate device, as shown in Figure 2-12. In direct mode, DAD packets are bridge protocol data units (BPDUs), so the intermediate device must be configured to transparently transmit BPDUs. For details on the configuration method, see Configuring Interface-based Layer 2 Protocol Transparent Transmission in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Ethernet Switching*.

Figure 2-12 DAD through direct links to an intermediate device



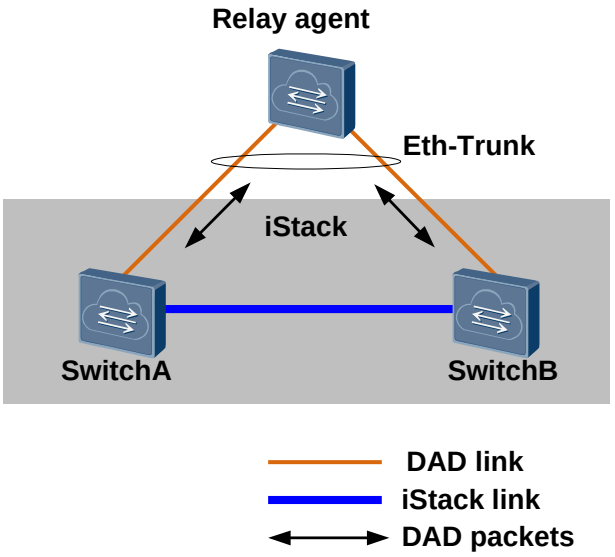
- **Proxy mode through Eth-Trunk interfaces**

  In this mode, DAD detection is performed through an inter-device Eth-Trunk link connected to a relay agent, as shown in Figure 2-13. The DAD proxy function must be enabled on the relay agent. Compared with the direct mode, the relay mode does not require additional interfaces because the Eth-Trunk interface can perform DAD relay detection while running other services.

NOTE

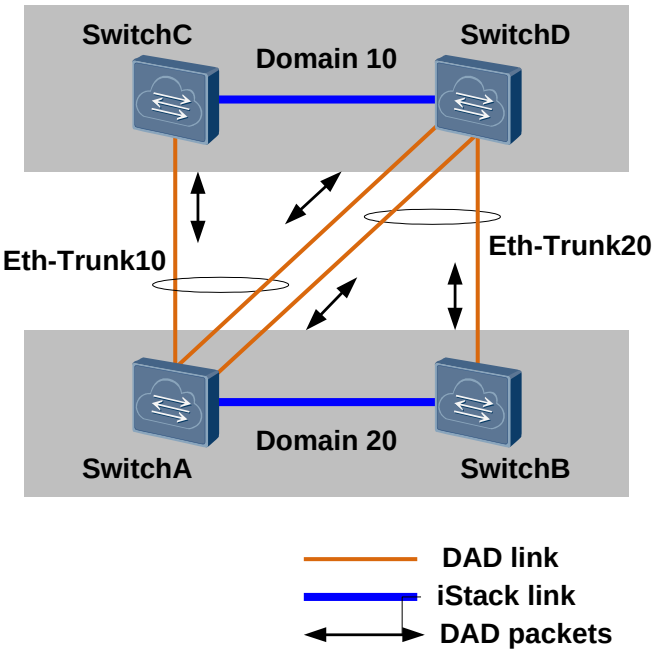
To enable DAD packets to be forwarded over Eth-Trunk member links, use a switch that supports the DAD proxy function as the relay agent. All Huawei CloudEngine series switches support the DAD proxy function. Huawei S series switches support this function since V200R002.

Figure 2-13 DAD in reply mode



The relay agent can be a standalone switch or a stack. That is, two stacks can function as a proxy for each other, as shown in Figure 2-14.

Figure 2-14 Two stacks as DAD relay agents of each other



NOTE

To avoid interference to DAD in the two stacks, configure different domain IDs for the two stacks. In addition, the Eth-Trunk interface used for DAD detection must be different from the Eth-Trunk interface working as the proxy.

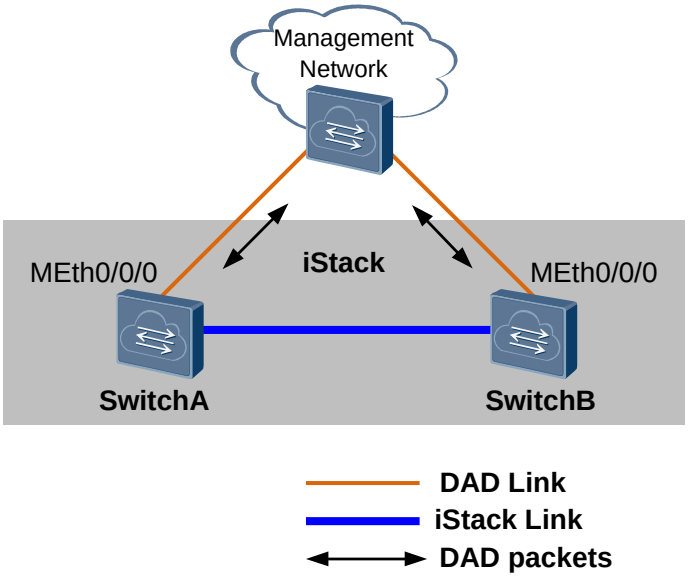
- **DAD through management interfaces**

In this mode, links established on management interfaces of the stack member switches are used as DAD links, as shown in Figure 2-15. This mode can be used when all stack member switches connect to the management network through their management interfaces. This mode does not occupy additional ports and does not require a DAD relay agent.

NOTE

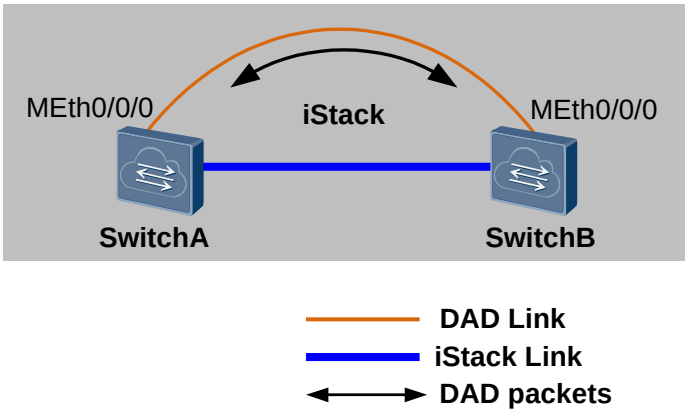
To implement DAD through management interfaces, ensure that IP addresses are configured for management interfaces.

Figure 2-15 DAD through management interfaces



As shown in Figure 2-16, when no management network exists, DAD can be implemented when stack member switches directly connect to each other through management interfaces. In this situation, the management interfaces must also have IP addresses configured.

Figure 2-16 DAD through directly connected management interfaces



Dual-Active Conflict Handling and Fault Recovery

After DAD is configured in a stack, the master switch periodically sends DAD competition packets over the detection links. After the stack splits, the switches exchange DAD competition packets and compare information in the received DAD competition packet with local information. If local information is better, the local switch remains in Active state and continues forwarding service packets. If the received information is better, the switch stack turns to the Recovery state. In this case, all the service interfaces except the excluded ones on the switch are shut down and stop forwarding service packets.

After a stack splits, the switches compare the following items in the listed order to determine the Active/Recovery state (the election ends when a winning switch is found):

1. Stack priority: The switch with a higher stack priority wins.
2. MAC address of the switch: The switch with a smaller MAC address wins.

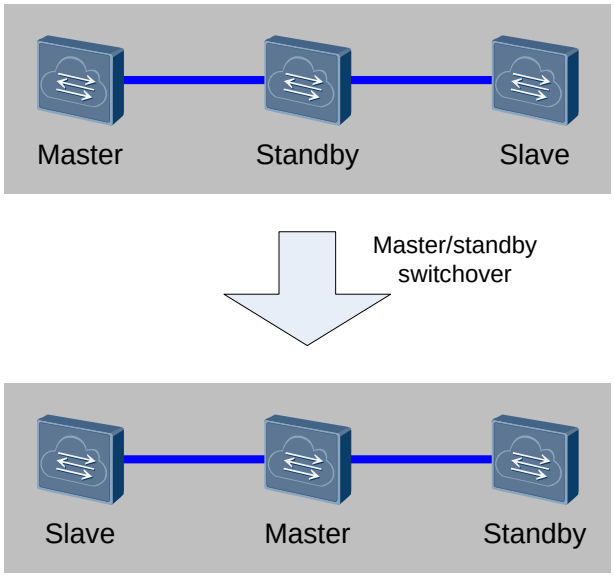
After the stack links recover, the stacks merge into one. The switches in Recovery state restart and restore the shutdown service interfaces. Then the entire stack recovers.

If the switch in Active state also fails before the faulty stack links recover, remove this switch from the network first, and then use a command to start the switches in Recovery state, enabling the switches to take over services on the original switch in Active state. After the faulty switch and stack links recover, connect the switch to the network again so that the stacks can merge.

2.8 Master/Standby Switchover

A master/standby switchover occurs in a stack when the master switch restarts or when a user runs the switchover command. Figure 2-17 illustrates how the roles of member switches change after a master/standby switchover.

Figure 2-17 Changes of member switch roles after a master/standby switchover



1. The original standby switch becomes the master switch.
2. The new master switch selects a standby switch.

3. The original master switch rejoins the stack as a slave switch after it restarts.

2.9 Stack Upgrade

A stack can be upgraded using the traditional upgrade method (specify the next-startup files and restart the entire stack) or the fast upgrade or in-service software upgrade (ISSU) function:

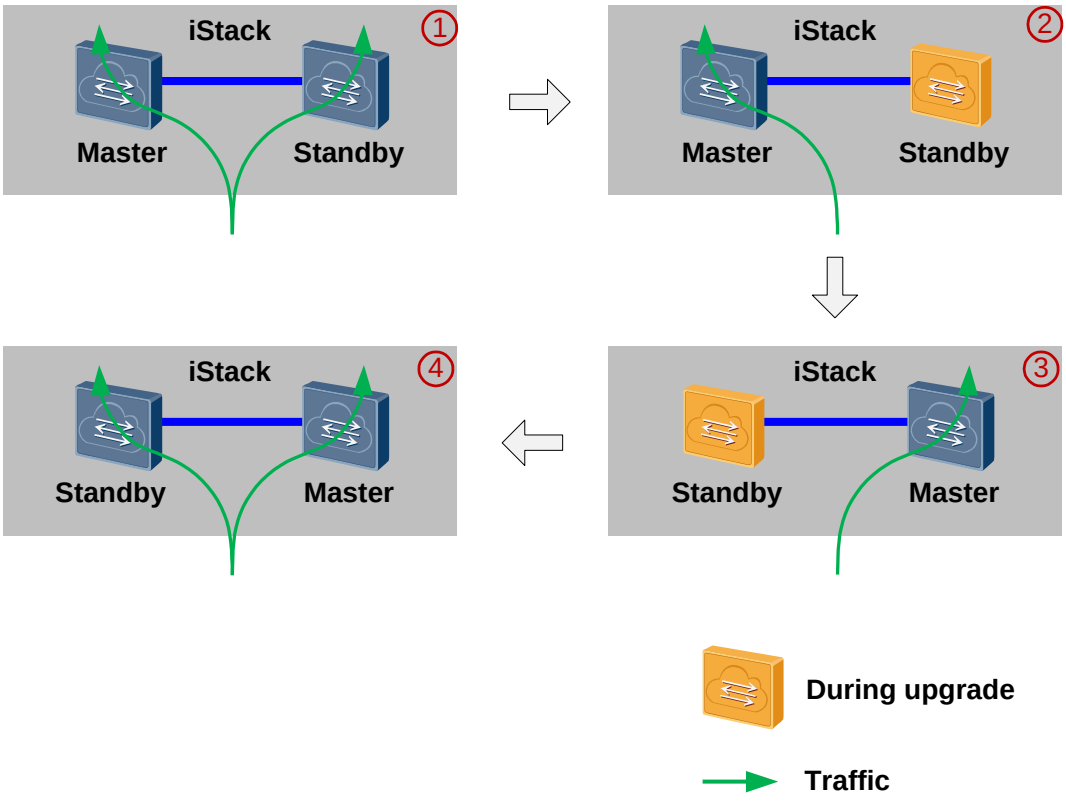
- Traditional upgrade method: You need to specify next-startup files and restart the entire stack. This method causes service interruption in a long time and is therefore not applicable to scenarios requiring short service interruption time.
- Fast upgrade: This upgrade method provides a mechanism to minimize the service interruption time during software upgrade of stack member switches, reducing impact of the upgrade on services.

NOTE

- Only the stack containing two member switches supports fast upgrade.
- If 40GE high-speed cables are used to connect stack member devices, you cannot fast upgrade switches from versions earlier than V100R003C00 to later versions.
- It is recommended that the upstream and downstream devices be connected to the stack through Eth-Trunk links to reduce the traffic interruption time during an upgrade.
- It is recommended to configure a backup IP address for the stack management interface before a fast upgrade to prevent a failure to manage member devices when the stack fails the fast upgrade and splits.

Figure 2-18 shows traffic forwarding during a fast upgrade. First, the standby switch restarts with the new system software. Data traffic is forwarded by the master switch in this period. After the standby switch is upgraded, it becomes the master switch and starts to forward data traffic. Then the original master switch restarts with the new system software. After the upgrade is complete, the original master switch becomes the backup switch in the stack.

Figure 2-18 Traffic forwarding during a fast upgrade



If the upgrade fails due to a stack link failure, the system software rolls back to the original version.

- ISSU upgrade: The ISSU function completes an upgrade through a card switchover. This upgrade method ensures higher reliability and shorter service interruption time. For more information about ISSU upgrade, see ISSU Configuration in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Basic Configurations*.

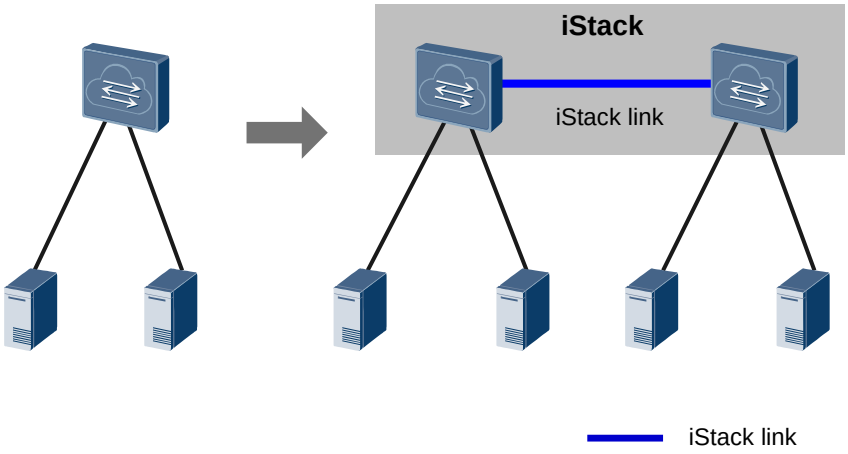
3 Applications

This section describes stack application scenarios.

Increasing the Number of Ports

As shown in Figure 3-1, when the port density of a switch is insufficient for an increased number of users, you can connect another switch to the switch using stack cables. The two switches can set up a stack to provide more ports.

