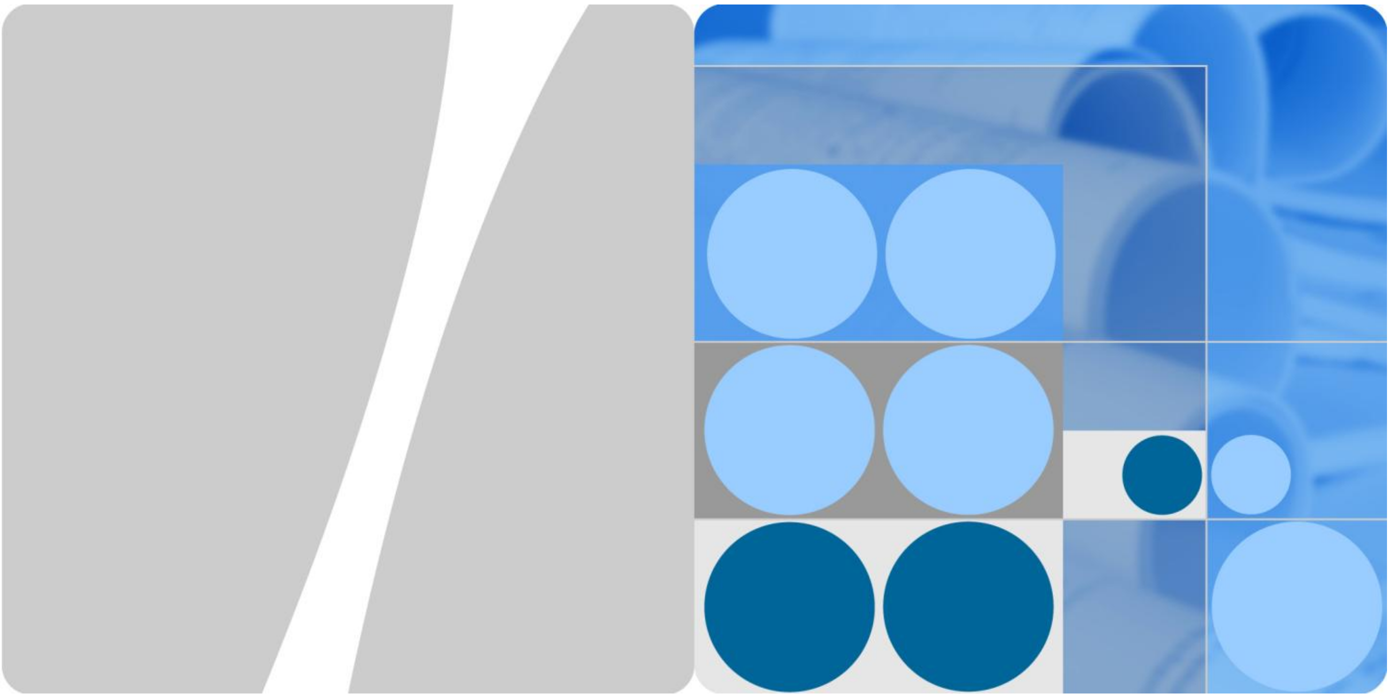


CloudEngine 12800 Series Switches

CSS Technology White Paper

Issue	**03**
Date	**2016-01-05**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

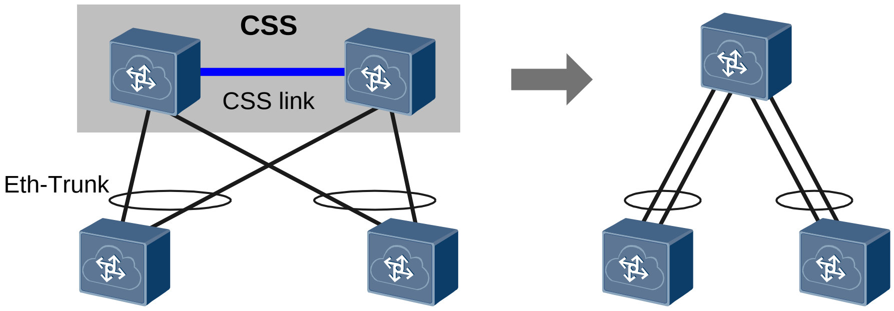
1 Stack Overview

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

Definition

A cluster switch system (CSS) is also called a stack. (The term stack is used throughout this document.) Stacking technology combines two 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.

- 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

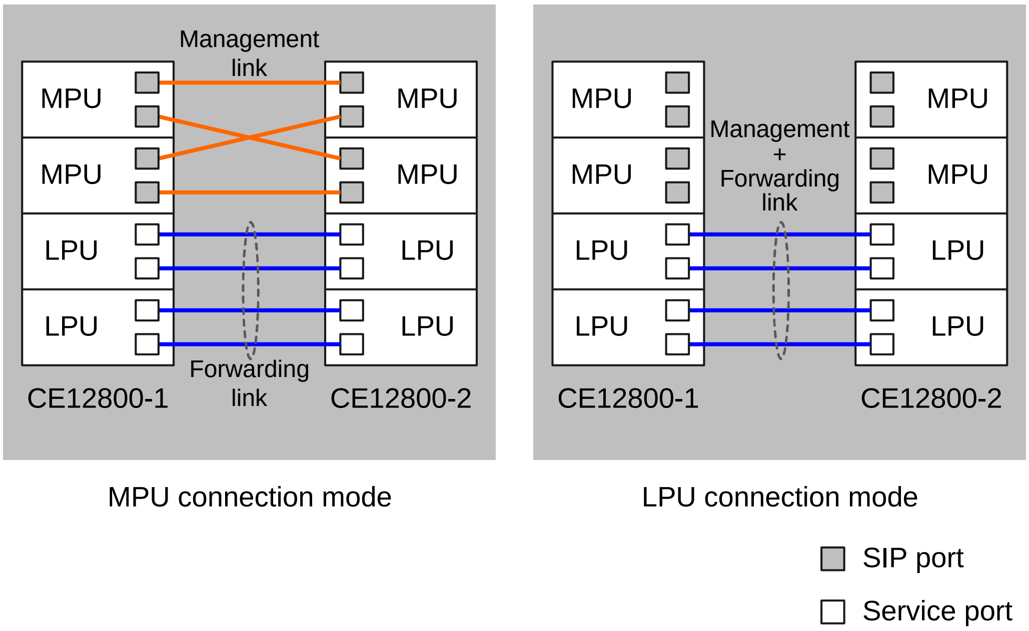
  A stack port is a logical port exclusively used for stacking and includes several physical stack ports. Multiple physical member ports can be added to a stack port to improve stack link bandwidth and reliability.

  Each switch supports one stack port. Before the stacking function is enabled, the stack port is named Stack-Port1. After the stacking function is enabled, the stack port is named Stack-Port*n*/1, where *n* is the stack member ID of the switch.

2.2 Stack Connection Modes

Links in a stack fall into two types: management links and forwarding links. Management links are used to forward management packets of the stack, and forwarding links are used to forward service packets between stack member switches. Stack member switches can be connected in two modes: main processing unit (MPU) connection and line processing unit (LPU) connection, distinguished by the connections of management links. Figure 2-2 shows the two stack connection modes.

Figure 2-2 Stack connection modes



- In MPU connection mode, management links and forwarding links are separated. Management links are connected through the system inter-connect ports (SIPs) on MPUs, and forwarding links are connected through ports on LPUs.

  For details on how to connect the SIP ports and service ports, see SIP Port Connections and Service Port Connections.
- In LPU connection mode, management links and forwarding links are integrated and both connected through ports on LPUs. SIP ports on the MPUs are not connected.

Table 2-1 describes the comparisons between the two connection modes.

Table 2-1 Comparisons between the two connection modes

Characteristics	MPU Connection	LPU Connection
Relationship between management links and forwarding links	Management links and forwarding links are separated from each other and do not affect each other.	Management links and forwarding links are integrated and will affect each other.
Whether management packets occupy bandwidth	No	Yes
System complexity	Low	High
Delay in communication between stack member switches	Short	Long
Number of potential failure points on the stack management channel	Few	Many

Characteristics	MPU Connection	LPU Connection
Whether additional cables need to be deployed	Yes	No
Reliability	**High**	**Low**

You are advised to preferentially use the MPU connection mode. This mode separates management links from forwarding links, ensuring high reliability of the stack system.

SIP Port Connections

SIP ports are located on MPUs. Each MPU has two SIP ports, as shown in Figure 2-3. A SIP port is a combo port consisting of a GE electrical port and a GE optical port. It starts to work immediately after a cable is connected and does not require any configuration. By default, the working mode of a combo port depends on whether the electrical port or optical port has a cable connected first. If the electrical and optical ports are connected at the same time, the combo port works as an optical port.

NOTE

After a copper module that does not have a cable connected is installed in the optical port of a SIP port on a CE12800S MPU, the optical port becomes Down and will not change into an electrical port. You need to remove the copper module so that the electrical port can become Up.

Figure 2-3 SIP ports on an MPU

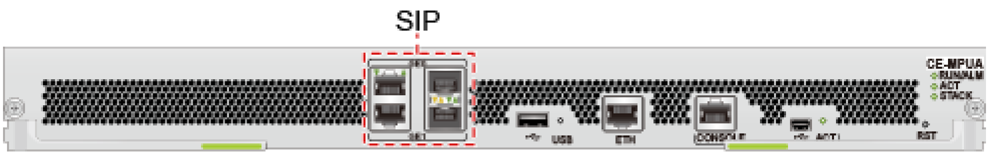
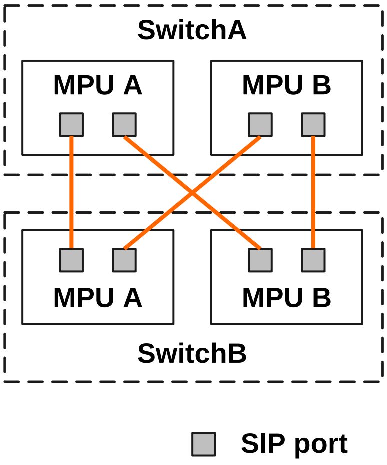


Figure 2-4 shows the recommended SIP port connections when each stack member switch has two MPUs.

Figure 2-4 SIP port connections



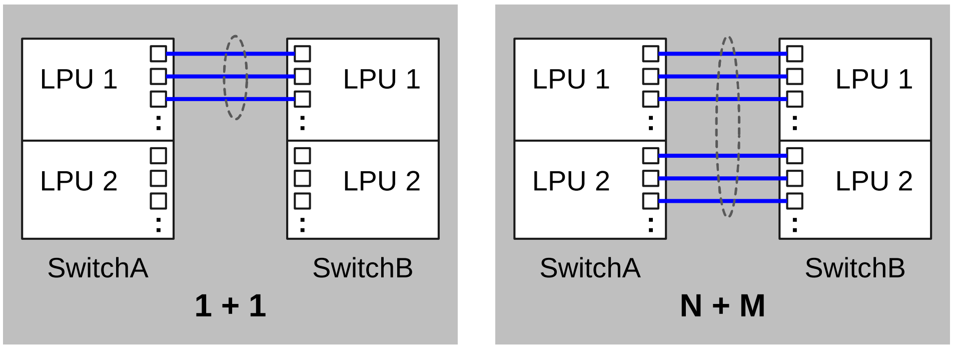
NOTE

- Each switch must have at least one SIP port connected.
- A SIP port on one switch can only be connected to a SIP port on the other switch, and cannot be connected to other SIP ports on the same switch.

Service Port Connections

A logical stack port can contain physical member ports on the same LPU or different LPUs. A maximum of 32 physical member ports can be added to a stack port to improve stack link bandwidth and reliability. Two networking modes are available according to the distribution of member ports, as shown in Figure 2-5.

Figure 2-5 Service port connections



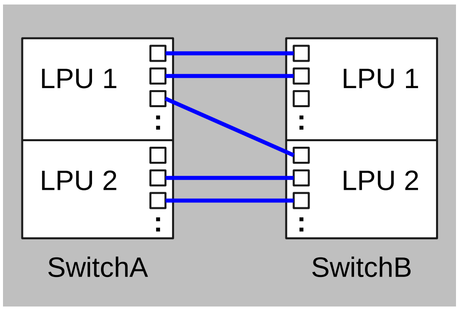
- 1+1 networking: Physical member ports are located on one LPU. Connect the two LPUs of the two switches to form a stack.
- N+M networking (N ≥ 2, M ≥ 2): Physical member ports are located on multiple LPUs, and stack links of different LPUs back up each other.

NOTE

The N+M networking is more reliable and is recommended.

In N+M networking, physical member ports on an LPU of the local switch can be connected to multiple LPUs of the peer switch. That is, the cross connection mode is supported, as shown in Figure 2-6.

Figure 2-6 Cross connection mode



NOTE

Local physical member ports cannot connect to remote common service ports. Otherwise, traffic forwarding may fail or the device restarts unexpectedly. Ports on both ends must be configured as physical member ports or service ports simultaneously.

2.3 Stack Setup

After two switches are connected using stack cables and configured with required stack parameters, they can set up a stack.

Role Election

After a stack is set up, member switches exchange stack competition packets to elect a master switch. The switch that wins the competition becomes the master switch and manages the entire stack. The other switch becomes the standby switch and works as a backup of the master switch.

