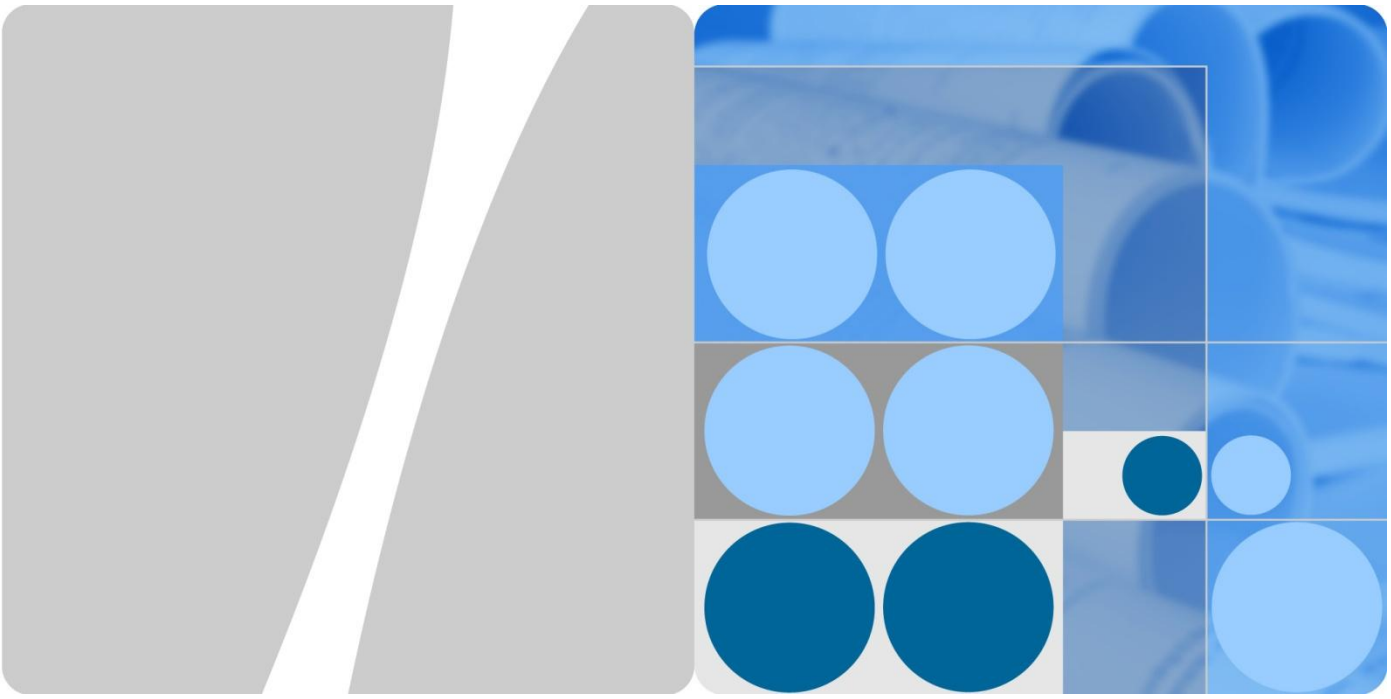


Smart Link & Monitor Link Technology White Paper

Issue 01

Date 2012-09-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Smart Link & Monitor Link

About This Chapter

1.1 Introduction to Smart Link

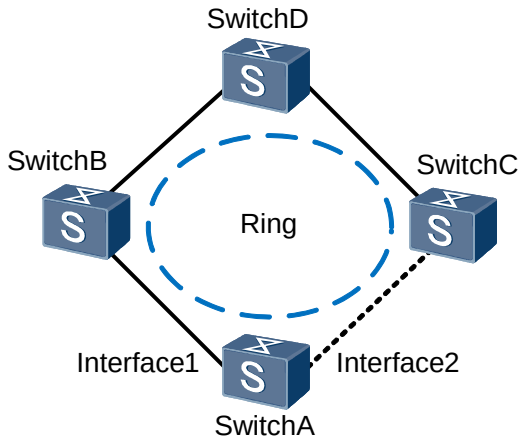
Definition

Smart Link is a link backup feature. A Smart Link group consists of two interfaces. One interface is the backup of the other. The Smart Link function implements link backup and rapid switchover on a dual-homed network.