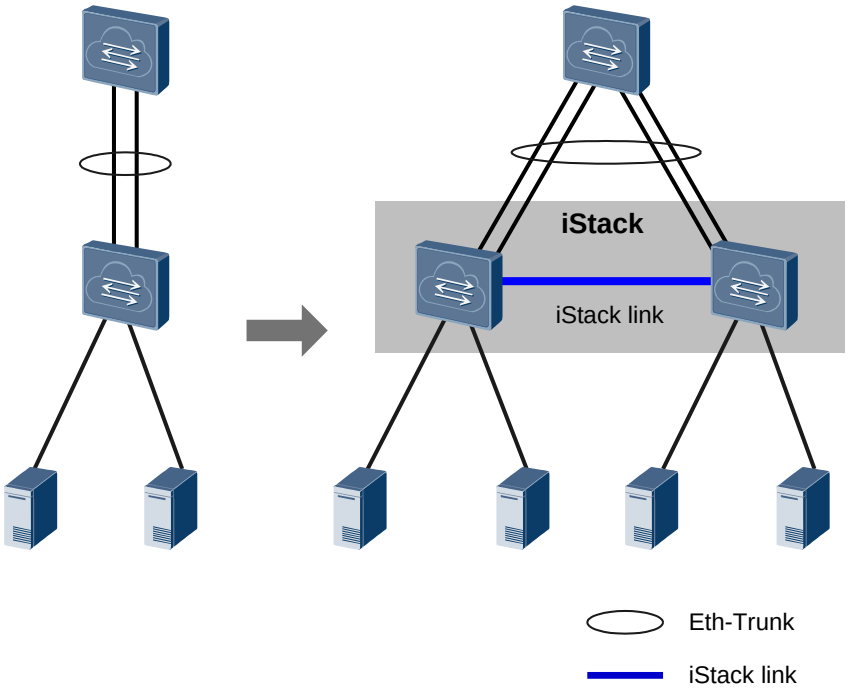
Figure 3-1 Increasing the number of ports



Increasing Bandwidth

As shown in Figure 3-2, you can use two switches to set up a stack and bundle physical links of the two switches into a link aggregation group to increase the uplink bandwidth.

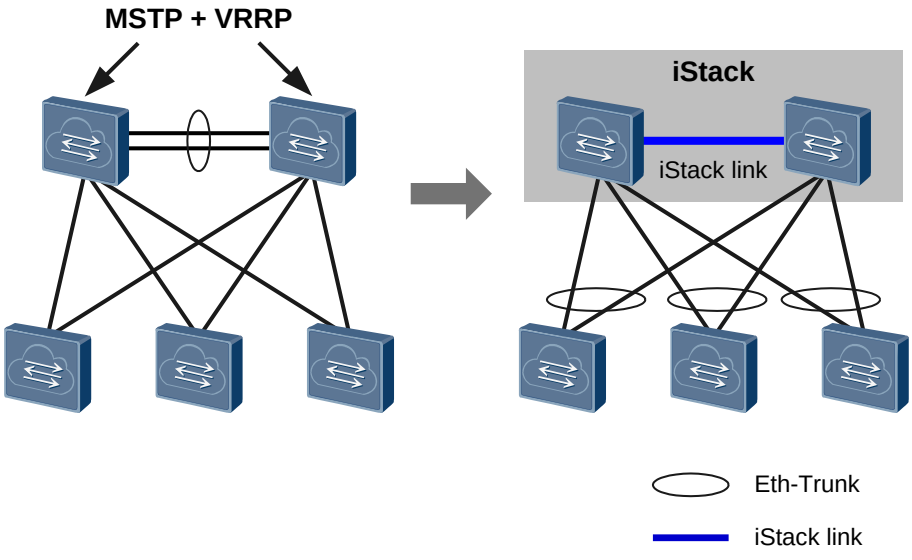
Figure 3-2 Increasing uplink bandwidth



Simplifying Network Topology

As shown in Figure 3-3, multiple switches are virtualized into a logical switch. This simplified network does not require MSTP or VRRP, so network configuration is much simpler. Inter-device link aggregation also speeds up network convergence and improves network reliability.

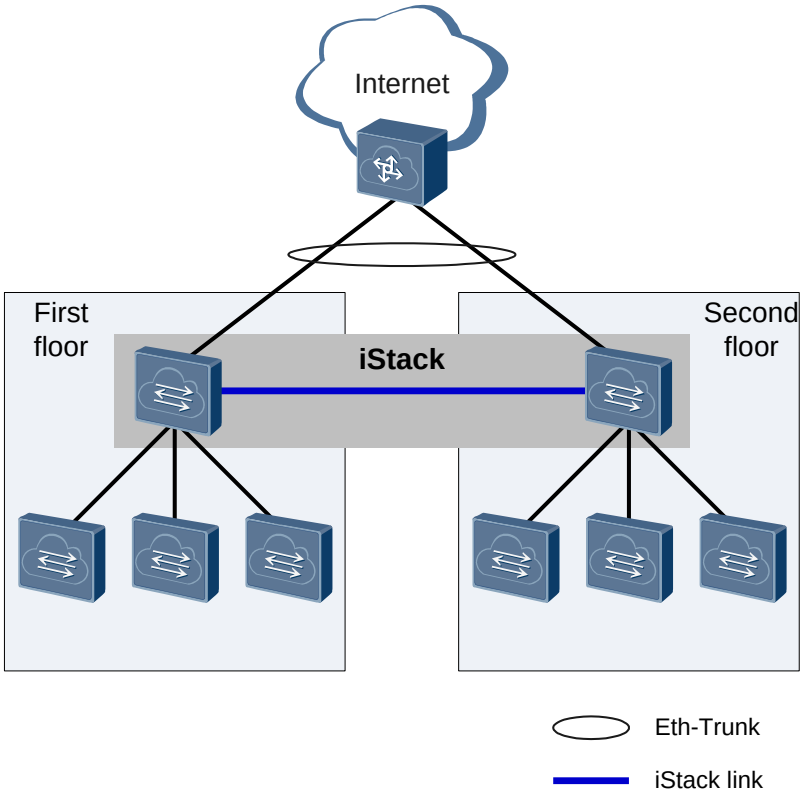
Figure 3-3 Simplifying network topology



Long-Distance Stacking

Long-distance stacking enables switches far from each other to set up a stack. As shown in Figure 3-4, aggregation switches on the two floors set up a stack over a long-distance connection and work like one aggregation device. In this way, the network structure is simplified, and the management and maintenance costs are reduced. In addition, each floor is connected to the core network through two links, which greatly improves service reliability.

Figure 3-4 Long-distance stacking



4 Configuration Notes

This section provides the points of attention when configuring a stack.

Hardware and Software Requirements

To establish a stack successfully, confirm the hardware and software requirements beforehand, for example, the device model and cable type used. Table 4-1 describes the hardware and software requirements for establishing a stack.

Table 4-1 Hardware and software requirements for establishing a stack

Device Model	Number of Member Switches	Version Support	Ports Supporting Stack	Remarks
CE5810EI	9	V100R002C00 and later versions	10GE optical ports	Among the four 10GE optical ports of a CE5810-48T4S-EI, 10GE1/0/1 and 10GE1/0/2 must be added to the same stack port, and 10GE1/0/3 and 10GE1/0/4 must be added to another stack port. There is no such restriction on other models.
CE5850EI	16	V100R001C00 and later versions	• 10GE optical ports • 40GE optical ports	-
CE5855EI	9	V100R005C10 and later	• 10GE optical ports	To use 10GE optical ports of a

Device Model	Number of Member Switches	Version Support	Ports Supporting Stack	Remarks
		versions	• 40GE optical ports	CE5855-48T4S2Q-EI switch for stack connection, you can only add 10GE1/0/1 to 10GE1/0/2 and 10GE ports split from 40GE1/0/1 (40GE1/0/1:1 to 40GE1/0/1:4) to the same logical stack port or add 10GE1/0/3 to 10GE1/0/4 and 10GE ports split from 40GE1/0/2 (40GE1/0/2:1 to 40GE1/0/2:4) to the same logical stack port. To use 40GE optical ports of the switch for stack connection, do not add 40GE1/0/1 and 40GE1/0/2 to the same logical stack port.
CE5850HI	9	V100R003C00 and later versions	• 10GE optical ports • 40GE optical ports	-
CE6810EI	16	V100R003C00 and later versions	• 10GE optical ports • 40GE optical ports	-
CE6810LI	16	V100R003C10 and later versions	• 10GE optical ports • 10GE electrical ports • 40GE	-

Device Model	Number of Member Switches	Version Support	Ports Supporting Stack	Remarks
			optical ports	
CE6850EI	16	V100R001C00 and later versions	• 10GE optical ports • 10GE electrical ports • 40GE optical ports	-
CE6850HI/CE6850U-HI	16	V100R005C00 and later versions	• 10GE optical ports • 10GE electrical ports • 40GE optical ports	CE6850-48T6Q-HI can set up a stack only with CE6850-48T6Q-HI but not with CE6850-48S6Q-HI, CE6850U-48S6Q-HI, or CE6850U-24S2Q-HI.
CE6851HI	16	V100R005C10 and later versions	• 10GE optical ports • 40GE optical ports	-
CE7850EI	16 In V100R003C00, at most four CE7850EIs can set up a stack. In V100R003C10 and later versions, at most 16 CE7850EIs can set up a stack.	V100R003C00 and later versions	• 40GE optical ports	-
CE8860EI	9	V100R006C00 and later versions	• 10GE optical ports • 10GE electrical ports • 25GE optical ports • 40GE optical ports	Split 10GE and 25GE ports can be used for stack connections. Physical ports on different subcards can be added to the same stack port.

Device Model	Number of Member Switches	Version Support	Ports Supporting Stack	Remarks
			• 100GE optical ports	10GE/25GE SFP28 ports cannot be used for stack connections after their rate is configured to 10 Gbit/s using the **port mode 10g** command. 40GE/100GE QSFP28 ports cannot be used for stack connections after their rate is configured to 40 Gbit/s using the **speed** command.

Pay attention to the following points:

- Switches of different series cannot set up a stack. For example, CE5850HI and CE5850EI switches cannot set up a stack; CE6850HI and CE6851HI switches cannot set up a stack.
- A stack port can contain 1 to 16 physical member ports. The number of physical member ports varies according to the device model. Devices of different models have different numbers of physical member ports. The number of physical member ports is recommended as 2*N (N≥1).
- Physical member ports of stack ports on two member switches can be connected in any sequence.
- Physical member ports in a stack port must be the same type. For example, 10GE and 40GE ports cannot be added to the same stack port.
- 10GE optical ports can be used for stack connection only when they have 10GE optical modules installed. If the GE optical or copper modules are installed on 10GE optical ports, the ports cannot be used to set up a stack.
- 10GE optical ports derived from 40GE optical ports on devices except CE7850EI can be used for stack connection.
- Only 40GE ports aggregated from CE6810-48S-LI's 10GE ports can be used for stack connection.
- On the CE6850EI, CE6810EI, CE6810LI, and CE5850EI, if a 10GE port with port number in the range 4N+1 to 4N+4 (N=0, 1, 2, 3...) is configured as a physical member port, all the ports with port numbers 4N+1 to 4N+4 are configured as physical member ports.
- When configuring a CE8860EI's ports as physical member ports, pay attention to the following points:
  - If a 10GE/25GE SFP28 optical port or 10GE RJ45 electrical port with port number in the range 4N+1 to 4N+4 (N=0, 1, 2, 3...) needs to be configured as a physical

Device Model	Number of Member Switches	Version Support	Ports Supporting Stack	Remarks
member port, all the ports with port numbers 4N+1 to 4N+4 must be configured as physical member ports. – If a 40GE QSFP+ optical port needs to be configured as a physical member port, two contiguous ports must be configured as physical member ports; alternatively, four 10GE optical ports split from two contiguous 40GE optical ports can be configured as physical member ports. A 40GE QSFP+ optical port can be split into two 10GE optical ports. – Each 40GE/100GE QSFP28 optical port can be independently configured as a physical member port. If a 10GE or 25GE optical port split from a 40GE or 100GE QSFP28 optical port needs to be configured as a physical member port, four contiguous ports must be configured as physical member ports simultaneously. • In versions earlier than V100R005C00, you can use some 10GE ports split from CE5850HI 40GE ports as service ports and some as stack physical member ports. In V100R005C00 and later versions, you must use all such 10GE ports split from CE5850HI 40GE ports as stack physical member ports. A stack may fail to be set up if the following conditions are met: 1. A CE5850HI uses some 10GE ports split from 40GE ports as stack physical member ports. 2. Some 10GE service ports split from 40GE ports have the service configuration that conflicts with the stack during an upgrade from a version earlier than V100R005C00 to V100R005C00 or later. To solve this problem, you need to delete the service configuration that conflicts with the stack from the service ports.				

High-speed cables, AOC cables, optical modules and fibers, or network cables can be used to connect stack member switches. Table 4-2 describes the cables applicable to different ports.

Table 4-2 Requirements for stack cables

Port Type	High-Speed Cable	AOC Cable	Optical Module	Network Cable
10GE optical port	SFP+ to SFP+ high-speed cable SFP+ to SFP+ high-speed cables are available in lengths of 1 m, 3 m, 5 m, 7 m, and 10 m, among which 7 m and 10 m SFP+ to SFP+ high-speed cables are	SFP+ to SFP+ AOC cable. SFP+ to SFP+ AOC cables are available in lengths of 3 m, 10 m, and 20 m.	10GE SFP/SFP+ optical module The required optical fibers are determined by the optical modules you select.	-

Port Type	High-Speed Cable	AOC Cable	Optical Module	Network Cable
	active cables.			
10GE electrical port	-	-	-	10GE electrical ports use Category 6, Category 6A, or Category 7 cables that comply with IEEE 802.3an.
10GE/25GE SFP28 optical port	-	-	-	-
40GE optical port	QSFP+ to QSFP+ high-speed cable QSFP+ to QSFP+ high-speed cables are available in lengths of 1 m, 3 m, and 5 m.	QSFP+ to QSFP+ AOC cable. QSFP+ to QSFP+ AOC cables are available in lengths of 10 m.	40GE QSFP optical module The required optical fibers are determined by the optical modules you select.	-
40GE/100GE QSFP28 optical port	QSFP28 to QSFP28 high-speed cable QSFP28 to QSFP28 high-speed cables are available in lengths of 1 m, 3 m, and 5 m.	-	QSFP28 optical module The required optical fibers are determined by the optical modules you select.	-

Involved Network Elements

Other network elements are not required.

License Support

Stack is a basic feature of a switch and is not under license control.

Version Support

For details, see Hardware and Software Requirements.

Feature Dependencies and Limitations

Precautions

When setting up a stack, pay attention to the following points:

- Huawei-certified optical or copper modules must be used. If high-speed cables or AOCs are used, you must purchase cables from Huawei.

  Non-Huawei-certified optical or copper modules or cables that are not purchased from Huawei cannot ensure transmission reliability and may affect service stability. Huawei is not liable for any problem caused by the use of non-Huawei-certified optical or copper modules, or cables not purchased from Huawei, and will not fix such problems.
- Before the master and standby switches complete batch backup, do not shut down or remove stack links to prevent switch restart.