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):

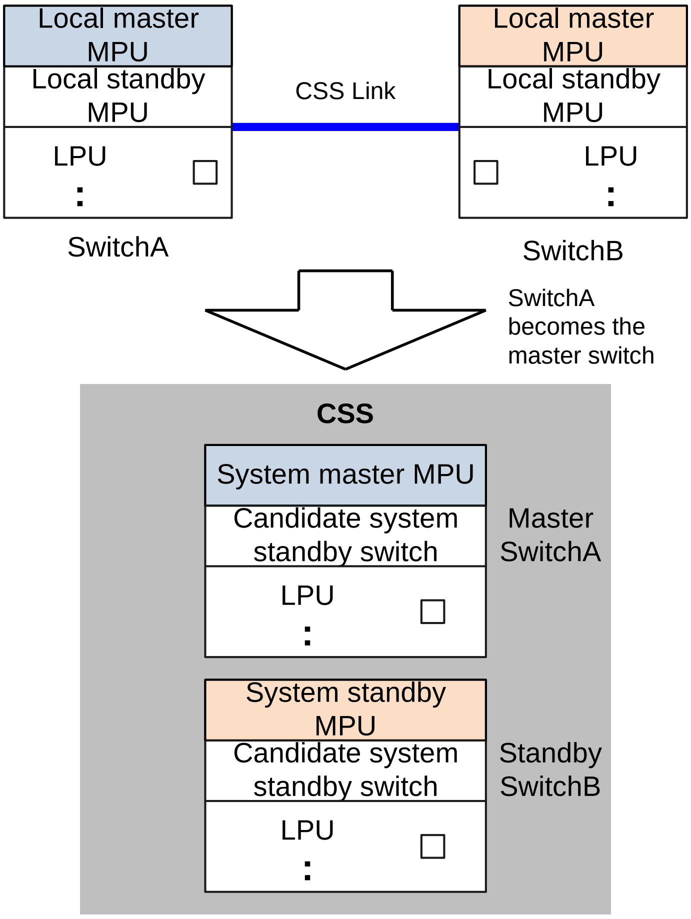
1. Running status: The switch that completes startup and enters stack running state first becomes the master switch.
2. Stack priority: The switch with a higher stack priority becomes the master switch.
3. Software version: The switch running a later software version becomes the master switch.
4. Number of main processing units (MPUs): The switch with two MPUs is preferred over the switch with only one MPU.
5. Bridge MAC address: The switch with the smallest bridge MAC address becomes the master switch.

   During the delivery of a device, 256 MAC addresses are allocated to the device, among which the smallest MAC address becomes the bridge MAC address. On a standalone device, the bridge MAC address of the device is the system MAC address. In a stack, the bridge MAC address of a member switch is the system MAC address. By default, the bridge MAC address of the master switch is the system MAC address.

If the master and standby switches have the same stack member ID, the master switch assigns a new stack member ID to the standby switch. Then the standby switch restarts and rejoins the stack.

After a stack is set up, the master MPU of the master switch works as the system master MPU to manage the entire stack. The master MPU of the standby switch works as the system standby MPU. The standby MPUs of the master and standby switches work as candidate system standby MPUs. Figure 2-7 shows the role election result after a stack is set up. In this example, SwitchA is elected as the master switch.

Figure 2-7 Role election in a stack



Software Version Synchronization

A stack supports software version synchronization between 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 other. If the software version running on the standby switch is different from that on the master switch, the standby 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 setting up a stack, member switches first start with their own configuration files. After they complete the startup process, the standby switch combines its stack configuration with the configuration file of the master switch. This configuration file is then used as the configuration file of the stack.
- When the stack is running normally, the master switch manages the entire stack, and synchronizes configurations made by users to the standby switch in real time to maintain configuration consistency between them.

Real-time configuration file synchronization ensures that both member switches in a stack maintain the same configuration. When the master switch fails, the standby switch can provide the same functions using the same configuration.

Configuration Combination and Conflict Detection

Configuration Combination

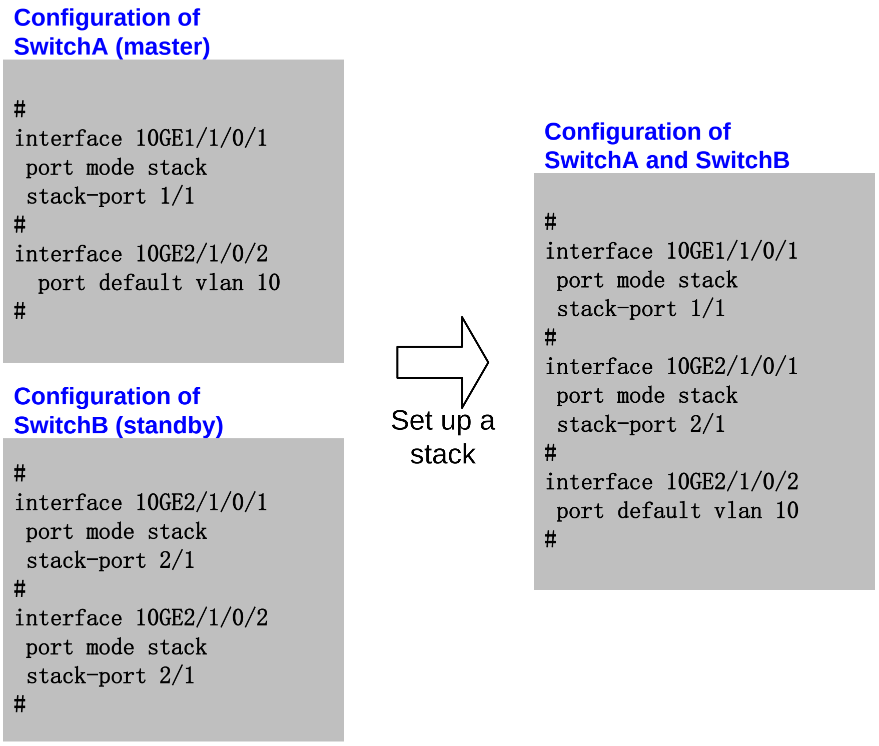
Stack configuration on a switch is saved in the configuration file. When a stack is set up, the standby switch combines its own stack configuration with that of the master switch. The configuration combination rules are as follows:

- The standby switch combines its stack configuration 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 configuration of the standby switch, the stack configuration of the master switch takes effect.

  As shown in Figure 2-8, SwitchA and SwitchB in a stack combine their port configurations. Port 10GE2/1/0/2 on SwitchA has common service configuration, which conflicts with the configuration on SwitchB. SwitchA is the master switch, so the port configuration on SwitchA takes effect.
- After a stack is set up, the standby switch synchronizes its configuration file with that of the master switch to maintain the same configuration with the master switch.

  As shown in Figure 2-8, SwitchB synchronizes its configuration file with that of SwitchA after the stack is set up.

Figure 2-8 Port configuration combination



Configuration of SwitchA (master)

```
#
interface 10GE1/1/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE2/1/0/2
  port default vlan 10
#
```

Configuration of SwitchB (standby)

```
#
interface 10GE2/1/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/1/0/2
 port mode stack
 stack-port 2/1
#
```

Configuration of SwitchA and SwitchB

```
#
interface 10GE1/1/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE2/1/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/1/0/2
 port default vlan 10
#
```

Configuration Conflict Detection

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

- In MPU connection mode:
  - All SIP ports on the standby switch are disabled using the **shutdown** command on the master switch.
- In line processing unit (LPU) connection mode:
  - 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 configured on the standby switch are disabled using the **shutdown** command on the master switch or conflict with the configuration on the master switch.
  - Stack ports of the standby 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.

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

Configuration File Backup

When the stacking function is enabled or disabled on a switch, the switch automatically backs up its configuration file. In this way, the switch can restore the original configuration after the stacking function is disabled or enabled. The backup configuration file is saved in flash:/, and the file name contains the original configuration file name and the time when the file is saved (in the yyyymmddhhmmss format). For example, if the original configuration file is **vrpcfg.cfg** and you enable the stacking function at 11:17:16 on 2012-12-11, the backup configuration file is named **vrpcfg20121211111716.cfg**.

2.4 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.

2.4.1 Member Switch Management

Member switches in a stack are managed on a per-chassis 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, before the stacking function is enabled on a switch, you can run **display device slot 1** to view information about the card in slot 1. After the stacking function is enabled, you need to run **display device slot 2/1** to view information about this card. Here, **2** is the stack member ID of the switch.

In a stack, interface numbers contain stack member IDs. Before the stacking function is enabled, interface numbers are in the *slot ID/subcard ID/port number* format. After the stacking function is enabled, the format of interface numbers changes to *stack member ID/slot ID/subcard ID/port number*. For example, an interface on a switch is numbered 10GE1/0/1 before the stacking function is enabled. After the switch joins a stack and is assigned stack member ID 2, the interface number changes to 10GE2/1/0/1.

2.4.2 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.

2.4.3 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 master MPU.
  - **slave#flash**: indicates the root directory of the flash storage on the standby MPU.
- In a stack:
  - **flash**: indicates the root directory of the flash storage on the system master MPU.
  - **Stack member ID/slot ID#flash**: indicates the root directory of the flash storage on the system standby MPU or a candidate standby MPU. For example, **1/6#flash** indicates the root directory of the flash storage on the MPU in slot 6 of the switch with stack member ID 1.

For more information about the file system, see section "File System Overview" in the *CloudEngine 12800 Series Switches Configuration Guide - Basic Configurations*.

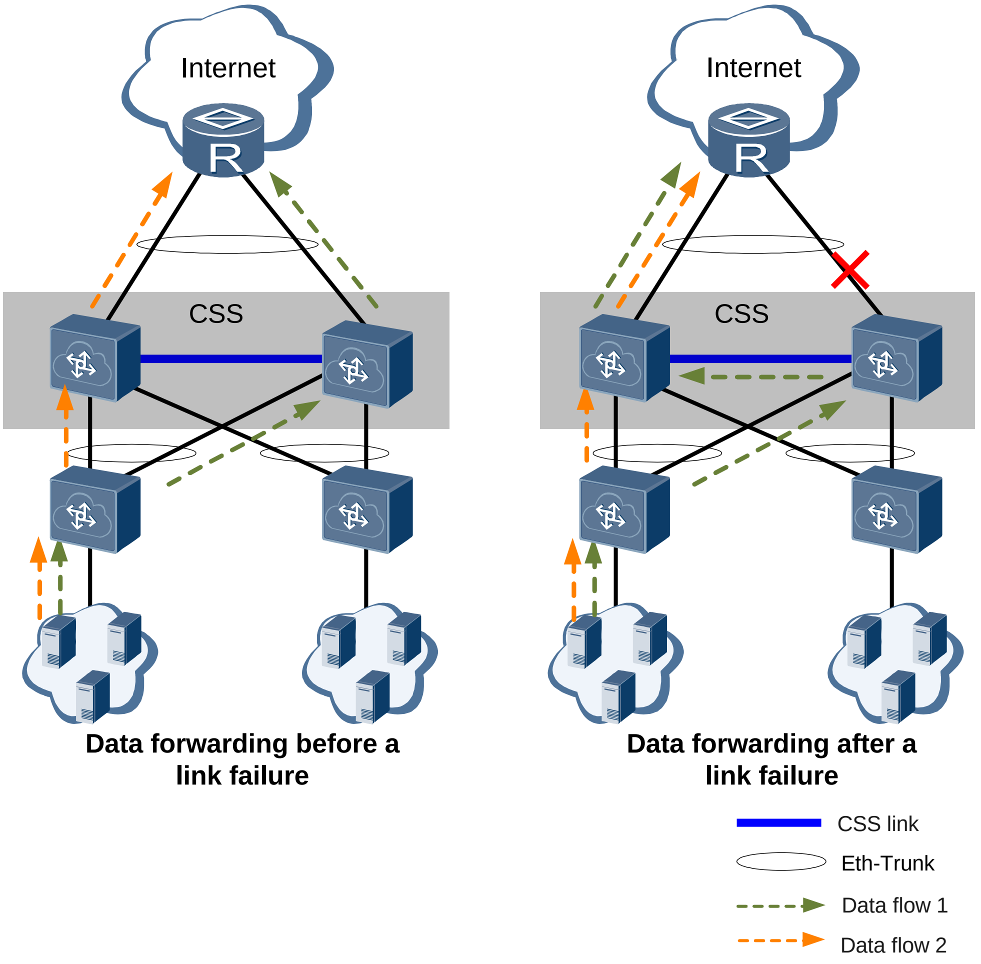
2.5 Inter-Device Link Aggregation and Local Preferential Forwarding

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.

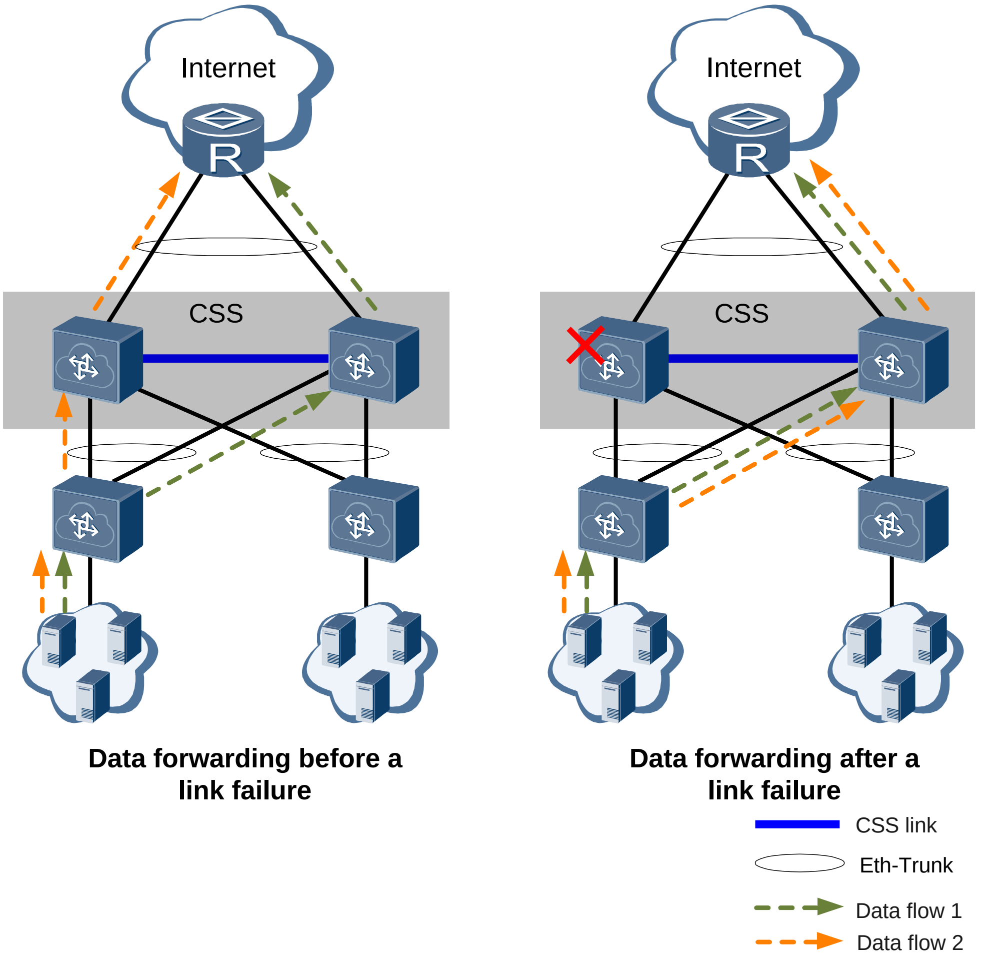
As shown in Figure 2-9, traffic sent to the core device on the network is equally distributed to member links of an Eth-Trunk set up between the stack member switches. When an Eth-Trunk member link fails, traffic on this link is distributed to the other link. This link backup mechanism improves network reliability.