Purpose

If a device connects to an upstream device through only one link, services are interrupted when single point failures occur. In a dual-homed networking, a downstream device is connected to two upstream devices to reduce impact of single point failures. This networking improves network reliability.

Figure 1-1 Dual-homing networking



As shown in Figure 1-1, SwitchA is dual-homed to SwitchB and SwitchC through two links: SwitchA->SwitchB->SwitchD and SwitchA->SwitchC->SwitchD. One link backs up the other. However, the loop (SwitchA->SwitchB->SwitchC->SwitchD->SwitchA)) on the network may cause network storms. Generally, the Spanning Tree Protocol (STP) is used to prevent loops. However, the long STP convergence time causes loss of many packets. STP is not applicable to networks that require fast convergence. Another loop prevention protocol Rapid Ring Protection Protocol (RRPP) shortens the network convergence time. However, RRPP applies to complex ring networks and its configuration is complicated. Huawei offers a Smart Link solution to prevent loops in dual-homing networking.

Benefits

Smart Link is a reliability solution designed for dual-homing. This solution brings the following benefits for customers:

- When both uplinks are working properly, one link works in forwarding state, and the other stays in inactive state to prevent loops.
- Compared to STP, Smart Link provides higher convergence performance. When the active link fails, traffic is switched to the standby link in milliseconds. The fast convergence minimizes packet loss.
- Compared to RRPP, Smart Link is easier to configure and use.

1.2 Reference Standards and Protocols for Smart Link

Smart Link is a Huawei proprietary protocol, and no reference or protocol available.

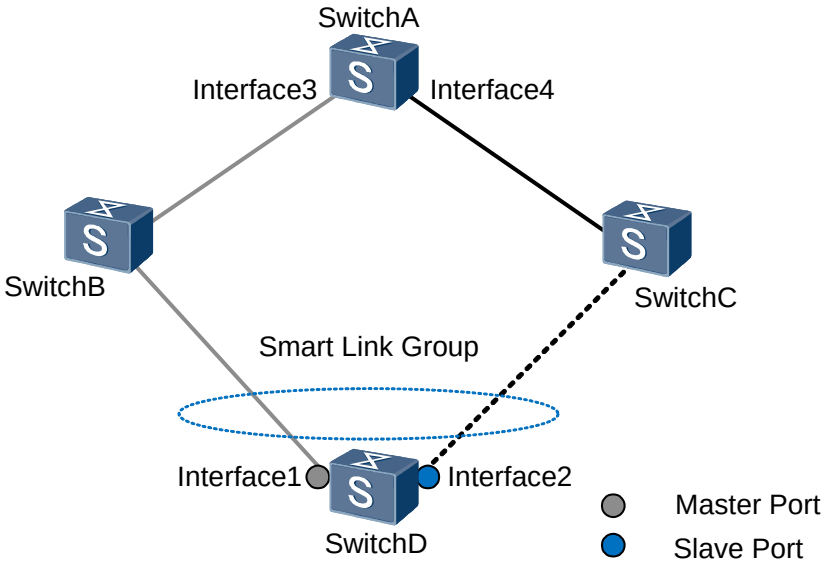
1.3 Smart Link Principles

1.3.1 Basic Concepts of Smart Link

Smart Link improves reliability by implementing backup between two interfaces. The two interfaces constitute a Smart Link group. One interface is called master interface and the other

is called slave interface. Smart Link also uses Flush packet, Smart Link instance, and control VLAN to implement fast switchover and load balancing.