  To check the batch backup status between master and standby switches, run the **display switchover state** command.
- If 40GE high-speed cables are used to connect stack member devices, you cannot fast upgrade switches from versions earlier than V100R003C00 to later versions.
- If CE6851HI, CE6850-48T6Q-HI, CE6810-32T16S4Q-LI, and CE5855EI set up a stack using 40GE high-speed cables, member switches must be upgraded to the same version so that they can set up a stack. For example, switches running V100R005C10SPC100 and V100R005C10SPC200 or later version cannot set up a stack.

  After a stack is set up, it cannot be upgraded from V100R005C10SPC100 to V100R005C10SPC200 or later version using ISSU or the fast upgrade function.

Feature Support in a Stack

In a stack, support for most features except the following features is the same as support on a single device. Table 4-3 shows the difference in support for some features.

Table 4-3 Feature support in a stack

Feature	Feature Support in a Stack
Mirroring	In a stack, physical member interfaces do not support inter-chassis mirroring; the mirrored port and physical member interface that functions as the observing port must be on the same device.
Port split	If a 40GE optical port has been configured as a physical member port, it cannot be split.
USB-based deployment	USB-based deployment is not supported in a stack.
ISSU	In-service software upgrade (ISSU) is supported in a stack but not supported on a single device.

5 Default Configuration

This section provides default settings of stack parameters.

Table 5-1 Default stack configuration

Parameter	Default Setting
Stacking function	Enabled
Stack member ID	1
Domain ID	No default value
Stack priority	100

6 Establishing a Stack

About This Chapter

This section describes how to establish a stack.

Before establishing a stack, make a proper network plan, confirm software and hardware requirements, and determine roles and functions of member switches. Then connect the switches using stack cables and complete software configuration.

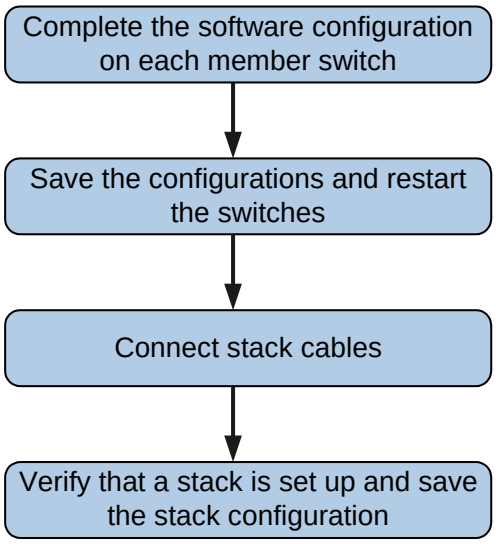
Stack cable connection and software configuration can be performed in either sequence. The stack setup procedure varies depending on which task is performed first.

- 6.1 Setting Up a Stack by Configuring Software and Then Connecting Stack Cables. The configuration is simple. This method applies to onsite configuration scenarios.
- 6.2 Setting Up a Stack by Connecting Stack Cables and Then Configuring Software. The configuration is more complex. This method applies to remote configuration.

6.1 Setting Up a Stack by Configuring Software and Then Connecting Stack Cables

You can complete software configuration before connecting stack cables if you are at the device deployment site. This stack setup procedure is simple, as shown in Figure 6-1.

Figure 6-1 Setting up a stack by configuring software and then connecting stack cables



6.1.1 Configuring Software

(Optional) Configuring a Stack Member ID

Context

Stack member IDs are used to identify and manage member switches in a stack. Each member switch has a unique stack member ID.

If stack member IDs conflict in a stack, the master switch assigns new stack member IDs to member switches. That is, the master switch checks stack member IDs in ascending order (from 1 to the largest stack member ID) to find an unused stack member ID and then assigns the stack member ID to a member switch with a conflicting stack member ID.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **stack** command to enter the stack management view.

Step 3 Run the **stack member** *member-id* **renumber** *new-member-id* [**inherit-config**] command to configure a stack member ID for the local switch.

By default, the stack member ID of a switch is 1. After changing the stack member ID, restart the switch for the configuration to take effect.

NOTE

- If you specify **inherit-config**, the switch inherits the original stack configuration after it restarts, including the stack priority, stack domain ID, and physical member port configuration. The common service port configuration will be lost. For example, the port split configuration will be lost, but the split configuration of physical member ports is inherited.
- If you do not specify **inherit-config**, the current stack configuration and common service port configuration are lost after the switch restarts, and the configuration related to the new stack member ID in the configuration file takes effect.
- If the configuration file contains offline configuration for the new stack member ID, do not specify **inherit-config** in the command.

Step 4 Run the **commit** command to commit the configuration.

----End

(Optional) Configuring a Stack Priority

Context

The stack priority of a member switch determines its role in the stack. A larger value indicates a higher priority and higher probability that the member switch is elected as the master switch.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **stack** command to enter the stack management view.

Step 3 Run the **stack member** { *member-id* | **all** } **priority** *priority-value* command to configure a stack priority for the switch.

By default, the stack priority of a switch is 100. After changing the stack priority, restart the switch for the configuration to take effect.

Step 4 Run the **commit** command to commit the configuration.

----End

Configuring a Stack Domain ID

Context

After switches are connected using stack links and set up a stack, they form a stack domain. Multiple stacks can be deployed on a network to support various applications. These stacks are identified by their domain IDs.

NOTE

Member switches in a stack must be configured with the same domain ID. Otherwise, they cannot set up a stack.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **stack** command to enter the stack management view.

Step 3 Run the **stack member** { *member-id* | **all** } **domain** *domain-id* command to configure a stack domain ID.

By default, a switch has no stack domain ID. If the switch has no stack domain ID, the configuration takes effect after you save the configuration. If you change the existing stack domain ID, the new ID takes effect after the switch restarts.

Step 4 Run the **commit** command to commit the configuration.

----End

Configuring a Stack Port

Context

Multiple physical member ports can be added to a stack port to improve stack link bandwidth and reliability.

NOTE

- Physical member ports in a stack port must be the same type. For example, 10GE and 40GE ports cannot be added to the same stack port.
- A stack port can contain 1 to 16 physical member ports. The number of physical member ports varies according to the device model. Devices of different models have different numbers of physical member ports. The number of physical member ports is recommended as 2*N (N≥1).
- On the CE6850EI, CE6810EI, CE6810LI, and CE5850EI, if a 10GE port with port number in the range 4N+1 to 4N+4 (N=0, 1, 2, 3...) is configured as a physical member port, all the ports with port numbers 4N+1 to 4N+4 are configured as physical member ports.
- When configuring a CE8860EI's ports as physical member ports, pay attention to the following points:
- If a 10GE/25GE SFP28 optical port or 10GE RJ45 electrical port with port number in the range 4N+1 to 4N+4 (N=0, 1, 2, 3...) needs to be configured as a physical member port, all the ports with port numbers 4N+1 to 4N+4 must be configured as physical member ports.
- If a 40GE QSFP+ optical port needs to be configured as a physical member port, two contiguous ports must be configured as physical member ports; alternatively, four 10GE optical ports split from two contiguous 40GE optical ports can be configured as physical member ports. A 40GE QSFP+ optical port can be split into two 10GE optical ports.
- Each 40GE/100GE QSFP28 optical port can be independently configured as a physical member port. If a 10GE or 25GE optical port split from a 40GE or 100GE QSFP28 optical port needs to be configured as a physical member port, four contiguous ports must be configured as physical member ports simultaneously.
- You are advised to configure the same number of physical member ports on member switches. If a smaller number of physical member ports are configured on a low-priority switch, this switch may be initialized earlier than the other member switch after it restarts and becomes the master switch.

Procedure

Step 1 Create a stack port.

1. Run the **system-view** command to enter the system view.
2. Run the **interface stack-port** *member-id*/*port-id* command to create a stack port.

   By default, no stack port exists in the system.
3. (Optional) Run the **description** *description* command to configure a description for the stack port.

   By default, no description is configured for a stack port.
4. Run the **commit** command to commit the configuration.

Step 2 Add service ports to the stack port.

NOTE

Configurations in the stack management view and the interface view are the same. You can choose either one.

Service ports are automatically configured as physical member ports after being added to a stack port. Alternatively, run the **port mode stack interface** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-32> command in the stack management view or run the **port mode stack** command in the interface view to configure service ports as physical member ports and then add the physical member ports to a stack port.

- Configuration in the stack port view:

1. Run the **system-view** command to enter the system view.
2. Run the **interface stack-port** *member-id*/*port-id* command to enter the stack port view.
3. Run the **port member-group interface** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-32> command to add physical member ports to the stack port.
4. Run the **commit** command to commit the configuration.

- Configuration in the interface view:

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **stack-port** *member-id*/*port-id* command to add the physical port to the stack port.
4. Run the **commit** command to commit the configuration.

Step 3 (Optional) Configure the working mode for a 40GE port that has a high-speed cable installed.

1. Run the **system-view** command to enter the system view.
2. Run the **interface** *interface-type interface-number* command to enter the interface view.
3. Run the **port copper mode** { **sr4** | **cr4** }command to configure the working mode for a 40GE port that has a high-speed cable installed.

   By default,

- On CE6810-32T16S4Q-LI, CE6850-48T6Q-HI, CE6851-48S6Q-HI, CE5855-24T4S2Q-EI, and CE5855-48T4S2Q-EI, the working mode of 40GE ports that have high-speed cables installed is SR4.
- On CE6810-48S4Q-LI and CE6810-24S2Q-LI, 40GE ports that have high-speed cables installed can auto-negotiate to work in CR4 or SR4 mode.
- On other switch models, 40GE ports that have high-speed cables installed can auto-negotiate to work in CR4 or SR4 mode. After being added to stack ports, these 40GE ports work in CR4 mode.

  By default, if a CE6810-32T16S4Q-LI, CE6850-48T6Q-HI, CE6851-48S6Q-HI, CE5855-24T4S2Q-EI, or CE5855-48T4S2Q-EI sets up a stack system with other device model using 40GE ports that have high-speed cables installed, the connected device can enable the 40GE ports on both ends to work in the same mode through auto-negotiation. If the two ports work in different modes, they will become Down. However, auto-negotiation lasts a certain period. To ensure that the two ports can rapidly become Up, you are advised to run this command on the connected device to configure the 40GE port to work in SR4 mode. This configuration ensures that 40GE ports on both ends work in SR4 mode.

NOTE

If a CE6810-48S4Q-LI and a CE6810-24S2Q-LI set up a stack using 40GE ports that have high-speed cables installed, you are advised to use this command to set the same working mode for the 40GE ports on both ends.

4. Run the **commit** command to commit the configuration.

Step 4 (Optional) Configure a load balancing mode for the stack port.

1. Run the **system-view** command to enter the system view.
2. Run the **interface stack-port** *member-id*/*port-id* command to enter the stack port view.
3. Run the **load-balance** { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** } command to configure a load balancing mode for the stack port.

   By default, the load balancing mode used in a stack port is **src-dst-ip**.
4. Run the **commit** command to commit the configuration.

Step 5 (Optional) Set an alarm threshold for the number of stack member links.

1. Run the **system-view** command to enter the system view.
2. Run the **stack** command to enter the stack management view.
3. Run the **stack port-link threshold** *alarm-threshold* command to set an alarm threshold for the number of stack links.

   By default, the alarm threshold for the number of stack links is 1.

   If some stack links fail and the number of available stack links falls below the alarm threshold, the system generates an alarm. When the number of available stack links is larger than or equal to the alarm value, the system generates a clear alarm.

NOTE

A single-chassis stack does not generate alarms on the number of stack links.

4. Run the **commit** command to commit the configuration.

----End

Restarting the Switch After Saving the Configuration

Context

To prevent loss of stack configuration caused by power failure or restart of member switches, you are advised to save the configuration immediately after you complete the software configuration. Save the configuration such as the stack member ID and priority, and restart the switch to make the configuration take effect.

Procedure

Step 1 Run the **save** command to save the configuration.

Step 2 Run the **reboot** command to reboot the switch.

----End

6.1.2 Connecting Stack Cables

Preparations

- Required components: high-speed cables or optical modules and matching optical fibers
- Required tools: cable ties, fiber binding tapes, labels, and electrostatic discharge (ESD) wrist strap or ESD gloves

Precautions

DANGER

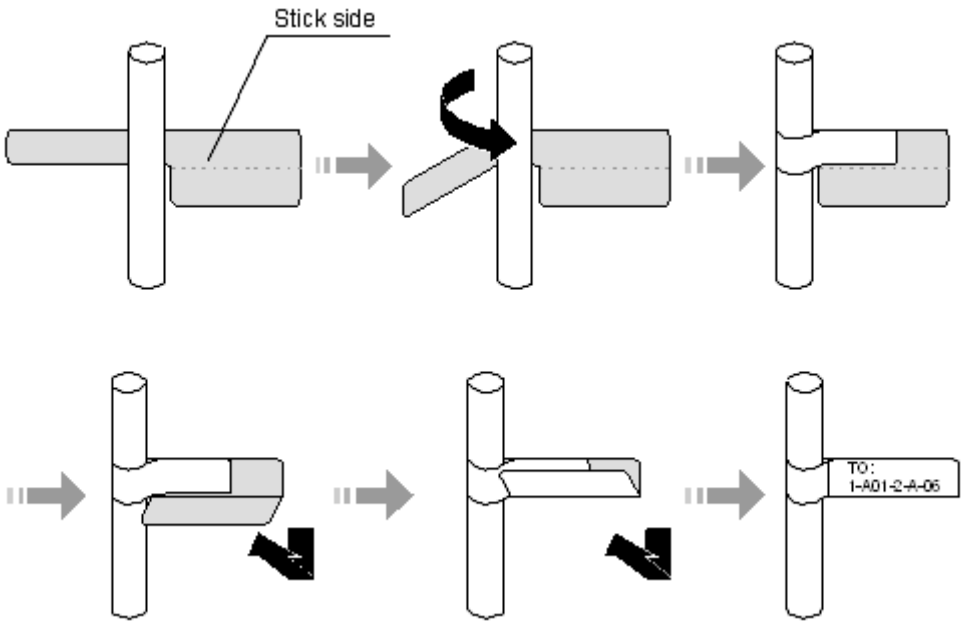
When installing or removing optical fibers, do not look into optical ports or connectors without eye protection.

- Wear an ESD wrist strap or ESD gloves when connecting stack cables.
- Ensure that the stack cables are not tangled with other cables.
- Install or remove optical fibers carefully to avoid damages to fiber connectors.
- The bend radius of optical fibers or high-speed cables must be larger than the minimum bend radius.
- If a fiber connector is dirty, use an alcohol swab or a piece of air-laid paper to gently wipe the fiber connector in one direction.
- To remove a high-speed cable, gently push the cable connector and then pull out the cable by the pull ring.

Procedure

1. Wear an ESD wrist strap and connect the ground terminal to the ESD jack on the rack.
2. Attach labels to both ends of each stack cable and number these labels starting with 1, as shown in Figure 6-2.