Figure 2-9 Link backup through inter-device link aggregation


Internet
R
CSS
Data forwarding before a link failure
Internet
R
CSS
Data forwarding after a link failure
CSS link
Eth-Trunk
Data flow 1
Data flow 2

As shown in Figure 2-10, 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 2-10 Device backup through inter-device link aggregation


Internet
R
CSS
Internet
R
CSS
Data forwarding before a link failure
Data forwarding after a link failure
CSS link
Eth-Trunk
Data flow 1
Data flow 2

Local Preferential Forwarding

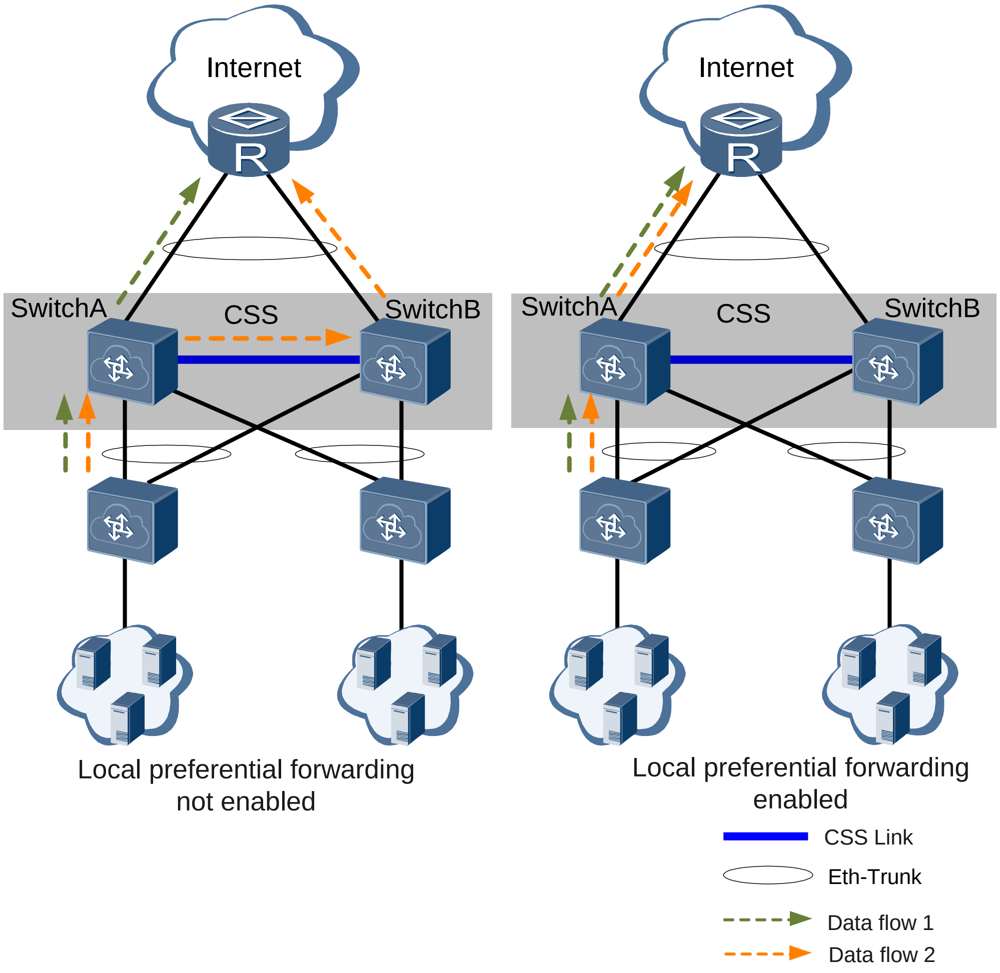
When an inter-device Eth-Trunk is configured in a stack, the stack uses the hash algorithm to select outbound interfaces in the Eth-Trunk. Therefore, traffic received on a member switch may be forwarded through the other member switch. Inter-device forwarding consumes bandwidth on stack links. As bandwidth 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 2-11, 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 2-11 Local preferential forwarding

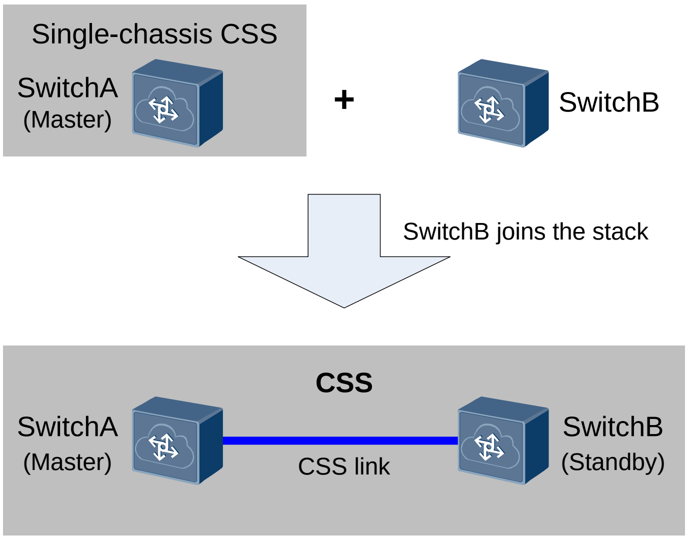


2.6 New Member Joining and Stack Merging

Joining of a Member Switch

A new member switch can join a running single-chassis stack (a standalone switch running the stacking function). As shown in Figure 2-12, SwitchA is a single-chassis stack. After SwitchB joins the stack, the two switches set up a new stack. Then SwitchA becomes the master switch, and SwitchB becomes the standby switch.

Figure 2-12 New member switch joins a single-chassis stack



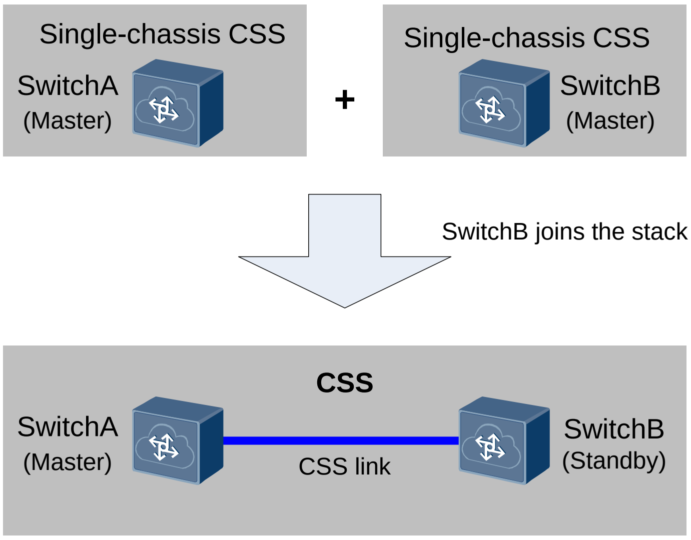
A new member switch joins a single-chassis stack in either of the following situations:

- After two switches are connected using stack cables, one switch is configured with the stacking function and restarted. This switch enters the single-chassis stack state. After the other switch is configured with the stacking function and restarted, it joins the stack as the standby switch.
- In a running two-chassis stack, one switch restarts. Then this switch rejoins the stack as the standby switch.

Stack Merging

Two stacks in the running state can merge into one stack. As shown in Figure 2-13, two single-chassis stacks merge into one and elect a master switch (following the same master election rules used in a stack). The master switch retains its original configuration, and its services are not affected. The standby switch restarts, joins the new stack as the standby switch, and synchronizes the configuration file with the master switch. Original services on this switch are interrupted.

Figure 2-13 Two stacks merge



Stack merging occurs in either of the following situations:

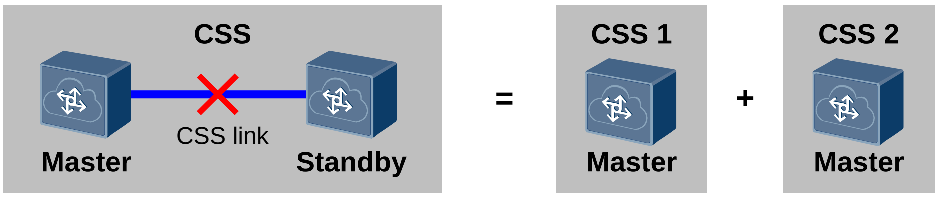
- After two switches are configured with the stacking function and restarted, they run as single-chassis stacks. After they are connected using stack cables, they merge into one stack.
- A stack splits due to a failure of a stack link or member switch. When the link or switch recovers, the two single-chassis stacks merge into one.

2.7 Stack Split and Dual-Active Detection

Stack Split

After a stack is set up, the master and standby switches periodically send heartbeat packets to maintain the stack state. If communication between the two switches is interrupted due to failures of stack cables or MPUs or power failure or restart of a switch, the stack splits into two standalone switches, as shown in Figure 2-14.

Figure 2-14 Stack split



After a stack splits, the two switches use the same global configuration if they are running normally. In this case, the two switches use the same IP address and MAC address to communicate with other network devices. The address conflict causes a communication failure on the entire network. Dual-active detection (DAD) can be configured to ensure that only one master switch exists after the stack splits.

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.

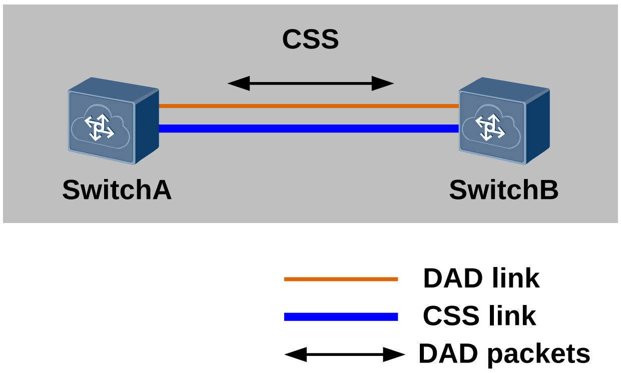
DAD Detection Modes

DAD can be implemented in the following modes:

- **Direct mode through service ports**

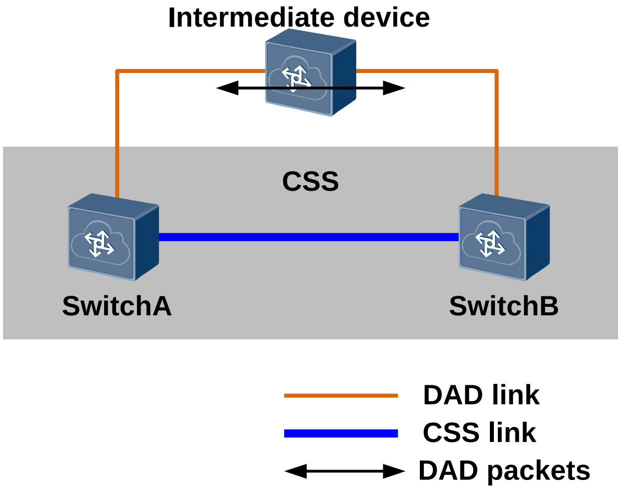
  In this mode, DAD is performed through dedicated direct links between member switches, as shown in Figure 2-15.

Figure 2-15 DAD in direct mode



The direct detection links can also be connected through an intermediate device, as shown in Figure 2-16. 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 12800 Series Switches Configuration Guide - Ethernet Switching*.

Figure 2-16 DAD through direct links to an intermediate device



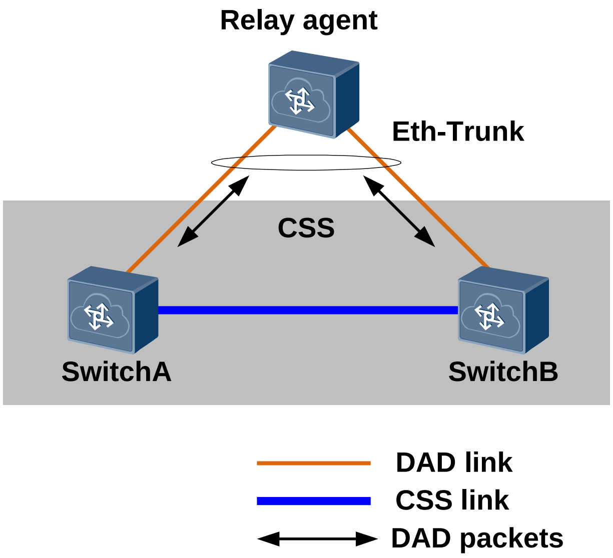
- **Proxy mode through Eth-Trunk interfaces**

  In this mode, DAD detection is performed through an inter-device Eth-Trunk link connected to a relay agent, as shown in Figure 2-17. 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

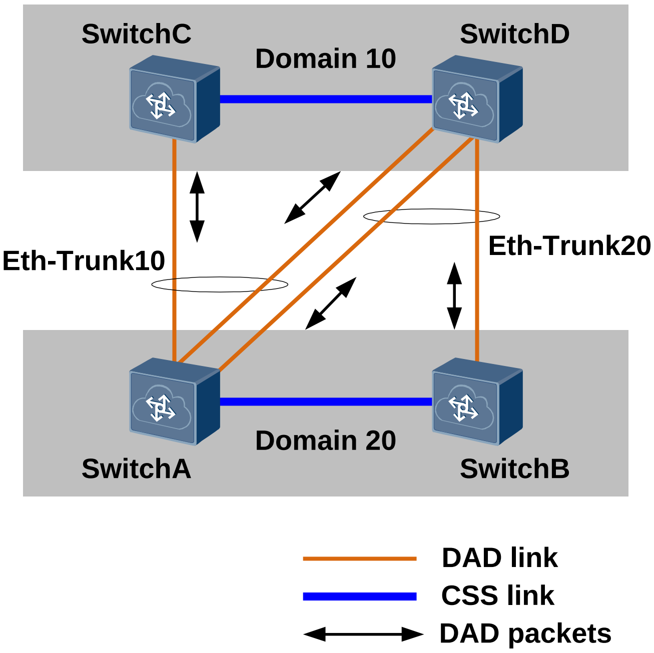
To enable DAD packets to be forwarded over Eth-Trunk member links, use a switch that supports the DAD proxy function as the relay agent. All Huawei CloudEngine series switches support the DAD proxy function. Huawei S series switches support this function since V200R002.