Figure 1-2 Smart Link networking



Smart Link Group

A Smart Link group consists of a maximum of two interfaces. One is the master interface, and the other is the slave interface. The master interface is in active state; the slave interface is in inactive state.

As shown in Figure 1-2, interface1 and interface2 on SwitchD form a Smart Link group.

Master Interface

The master interface in a Smart Link group is in the interface that enters the active state first. The master interface is not always active. When it is faulty and the traffic is switched to the other link, the slave interface becomes active. The master interface remains inactive until the next switchover even if its fault is rectified before the switchover. If the revertive switchover function is configured, services are switched to the master link after the failback interval. As shown in Figure 1-2, interface1 is configured as the master interface for a Smart Link group.

Slave Interface

Slave interface is also called inactive interface. When both the master and slave interfaces are in inactive state, the slave interface remains the inactive state. The slave interface is not always inactive. When traffic is switched from the active link to the standby link, the slave interface transits to forwarding state. As shown in Figure 1-2, interface2 is configured as the slave interface for a Smart Link group.

Flush Packet

When a switchover occurs between the active and inactive links of a Smart Link group, the existing forwarding entries no longer apply to the new topology. All the MAC address entries and Address Resolution Protocol (ARP) entries on the network need to be updated. Therefore, the Smart Link group sends Flush packets to request other devices to update their MAC address tables and ARP tables. As shown in Figure 1-2, when a link switchover occurs in the

Smart Link group, SwitchD sends a Flush packet to request SwitchA, SwitchB, and SwitchC to update their MAC address entries and ARP entries. Flush packets are multicast packets.

Smart Link Instance

Smart Link can use Multiple Spanning Tree Protocol (MSTP) instances. Each instance maps a range of VLANs. Multiple instances can be bound to the inactive link to implement load balancing.

Control VLAN

- Control VLAN for sending Flush packets

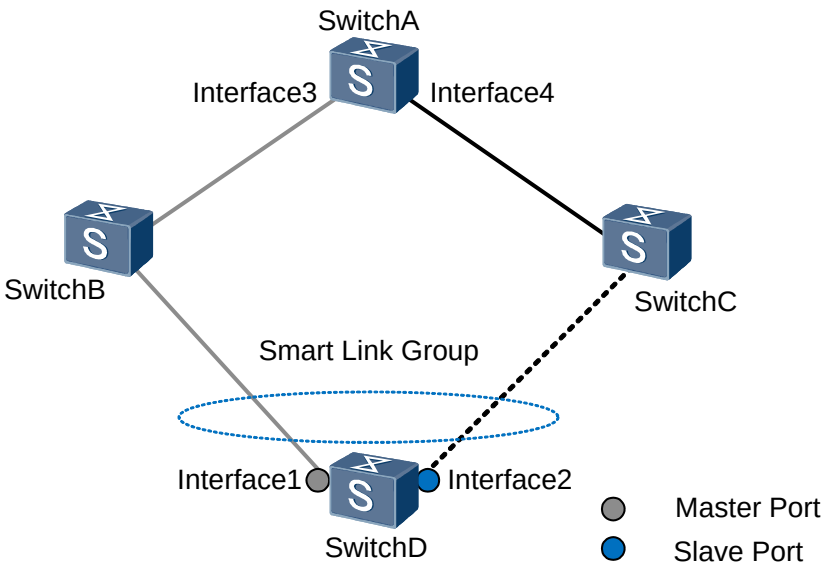
  A Smart Link group uses this control VLAN to send Flush packets in broadcast mode. As shown in Figure 1-2, if SwitchD is enabled to send Flush packets, it sends Flush packets in broadcast mode using a new link when a traffic switchover occurs.
- Control VLAN for receiving Flush packets

  The upstream devices use this control VLAN to receive and process Flush packets. The upstream devices (for example, SwitchA, SwitchB, and SwitchC) recognize Flush packets and are enabled to receive Flush packets. When the traffic is switched on links, the upstream devices process the received Flush packets and then update the MAC address entries and ARP entries.