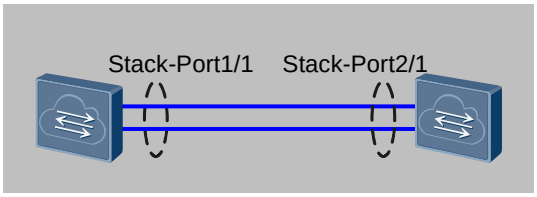
Figure 6-2 Attaching labels



3. Connect the stack cables according to the connection rules.

   Stack member switches are connected using physical member ports, which are bound to logical stack ports. A stack port can have one or more physical member ports. You can bind multiple physical member ports to one stack port to implement link redundancy and increase link bandwidth.

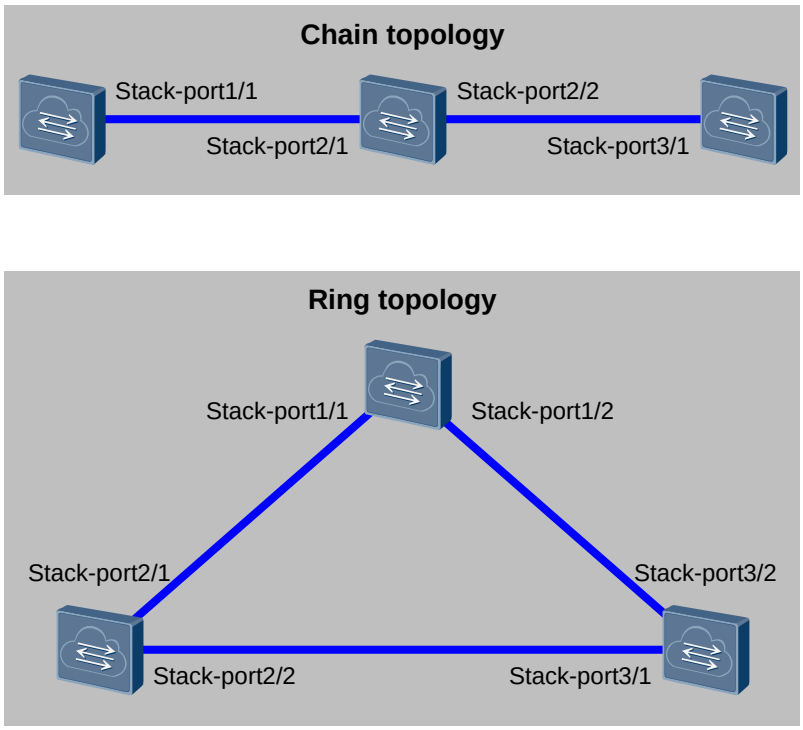
Figure 6-3 Stack connection



Each switch supports two stack ports, named Stack-Port*n*/1 and Stack-Port*n*/2, where *n* is the stack member ID of the switch.

A stack can be connected in a chain or ring topology, as shown in Figure 6-4.

Figure 6-4 Stack topologies



6.1.3 Checking Whether a Stack Is Set Up Successfully

After completing the stack configuration, observe the indicators on the member switches to check whether the stack is set up successfully. If the stack is set up successfully, log in to the stack and run commands to check the stack running state and configure enhanced stack functions. If the stack fails to be set up, analyze the cause of the failure according to indicator states, or log in to any member switch and run commands to analyze the cause.

NOTE

After a stack is set up successfully, you are advised to run the **save** command immediately to save the configuration.

Observing Indicators to Check Whether a Stack Is Set Up

Background

After you complete stack connection and configuration, you can view indicators on the switch panels to check whether a stack is set up successfully.

Procedure

- Press the mode switch button on any member switch until the STACK indicator is steady green.

NOTE

This method applies to V100R002 and later versions.

  - If STACK indicators on all the member switches are steady green, the stack is set up successfully. Then, you can check the MST indicators on the member switches to

identify the master switch. The MST indicator on the master switch is steady green, and the MST indicators on the other member switches are off.

- If some member switches have their STACK indicators off, the stack fails to be set up.

- View the MST indicators on all the member switches.
  - If the MST indicator of one switch is steady green and MST indicators of the other switches are off, the stack is set up successfully. The master switch is the one where the MST indicator is steady green.
  - If MST indicators on multiple switches are steady green or yellow, the stack fails to be set up.

Stack-related Indicators

Table 6-1 Description of stack-related indicators on switch panels

Indicator/Button	Color	Description
MST: stack master/slave indicator	-	Off: The switch is not the stack master switch.
	Green	Steady on: The switch is the stack master switch or a standalone switch.
STACK: STACK mode indicator	Green	• Off: The STACK mode is not selected. • Steady on: The STACK mode is selected. In this mode, service port indicators show the stack member ID of the local switch. If the port of a service port is steady on, the number of the service port is the stack member ID of the local switch. **NOTE** In V100R002C00 and later versions, if the indicator mode on any stack member switch is changed to STACK by pressing the MODE button, all the other member switches in the stack change the indicator mode to STACK. In this case, service port indicators on the member switches show stack member IDs of these switches.
MODE: mode switch button	-	• When you press the button once, the SPEED indicator turns green, and the service port indicators show the speeds of service ports.

Indicator/Button	Color	Description
		• When you press the MODE button a second time, the STACK indicator turns green and the service port indicators show the stack member ID of the local switch. • When you press the MODE button a third time, the STAT indicator turns green (default mode). If you do not press the MODE button within 45 seconds, the mode indicators restore to the default states. That is, the STAT indicator is steady green, and the SPEED and STACK indicators are off.

Logging In and Checking Whether a Stack Is Set Up Successfully

Context

You can observe indicators on member switches or log in to the system and use commands to check whether a stack is set up successfully. If the stack fails to be established, you can locate the fault according to the command output.

Procedure

Step 1 Log in to the stack.

- Local login: Log in through the console interface of any member switch.
- Remote login: Log in through the management interface or another Layer 3 interface of any member switch. You can use remote login modes, such as Telnet and STelnet, if there are reachable routes between the switch and your operation terminal.

NOTE

- After a stack is set up, the configuration file of the master switch takes effect in the stack. Therefore, you must specify the IP address of the master switch when logging in to the stack remotely.
- If multiple management interfaces are available in a stack, only one management interface takes effect.
- If indicators on member switches show that the switches fail to set up a stack, log in to each switch to analyze the cause.

Step 2 Check whether the stack is set up successfully.

Run the **display stack** command to check information about the stack member switches. If all member switches are displayed, the stack is set up successfully.

```
<HUAWEI> display stack
--------------------------------------------------------------------------------
MemberID Role     MAC            Priority   DeviceType        Description
--------------------------------------------------------------------------------
+1       Master   0004-9f31-d520   150       CE6850-48T4Q-EI
 2       Standby  0004-9f62-1f40   100       CE6850-48T4Q-EI
 3       Slave    0004-9f69-a391   100       CE6850-48T4Q-EI
--------------------------------------------------------------------------------
+ indicates the device through which the user logs in.
```

If only some of member switches are displayed, the stack fails to be established. See Handling a Stack Setup Failure to handle the problem.

----End

Handling a Stack Setup Failure

1. Run the **display device** command to check the device model. Switches of different series cannot set up a stack.
2. Run the **display interface brief** command to check whether physical ports with stack cable connected are Up. If a port is Down, check whether the stack cable is securely connected to the port. If the stack cable is securely connected, the cable or the optical module on the port may be faulty. Replace the cable or optical module.
3. Run the **display stack configuration** command to check whether stack domain IDs on the member switches are the same. If the member switches use different stack domain IDs, modify the configuration and restart the switches.
4. Run the **display stack troubleshooting** command to check stack fault events. The command displays some causes of stack setup failures.
5. Run the **display stack link-state last-down-reason** command to check the reason why stack link protocol is Down.

Follow-up Procedure

- **Ports of some member switches are in Error-Down state.**

  During the setup of a stack, if the number of member switches exceeds the upper threshold because of incorrect configuration or connection, excess devices cannot join the stack and ports of these devices enter the Error-Down state (The device records the status of an interface as Error-Down when it detects that a fault occurs. The interface in Error-Down state cannot receive or send packets and the interface indicator is off.). In the following example, a service port is in Error-Down state.

  ```
  <HUAWEI> display interface 10ge 1/0/1
  10GE1/0/1 current state : ERROR DOWN(stack-member-exceed-limit) (ifindex: 12)
  Line protocol current state : DOWN
  ......
  ```

  After ports of excess devices enter the Error-Down state, modify the configuration or connection to remove excess devices and then check whether the ports recover from the Error-Down state.

  You can recover ports from the Error-Down state using either of the following methods:

  - Manually recover ports from the Error-Down state (after the ports become Error-Down).

- Run the **shutdown** and then **undo shutdown** commands or run the **restart** command on each port to restart the port.
- Run the **reboot** command to restart member switches one by one to recover all the ports from the Error-Down state.
- Enable ports to automatically recover from the Error-Down state (before the ports become Error-Down).

  To enable service ports to automatically recover from the Error-Down state, run the **error-down auto-recovery cause stack-member-exceed-limit interval** *interval-value* command in the system view to enable ports in Error-Down state to become Up automatically and set the delay after which ports become Up automatically.

NOTE

This method takes effect only for the ports that become Error-Down after this command is executed but not for those that have been in Error-Down state before this command is executed.

- **The stack fails to be set up, and service ports of some member switches are in Error-Down state.**

  During the setup of a stack, if the standby or slave switch has the stack configuration that conflicts with the master switch, the stack may fail to be set up, and service ports of the standby or slave switch will enter the Error-Down state (The device records the status of an interface as Error-Down when it detects that a fault occurs. The interface in Error-Down state cannot receive or send packets and the interface indicator is off.). In the following example, a service port is in Error-Down state.

```
<HUAWEI> display interface 10ge 1/0/1
10GE1/0/1 current state : ERROR DOWN(stack-config-conflict) (ifindex: 12)
Line protocol current state : DOWN
......
```

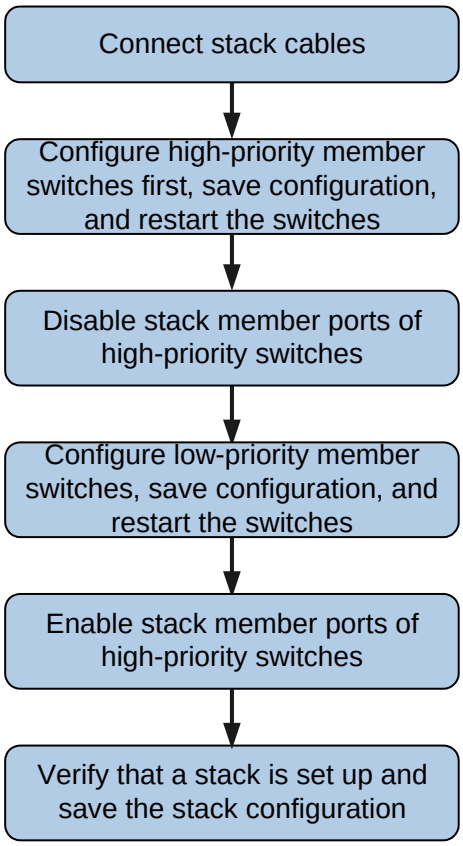
  After service ports of a member switch enter the Error-Down state, you can run the **display stack troubleshooting** command to check the conflicting configuration and then modify the configuration to meet service requirements. Subsequently, restart the switch to enable the stack to be set up again and recover the service ports from the Error-Down state.

6.2 Setting Up a Stack by Connecting Stack Cables and Then Configuring Software

Context

Figure 6-5 shows the procedure for setting up a stack by connecting stack cables and then configuring software. You can use this method in for remote configuration of a stack.

Figure 6-5 Setting up a stack by connecting stack cables and then configuring software



You must disable the stack port on the high-priority switch, and then enable the stack port after configuring the low-priority switch. Otherwise, the low-priority switch will restart due to stack merging, and its configuration will be lost. As a result, the stack cannot be set up.

Procedure

Step 1 Connect the member switches using stack cables according to the connection rules described in 6.1.2 Connecting Stack Cables.

Step 2 According to the network plan, log in the high-priority switch first and complete software configuration on the switch. For the configuration procedure, see 6.1.1 Configuring Software.

After completing the software configuration, run the **save** command in the user view to save the configuration. If some settings take effect after a restart, run the **reboot** command in the user view to restart the switch.

Step 3 Disable the stack port of the high-priority switch connected to the low-priority switch. On the high-priority switch, run the **interface stack-port** *member-id*/*port-id* command in the system view to enter the stack port view, and then run the **shutdown** command to disable the stack port.

Step 4 Log in to the low-priority switch and complete the software configuration according to 6.1.1 Configuring Software.

After completing the software configuration, run the **save** command in the user view to save the configuration. If some settings take effect after a restart, run the **reboot** command in the user view to restart the switch.

Step 5 Enable the stack port on the high-priority switch. On the high-priority switch, run the **interface stack-port** *member-id*/*port-id* command in the system view to enter the stack port view, and then run the **undo shutdown** command to enable the stack port.

Then the two single-chassis stacks merge into one. The low-priority switch restarts and joins the stack.

Step 6 Check whether the stack is set up successfully according to 6.1.3 Checking Whether a Stack Is Set Up Successfully.

If the stack is set up successfully, run the **save** command in the user view to save the configuration of the stack.

----End

7 Configuring Enhanced Functions for a Stack

About This Chapter

After a stack is set up, you can configure enhanced functions to improve stack system reliability and operability.

The enhanced functions can be configured in any sequence.

NOTE
It is recommended that you configure dual-active detection (DAD) for a stack to minimize the impact of a split on services.

7.1 Configuring DAD

Context

Dual-active detection (DAD) can detect a dual-master condition after a stack splits.

Configuration Process

You must select one or more of the following tasks to implement the DAD function: 7.1.1 Configuring DAD in Direct Mode on A Service Port, 7.1.2 Configuring DAD in Relay Mode on An Eth-Trunk, 7.1.3 Configuring DAD Through Management Interfaces. The other configuration tasks are optional and can be selected according to your needs.

NOTE
7.1.1 Configuring DAD in Direct Mode on A Service Port and 7.1.2 Configuring DAD in Relay Mode on An Eth-Trunk are mutually exclusive.

7.1.1 Configuring DAD in Direct Mode on A Service Port

Context

If stack member switches have idle ports, you can configure dual-active detection (DAD) in direct mode on the ports. The ports are then exclusively used for DAD and cannot forward data traffic.

NOTE

- The direct mode on a service port and relay mode on an Eth-Trunk interface cannot be configured simultaneously in a stack.
- You can configure a maximum of four direct detection links to ensure reliable DAD detection. A dual-active condition can be detected as long as one of the direct detection links is working normally.
- After configuring DAD in direct mode on a service port, you are advised to disable STP on the port (STP is enabled by default) to prevent the port status change from causing the STP status change.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface** *interface-type interface-number* command to enter the interface view.

Step 3 Run the **dual-active detect mode direct** command to enable DAD in direct mode on the service port.

By default, DAD in direct mode is disabled on an interface.

NOTE

- After DAD in direct mode is configured on a service port, the interface is blocked. The interface then processes only bridge protocol data units (BPDUs) and does not forward service packets.
- The direct detection links can also be connected through an intermediate device. DAD packets are BPDUs, so the intermediate device must be configured to transparently transmit BPDUs. For details on the configuration method, see Configuring Interface-based Layer 2 Protocol Transparent Transmission in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Ethernet Switching*.

Step 4 Run the **commit** command to commit the configuration.