Figure 2-17 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 2-18.

Figure 2-18 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.

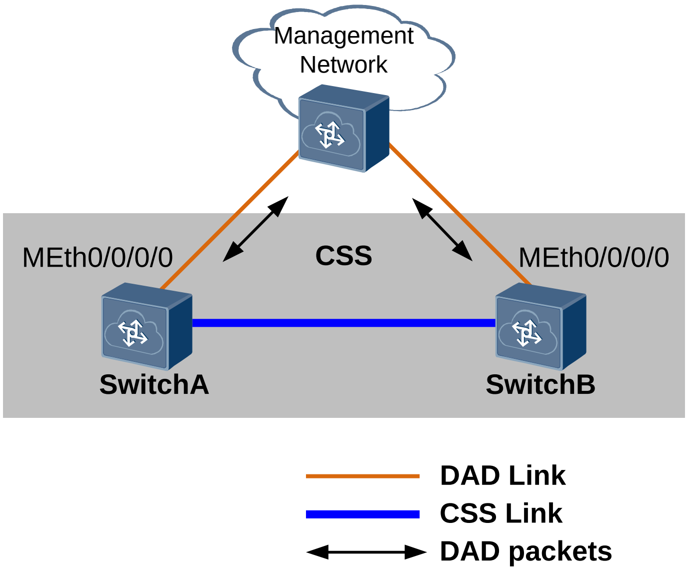
- **DAD through management interfaces**

  In this mode, links established on management interfaces of the stack member switches are used as DAD links, as shown in Figure 2-19. 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

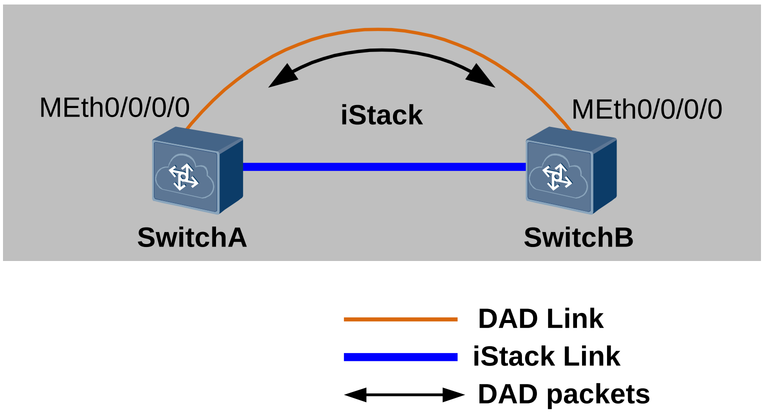
To implement DAD through management interfaces, ensure that IP addresses are configured for management interfaces.

Figure 2-19 DAD through management interfaces



As shown in Figure 2-20, 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 2-20 DAD through directly connected management interfaces



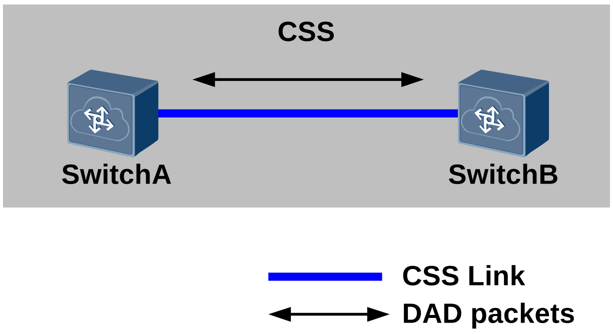
- **DAD through physical stack member ports**

  In this mode, links established between physical stack member ports of the stack member switches are used as DAD links, as shown in Figure 2-21. This mode uses stack links as DAD links and do not occupy additional ports.

📖 **NOTE**

This mode can be used only when the stack is set up through MPU connection.

Figure 2-21 DAD through physical stack member ports



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

Many factors can cause master/standby switchovers in a stack. This section describes the master/standby switchovers triggered by MPU failures or commands.

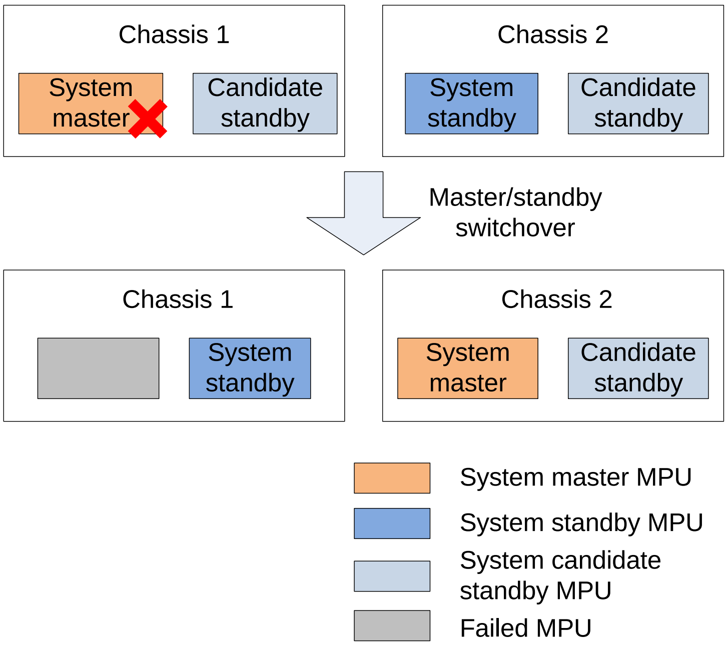
Master/Standby Switchover Triggered by an MPU Failure

Roles in a stack may change if an MPU in the stack fails.

- The system master MPU fails.

  Figure 2-22 shows the changes of roles in a stack after the system master MPU fails.

Figure 2-22 Changes of roles after a failure of the system master MPU

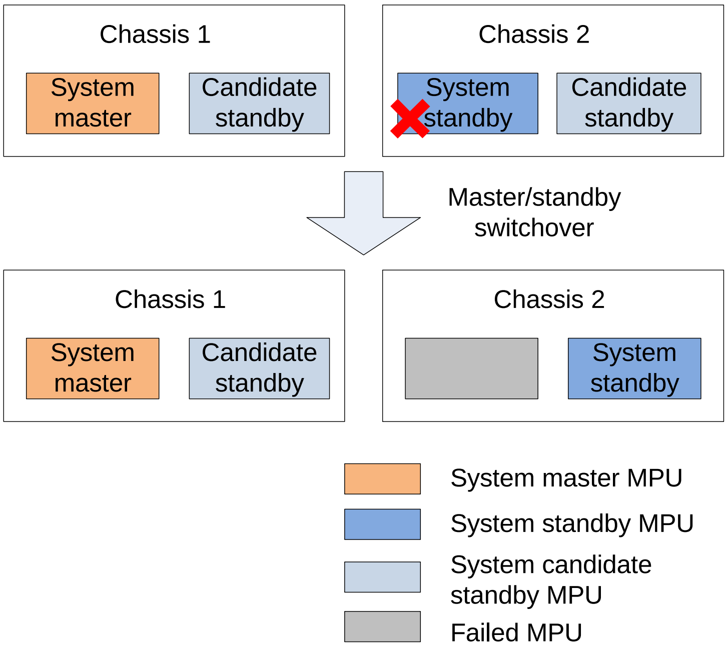


- The original standby switch becomes the master switch, and the original system standby MPU becomes the system master MPU.
- The original master switch becomes the standby switch.
- The standby MPU of the original master switch becomes the system standby MPU and synchronizes data with the system master MPU.

- The system standby MPU fails.

  Figure 2-23 shows the changes of roles in a stack after the system standby MPU fails.

Figure 2-23 Changes of roles after a failure of the system standby MPU



- The master and standby switches retain their roles.
- The standby MPU of the standby switch becomes the system standby MPU and synchronizes data with the system master MPU.

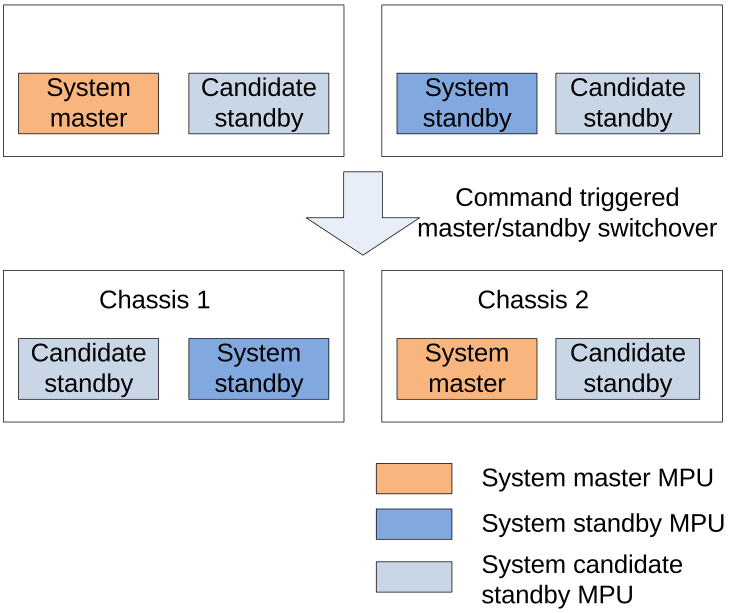
- A system candidate standby MPU fails.

  Failures of candidate standby MPUs do not cause any change of roles in the stack.

Master/Standby Switchover Triggered by Commands

Figure 2-24 shows the changes of roles in a stack after a master/standby switchover is triggered by a command.

Figure 2-24 Changes of roles after a command-triggered master/standby switchover



- The original standby switch becomes the master switch, and the original system standby MPU becomes the system master MPU.
- The original system master MPU becomes a candidate system standby MPU, and the original master switch becomes the standby switch.
- The standby MPU of the original master switch becomes the system standby MPU and synchronizes data with the system master MPU.

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:

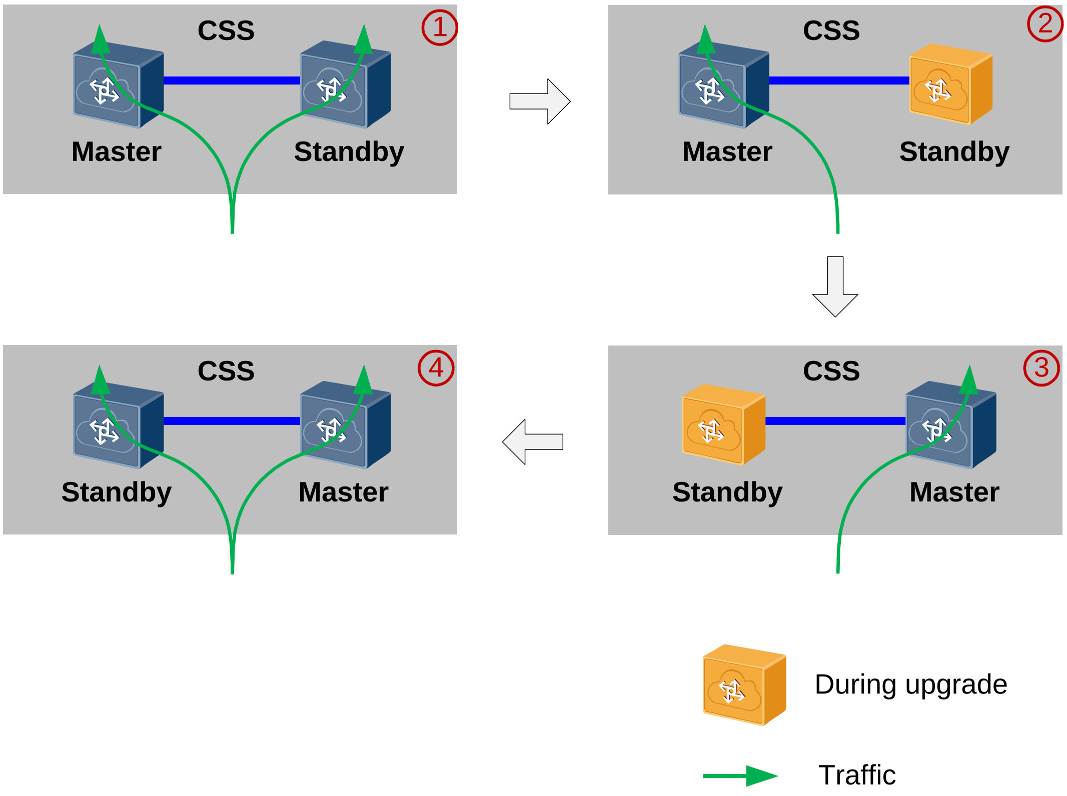
- Traditional upgrade method: You need to specify next-startup files and restart the entire stack. This method causes service interruption in a long time and is therefore not applicable to scenarios requiring short service interruption time.
- Fast upgrade: This upgrade method provides a mechanism to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

NOTE

- 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 the current stack connection mode is different from the stack connection mode for the next startup, the stack fast upgrade cannot be performed. Otherwise, a version rollback occurs.
- During the fast upgrade of a stack, the SFU reset due to heartbeat loss is a normal situation and does not affect services.
- 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 2-25 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 2-25 Traffic forwarding during a fast upgrade



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

NOTE

In LPU connection mode, a device may restart multiple times during the rollback in a fast upgrade.

- ISSU upgrade: The ISSU function completes an upgrade through a card or process switchover. This upgrade method ensures higher reliability and shorter service interruption time. For more information about ISSU upgrade, see ISSU Configuration in the *CloudEngine 12800 Series Switches Configuration Guide - Basic Configurations*.