1.3.2 Smart Link Implementation

This section describes how Smart Link works when both links are working properly, a link fails, and the link fault is rectified using the network in Figure 1-3 as an example.

Figure 1-3 Smart Link networking



Both Links Work Normally

Interface1 (master) and interface2 (slave) on SwitchD form a Smart Link group. When both uplinks work normally, the master interface is in forwarding state, and the link connected to the master interface is the active link. The slave interface is in inactive state, and the link connected to the slave interface is the standby link. Data is transmitted through the path

SwitchD->SwitchB->SwitchA. No loop exists on the network, so broadcast storms will not occur on the network.

Active Link Fails

When the active link on SwitchD is faulty, the master interface (interface1) transits to inactive state, and the slave interface (interface2) transits to forwarding state. Therefore, the existing MAC address entries and ARP entries on the network no longer apply to some devices. A mechanism is required to update the MAC address entries and ARP entries. Two mechanisms are available:

Automatically update entries based on traffic

This method is applicable when upstream devices (including non-Huawei devices) do not support the Smart Link function. These devices update MAC address entries and ARP entries in traffic-based triggering mode.

- If no upstream traffic from SwitchD triggers update of MAC address entries and ARP entries on SwitchA, SwitchA forwards data packets to SwitchD through Interface3. However, the packets cannot reach SwitchD, which leads to traffic loss. Traffic can be forwarded to SwitchD correctly until the original MAC address entries or ARP entries on SwitchA are aged out.
- The MAC address entries and ARP entries on SwitchD are wrong. Therefore, SwitchD cannot send its upstream traffic until the original entries are aged out and SwitchD relearns new entries. When SwitchA receives the upstream traffic through interface4, it updates its MAC address entries and ARP entries. When SwitchA receives a data packet destined for SwitchD, it forwards this packet through interface4. The packet is then forwarded to SwitchD by SwitchC.

Send Flush packets to request devices to update entries

This method is applicable when the upstream devices (for example, SwitchA, SwitchB, and SwitchC, as shown in Figure 1-3) support the Smart Link function and can process Flush packets. To implement fast switchover, SwitchD is enabled to send Flush packets and all interfaces on the uplinks are enabled to accept Flush packets.

- When a switchover occurs on SwitchD, SwitchD sends a Flush packet through the new active link (interface2).
- When an upstream device receives a Flush packet, it checks whether the control VLAN carried by this Flush packet is in the list of VLANs allowed by the interface. If so, the device processes this Flush packet and updates the MAC address entries and ARP entries. If not, the device does not process this Flush packet and forwards it.
- When SwitchA receives a data packet destined for SwitchD, SwitchA forwards this packet according to the updated MAC address entries or ARP entries. In this way, data traffic is transmitted correctly.

Flush packets enable upstream devices to update their MAC address entries and ARP entries before the entries are aged out, which reduces the time required to update the entries. In general, traffic is switched to the standby link in milliseconds, which minimizes traffic loss.

Active Link Recovers

Interface1 remains blocked after the original active link recovers from the fault. Use following mechanisms to switch the traffic to the original active link:

- Enable the Smart Link revertive switchover function on SwitchD. When the original active link recovers from the fault, Smart Link automatically switches the traffic back to it after the revertive switchover timer times out.
- Use a command to forcible switch the traffic back to the original active link.

SwitchD is configured with the revertive switchover function of a Smart Link group. When the link of interface1 recovers from the fault, traffic is switched back to interface1 after the revertive switchover timer times out. If you use a command to switch the traffic back to the original active link, interface2 is blocked and changes to inactive state immediately, while interface1 changes to forwarding state.

Example of Basic Smart Link Configuration (Major Steps)

NOTE

This section provides only major steps in Smart Link configuration. Here, S9300 V200R001C00 is used as an example.