----End

Follow-up Procedure

After DAD is configured and a stack splits into multiple stacks, these stacks will send competition packets to each other and all the service ports except reserved ports on the switches that fail in DAD competition will enter the Error-Down state (The device records the status of an interface as Error-Down when it detects that a fault occurs. The interface in Error-Down state cannot receive or send packets and the interface indicator is off.). In the following example, a service port is in Error-Down state.

```
<HUAWEI> display interface 10ge 1/0/1
10GE1/0/1 current state : ERROR DOWN(dual-active-fault-event) (ifindex: 12)
Line protocol current state : DOWN
......
```

After ports enter the Error-Down state, you need to rectify the link fault leading to the stack split. After the link fault is rectified, the multiple stacks will be merged, the switches that fail in DAD competition will restart automatically, and service ports in Error-Down state will recover automatically after the switches restart.

7.1.2 Configuring DAD in Relay Mode on An Eth-Trunk

Context

You can configure DAD in relay mode for a stack when an inter-device Eth-Trunk is established in the stack. To use this detection mode, configure DAD in relay mode on the inter-device Eth-Trunk and enable the DAD proxy function on the relay agent. Unlike the direct mode on service ports, the relay mode does not require exclusive ports or affect service packet forwarding on the Eth-Trunk.

NOTE

- The direct mode on a service port and relay mode on an Eth-Trunk interface cannot be configured simultaneously in a stack.
- You can configure DAD relay on a maximum of four Eth-Trunk interfaces to ensure reliable DAD detection. A dual-active condition can be detected as long as one of the Eth-Trunk interfaces is working normally.

Procedure

- Configure the stack.

1. Run the **system-view** command to enter the system view.
2. Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
3. Run the **dual-active detect mode relay** command to configure the DAD relay function on the Eth-Trunk interface.

   By default, the DAD relay function is disabled on an Eth-Trunk interface.
4. Run the **commit** command to commit the configuration.

- Configure the relay agent.

1. Run the **system-view** command to enter the system view.
2. Run the **interface eth-trunk** *trunk-id* command to enter the Eth-Trunk interface view.
3. Run the **dual-active proxy** command to enable the DAD proxy function on the Eth-Trunk interface.

   By default, the DAD proxy function is disabled on an Eth-Trunk interface.
4. Run the **commit** command to commit the configuration.

----End

Follow-up Procedure

After DAD is configured and a stack splits into multiple stacks, these stacks will send competition packets to each other and all the service ports except reserved ports on the switches that fail in DAD competition will enter the Error-Down state (The device records the status of an interface as Error-Down when it detects that a fault occurs. The interface in Error-Down state cannot receive or send packets and the interface indicator is off.). In the following example, a service port is in Error-Down state.

```
<HUAWEI> display interface 10ge 1/0/1
10GE1/0/1 current state : ERROR DOWN(dual-active-fault-event) (ifindex: 12)
```

```
Line protocol current state : DOWN
......
```

After ports enter the Error-Down state, you need to rectify the link fault leading to the stack split. After the link fault is rectified, the multiple stacks will be merged, the switches that fail in DAD competition will restart automatically, and service ports in Error-Down state will recover automatically after the switches restart.

7.1.3 Configuring DAD Through Management Interfaces

Context

When all stack member switches connect to a management network through their management interfaces, DAD can be implemented using the management interfaces. This mode does not occupy additional ports and does not require a DAD relay agent.

NOTE

- To implement DAD through management interfaces, ensure that IP addresses are configured for management interfaces.
- When DAD is implemented through management interfaces, a dual-active situation is detected if different stacks have management interfaces connected to the same management network and have the same stack domain ID and management IP address configured. As a result, ports on the low-priority device will become Error-Down.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface meth 0/0/0** command to enter the management interface view.

Step 3 Run the **dual-active detect enable** command to enable DAD on the management interface.

By default, DAD is disabled on a management interface.

Step 4 Run the **commit** command to commit the configuration.

----End

Follow-up Procedure

After DAD is configured and a stack splits into multiple stacks, these stacks will send competition packets to each other and all the service ports except reserved ports on the switches that fail in DAD competition will enter the Error-Down state (The device records the status of an interface as Error-Down when it detects that a fault occurs. The interface in Error-Down state cannot receive or send packets and the interface indicator is off.). In the following example, a service port is in Error-Down state.

```
<HUAWEI> display interface 10ge 1/0/1
10GE1/0/1 current state : ERROR DOWN(dual-active-fault-event) (ifindex: 12)
Line protocol current state : DOWN
......
```

After ports enter the Error-Down state, you need to rectify the link fault leading to the stack split. After the link fault is rectified, the multiple stacks will be merged, the switches that fail

in DAD competition will restart automatically, and service ports in Error-Down state will recover automatically after the switches restart.

7.1.4 (Optional) Specifying Excluded Ports

Context

After the DAD module detects a stack split, member switches compete to determine their active/recovery states. The member switch that fails in the competition shuts down all its service ports to prevent network flapping caused by MAC or IP address flapping. If some ports only transparently transmit packets, they do not affect network operation in a dual-active condition. If you want to retain services on these ports, specify the ports as excluded ports. These ports will not be shut down when a dual-active condition occurs.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dual-active exclude interface** *interface-type interface-number1* [**to** *interface-number2*] command to specify excluded ports.

By default, the physical ports working in stack mode are excluded ports, and all the other service ports are non-excluded ports.

Step 3 Run the **commit** command to commit the configuration.

----End

7.1.5 (Optional) Setting the Backup IP Address

Context

After the stack system configured with DAD is split, the service interfaces and management interfaces (except reserved interfaces) on the switch that fails the competition are disabled. You can log in to the switch only through the console interface and cannot remotely log in through the management interface.

If the backup IP address is configured for a stack member switch and the switch fails the DAD competition, enable the management interface and switch the IP address to the backup IP address to prevent conflict with the management IP addresses of other switches. You can then remotely log in to the switch to locate and rectify faults.

NOTE

If a management interface is configured as a reserved interface, it is disabled after being configured as a non-reserved interface when the IP address is switched.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **interface meth 0/0/0** command to enter the management interface view.

Step 3 Set a backup IPv4 address for the stack member switch.

- Run the **dual-active backup ip address** *ipv4-address* { *mask* | *mask-length* } **member** { *member-id* | **all** } command to set a backup IPv4 address for the stack member switch.

- Run the **dual-active backup ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* | *ipv6-address* **link-local** } [**cga**] **member** { *member-id* | **all** } command to set a backup IPv6 address for the stack member switch.

By default, no backup IP address is set for a stack member switch.

Step 4 Run the **commit** command to commit the configuration.

----End

7.1.6 (Optional) Restoring Shutdown Ports

Context

The DAD mechanism requires stack members switches to compete after a stack splits. The switch that wins the competition retains in Active state and works normally. The other switch that fails in the competition turns to the Recovery state and shuts down all its service ports except the excluded ones. Services on the shutdown ports are interrupted. If the switch in Active state fails or is removed from the network before the stack recovers, you can restore shutdown ports on the switch in Recovery state. Then the switch takes over services on the faulty switch to minimize impact on services.

NOTE
Do not use the **dual-active restore** command if the switch in active state is working normally. Otherwise, a dual-active condition occurs again and the service ports are shut down, causing port status flapping.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **dual-active restore** command to restore the ports that have been shut down by DAD.

----End

7.1.7 Checking the Configuration

Procedure

- Run the **display dual-active** [**proxy**] command to check the DAD configuration.

----End

7.2 Configuring the Stack MAC Address

Context

By default, a stack's MAC address is the MAC address of the master switch elected when the stack is set up. However, the stack MAC address may change after the stack restarts. To retain the stack MAC address, set the stack MAC address to the MAC address of a member switch. The stack then uses the same MAC address every time it restarts.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **stack** command to enter the stack management view.

Step 3 Run the **set system mac-address slot** *slot-id* command to configure the stack MAC address.

If the current stack MAC address is different from the one configured using this command, the stack MAC address is changed to the configured one immediately after the command is executed.

----End

7.3 Configuring a Stack MAC Address Switching Delay

Context

A stack is a logical switch, in which all member switches have the same MAC address. If a member switch is moved to another node on the network, its MAC address may conflict with the stack MAC address. To prevent MAC address conflicts in such conditions, configure a stack MAC address switching delay according to situations on your network. If the MAC address of the switch that leaves the stack is the stack MAC address and the switch does not join the stack within the delay time, the stack MAC address changes to the MAC address of the master switch.

NOTE

After you run the **set system mac-address slot** *slot-id* command to set a fixed stack MAC address, the MAC address switching delay becomes invalid.

Procedure

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **stack** command to enter the stack management view.

Step 3 Run the **set system mac-address switch-delay** { *delay-time* | **immediately** } command to configure a stack MAC address switching delay.

By default, the stack MAC address switching delay is 10 minutes. If you specify **immediately** in the command, the stack MAC address will change immediately after the switch with the stack MAC address leaves the stack. If you set *delay-time* to 0, the stack MAC address does not change.

Step 4 Run the **commit** command to commit the configuration.

----End

7.4 Configuring the Description of a Stack Member Switch

Context

To facilitate management and identification of a stack member switch, configure the description of the stack member switch.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
stack
```

The stack management view is displayed.

Step 3 Run:

stack member *member-id* **description** *description*

The description of a stack member switch is configured.

By default, no description is configured for a stack member switch.

Step 4 Run:

```
commit
```

The configuration is committed.

----End

8 Maintaining a Stack

About This Chapter

This section describes how to maintain a stack.

8.1 Monitoring the Stack Status

Context

To ensure normal system operations or locate faults that occur in the stack, run the following command in any view to monitor the stack running status.

Procedure

- Run the **display stack** [**member** *member-id*] command to check information about stack member switches.
- Run the **display stack configuration** [**member** *member-id* | **all**] command to check the stack configuration.
- Run the **display stack topology**[**link** | **neighbor**] command to check stack topology information.
- Run the **display stack troubleshooting** [**member** *member-id*] command to check the stack fault events.
- Run the **display stack link-state last-down-reason** command to check why the stack link protocol becomes Down.
- Run the **display stack blocked-interface** [**member** *member-id*] command to check packet congestion information on stack ports in a stack.

----End

8.2 Performing a Master/Standby Switchover

Context

You can manually trigger a master/standby switchover in a stack if the current roles of member switches do not meet your requirement. For example, you can perform a master/standby switchover to change the roles after a restart or restore the original roles after an upgrade.

Procedure

Step 1 (Optional) Run the **display switchover state** command to check whether the stack meets switchover requirements.

You can perform a switchover only if the Switchover State field is **Ready**.

Step 2 Run the **system-view** command to enter the system view.

Step 3 Run the **slave switchover enable** command to enable the master/standby switchover function.

By default, the master/standby switchover function is enabled.

Step 4 Run the **slave switchover** command to perform a master/standby switchover.

----End

8.3 Upgrading Stack Software

Context

Three methods can be used to upgrade the software version of a stack: system restart, fast upgrade, and in-service software upgrade (ISSU). The following table compares these upgrade methods.

Table 8-1 Upgrade method comparison

Upgrade Method	Upgrade Mechanism	Usage Scenario
System restart	After you specify the new system software to use at the next startup, the stack restarts.	This upgrade method is commonly used, but it causes service interruption in a long time. Therefore, this method can be used in scenarios insensitive to the service interruption time.
Fast upgrade	An upgrade is completed through switchovers between the stack member switches. The standby switch is upgraded first, and then the master switch.	• This upgrade method shortens service interruption time and can be used in scenarios sensitive to the service interruption time. • The fast upgrade function applies only to a

Upgrade Method	Upgrade Mechanism	Usage Scenario
		stack with two member switches.
ISSU upgrade	An upgraded is completed through card switchovers. For more information about ISSU upgrade, see ISSU Configuration in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Basic Configurations*.	• This upgrade method ensures the shortest service interruption time and can be used in scenarios that have high requirement on service continuity. • This method can upgrade a stack with two or more member switches.

NOTE

- Do not remove or reinstall cards, optical module or power cycle the switch during a software upgrade.
- Ensure network stability and do not perform other service configurations on the network during a software upgrade.

Procedure

Step 1 Upload the system software.

1. Load the new system software to the master switch. For details on how to upload the system software, see File Management in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Basic Configurations*.
2. Run the **copy** *source-filename destination-filename* **all** command to copy the system software to all the member switches.

Step 2 Perform a software upgrade.

- **System restart**

1. Run the **startup system-software** *system-file* **all** command to specify the name of the system software to use at the next startup.
2. Run the **reboot** command to restart the stack.

- **Quick upgrade**

1. Run the **startup system-software** *system-file* **all** command to specify the name of the system software to use at the next startup.
2. Run the **system-view** command to enter the system view.
3. Run the **stack** command to enter the stack management view.
4. Run the **stack upgrade fast** command to start a fast upgrade.

   After performing a fast upgrade, you can run the **display stack upgrade status** command to check the upgrade status.

NOTE

- Only the stack containing two member switches supports fast upgrade.
- If 40GE high-speed cables are used to connect stack member devices, you cannot fast upgrade switches from versions earlier than V100R003C00 to later versions.
- It is recommended that the upstream and downstream devices be connected to the stack through Eth-Trunk links to reduce the traffic interruption time during an upgrade.
- It is recommended to configure a backup IP address for the stack management interface before a fast upgrade to prevent a failure to manage member devices when the stack fails the fast upgrade and splits.

- **ISSU upgrade**

1. Run the **issu check** *system-file* [**patch** *patch-name*] command to check whether the system is ready for an ISSU upgrade.
2. Run the **issu start** [**rollback-timer** [*time*]] *system-file* [**patch** *patch-name* | **startup-configuration**] * command to start an ISSU upgrade.

   During an ISSU upgrade, you can run the **display issu state** command to check the upgrade status.

   This section provides only brief ISSU upgrade steps. For detailed operation guides and precautions, see ISSU Configuration in the *CloudEngine 8800&7800&6800&5800 Series Switches Configuration Guide - Basic Configurations*.

----End

9 Splitting a Stack

This section describes how to split a stack.

Context

If a stack is not required, split the stack to restore the member switches to standalone switches. The recommended procedure for splitting a stack is as follows:

1. Back up the stack configuration file in case the stack will be used again.
2. Remove stack cables.
3. Restore the physical member ports as service ports.
4. Restore the stack member ID to the default value.
5. Restart the switches.

Procedure

Step 1 Run the **save** command in the user view to save the configuration.

Step 2 Run the **copy** *source-filename destination-filename* **all** command to back up the configuration file to all the member switches.

Step 3 Remove stack cables between the member switches.

Step 4 Delete the physical member ports from the stack ports using either of the following methods:

- Run the **undo port member-group interface** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-32> command in the stack port view.
- Run the **undo stack-port** [*member-id*/*port-id*] command in the interface view.

Step 5 Restore the physical member ports as service ports using either of the following methods:

- Run the **undo port mode stack interface** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-32> command in the stack port view.
- Run the **undo port mode stack** command in the interface view.

Step 6 Run the **stack member** *member-id* **renumber 1** command in the stack management view to restore the stack member ID to 1.

Step 7 Run the **save** command in the user view to save the configuration.

Step 8 Run the **reboot** command in the user view to restart the switch.

NOTE

Perform steps 4 to 8 on each member switch.

----End

10 Configuration Examples

About This Chapter

This section provides stack configuration examples, including networking requirements, configuration roadmap, and configuration procedure.

10.1 Example for Establishing a Stack in a Chain Topology

Networking Requirements

An enterprise network needs to provide sufficient number of ports for access devices, and the network structure should be simple to facilitate configuration and management.

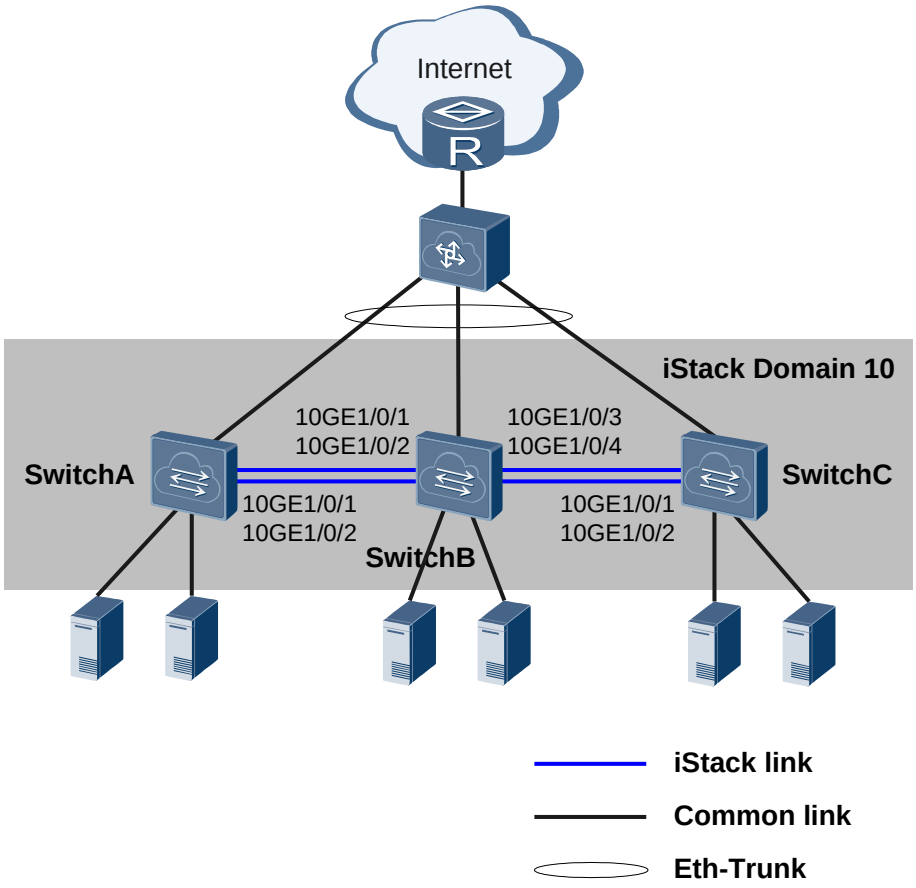
As shown in Figure 10-1, SwitchA, SwitchB, and SwitchC need to set up a stack in a chain topology. For stack connections, add 10GE1/0/1 and 10GE1/0/2 of SwitchA to stack port 1/1, 10GE1/0/1 and 10GE1/0/2 of SwitchB to stack port 1/1, 10GE1/0/3 and 10GE1/0/4 of SwitchB to stack port 1/2, and 10GE1/0/1 and 10GE1/0/2 of SwitchC to stack port 1/1.

NOTE

CE6850EIs are used to set up a stack in this example.

If you use CE5810EIs to set up a stack, you can use some 10GE optical ports as physical member ports and retain some 10GE optical ports as uplink service ports.

Figure 10-1 Stack in a chain topology



Configuration Roadmap

The configuration roadmap is as follows:

1. To enable the switches to set up a stack and distinguish the stack from other stacks on the network, configure stack parameters for the switches, including the stack member ID, priority, and stack domain ID.
2. To enable data packets to be forwarded between stack member switches, configure stack ports on the switches. Multiple physical member ports can be added to a stack port to improve stack link bandwidth and reliability.
3. To make the configuration effective and ensure that the stack can be set up successfully, save the stack configuration, restart the switches, connect the switches using stack cables.

Procedure

Step 1 Configure stack parameters on SwitchA, SwitchB, and SwitchC.

On SwitchA, set the stack member ID to 1, stack priority to 150, and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
```

```
[~SwitchA] stack
[~SwitchA-stack] stack member 1 priority 150
[*SwitchA-stack] stack member 1 domain 10
[*SwitchA-stack] quit
[*SwitchA] commit
```