3 Applications

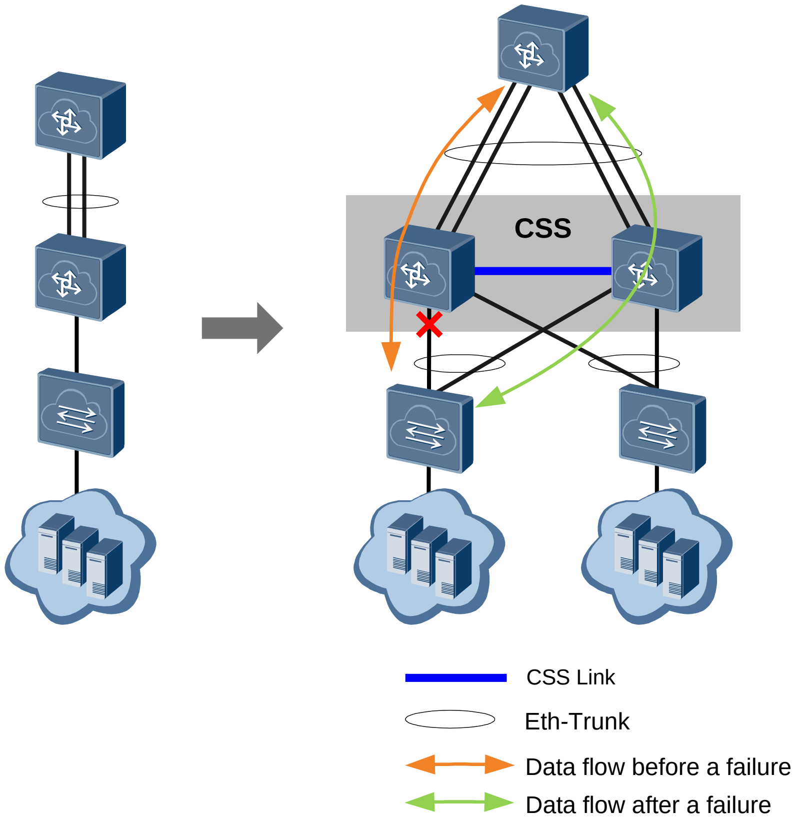
This section describes stack application scenarios.

Bandwidth Expansion and Inter-Device Link Redundancy

As shown in Figure 3-1, when the network expands and higher uplink bandwidth is required, you can connect a new switch to the original one using stack cables so that the two switches can set up a stack. Then bundle physical links of the member switches into a link aggregation group to increase the uplink bandwidth.

Downstream switches connect to the stack through inter-device Eth-Trunk links. This networking implements redundancy between devices and links, enhancing network reliability.

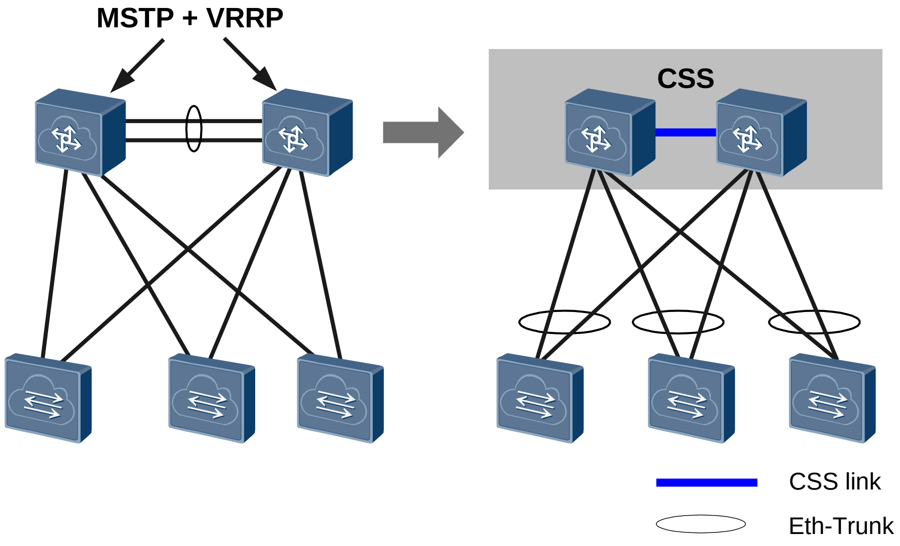
Figure 3-1 Bandwidth expansion and inter-device link redundancy



Simplifying Network Topology

As shown in Figure 3-2, two switches are virtualized into a logical switch. This simplified network does not require Multiple Spanning Tree Protocol (MSTP) or Virtual Router Redundancy Protocol (VRRP), so network configuration is much simpler. Inter-device link aggregation also speeds up network convergence and improves network reliability.

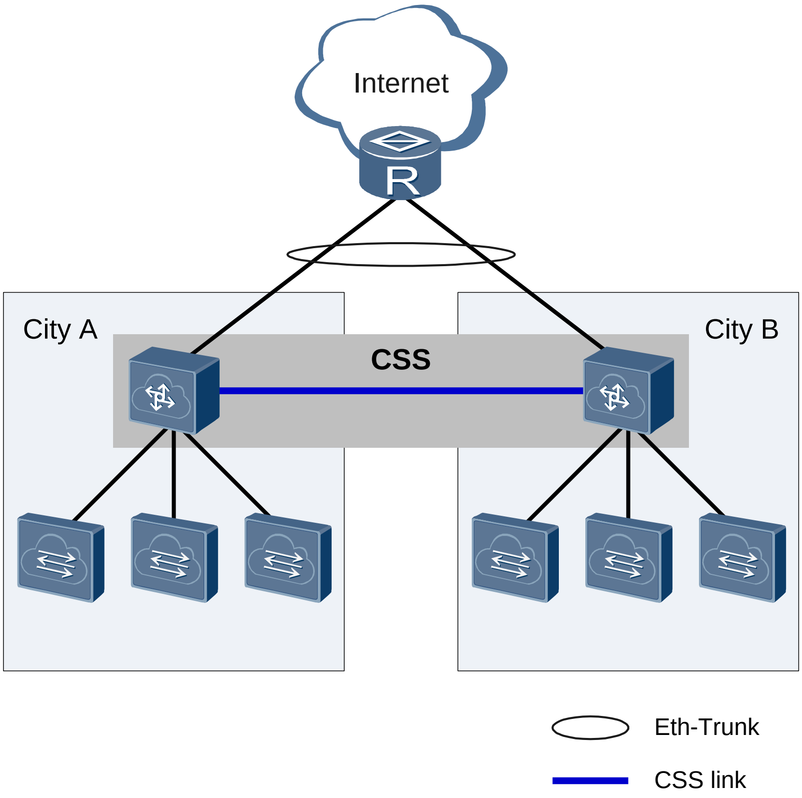
Figure 3-2 Simplifying network topology



Long-Distance Stacking

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

Figure 3-3 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

Item	Requirement	Remarks
Switch model	• CE12804, CE12808, CE12812, CE12816 • CE12804S, CE12808S	• CE12800 switches of different models can set up a stack. For example, a CE12804 switch and a CE12808 can set up a stack. • CE12800S switches of different models can set up a stack. For example, a CE12804S switch and a CE12808S can set up a stack. • CE12800 and CE12800S switches cannot set up a stack.
Number of member switches	2	-
Number of MPUs in each switch	At least one MPU in each switch	It is recommended that you install two MPUs in each switch to improve system reliability.
Type of ports used for stack connection	• 10GE optical ports • 10GE electrical ports • 40GE optical ports	• 10GE optical ports can be used for stack connection only when they have 10GE optical

Item	Requirement	Remarks
	- 100GE optical ports 10GE electrical ports can be used for stack connection in V100R005C00 and later versions.	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 can be used for stack connection. If 40GE optical ports have been configured as the stack physical member ports, they cannot be split. - In V100R003C00 and V100R003C10, 10GE optical ports derived from 100GE optical ports cannot be used for stack connection. In V100R005C00 and later versions, 10GE or 40GE optical ports derived from 100GE optical ports can be used for stack connection.
Number of physical member ports in a stack port	1-32	- 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 and 10GE electrical ports can be added to the same stack port. - It is recommended that you add at least two physical member ports to a stack port to improve stack link bandwidth and reliability.

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 active cables.	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.	-
10GE electrical port	-	-	-	10GE electrical ports use Category 6, Category 6A, or Category 7 cables that comply with IEEE 802.3an.
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.	-
100GE optical port	CXP to CXP high-speed cable CXP to CXP high-speed cables are available in lengths of 1.5 m and 3 m.	CXP to CXP AOC cable. CXP+ to CXP+ AOC cables are available in lengths of 10 m.	100GE CFP/CXP/CFP2 optical module The required optical fibers are determined by the optical modules you select.	-
SIP port	-	-	GE optical modules and	Ethernet cables.

Port Type	High-Speed Cable	AOC Cable	Optical Module	Network Cable
			LC optical fibers.	

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.
- You are advised to preferentially use the MPU connection mode. This mode separates management links from forwarding links, ensuring high reliability of the stack system.
- Before using cards with 40GE or 100GE ports to set up a stack, determine whether these ports need to be split. This is because splitting or merging ports will restart cards where the ports reside and subsequently affect the stack topology after a stack is set up.
- 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.
- Local physical member ports cannot connect to remote common service ports. Otherwise, traffic forwarding may fail or the device restarts unexpectedly. Ports on both ends must be configured as physical member ports or service ports simultaneously.
- When you change the system software for a stack that is set up in LPU connection mode and reboot the system, do not close the terminal window before the **reboot** command execution is complete. Otherwise, the standby switch in the stack will restart repeatedly.
- Ports on the board CE-FWA/CE-IPSA cannot be used to set up a stack.

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 system, the observing and mirrored ports in traffic mirroring can be configured on different chassis. In V100R003C00 and earlier versions, the observing and mirrored ports in port mirroring must be configured on the same chassis. In V100R003C10 and later versions, the observing and mirrored ports in port mirroring can be configured on different chassis. Packets mirrored from one chassis to the other may be changed or discarded. Therefore, you are not advised to configure the observing and mirrored ports on different chassis.
Port split	If a 100GE or 40GE optical port has been configured as a physical member port, it cannot be split.
Super virtual fabric (SVF)	SVF and cluster switch system (CSS) conflict and cannot be configured together.

5 Default Configuration

This section provides default settings of stack parameters.

Table 5-1 Default stack configuration

Parameter	Default Setting
Stacking function	Disabled
Stack connection mode	MPU connection
Stack member ID	1
Domain ID	No default value
Stack priority	100

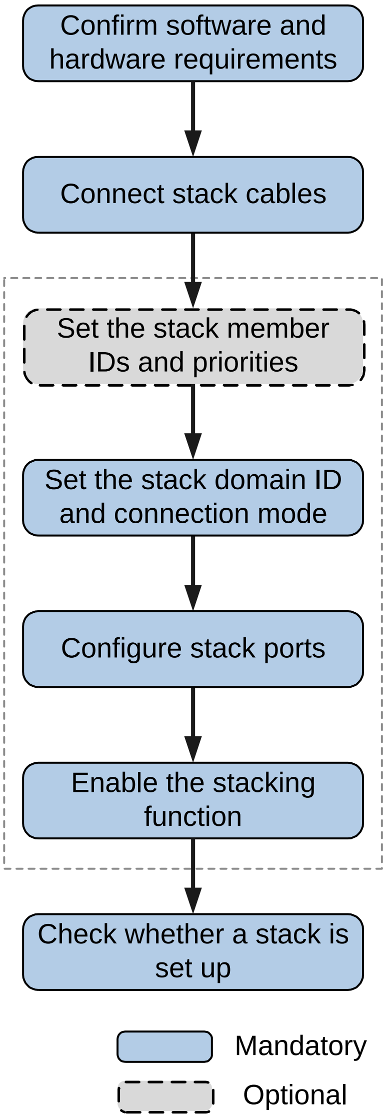
6 Establishing a Stack

About This Chapter

This section describes how to establish a stack.

Figure 6-1 shows the procedure for establishing 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 member switches using cables and complete software configuration.

Figure 6-1 Procedure for establishing a stack


Confirm software and hardware requirements
Connect stack cables
Set the stack member IDs and priorities
Set the stack domain ID and connection mode
Configure stack ports
Enable the stacking function
Check whether a stack is set up
Mandatory
Optional

6.1 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

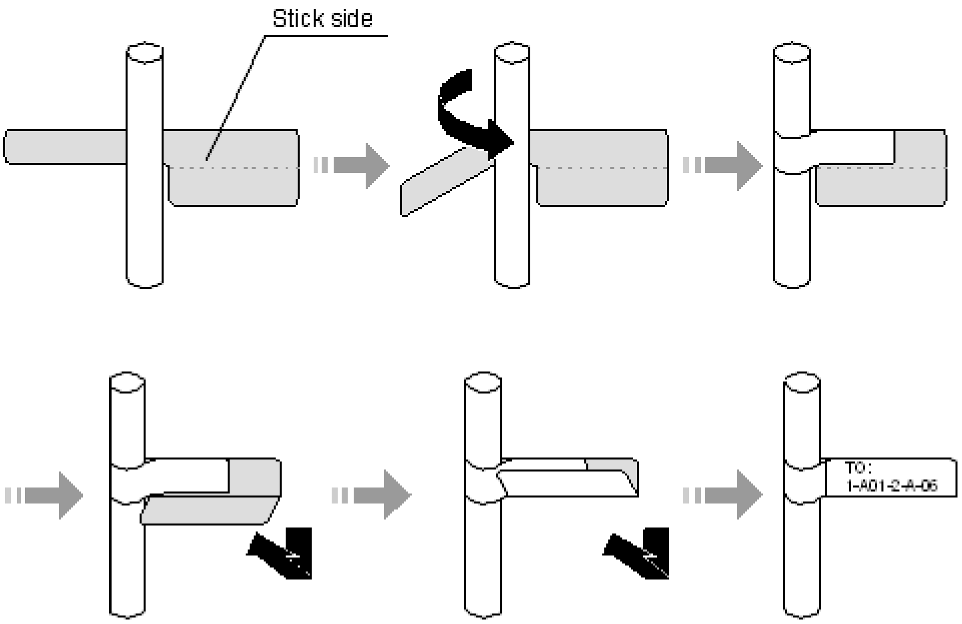
When installing or removing optical fibers, do not look into optical ports or connectors without eye protection.

- 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.

Installation 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.
   - **System interconnect port (SIP) connection rules**

NOTE

If you use the LPU connection mode, you do not need to connect the SIP ports.

SIP ports are located on MPUs. Each MPU has two SIP ports, as shown in Figure 6-3. A SIP port is a combo port consisting of a GE electrical port and a GE optical port. It starts to work immediately after a cable is connected and does not require any configuration. By default, the working mode of a combo port depends on whether the electrical port or optical port has a cable connected first. If the electrical and optical ports are connected at the same time, the combo port works as an optical port.

NOTE

After a copper module that does not have a cable connected is installed in the optical port of a SIP port on a CE12800S MPU, the optical port becomes Down and will not change into an electrical port. You need to remove the copper module so that the electrical port can become Up.