Create Smart Link group 1 on SwitchD. Configure GE1/0/1 as the master interface and GE1/0/2 as the slave interface.

```
[SwitchD] smart-link group 1
[SwitchD-smlk-group1] port gigabitethernet 1/0/1 master
[SwitchD-smlk-group1] port gigabitethernet 1/0/2 slave
```

Enable SwitchD to send Flush packets. In this example, SwitchD is configured to send Flush packets carrying simple password 123.

```
[SwitchD-smlk-group1] flush send control-vlan 10 password simple 123
```

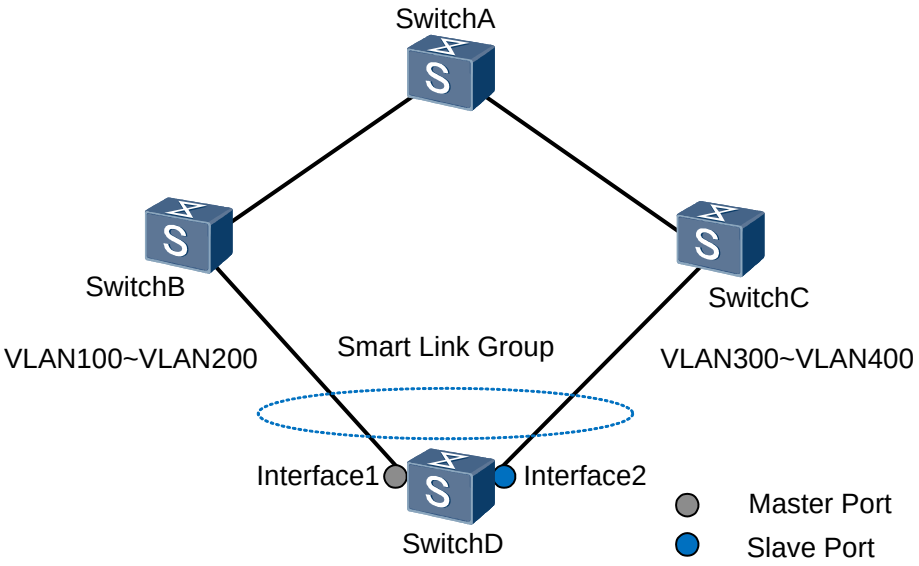
Enable upstream interfaces connected to SwitchD to receive Flush packets. The Flush packet configuration on the receiving end must be the same as that on the sending end. Therefore, the password for Flush packets must also be set to simple password 123 on SwitchB. Otherwise, SwitchB cannot receive Flush packets from SwitchD.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] smart-link flush receive control-vlan 10 password
simple 123
[SwitchB-GigabitEthernet1/0/1] quit
```

1.3.3 Smart Link Load Balancing

A switch may need to forward traffic sent from multiple VLANs. Generally, only the active link transmits data traffic, and the standby link is idle. Smart Link supports load balancing, which allows traffic from different VLANs to be forwarded through different links. Load balancing improve the link usage efficiency. After a load balancing instance is configured for a Smart Link group, the standby link transmits traffic of the VLANs specified in the load balancing instance. The active link does not transmit traffic of these VLANs. As the active and standby links transmit data traffic of different VLANs, load balancing is implemented between the two links in the Smart Link group.

Figure 1-4 Smart Link load balancing



As shown in Figure 1-4, when no load balancing instance is configured, SwitchD forwards all packets through the active link connected to Interface1. To improve the link usage efficiency, configure a load balancing instance on SwitchD and associate VLAN 300 to VLAN 400 with the instance. Then data packets sent from these VLANs are forwarded through Interface2. VLAN 100 to VLAN 200 are not associated with the load balancing instance, so packets sent from these VLANs are forwarded through Interface1. In this way, traffic from different VLANs is loaded balanced between the two links.

Example of Smart Link Load Balancing Configuration (Major Steps)

NOTE

This section provides only major steps in Smart Link configuration. Here, S9300 V200R001C00 is used as an example.

Configure a mapping between VLAN 300 to VLAN 400 and MST instance 10 on SwitchD.