NOTE

By default, the stack member ID of a switch is 1. In this example, SwitchA retains the default stack member ID 1, and you do not configure this parameter.

On SwitchB, set the stack member ID to 2 and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] stack
[~SwitchB-stack] stack member 1 renumber 2 inherit-config
Warning: The stack configuration of member ID 1 will be inherited to member ID 2 after
the device resets. Continue? [Y/N]: y
[*SwitchB-stack] stack member 1 domain 10
[*SwitchB-stack] quit
[*SwitchB] commit
```

On SwitchC, set the stack member ID to 3 and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchC
[*HUAWEI] commit
[~SwitchC] stack
[~SwitchC-stack] stack member 1 renumber 3 inherit-config
Warning: The stack configuration of member ID 1 will be inherited to member ID 3 after
the device resets. Continue? [Y/N]: y
[*SwitchC-stack] stack member 1 domain 10
[*SwitchC-stack] quit
[*SwitchC] commit
```

NOTE

When you run the **stack renumber** *new-member-id* [**inherit-config**] command to change the stack member ID:

- If you specify **inherit-config**, the switch inherits the original stack configuration after it restarts, including the stack priority, stack domain ID, and physical member port configuration. The common service port configuration will be lost. For example, the port split configuration will be lost, but the split configuration of physical member ports is inherited.
- If you do not specify **inherit-config**, the current stack configuration and common service port configuration are lost after the switch restarts, and the configuration related to the new stack member ID in the configuration file takes effect.
- If the configuration file contains offline configuration for the new stack member ID, do not specify **inherit-config** in the command.

Step 2 Configure stack ports.

On SwitchA, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1.

```
[~SwitchA] interface stack-port 1/1
[*SwitchA-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
```

```
[*SwitchA-Stack-Port1/1] quit
[*SwitchA] commit
[~SwitchA] quit
```

On SwitchB, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1, and add 10GE1/0/3 and 10GE1/0/4 to stack port 1/2.

```
[~SwitchB] interface stack-port 1/1
[*SwitchB-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
[*SwitchB-Stack-Port1/1] quit
[*SwitchB] interface stack-port 1/2
[*SwitchB-Stack-Port1/2] port member-group interface 10ge 1/0/3 to 1/0/4
[*SwitchB-Stack-Port1/2] quit
[*SwitchB] commit
[~SwitchB] quit
```

On SwitchC, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1.

```
[~SwitchC] interface stack-port 1/1
[*SwitchC-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
[*SwitchC-Stack-Port1/1] quit
[*SwitchC] commit
[~SwitchC] quit
```

Step 3 Check the stack configuration.

After completing the stack configuration, run the **display stack configuration** command on the switches to check whether the configuration is the same as expected. The command output on SwitchA is used as an example.

```
<SwitchA> display stack configuration
Oper : Operation
Conf : Configuration
*    : Offline configuration
Isolated Port: The port is in stack mode, but does not belong to any Stack-Port

Attribute Configuration:
-----------------------------------------
 MemberID     Domain        Priority
Oper(Conf)   Oper(Conf)     Oper(Conf)
-----------------------------------------
1(1)        --(10)         100(150)
-----------------------------------------

Stack-Port Configuration:
-------------------------------------------------------------------------------
Stack-Port         Member Ports
-------------------------------------------------------------------------------
Stack-Port1/1       10GE1/0/1    10GE1/0/2
-------------------------------------------------------------------------------
```

```
Isolated Port Configuration:
10GE1/0/3     10GE1/0/4
```

Step 4 Save the configuration and restart the switch.

Save the configurations of SwitchA, SwitchB, and SwitchC, and restart the switches. The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA, and are not mentioned here.

```
<SwitchA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<SwitchA> reboot
Warning: The system will reboot. Continue? [Y/N]: y


#
```

Step 5 Connect the switches using stack cables to set up a stack.

Step 6 Verify the configuration.

Check information about the stack member switches.

```
<SwitchA> display stack
--------------------------------------------------------------------------------
MemberID Role    MAC            Priority   DeviceType        Description
--------------------------------------------------------------------------------
+1       Master  0004-9f31-d520  150        CE6850-48S4Q-EI
 2       Standby 0004-9f62-1f40  100        CE6850-48S4Q-EI
 3       Slave   0004-9f69-a391  100        CE6850-48S4Q-EI
--------------------------------------------------------------------------------
+ indicates the device through which the user logs in.
```

Display stack topology information.

```
<SwitchA> display stack topology
Stack Topology:
-----------------------------------------------
          Stack-Port 1     Stack-Port 2
MemberID   Status Neighbor   Status Neighbor
-----------------------------------------------
1         up    2         --    --
2         up    1         up    3
3         up    2         --    --
-----------------------------------------------

Stack Link:
--------------------------------------------------------------------------
Stack-Port      Port          Status    PeerPort      PeerStatus
--------------------------------------------------------------------------
Stack-Port1/1   10GE1/0/1     up        10GE2/0/1     up
Stack-Port1/1   10GE1/0/2     up        10GE2/0/2     up
Stack-Port2/1   10GE2/0/1     up        10GE1/0/1     up
Stack-Port2/1   10GE2/0/2     up        10GE1/0/2     up
Stack-Port2/2   10GE2/0/3     up        10GE3/0/1     up
Stack-Port2/2   10GE2/0/4     up        10GE3/0/2     up
Stack-Port3/1   10GE3/0/1     up        10GE2/0/3     up
```

```
Stack-Port3/1    10GE3/0/2     up        10GE2/0/4     up
------------------------------------------------------------------------------
```

Step 7 Save the configuration.

NOTE

After the stack is set up, you are advised to run the **save** command to save the configuration immediately.

```
<SwitchA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
```

----End

Configuration Files

- Configuration file of the stack

```
#
sysname SwitchA
#
stack
 #
 stack member 1 domain 10
 stack member 1 priority 150
 #
 stack member 2 domain 10
 #
 stack member 3 domain 10
#
interface Stack-Port1/1
#
interface Stack-Port2/1
#
interface Stack-Port2/2
#
interface Stack-Port3/1
#
interface 10GE1/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/3
 port mode stack
#
interface 10GE1/0/4
 port mode stack
#
interface 10GE2/0/1
 port mode stack
 stack-port 2/1
#
```

```
interface 10GE2/0/2
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/3
 port mode stack
 stack-port 2/2
#
interface 10GE2/0/4
 port mode stack
 stack-port 2/2
#
interface 10GE3/0/1
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/2
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/3
 port mode stack
#
interface 10GE3/0/4
 port mode stack
#
return
```

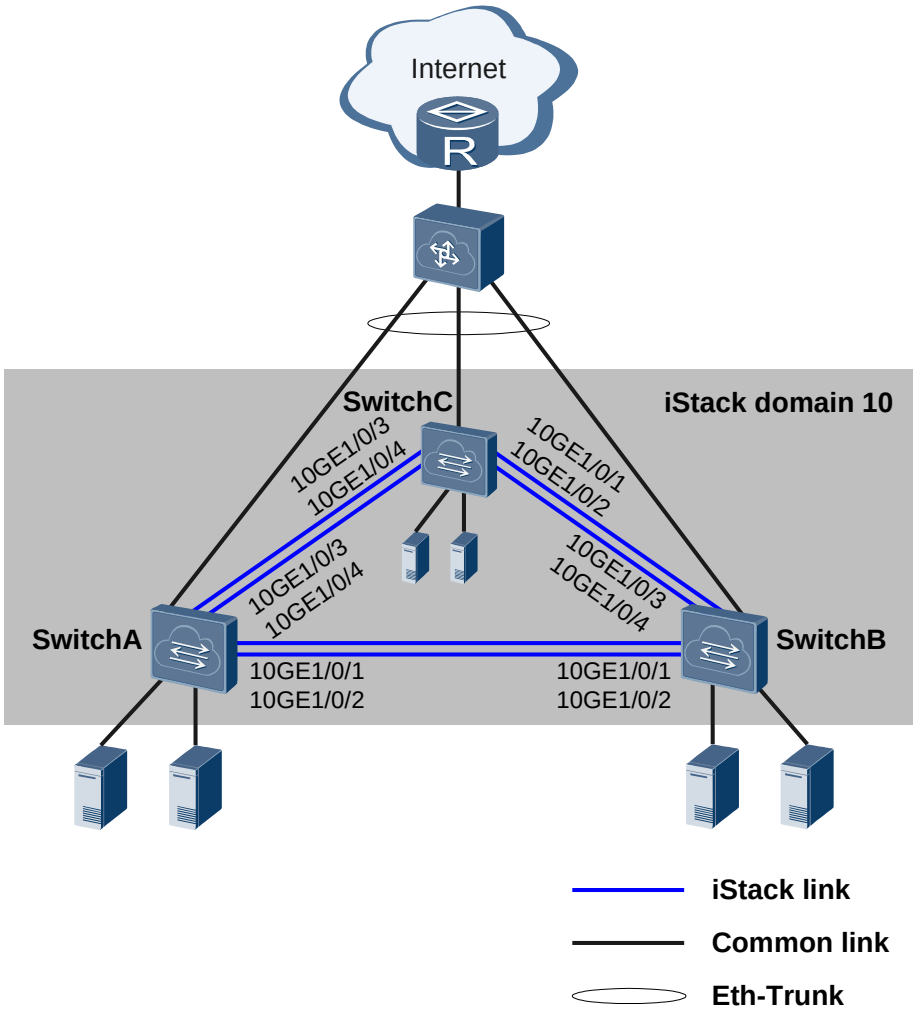
10.2 Example for Establishing a Stack in a Ring Topology

Networking Requirements

An enterprise network needs to provide sufficient number of ports for access devices, and the network structure should be simple to facilitate configuration and management.

As shown in Figure 10-2, SwitchA, SwitchB, and SwitchC need to set up a stack in a ring topology. For stack connections, add physical ports 10GE1/0/1 and 10GE1/0/2 to stack port 1/1 and physical ports 10GE1/0/3 and 10GE1/0/4 to stack port 1/2 on each switch.

Figure 10-2 Stack in a ring topology



Configuration Roadmap

The configuration roadmap is as follows:

1. To enable the switches to set up a stack and distinguish the stack from other stacks on the network, configure stack parameters for the switches, including the stack member ID, priority, and stack domain ID.
2. To enable data packets to be forwarded between stack member switches, configure stack ports on the switches. Multiple physical member ports can be added to a stack port to improve stack link bandwidth and reliability.
3. To make the configuration effective and ensure that the stack can be set up successfully, save the stack configuration, restart the switches, connect the switches using stack cables.

Procedure

Step 1 Configure stack parameters on SwitchA, SwitchB, and SwitchC.