Figure 6-3 SIP ports on an MPU

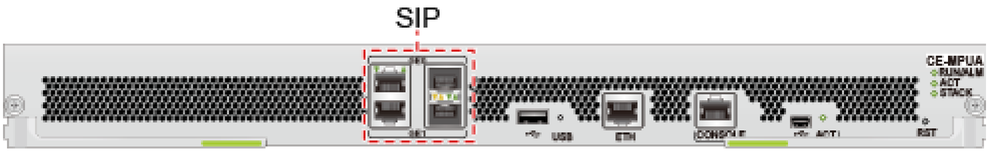
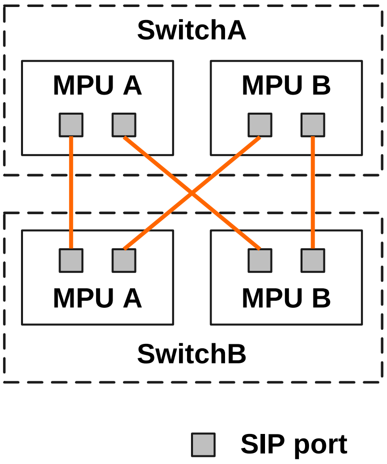


Figure 6-4 shows the recommended SIP port connections when each stack member switch has two MPUs.

Figure 6-4 SIP port connections



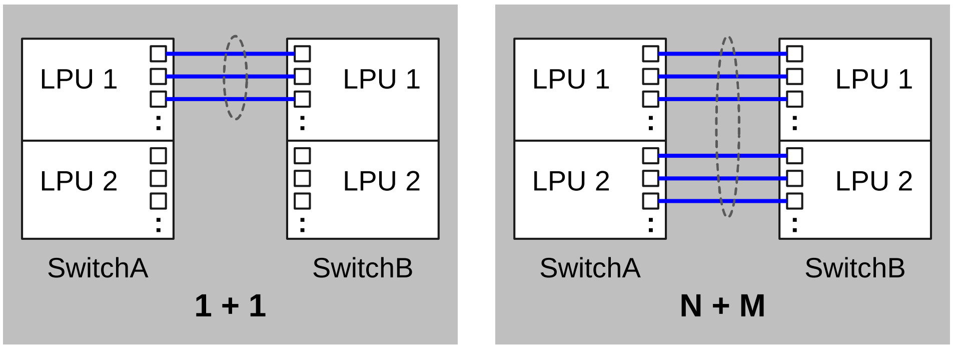
NOTE

- Each switch must have at least one SIP port connected.
- A SIP port on one switch can only be connected to a SIP port on the other switch, and cannot be connected to other SIP ports on the same switch.

– **Service port connection rules**

A logical stack port can contain physical member ports on the same LPU or different LPUs. A maximum of 32 physical member ports can be added to a stack port to improve stack link bandwidth and reliability. Two networking modes are available according to the distribution of member ports, as shown in Figure 6-5.

Figure 6-5 Service port connections



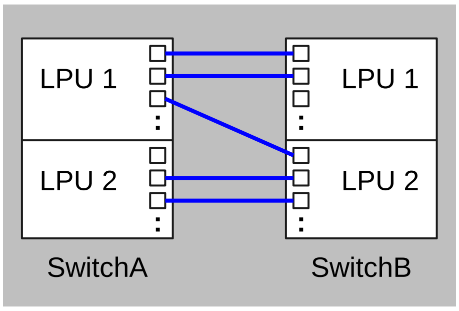
- 1+1 networking: Physical member ports are located on one LPU. Connect the two LPUs of the two switches to form a stack.
- N+M networking (N ≥ 2, M ≥ 2): Physical member ports are located on multiple LPUs, and stack links of different LPUs back up each other.

NOTE

The N+M networking is more reliable and is recommended.

In N+M networking, physical member ports on an LPU of the local switch can be connected to multiple LPUs of the peer switch. That is, the cross connection mode is supported, as shown in Figure 6-6.

Figure 6-6 Cross connection mode



NOTE

Local physical member ports cannot connect to remote common service ports. Otherwise, traffic forwarding may fail or the device restarts unexpectedly. Ports on both ends must be configured as physical member ports or service ports simultaneously.

6.2 Configuring Software

6.2.1 (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** *new-member-id* 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.

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

----End

6.2.2 (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 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

6.2.3 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 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

6.2.4 Configuring the Stack Connection Mode

Context

Stack member switches can be connected through MPU or LPU connection mode. The two connection modes differ in locations of stack management links:

- MPU connection mode: Stack management links are established on SIP ports of MPUs. This mode separates management links from forwarding links to improve system reliability.
- LPU connection mode: Stack management links are integrated with data forwarding links. This mode does not use SIP ports on MPUs and therefore simplifies network deployment and maintenance.

NOTE

- Stack member switches must use the same connection mode. Otherwise, they cannot set up a stack.
- You are advised to preferentially use the MPU connection mode. This mode separates management links from forwarding links, ensuring high reliability of the stack system.
- When setting up a stack in LPU connection mode, you are advised to install the same software version on two stack member switches to reduce the stack setup time.

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 link-type** { **mainboard-direct** | **linecard-direct** } command to specify the stack connection mode.

By default, the MPU connection mode is used. After changing the stack connection mode, restart the switch for the configuration to take effect.

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

----End

6.2.5 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 a maximum of 32 physical member ports.
- Disable physical ports before adding them to or deleting them from a stack port. After adding or deleting the physical ports, enable them.
- 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** *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 Disable the service ports that you want to add to the stack port.

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 **shutdown** command to disable the interface.
4. Run the **quit** command to return to the system view.
5. Run the **commit** command to commit the configuration.

Repeat the preceding operations to disable multiple service ports.

Step 3 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** *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** *port-id* command to add the physical port to the stack port.
4. Run the **commit** command to commit the configuration.

Step 4 Enable the physical member ports.

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 **undo shutdown** command to enable the interface.
4. Run the **quit** command to return to the system view.
5. Run the **commit** command to commit the configuration.

Repeat the preceding operations to enable the other physical member ports.

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

6.2.6 Enabling the Stacking Function

Context

Before enabling the stacking function on a switch, run the **display stack configuration** command to check the stack configuration. Enable the stacking function after you verify that the stack configuration is correct.

The switch restarts after you enable or disable the stacking function. Before the restart, the switch backs up the running configuration in flash:/ and names the backup configuration file by adding the file backup time (in the yyyymmddhhmmss format) to the original configuration file name. For example, if the original configuration file is **vrpcfg.cfg** and you enable the stacking function at 11:17:16 on 2012-12-11, the backup configuration file is named **vrpcfg20121211111716.cfg**.

After you disable the stacking function, the switch restarts without a configuration file.

NOTE

- It is recommended that you run the **save** command to save the configuration before enabling the stacking function.
- After the switch restarts and the stack is set up successfully, run the **save** command immediately to save the configuration.

Procedure

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

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

Step 3 Run the **stack** command to enter the stack management view.

Step 4 Run the **stack enable** command to enable the stacking function.

By default, the stacking function is disabled.

----End

6.3 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.

6.3.1 Observing Indicators to Check Whether a Stack Is Set Up

Background

After completing the stack configuration, you can observe indicators on the member switches to check stack state information, including the master/standby roles of the switches and stack link states.

Checking Whether Indicators Are in Normal States

If a stack is set up successfully, indicator states on the member switches are as follows:

- On one switch, the STACK indicator on an MPU is steady green. This switch is the master switch. On the other switch, the STACK indicators on both MPUs are blinking green. This switch is the standby switch.

  If both switches have a STACK indicator in steady green state, the two switches are running the stacking function but they fail to set up a stack.
- The LINK indicators of the SIP ports on the MPUs or service ports used for stack connection are steady green.

Table 6-1 describes the indicator states and meanings.

Table 6-1 Indicator description

Indicator Location	Indicator	Color	Description
MPU	ACT: active/standby status indicator	Green	• Steady on: The MPU is the active MPU of the local switch. • Off: The MPU is the standby MPU of the local switch.
	STACK: stack status indicator	Green	• Steady on: The stacking function is enabled, and the MPU is the system master MPU of the stack. • Blinking: The stacking function is enabled, and the MPU is not the system master MPU of the stack. • Off: The stacking function is not enabled.
	LINK: SIP port status indicator	Green	• Steady on: The link status of the SIP port is Up. • Off: The link status of the SIP port is Down.
LPU	LINK: port status indicator	Green	• Steady on: The link status of the SIP port is Up. • Off: The link status of the port is Down.

6.3.2 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 two member switches are displayed, the stack is set up successfully.

```
<HUAWEI> display stack
--------------------------------------------------------------------------------
MemberID Role     MAC            Priority  DeviceType        Description
--------------------------------------------------------------------------------
1        Master   006d-8835-2b00   150       CE12804
2        Standby  006d-8835-2c00   100       CE12804
--------------------------------------------------------------------------------
```

If only one member switch is displayed, the stack fails to be established. See Handling a Stack Setup Failure to handle the problem.

----End

Handling a Stack Setup Failure

1. Check the stack cable connections against the rules described in 6.1 Connecting Stack Cables. If the stack cable connections are incorrect, reconnect the stack cables according to the rules.
2. Check whether the physical ports (including SIP ports on MPUs and service ports on LPUs) with stack cables connected are Up. Check the SIP ports only when the MPU connection mode is used. Run the **display interface brief** command to check the port status.

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 all** command to check whether the current stack configuration meets the requirements for setting up a stack. If not, run some or all the following commands as required to modify the configuration, and then restart the switch.
   - Run the **stack member** { *member-id* | **all** } **domain** *domain-id* command in the stack management view to change the stack domain ID.
   - Run the **stack member** { *member-id* | **all** } **link-type** { **mainboard-direct** | **linecard-direct** } command in the stack management view to change the stack connection mode.
   - Run the **stack member** *member-id* **renumber** *new-member-id* [**inherit-config**] command in the stack management view to change the stack member ID.
   - Run the **stack member** { *member-id* | **all** } **priority** *priority-value* command in the stack management view to change the stack priority.
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.**

  In MPU connection mode, 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 1/1/0/1
10GE1/1/0/1 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.

- **Ports of a member switch are in Error-Down state.**

  In MPU connection mode, if there is no forwarding link between two member devices, service ports of one member device enter the Error-Down state.

  - If two member devices are not connected through the forwarding link when setting up a stack or the forwarding link has not been Up after a stack is set up, service ports on the standby switch enter the Error-Down state.
  - If the forwarding link changes from Up to Down, service ports on the member device with fewer LPUs enter the Error-Down state. If the two member devices have the same number of LPUs, service ports on the standby switch enter the Error-Down state.

  In the following example, a service port is in Error-Down state.

  ```
  <HUAWEI> display interface 10ge 1/1/0/1
  10GE1/1/0/1 current state : ERROR DOWN(no-stack-link-event) (ifindex: 12)
  Line protocol current state : DOWN
  ......
  ```

  After the link fault is rectified and the forwarding link becomes Up, the Error-Down fault is automatically rectified.

- **Service ports on a stack card are in Error-Down state.**

  In LPU connection mode, if a stack card has different resource modes (including TCAM resource mode, Eth-Trunk resource mode, Tunnel Mode, and ARP resource mode) than the configured resource modes during startup, all service ports except physical member ports on the stack card 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 1/1/0/1
  10GE1/1/0/1 current state : ERROR DOWN(resource-mismatch) (ifindex: 12)
  Line protocol current state : DOWN
  ......
  ```

  After service ports enter the Error-Down state, you can save the configuration and then restart the faulty card to recover the service ports.

- **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 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 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 1/1/0/1
  10GE1/1/0/1 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.

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, 7.1.4 Configuring DAD Through Stack Ports. 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 12800 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 1/1/0/1
10GE1/1/0/1 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 1/1/0/1
10GE1/1/0/1 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 0/0/0/0** 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 1/1/0/1
10GE1/1/0/1 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 Configuring DAD Through Stack Ports

Context

When the MPU connection mode is used, stack ports can be used for DAD. This detection mode uses stack links as DAD links and does not require additional ports.

NOTE

This mode can be used only when the stack is set up through MPU connection.

Procedure

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

Step 2 Run the **interface stack-port** *member-id*/*port-id* command to enter the stack port view.

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

By default, DAD is disabled on a stack port.

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 1/1/0/1
10GE1/1/0/1 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.

7.1.5 (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

7.1.6 (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 0/0/0/0** 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

7.1.7 (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

7.1.8 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 chassis** *chassis-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 chassis** *chassis-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 does not change. 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

7.5 Configuring Ports Excluded from Shutdown When a Stack Has No Forwarding Link

Context

In MPU connection mode, if there is no forwarding link between two member devices, service ports of one member device enter the error-down state.

- If two member devices are connected through the forwarding link when setting up a stack or the forwarding link has not been Up after a stack is set up, service ports on the standby switch enter the error-down state.
- If the forwarding link changes from Up to Down, service ports on the member device with fewer LPUs enter the error-down state. If the two member devices have the same number of LPUs, service ports on the standby switch enter the error-down state.

To retain services on some ports, configure these ports as ports excluded from shutdown. These ports then will not set to error-down state.

NOTE

Physical member ports cannot be configured as ports excluded from shutdown. Ports excluded from shutdown cannot be configured as physical member ports either.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
stack
```

The stack management view is displayed.

Step 3 Run:

```
no-stack-link exclude interface interface-type { interface-number1 [ to
interface-number2 ] } &<1-32>
```

Specified ports are configured as ports excluded from shutdown.

By default, no port is configured as a port excluded from shutdown.

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.

----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.

NOTE

Before performing a master/standby switchover, ensure that the master switch has two MPUs.

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	This upgrade method shortens service interruption time and can be used in scenarios sensitive to the service interruption time.

Upgrade Method	Upgrade Mechanism	Usage Scenario
	then the master switch.	
ISSU upgrade	An upgraded is completed through card or process switchovers. For more information about ISSU upgrade, see ISSU Configuration in the *CloudEngine 12800 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. - Each member switch must have two MPUs.

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 system master MPU. For details on how to upload the system software, see File Management in the *CloudEngine 12800 Series Switches Configuration Guide - Basic Configurations*.
2. Run the **copy** *source-filename destination-filename* **all** command to copy the system software to all the MPUs.

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

- 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 the current stack connection mode is different from the stack connection mode for the next startup, the stack fast upgrade cannot be performed. Otherwise, a version rollback occurs.
- During the fast upgrade of a stack, the SFU reset due to heartbeat loss is a normal situation and does not affect services.
- 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 12800 Series Switches Configuration Guide - Basic Configurations*.

----End

9 Splitting a Stack

If a stack is not required, split the stack to restore the member switches to standalone switches.