```
[SwitchD] stp region-configuration
[SwitchD-mst-region] instance 10 vlan 300 to 400
[SwitchD-mst-region] active region-configuration
[SwitchD-mst-region] quit
```

Configure instance 10 as the load balancing instance for Smart Link group 1 so that data traffic from VLANs mapped to instance 10 is forwarded through the standby link.

```
[SwitchA-smlk-group1] load-balance instance 10 slave
```

1.4 Introduction to Monitor Link

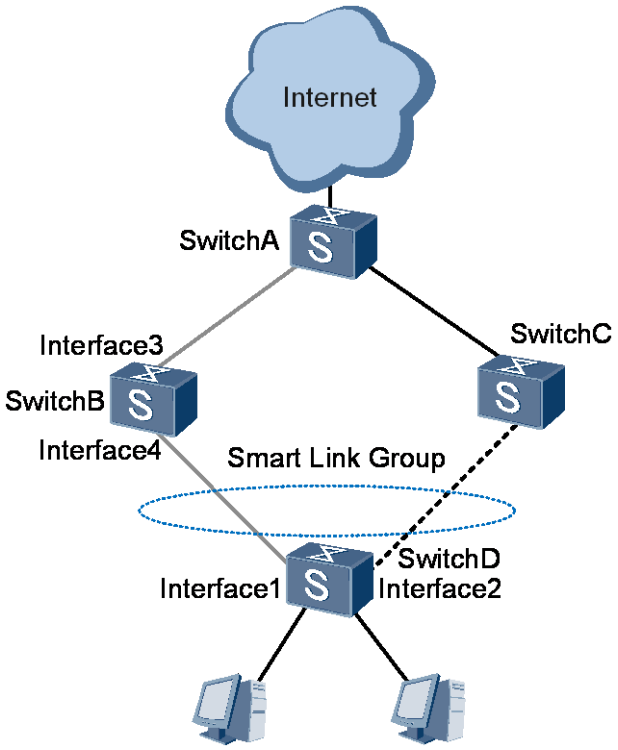
Definition

Monitor Link is an interface association mechanism used to monitor the uplink interface. If the state of the uplink interface switches between Up and Down, Monitor Link requests the

downlink interfaces to switch their states. In this case, the topology protocol on downstream devices triggers an active/standby switchover.

Purpose

Figure 1-5 Monitor Link networking



As shown in Figure 1-5, a Smart Link group is configured on SwitchD, with Interface1 as the master interface and Interface2 as the slave interface. When the active link connected to Interface1 fails, traffic can be quickly switched to the standby link connected to Interface2. This configuration implements highly efficient and reliable link backup and fast switchover.

However, when the uplink connected to Interface3 of SwitchB fails, SwitchD cannot detect the failure because the link directly connected to Interface1 is still working normally. Smart Link does not trigger a link switchover in this situation. Because packets cannot be forwarded to SwitchA through the link connected to Interface1, traffic is interrupted. Huawei offers a Monitor Link solution to enable a Smart Link group to quickly detect failures of uplinks.

Benefits

Monitor Link can associate with Smart Link to expand the scope of Smart Link and provides customers with more choices for networking.

1.5 Reference Standards and Protocols for Monitor Link

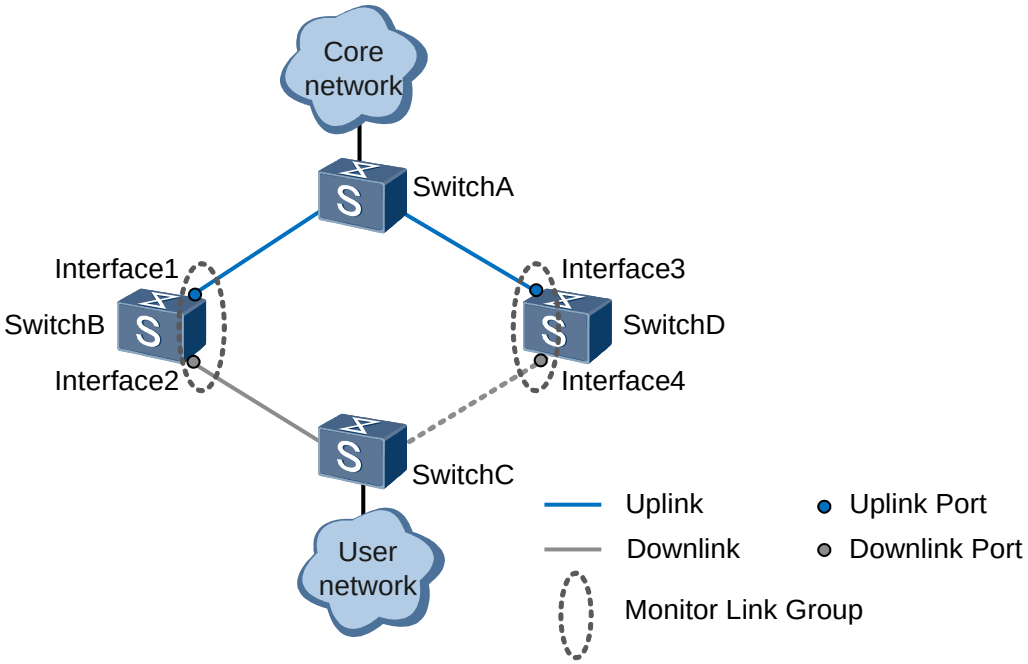
Monitor Link is a Huawei proprietary protocol, and no reference or protocol available.

1.6 Monitor Link Principles

1.6.1 Basic Concepts of Monitor Link