On SwitchA, set the stack member ID to 1, stack priority to 150, and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchA
[*HUAWEI] commit
[~SwitchA] stack
[~SwitchA-stack] stack member 1 priority 150
[*SwitchA-stack] stack member 1 domain 10
[*SwitchA-stack] quit
[*SwitchA] commit
```

NOTE

By default, the stack member ID of a switch is 1. In this example, SwitchA retains the default stack member ID 1, and you do not configure this parameter.

On SwitchB, set the stack member ID to 2 and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] stack
[~SwitchB-stack] stack member 1 renumber 2 inherit-config
Warning: The stack configuration of member ID 1 will be inherited to member ID 2 after
the device resets. Continue? [Y/N]: y
[*SwitchB-stack] stack member 1 domain 10
[*SwitchB-stack] quit
[*SwitchB] commit
```

On SwitchC, set the stack member ID to 3 and stack domain ID to 10.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchC
[*HUAWEI] commit
[~SwitchC] stack
[~SwitchC-stack] stack member 1 renumber 3 inherit-config
Warning: The stack configuration of member ID 1 will be inherited to member ID 3 after
the device resets. Continue? [Y/N]: y
[*SwitchC-stack] stack member 1 domain 10
[*SwitchC-stack] quit
[*SwitchC] commit
```

NOTE

When you run the **stack renumber** *new-member-id* [**inherit-config**] command to change the stack member ID:

- If you specify **inherit-config**, the switch inherits the original stack configuration after it restarts, including the stack priority, stack domain ID, and physical member port configuration. The common service port configuration will be lost. For example, the port split configuration will be lost, but the split configuration of physical member ports is inherited.
- If you do not specify **inherit-config**, the current stack configuration and common service port configuration are lost after the switch restarts, and the configuration related to the new stack member ID in the configuration file takes effect.
- If the configuration file contains offline configuration for the new stack member ID, do not specify **inherit-config** in the command.

Step 2 Configure stack ports.

On SwitchA, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1, and add 10GE1/0/3 and 10GE1/0/4 to stack port 1/2.

```
[~SwitchA] interface stack-port 1/1
[*SwitchA-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
[*SwitchA-Stack-Port1/1] quit
[*SwitchA] interface stack-port 1/2
[*SwitchA-Stack-Port1/2] port member-group interface 10ge 1/0/3 to 1/0/4
[*SwitchA-Stack-Port1/2] quit
[*SwitchA] commit
[~SwitchA] quit
```

On SwitchB, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1, and add 10GE1/0/3 and 10GE1/0/4 to stack port 1/2.

```
[~SwitchB] interface stack-port 1/1
[*SwitchB-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
[*SwitchB-Stack-Port1/1] quit
[*SwitchB] interface stack-port 1/2
[*SwitchB-Stack-Port1/2] port member-group interface 10ge 1/0/3 to 1/0/4
[*SwitchB-Stack-Port1/2] quit
[*SwitchB] commit
[~SwitchB] quit
```

On SwitchC, add 10GE1/0/1 and 10GE1/0/2 to stack port 1/1, and add 10GE1/0/3 and 10GE1/0/4 to stack port 1/2.

```
[~SwitchC] interface stack-port 1/1
[*SwitchC-Stack-Port1/1] port member-group interface 10ge 1/0/1 to 1/0/2
Warning: The interface(s) (10GE1/0/1-1/0/4) will be converted to stack mode. [Y/N]:
y
[*SwitchC-Stack-Port1/1] quit
[*SwitchC] interface stack-port 1/2
[*SwitchC-Stack-Port1/2] port member-group interface 10ge 1/0/3 to 1/0/4
[*SwitchC-Stack-Port1/2] quit
[*SwitchC] commit
[~SwitchC] quit
```

Step 3 Check the stack configuration.

After completing the stack configuration, run the **display stack configuration** command on the switches to check whether the configuration is the same as expected. The command output on SwitchA is used as an example.

```
<SwitchA> display stack configuration
Oper : Operation
Conf : Configuration
*    : Offline configuration
Isolated Port: The port is in stack mode, but does not belong to any Stack-Port

Attribute Configuration:
----------------------------------------
 MemberID     Domain        Priority
Oper(Conf)   Oper(Conf)     Oper(Conf)
```

```
----------------------------------------
1(1)        --(10)        100(150)
----------------------------------------

Stack-Port Configuration:
--------------------------------------------------------------------------------
Stack-Port         Member Ports
--------------------------------------------------------------------------------
Stack-Port1/1       10GE1/0/1    10GE1/0/2
Stack-Port1/2       10GE1/0/3    10GE1/0/4
--------------------------------------------------------------------------------
```

Step 4 Save the configuration and restart the switch.

Save the configurations of SwitchA, SwitchB, and SwitchC, and restart the switches. The configurations of SwitchB and SwitchC are similar to the configuration of SwitchA, and are not mentioned here.

```
<SwitchA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<SwitchA> reboot
Warning: The system will reboot. Continue? [Y/N]: y


#
```

Step 5 Connect the switches using stack cables to set up a stack.

Step 6 Verify the configuration.

Check information about the stack member switches.

```
<SwitchA> display stack
--------------------------------------------------------------------------------
MemberID Role    MAC            Priority   DeviceType       Description
--------------------------------------------------------------------------------
+1      Master   0004-9f31-d520   150       CE6850-48S4Q-EI
 2      Standby  0004-9f62-1f40   100       CE6850-48S4Q-EI
 3      Slave    0004-9f69-a391   100       CE6850-48S4Q-EI
--------------------------------------------------------------------------------
+ indicates the device through which the user logs in.
```

Display stack topology information.

```
<SwitchA> display stack topology
Stack Topology:
-----------------------------------------------
          Stack-Port 1     Stack-Port 2
MemberID   Status Neighbor   Status Neighbor
-----------------------------------------------
1         up    2         up    3
2         up    1         up    3
3         up    2         up    1
-----------------------------------------------

Stack Link:
--------------------------------------------------------------------
```

```
Stack-Port      Port         Status    PeerPort      PeerStatus
--------------------------------------------------------------------------
Stack-Port1/1   10GE1/0/1     up        10GE2/0/1     up
Stack-Port1/1   10GE1/0/2     up        10GE2/0/2     up
Stack-Port1/2   10GE1/0/3     up        10GE3/0/3     up
Stack-Port1/2   10GE1/0/4     up        10GE3/0/4     up
Stack-Port2/1   10GE2/0/1     up        10GE1/0/1     up
Stack-Port2/1   10GE2/0/2     up        10GE1/0/2     up
Stack-Port2/2   10GE2/0/3     up        10GE3/0/1     up
Stack-Port2/2   10GE2/0/4     up        10GE3/0/2     up
Stack-Port3/1   10GE3/0/1     up        10GE2/0/3     up
Stack-Port3/1   10GE3/0/2     up        10GE2/0/4     up
Stack-Port3/2   10GE3/0/3     up        10GE1/0/3     up
Stack-Port3/2   10GE3/0/4     up        10GE1/0/4     up
--------------------------------------------------------------------------
```

Step 7 Save the configuration.

NOTE

After the stack is set up, you are advised to run the **save** command to save the configuration immediately.

```
<SwitchA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
```

----End

Configuration Files

- Configuration file of the stack

```
#
sysname SwitchA
#
stack
 #
 stack member 1 domain 10
 stack member 1 priority 150
 #
 stack member 2 domain 10
 #
 stack member 3 domain 10
#
interface Stack-Port1/1
#
interface Stack-Port1/2
#
interface Stack-Port2/1
#
interface Stack-Port2/2
#
interface Stack-Port3/1
#
interface Stack-Port3/2
#
interface 10GE1/0/1
```

```
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/3
 port mode stack
 stack-port 1/2
#
interface 10GE1/0/4
 port mode stack
 stack-port 1/2
#
interface 10GE2/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/2
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/3
 port mode stack
 stack-port 2/2
#
interface 10GE2/0/4
 port mode stack
 stack-port 2/2
#
interface 10GE3/0/1
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/2
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/3
 port mode stack
 stack-port 3/2
#
interface 10GE3/0/4
 port mode stack
 stack-port 3/2
#
return
```

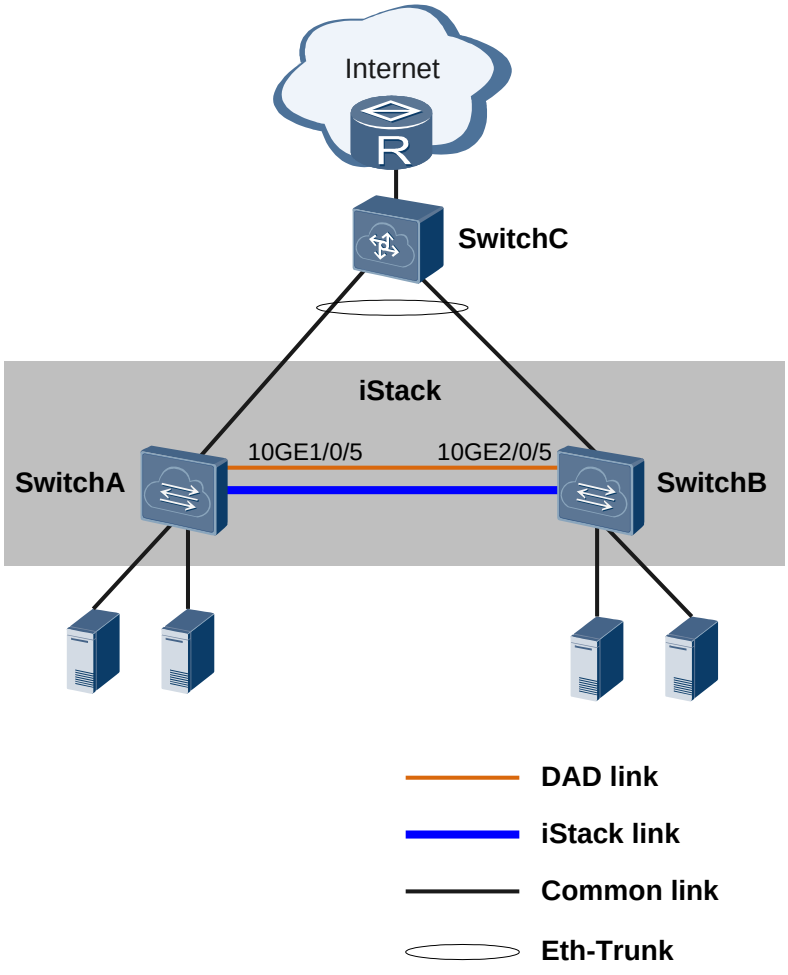
10.3 Example for Configuring DAD in Direct Mode on A Service Port

Networking Requirements

As shown in Figure 10-3, SwitchA and SwitchB set up a stack, and SwitchA is the master switch. The stack member ID of SwitchA is 1, and the stack member ID of SwitchB is 2.

If the stack splits due to a stack link failure, the network has two stacks with conflicting configurations. To avoid this dual-active condition, configure the DAD function in the stack. This function minimizes the impact of a stack split on the network.

Figure 10-3 DAD in direct mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure DAD in direct mode on interfaces of the stack member switches.

Procedure

Step 1 Configure DAD in direct mode on interfaces of the stack member switches.

Configure DAD in direct mode on 10GE1/0/5.

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/5
[~HUAWEI-10GE1/0/5] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue?
[Y/N]: y
[*HUAWEI-10GE1/0/5] commit
[~HUAWEI-10GE1/0/5] quit
```

Configure DAD in direct mode on 10GE2/0/5.

```
[~HUAWEI] interface 10ge 2/0/5
[~HUAWEI-10GE2/0/5] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue?
[Y/N]: y
[*HUAWEI-10GE2/0/5] commit
[~HUAWEI-10GE2/0/5] return
```

Step 2 Verify the configuration.

Check the detailed DAD configuration on the stack.

```
<HUAWEI> display dual-active
Dual-active status: Normal
Dual-active detect mode: Direct
Dual-active detect configuration of MEth: Disable
Dual-active direct detect interfaces configured:
 10GE1/0/5   up
 10GE2/0/5   up
Dual-active relay detect interfaces configured:
 -
Excluded ports(configurable):
 -
Excluded ports(can not be configured):
 10GE1/0/1
 10GE1/0/2
 10GE1/0/3
 10GE1/0/4
 10GE2/0/1
 10GE2/0/2
 10GE2/0/3
 10GE2/0/4
```

Step 3 Verify the DAD function.

When no service is configured on the stack after the DAD configuration is complete, trigger a stack split to verify whether the DAD function takes effect.

NOTE

Do not trigger a stack split when services are running on the stack. Otherwise, services are affected when the stack splits.

1. Trigger a stack split by shutting down all the ports with stack cable connected or removing all the stack cables.
2. Log in to each member switch to check the stack status. You can see that the stack has split into two single-chassis stacks.

```
<HUAWEI> display stack
--------------------------------------------------------------------------------
-
MemberID Role    MAC            Priority   Device Type       Description
--------------------------------------------------------------------------------
-
+1      Master   0004-9f31-d520   150        CE6850-48T4Q-EI
--------------------------------------------------------------------------------
-
+ indicates the device through which the user logs in.
```

3. Run the **display trapbuffer** command. A dual-active alarm is displayed.

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3, Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 190

Aug 15 2013 14:32:35 HUAWEI %%01DAD/1/hwDadConflictDetect(t):CID=0x807f0419-OID=
1.3.6.1.4.1.2011.5.25.246.1.1;Dual-active scenario is detected.
```

4. The preceding operations verify that the DAD function has been configured successfully.
5. Restore the physical member ports to Up state or connect stack cables. The two switches set up a stack again.

----End

Configuration Files

- Configuration file of the stack

```
#
stack
 #
 stack member 1 domain 10
 stack member 1 priority 150
 #
 stack member 2 domain 10
#
interface Stack-Port1/1
#
interface Stack-Port2/1
#
interface 10GE1/0/1
 port mode stack
 stack-port 1/1
#
```

```
interface 10GE1/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/3
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/4
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/5
 dual-active detect mode direct
#
interface 10GE2/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/2
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/3
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/4
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/5
 dual-active detect mode direct
#
return
```

10.4 Example for Configuring DAD in Relay Mode on An Eth-Trunk

Networking Requirements

As shown in Figure 10-4, SwitchA, SwitchB, and SwitchC set up a stack and connect to SwitchD through Eth-Trunk10.

If the stack splits due to a stack link failure, the network has two stacks with conflicting configurations. To avoid this dual-active condition, configure the DAD function in the stack. This function minimizes the impact of a stack split on the network.

Figure 10-4 DAD in relay mode

Configuration Roadmap

The configuration roadmap is as follows:

1. Use SwitchD as a DAD relay agent. On the stack, configure DAD in relay mode on Eth-Trunk10 connected to SwitchD.

NOTE

You must be use a switch that supports the DAD proxy function as the relay agent. All Huawei CloudEngine series switches support the DAD proxy function. Huawei S series switches support this function since V200R002.

2. On SwitchD, enable the DAD proxy function on Eth-Trunk10 so that DAD packets can be forwarded through Eth-Trunk10.

Procedure

Step 1 On the stack, configure DAD in relay mode on Eth-Trunk10.