Context

To split a stack, disable the stacking function, and then remove the stack cables between the member switches. After you run the **undo stack enable** command, the member switches back up the running configuration file and restart. After the restart, the switches run without any configuration file. Log in to the switches through console ports on their MPUs to configure the switches.

The backup configuration file is saved in flash:/, and the file name contains the original configuration file name and the time when the file is saved (in the yyyymmddhhmmss format). For example, if the original configuration file is **vrpcfg.cfg** and you disable the stacking function at 11:17:16 on 2012-12-11, the backup configuration file is named **vrpcfg20121211111716.cfg**.

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 **undo stack enable member** { *member-id* | **all** } command to disable the stacking function.

After you disable the stacking function, the member switches restart without a configuration file.

Step 4 Remove stack cables.

----End

10 Configuration Examples

About This Chapter

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

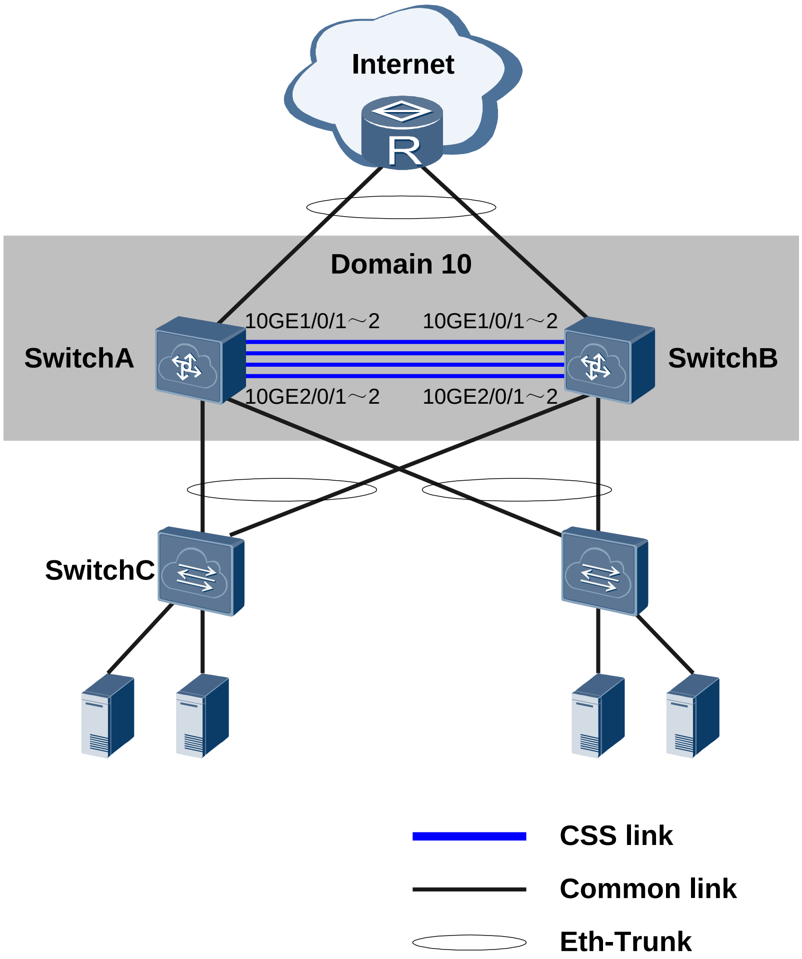
10.1 Example for Configuring a Stack

Networking Requirements

An enterprise builds a data center. The data center network must provide high reliability on the core layer and have a simple structure to facilitate configuration and management.

To meet requirements of the enterprise, core switches SwitchA and SwitchB set up a stack. Ports 10GE1/0/1 to 10GE1/0/2 and 10GE2/0/1 to 10GE2/0/2 of the two switches need to be connected using stack cables and added to stack ports. Figure 10-1 shows the network topology.

Figure 10-1 Stack networking



Configuration Roadmap

The configuration roadmap is as follows:

1. Connect SwitchA and SwitchB using stack cables. Connect four service ports on two LPUs of each switch to improve bandwidth and reliability.
2. Configure the same stack domain ID and stack connection mode on SwitchA and SwitchB, and configure different stack member IDs and stack priorities for the two switches.
3. Create a stack port on SwitchA and SwitchB, and add the physical member ports to the stack port.
4. Save the configurations of SwitchA and SwitchB and enable the stacking function on the two switches.
5. Check whether a stack is set up successfully.

Procedure

Step 1 Connect stack cables.

Connect SwitchA and SwitchB using stack cables. To use the MPU connection mode, connect SIP ports on the MPUs and physical member ports on the LPUs. To use the LPU connection mode, connect physical member ports on the LPUs.

For details about how to connect stack cables, see 2.2 Stack Connection Modes.

Step 2 Configure stack parameters on SwitchA and SwitchB.

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

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

# On SwitchB, set the stack member ID to 2, stack priority to 100, stack domain ID to 10, and stack connection mode to MPU connection.

```
<HUAWEI> system-view
[~HUAWEI] sysname SwitchB
[*HUAWEI] commit
[~SwitchB] stack
[~SwitchB-stack] stack member 2
Warning: The device will use the configuration of member ID 2 after the device resets.
Continue? [Y/N]: y
[*SwitchB-stack] stack priority 100
[*SwitchB-stack] stack domain 10
[*SwitchB-stack] stack link-type mainboard-direct
[*SwitchB-stack] quit
[*SwitchB] commit
```

NOTE

To use the LPU connection mode, run the **stack link-type linecard-direct** command.

Step 3 Configure stack ports.

# Create a stack port on SwitchA, and add physical ports 10GE1/0/1 to 10GE1/0/2 and 10GE2/0/1 to 10GE2/0/2 to the stack port. Create a stack port on SwitchB, and add physical ports 10GE1/0/1 to 10GE1/0/2 and 10GE2/0/1 to 10GE2/0/2 to the stack port. The configuration on SwitchB is similar to the configuration on SwitchA, and is not mentioned here.

```
[~SwitchA] port-group group1
[*SwitchA-port-group-group1] group-member 10ge 1/0/1 to 10ge 1/0/2
[*SwitchA-port-group-group1] group-member 10ge 2/0/1 to 10ge 2/0/2
[*SwitchA-port-group-group1] shutdown
[*SwitchA-port-group-group1] quit
[*SwitchA] commit
[~SwitchA] interface stack-port 1
[*SwitchA-Stack-Port1] port member-group interface 10ge 1/0/1 to 1/0/2
```

```
[*SwitchA-Stack-Port1] port member-group interface 10ge 2/0/1 to 2/0/2
[*SwitchA-Stack-Port1] quit
[*SwitchA] commit
[~SwitchA] port-group group1
[~SwitchA-port-group-group1] undo shutdown
[*SwitchA-port-group-group1] quit
[*SwitchA] commit
[~SwitchA] quit
```

Step 4 Check the stack configuration.

# After the configuration is complete, run the **display stack configuration** command to check whether the stack 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      Mode     Enable
Oper(Conf)   Oper(Conf)     Oper(Conf)   Oper(Conf)   Oper
---------------------------------------------------------------
1(1)       --(10)        100(150)    MB(MB)      Disable
---------------------------------------------------------------

Stack-Port Configuration:
--------------------------------------------------------------------------------
Stack-Port         Member Ports
--------------------------------------------------------------------------------
Stack-Port1        10GE1/0/1    10GE1/0/2    10GE2/0/1    10GE2/0/2
--------------------------------------------------------------------------------
```

Step 5 Enable the stacking function.

# Save the configuration of SwitchA and enable the stacking function.

```
<SwitchA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<SwitchA> system-view
[~SwitchA] stack
[~SwitchA-stack] stack enable
Warning: Make sure that one or more dual-active detection methods are configured once
the conversion is complete and the device ente
rs the stack mode.
Current configuration will be converted to the next startup saved-configuration file
of stack mode.
System will reboot. Continue? [Y/N]: y
```

# Save the configuration of SwitchB and enable the stacking function.

```
<SwitchB> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<SwitchB> system-view
[~SwitchB] stack
[~SwitchB-stack] stack enable
Warning: Make sure that one or more dual-active detection methods are configured once
the conversion is complete and the device ente
rs the stack mode.
Current configuration will be converted to the next startup saved-configuration file
of stack mode.
System will reboot. Continue? [Y/N]: y
```

Step 6 Check whether the stack is set up successfully.

# View indicators on the switches.

On SwitchA, the STACK indicator on one MPU is steady green. On SwitchB, the STACK indicators on both MPUs blink green. This indicates that a stack has been set up, in which SwitchA is the master switch, and SwitchB is the standby switch.

# Log in to the stack through the console interface or management interface of any switch and run the **display stack** command to check whether the stack is set up successfully. To log in through the management interface, specify the IP address of the master switch.

```
<SwitchA> display stack
--------------------------------------------------------------------------------
MemberID Role     MAC            Priority   DeviceType       Description
--------------------------------------------------------------------------------
1       Master   006d-8835-2b00   150       CE12804
2       Standby  006d-8835-2c00   100       CE12804
--------------------------------------------------------------------------------
```

Step 7 Save the configuration.

NOTE

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

```
<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 mode
 #
 stack member 1 domain 10
 stack member 1 priority 150
 #
 stack member 2 domain 10
#
interface Stack-Port1/1
#
interface Stack-Port2/1
#
interface 10GE1/1/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE1/1/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE1/2/0/1
 port mode stack
 stack-port 1/1
#
interface 10GE1/2/0/2
 port mode stack
 stack-port 1/1
#
interface 10GE2/1/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/1/0/2
 port mode stack
 stack-port 2/1
#
interface 10GE2/2/0/1
 port mode stack
 stack-port 2/1
#
interface 10GE2/2/0/2
 port mode stack
 stack-port 2/1
#
port-group group1
 group-member 10GE1/1/0/1
 group-member 10GE1/1/0/2
 group-member 10GE1/2/0/1
 group-member 10GE1/2/0/2
#
return
```

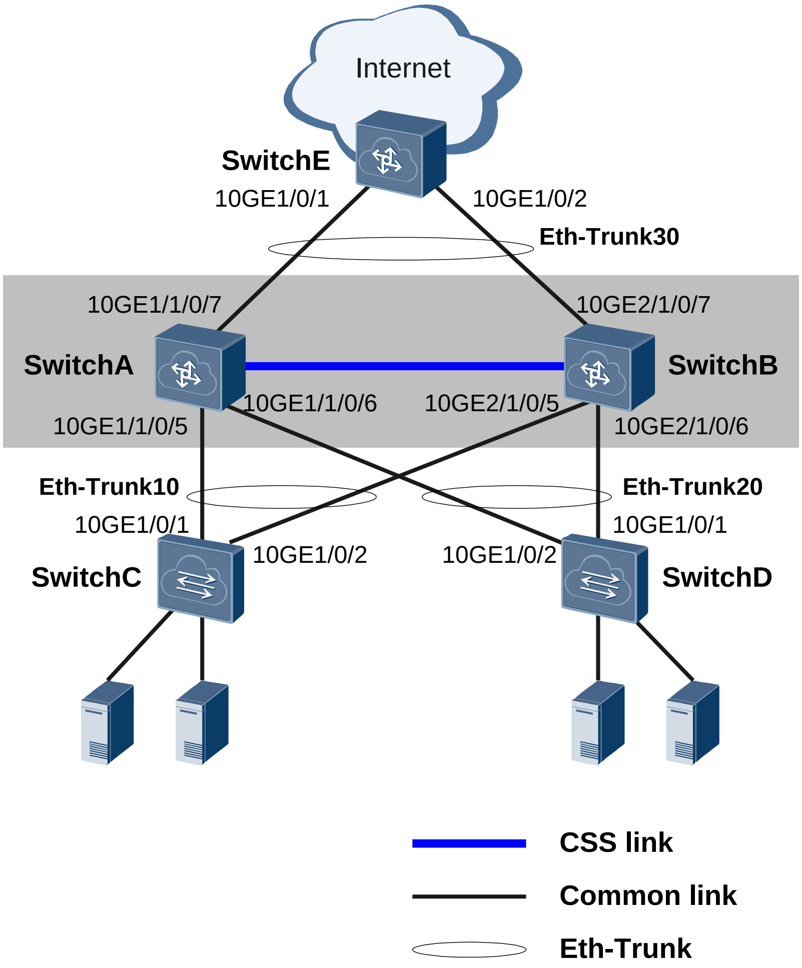
10.2 Example for Configuring Inter-Device Eth-Trunks

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 10-2, 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 10-2 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 CSS
[*HUAWEI] commit
[~CSS] interface eth-trunk 10
[*CSS-Eth-Trunk10] trunkport 10ge 1/1/0/5
[*CSS-Eth-Trunk10] trunkport 10ge 2/1/0/5
[*CSS-Eth-Trunk10] quit
[*CSS] interface eth-trunk 20
[*CSS-Eth-Trunk20] trunkport 10ge 1/1/0/6
[*CSS-Eth-Trunk20] trunkport 10ge 2/1/0/6
[*CSS-Eth-Trunk20] quit
[*CSS] interface eth-trunk 30
[*CSS-Eth-Trunk30] trunkport 10ge 1/1/0/7
[*CSS-Eth-Trunk30] trunkport 10ge 2/1/0/7
[*CSS-Eth-Trunk30] quit
[*CSS] 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.

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

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.

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

----End

Configuration Files

- Configuration file of the stack

```
#
sysname CSS
#
interface Eth-Trunk10
#
interface Eth-Trunk20
#
interface Eth-Trunk30
#
interface 10GE1/1/0/5
 eth-trunk 10
#
interface 10GE1/1/0/6
 eth-trunk 20
#
interface 10GE1/1/0/7
 eth-trunk 30
#
interface 10GE2/1/0/5
 eth-trunk 10
#
interface 10GE2/1/0/6
 eth-trunk 20
#
interface 10GE2/1/0/7
 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