```
<HUAWEI> system-view
[~HUAWEI] interface eth-trunk 10
```

```
[*HUAWEI-Eth-Trunk10] trunkport 10ge 1/0/5
[*HUAWEI-Eth-Trunk10] trunkport 10ge 2/0/5
[*HUAWEI-Eth-Trunk10] trunkport 10ge 3/0/5
[*HUAWEI-Eth-Trunk10] dual-active detect mode relay
[*HUAWEI-Eth-Trunk10] commit
[~HUAWEI-Eth-Trunk10] return
```

Step 2 On SwitchD, enable the DAD proxy function on Eth-Trunk10.

Log in to SwitchD and configure the DAD proxy function.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchD
[*HUAWEI] commit
[~SwitchD] interface eth-trunk 10
[*SwitchD-Eth-Trunk10] trunkport 10ge 1/0/1
[*SwitchD-Eth-Trunk10] trunkport 10ge 1/0/2
[*SwitchD-Eth-Trunk10] trunkport 10ge 1/0/3
[*SwitchD-Eth-Trunk10] dual-active proxy
[*SwitchD-Eth-Trunk10] commit
[~SwitchD-Eth-Trunk10] return
```

Step 3 Verify the configuration.

Check the detailed DAD configuration on the stack.

```
<HUAWEI> display dual-active
Dual-active status: Normal
Dual-active detect mode: Relay
Dual-active detect configuration of MEth: Disable
Dual-active direct detect interfaces configured:
 -             -
Dual-active relay detect interfaces configured:
 Eth-Trunk10
     10GE1/0/5   up
     10GE2/0/5   up
     10GE3/0/5   up
Excluded ports(configurable):
 -
Excluded ports(can not be configured):
 10GE1/0/1
 10GE1/0/2
 10GE1/0/3
 10GE1/0/4
 10GE2/0/1
 10GE2/0/2
 10GE2/0/3
 10GE2/0/4
 10GE3/0/1
 10GE3/0/2
 10GE3/0/3
 10GE3/0/4
```

Check the DAD proxy configuration on SwitchD.

```
<SwitchD> display dual-active proxy
Dual-active proxy interfaces configured:
 Eth-Trunk10
     10GE1/0/1    up
     10GE1/0/2    up
     10GE1/0/3    up
```

Step 4 Verify the DAD function.

When no service is configured on the stack after the DAD configuration is complete, trigger a stack split to verify whether the DAD function takes effect.

NOTE

Do not trigger a stack split when services are running on the stack. Otherwise, services are affected when the stack splits.

1. Trigger a stack split by shutting down all the ports with stack cable connected or removing all the stack cables.
2. Log in to each member switch to check the stack status. You can see that the stack has split into two single-chassis stacks.

```
<HUAWEI> display stack
--------------------------------------------------------------------------------
-
MemberID Role    MAC            Priority   Device Type       Description
--------------------------------------------------------------------------------
-
+1      Master   0004-9f31-d520   150        CE6850-48T4Q-EI
--------------------------------------------------------------------------------
-
+ indicates the device through which the user logs in.
```

3. Run the **display trapbuffer** command. A dual-active alarm is displayed.

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3, Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 190

Aug 15 2013 14:32:35 HUAWEI %%01DAD/1/hwDadConflictDetect(t):CID=0x807f0419-OID=
1.3.6.1.4.1.2011.5.25.246.1.1;Dual-active scenario is detected.
```

4. The preceding operations verify that the DAD function has been configured successfully.
5. Restore the physical member ports to Up state or connect stack cables. The two switches set up a stack again.

----End

Configuration Files

- Configuration file of the stack

```
#
stack
 #
 stack member 1 domain 10
 stack member 1 priority 150
 #
 stack member 2 domain 10
 #
 stack member 3 domain 10
#
interface Eth-Trunk10
 dual-active detect mode relay
#
interface Stack-Port1/1
#
interface Stack-Port2/1
#
interface Stack-Port2/2
#
interface Stack-Port3/1
#
interface 10GE1/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE1/0/3
 port mode stack
#
interface 10GE1/0/4
 port mode stack
#
interface 10GE1/0/5
 eth-trunk 10
#
interface 10GE2/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/2
 port mode stack
 stack-port 2/1
#
interface 10GE2/0/3
 port mode stack
 stack-port 2/2
#
interface 10GE2/0/4
 port mode stack
 stack-port 2/2
#
interface 10GE2/0/5
```

```
 eth-trunk 10
#
interface 10GE3/0/1
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/2
 port mode stack
 stack-port 3/1
#
interface 10GE3/0/3
 port mode stack
#
interface 10GE3/0/4
 port mode stack
#
interface 10GE3/0/5
 eth-trunk 10
#
return
```

- Configuration file of SwitchD

```
#
sysname SwitchD
#
interface Eth-Trunk10
 dual-active proxy
#
interface 10GE1/0/1
 eth-trunk 10
#
interface 10GE1/0/2
 eth-trunk 10
#
interface 10GE1/0/3
 eth-trunk 10
#
return
```

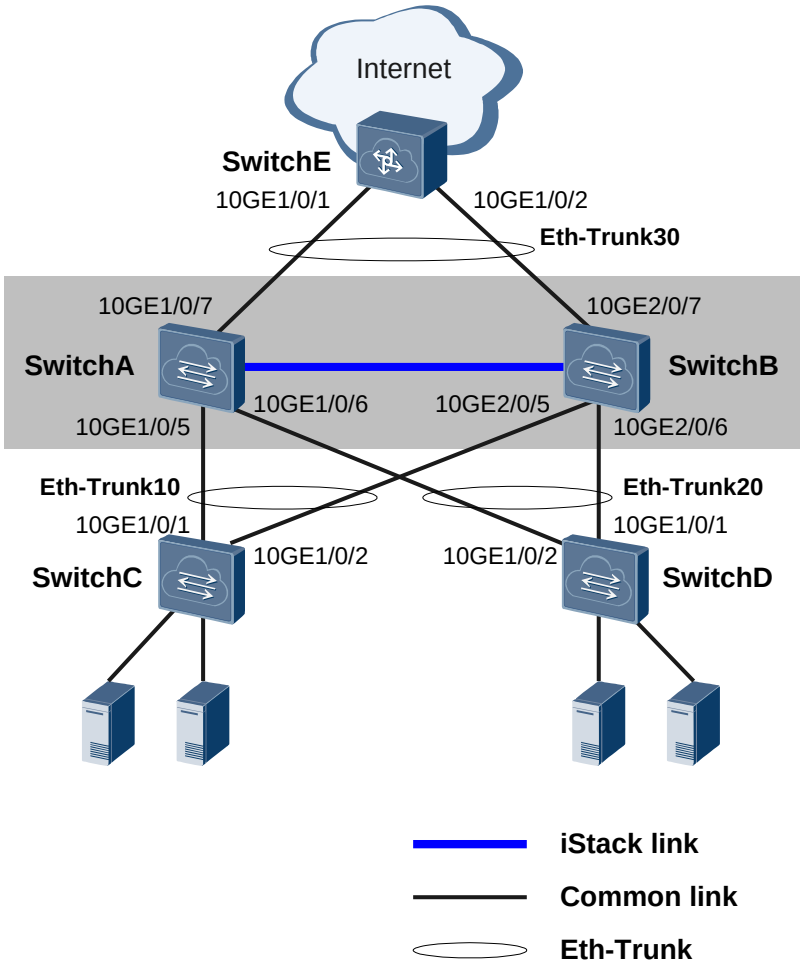
10.5 Example for Configuring Inter-Device Eth-Trunks

Networking Requirements

A network often uses link redundancy designs to improve link reliability, but link redundancy may cause loops on the network. Stacks can increase link bandwidth and improve link reliability while preventing loops on a network.

As shown in Figure 10-5, aggregation switches SwitchA and SwitchB set up a stack. SwitchA is the master switch, and SwitchB is the standby switch. The stack connects to the upstream and downstream devices through Eth-Trunks.

Figure 10-5 Inter-device Eth-Trunk networking



Configuration Roadmap

The configuration roadmap is as follows:

1. Add the links that connect the stack to the upstream and downstream devices to inter-device Eth-Trunks. This configuration improves link bandwidth and reliability, while preventing loops on the network.
2. Enable local preferential forwarding on the Eth-Trunks to improve forwarding efficiency and reduce loads on the stack links between stack member switches.

Procedure

Step 1 Configure inter-device Eth-Trunks.

On the stack, create Eth-Trunk10, Eth-Trunk20, and Eth-Trunk30, and add the interfaces connected to the upstream and downstream devices to the Eth-Trunks.

```
<HUAWEI> system-view
[~HUAWEI] sysname iStack
[*HUAWEI] commit
[~iStack] interface eth-trunk 10
```

```
[*iStack-Eth-Trunk10] trunkport 10ge 1/0/5
[*iStack-Eth-Trunk10] trunkport 10ge 2/0/5
[*iStack-Eth-Trunk10] quit
[*iStack] interface eth-trunk 20
[*iStack-Eth-Trunk20] trunkport 10ge 1/0/6
[*iStack-Eth-Trunk20] trunkport 10ge 2/0/6
[*iStack-Eth-Trunk20] quit
[*iStack] interface eth-trunk 30
[*iStack-Eth-Trunk30] trunkport 10ge 1/0/7
[*iStack-Eth-Trunk30] trunkport 10ge 2/0/7
[*iStack-Eth-Trunk30] quit
[*iStack] commit
```

On SwitchC, create Eth-Trunk10 and add 10GE1/0/1 and 10GE1/0/2 connected to the stack to Eth-Trunk10. The configurations on SwitchD and SwitchE are similar to the configuration on SwitchC, and are not mentioned here.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchC
[*HUAWEI] commit
[~SwitchC] interface eth-trunk 10
[*SwitchC-Eth-Trunk10] trunkport 10ge 1/0/1
[*SwitchC-Eth-Trunk10] trunkport 10ge 1/0/2
[*SwitchC-Eth-Trunk10] quit
[*SwitchC] commit
```

Step 2 Enable local preferential forwarding on the stack.

```
[~iStack] interface eth-trunk 10
[~iStack-Eth-Trunk10] undo local-preference disable
[*iStack-Eth-Trunk10] quit
[*iStack] interface eth-trunk 20
[*iStack-Eth-Trunk20] undo local-preference disable
[*iStack-Eth-Trunk20] quit
[*iStack] interface eth-trunk 30
[*iStack-Eth-Trunk30] undo local-preference disable
[*iStack-Eth-Trunk30] quit
[*iStack] commit
[~iStack] quit
```

NOTE

By default, local preferential forwarding is enabled on an Eth-Trunk.

Step 3 Verify the configuration.

After the configuration is complete, run the **display eth-trunk membership** *trunk-id* command in any view to view information about member interfaces of the Eth-Trunks. Information about member interfaces of Eth-Trunk10 on the stack is used as an example.

```
<iStack> display eth-trunk membership 10
Trunk ID: 10
Used Status: Valid
Type: Ethernet
Working Mode: Normal
Number Of Ports in Trunk: 2
```

```
Number Of Up Ports in Trunk: 2
Operating Status: up

Interface 10GE1/0/5, valid, operate up, weight=1
Interface 10GE2/0/5, valid, operate up, weight=1
```

----End

Configuration Files

- Configuration file of the stack

```
#
sysname iStack
#
interface Eth-Trunk10
#
interface Eth-Trunk20
#
interface Eth-Trunk30
#
interface 10GE1/0/5
 eth-trunk 10
#
interface 10GE1/0/6
 eth-trunk 20
#
interface 10GE1/0/7
 eth-trunk 30
#
interface 10GE2/0/5
 eth-trunk 10
#
interface 10GE2/0/6
 eth-trunk 20
#
interface 10GE2/0/7
 eth-trunk 30
#
return
```

- Configuration file of SwitchC

```
#
sysname SwitchC
#
interface Eth-Trunk10
#
interface 10GE1/0/1
 eth-trunk 10
#
interface 10GE1/0/2
 eth-trunk 10
#
return
```

- Configuration file of SwitchD

```
#
sysname SwitchD
#
interface Eth-Trunk20
#
interface 10GE1/0/1
 eth-trunk 20
#
interface 10GE1/0/2
 eth-trunk 20
#
return
```

- Configuration file of SwitchE

```
#
sysname SwitchE
#
interface Eth-Trunk30
#
interface 10GE1/0/1
 eth-trunk 30
#
interface 10GE1/0/2
 eth-trunk 30
#
return
```

11 FAQ

About This Chapter

This section provides answers to frequently asked questions about use of stacks.

11.1 How Can I Specify a Stack Member Switch as the Master Switch?

- Assume that SwitchA and SwitchB set up a stack, and you want SwitchA to be the master switch. If stack cables have been connected, complete stack configuration on SwitchA first and restart SwitchA. After SwitchA restarts, complete stack configuration on SwitchB and restart SwitchB. After SwitchB restarts, it joins the stack and becomes the standby switch. SwitchA functions as the master switch in the stack.
- If you complete stack configuration on the two switches before connecting stack cables, the two single-chassis stacks merge into one stack after they are connected. Set a higher stack priority for SwitchA and a lower stack priority for SwitchB, so that SwitchA becomes the master switch after the stacks merge.

11.2 How Do I Know Which Switch Is the Master Switch in a Stack?

After a stack is set up, you can observe indicators on member switches or use commands to determine which member switch is the master switch.

- Observing indicators

  If the MST indicator on a switch is steady green, the switch is the master switch. The MST indicators on the other member switches are off, and the switches are standby or slave switches.

- Using commands

  Run the **display stack** or **display device** command to check which member switch is the master switch.

```
<HUAWEI> display stack

--------------------------------------------------------------------------------
-
MemberID Role    MAC            Priority  DeviceType       Description
--------------------------------------------------------------------------------
-
3       Master  006d-a835-1700  160       CE5810-48T4S-EI
4       Slave   0019-8c68-3360  150       CE5810-24T4S-EI
5       Standby 0023-d856-1c00  140       CE5810-48T4S-EI
--------------------------------------------------------------------------------
-
<HUAWEI> display device
Device status:
--------------------------------------------------------------------------------
Slot  Card  Type            Online  Power Register   Alarm   Primary
--------------------------------------------------------------------------------
3     -     CE5810-48T4S-EI   Present  On   Registered  Normal  Master
      FAN1  -               Present  On   Registered  Normal  NA
      FAN2  -               Present  On   Registered  Normal  NA
      PWR2  -               Present  On   Registered  Normal  NA
4     -     CE5810-24T4S-EI   Present  On   Registered  Normal  Slave
      FAN1  -               Present  On   Registered  Normal  NA
      FAN2  -               Present  On   Registered  Normal  NA
      PWR1  -               Present  On   Registered  Normal  NA
      PWR2  -               Present  On   Registered  Normal  NA
5     -     CE5810-48T4S-EI   Present  On   Registered  Normal  Standby
      FAN1  -               Present  On   Registered  Normal  NA
      FAN2  -               Present  On   Registered  Normal  NA
      PWR2  -               Present  On   Registered  Normal  NA
--------------------------------------------------------------------------------
```

11.3 How to Load Patches for a Stack?

The process of loading patches for a stack is similar to that for a standalone device:

1. Upload patch files to the master switch.
2. Run the **patch load** *filename* **all run** command in the user view to load and run the patches.
3. Run the **display patch-information** command to check whether the patches are loaded successfully.

11.4 How to Restart a Stack Member Device?

Run the **reset slot** *slot-id* command in the user view to restart a specified stack member device.

Before restarting a member device, save the stack configurations of the device to ensure that the device can join the stack normally after being restarted.