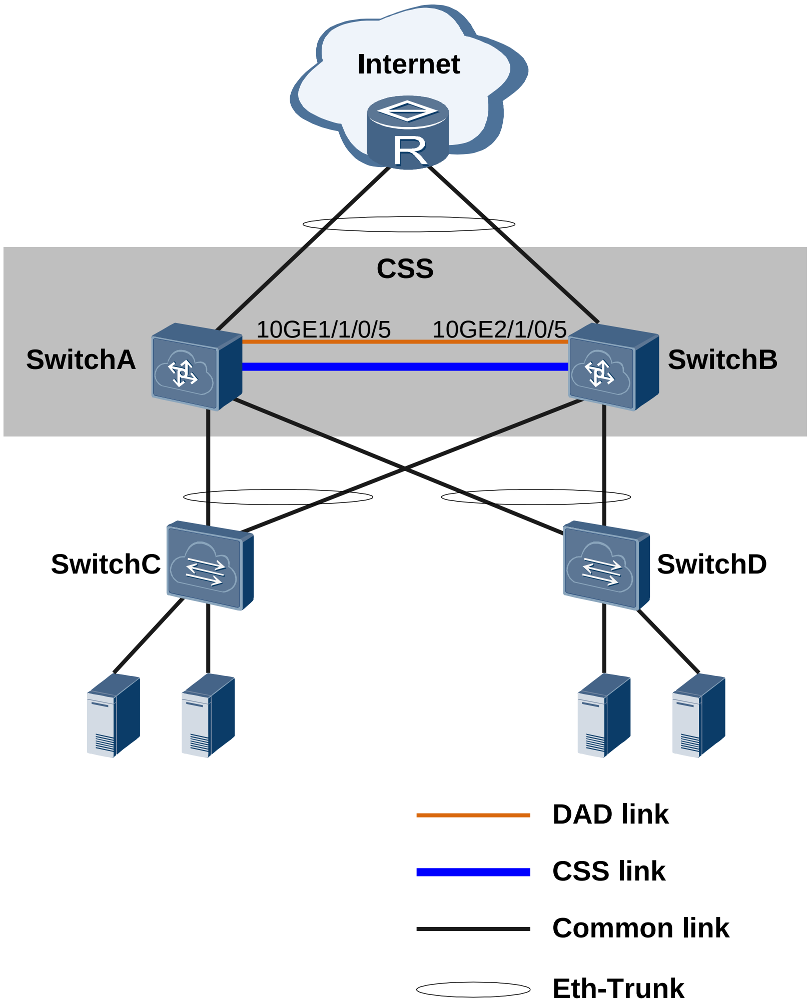
```
#
sysname SwitchE
#
interface Eth-Trunk30
#
interface 10GE1/0/1
 eth-trunk 30
#
interface 10GE1/0/2
 eth-trunk 30
#
return
```

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. If the stack splits due to link failures, the network will have two stack systems running conflicting configurations. To reduce impact of a stack split on the network, configure DAD on the stack.

Figure 10-3 DAD in direct mode



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure DAD in direct mode on 10GE1/1/0/5 and 10GE2/1/0/5.

Procedure

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

# Configure DAD in direct mode on 10GE1/1/0/5.

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

# Configure DAD in direct mode on 10GE2/1/0/5.

```
[~HUAWEI] interface 10ge 2/1/0/5
[~HUAWEI-10GE2/1/0/5] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue?
[Y/N]: y
[*HUAWEI-10GE2/1/0/5] commit
[~HUAWEI-10GE2/1/0/5] 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:
 10GE1/1/0/5    up
 10GE2/1/0/5    up
Dual-active relay detect interfaces configured:
 -
Excluded ports(configurable):
 -
Excluded ports(can not be configured):
 10GE1/1/0/1
 10GE1/1/0/2
 10GE1/1/0/3
 10GE1/1/0/4
 10GE2/1/0/1
 10GE2/1/0/2
 10GE2/1/0/3
 10GE2/1/0/4
```

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   e468-a3f9-1f00  150       CE12804
------------------------------------------------------------------------------
```

```
-
```

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 is 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

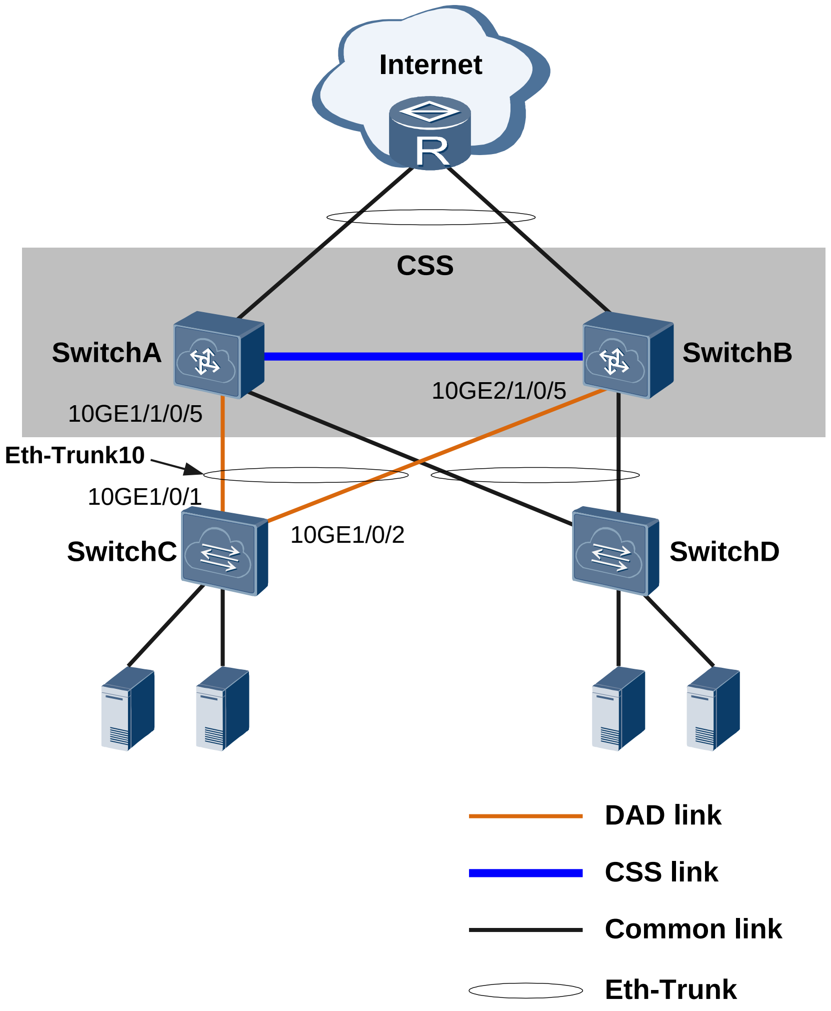
  ```
  #
  interface 10GE1/1/0/5
   dual-active detect mode direct
  #
  interface 10GE2/1/0/5
   dual-active detect mode direct
  #
  return
  ```

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

Networking Requirements

As shown in Figure 10-4, SwitchA and SwitchB set up a stack and connect to the upstream and downstream devices through Eth-Trunks. If the stack splits due to link failures, the network will have two stack systems running conflicting configurations. To reduce impact of a stack split on the network, configure DAD on the stack.

Figure 10-4 DAD in relay mode



Configuration Roadmap

The configuration roadmap is as follows:

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

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

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

```
<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] dual-active proxy
[*SwitchC-Eth-Trunk10] commit
[~SwitchC-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
     10GE1/1/0/5   up
     10GE2/1/0/5   up
Excluded ports(configurable):
 -
Excluded ports(can not be configured):
 10GE1/1/0/1
 10GE1/1/0/2
 10GE1/1/0/3
 10GE1/1/0/4
 10GE2/1/0/1
 10GE2/1/0/2
 10GE2/1/0/3
 10GE2/1/0/4
```

# Check DAD proxy information on SwitchC.

```
<SwitchC> display dual-active proxy
Dual-active proxy interfaces configured:
 Eth-Trunk10
     10GE1/0/1   up
     10GE1/0/2   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   e468-a3f9-1f00   150      CE12804
-------------------------------------------------------------------------------
-
```

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 is 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

```
#
interface 10GE1/1/0/5
 eth-trunk 10
#
interface 10GE2/1/0/5
 eth-trunk 10
#
interface Eth-Trunk10
 dual-active detect mode relay
#
return
```

- Configuration file of SwitchC

```
#
sysname SwitchC
#
interface 10GE1/0/1
 eth-trunk 10
#
interface 10GE1/0/2
 eth-trunk 10
#
interface Eth-Trunk10
 dual-active proxy
#
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?

- Method 1: Assume that SwitchA and SwitchB set up a stack, and you want SwitchA to be the master switch. If stack cables have been connected, enable the stacking function on SwitchA first. After SwitchA restarts and becomes a single-chassis stack, enable the stacking function on SwitchB. After SwitchB restarts, it joins the stack and becomes the standby switch. SwitchA functions as the master switch in the stack.
- Method 2: If you enable the stacking function 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.
- Method 3: If a stack is running but the master switch is not the one you expect, run the **slave switchover** command to perform a switchover in the stack. This method can be used when the master switch has two MPUs. If the master switch has only one MPU, power off the master switch to enable the standby switch to become the master switch. Then, power on the original master switch.

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

  On one switch, the STACK indicator on an MPU is steady green. This switch is the master switch. On the other switch, the STACK indicators on both MPUs are blinking green. This switch is the standby switch.

- 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
-------------------------------------------------------------------------------
-
1       Master  e468-a3f9-1f00   255       CE12804
2       Standby  006d-88f4-e600   100       CE12808
-------------------------------------------------------------------------------
-
<HUAWEI> display device
Chassis ID: 1 (Master Switch)
CE12804's Device status:
------------------------------------------------------------------------------
Slot  Card   Type        Online   Power Register    Alarm    Primary
------------------------------------------------------------------------------
1    -     CE-L24LQ-EA  Present  On    Registered   Normal   NA
2    -     CE-L48GT-EA  Present  On    Registered   Normal   NA
3    -     CE-L48GS-EA  Present  On    Registered   Normal   NA
4    -     CE-L48XS-EA  Present  On    Registered   Normal   NA
6    -     CE-MPUA     Present  On    Registered   Normal   System Master
7    -     CE-CMUA     Present  On    Registered   Normal   Master
8    -     CE-CMUA     Present  On    Registered   Normal   Slave
9    -     CE-SFU04A    Present  On    Registered   Normal   NA
10   -     CE-SFU04A    Present  On    Registered   Normal   NA
PWR3  -     -          Present  On    Registered   Normal   NA
FAN1  -     -          Present  On    Registered   Normal   NA
FAN2  -     -          Present  On    Registered   Normal   NA
FAN3  -     -          Present  On    Registered   Normal   NA
FAN4  -     -          Present  On    Registered   Normal   NA
FAN5  -     -          Present  On    Registered   Normal   NA
FAN6  -     -          Present  On    Registered   Normal   NA
FAN7  -     -          Present  On    Registered   Normal   NA
FAN8  -     -          Present  On    Registered   Normal   NA
FAN9  -     -          Present  On    Registered   Normal   NA
------------------------------------------------------------------------------
Chassis ID: 2 (Standby Switch)
CE12808's Device status:
------------------------------------------------------------------------------
Slot  Card   Type        Online   Power Register    Alarm    Primary
```

```
------------------------------------------------------------------------------
3    -     CE-L48GS-EA  Present  On    Registered   Normal   NA
5    -     CE-L48GT-EA  Present  On    Registered   Normal   NA
6    -     CE-L24LQ-EA  Present  On    Registered   Normal   NA
8    -     CE-L48XS-EA  Present  On    Registered   Normal   NA
10   -     CE-MPUA     Present  On    Registered   Normal   System Slave
12   -     CE-CMUA     Present  On    Registered   Normal   Master
14   -     CE-SFU08A    Present  On    Registered   Normal   NA
15   -     CE-SFU08A    Present  On    Registered   Normal   NA
17   -     CE-SFU08C    Present  On    Registered   Normal   NA
PWR1  -     -          Present  On    Registered   Normal   NA
PWR3  -     -          Present  On    Registered   Normal   NA
FAN1  -     -          Present  On    Registered   Normal   NA
FAN2  -     -          Present  On    Registered   Normal   NA
FAN3  -     -          Present  On    Registered   Normal   NA
FAN4  -     -          Present  On    Registered   Normal   NA
FAN5  -     -          Present  On    Registered   Normal   NA
FAN6  -     -          Present  On    Registered   Normal   NA
FAN7  -     -          Present  On    Registered   Normal   NA
FAN8  -     -          Present  On    Registered   Normal   NA
FAN9  -     -          Present  On    Registered   Normal   NA
FAN10 -     -          Present  On    Registered   Normal   NA
FAN11 -     -          Present  On    Registered   Normal   NA
FAN12 -     -          Present  On    Registered   Normal   NA
FAN13 -     -          Present  On    Registered   Normal   NA
------------------------------------------------------------------------------
```

11.3 Why Does a Member Switch Newly Added to a Stack Have Its Current Stack Configuration Different from the Next-Startup Stack Configuration?

Stack attributes of a switch (including the stack member ID, stack priority, and stack connection mode) take effect after the switch restarts. After a new member switch joins the stack, the switch starts with its own stack configuration. After startup, the member switch restores its configuration using the configuration file of the master switch in the stack. If the master switch has offline stack attributes configured for the new member switch, the offline stack configuration on the master switch is used as the next-startup configuration for the member switch.

11.4 What Precautions Should Be Taken During Network Expansion by Setting Up a Stack?

When connecting a new switch to an existing switch to set up a stack, pay attention to the following points:

- If the software version of the new member switch is different from the software version of the existing switch, you are advised to upgrade the new member switch to the version running on the existing switch. Otherwise, the new member switch needs to synchronize its software version with the existing switch, which causes the switch to restart. In addition, manually upgrading the new member switch can shorten the time spent in setting up a stack.

- Ensure that the stack priority of the new member switch is lower than the priority of the existing switch, so that existing switch becomes the master switch. If new member switch has a higher stack priority, stack merging occurs, causing the existing switch to restart. In this case, services are interrupted.

11.5 How to Load the License for a Stack?

In a stack, the process of loading a license is as follows:

1. Apply for a license and upload the license file to the system active MPU.

   A license is bound to the ESN of a physical device. Each stack member device has an independent ESN. You can apply for a license for two ESNs or each ESN.

2. Run the **license active** *file-name* command in the user view to activate the uploaded license.
   - If there are two license files, run the **license active** *file-name* command two times and specify two different license files. The system searches for matching ESNs to activate the licenses.
   - If there is only one license file, run the **license active** *file-name* command one time.
3. Run the **display license** command to check whether the license is loaded successfully.

You can also load the license on two devices and then form a stack on the two devices. The stack then supports all the features that the two member devices support. If only one device has the license loaded, the license takes effect in the stack.

If the stack splits, the license of a standalone device takes effect and services that have been activated but not enabled through the license can continue running.

11.6 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 system active MPU.
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.

11.7 How to Restart a Stack Member Device?

Run the **reset chassis** *chassis-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.