Monitor Link monitors an uplink to control the downlinks. The uplink interface and the downlink interfaces form a Monitor Link group.

Figure 1-6 Monitor Link networking example



Monitor Link Group

A Monitor Link group consists of an uplink interface and several downlink interfaces. A member of the Monitor Link group can be a single interface, static aggregation group, manual aggregation group, or Smart Link group. A Smart Link group can only function as the uplink interface. The state of the downlink interfaces changes with the state of the uplink interface. As shown in Figure 1-6, interface1 and interface2 form a Monitor Link group, and interface3 and interface4 form a Monitor Link group.

Uplink Interface

An uplink interface is monitored by the downlink interfaces in a Monitor Link group. If the uplink interface fails, the Monitor Link group is faulty, and all the downlink interfaces in the Monitor Link group are forcibly shut down. When the uplink interface is a Smart Link group, the uplink interface is considered faulty only if both the maser and slave interfaces of the Smart Link group are in inactive or Down state. In Figure 1-6, interface1 and interface3 are uplink interfaces.

Downlink Interface

Downlink interfaces monitor the uplink interface in a Monitor Link group. The fault of a downlink interface does not affect the uplink interface or the other downlink interfaces. In Figure 1-6, interface2 and interface4 are downlink interfaces.

NOTE

When a downlink interface in a Monitor Link group is an Eth-Trunk interface, all the member interfaces of the Eth-Trunk interface are forcibly shut down if the uplink interface fails. When the uplink interface recovers, all the member interfaces in the Eth-Trunk interface recover.

1.6.2 Monitor Link Implementation

After a Monitor Link group is configured, the uplink interface is monitored in real time. When a fault occurs on the uplink interface (such as link fault, unidirectional OAM connectivity, and failure to establish OAM connections), all the downlink interfaces in Up state in the Monitor Link group are forcibly shut down. When the uplink recovers, the downlink interfaces restore to the Up state.

As shown in Figure 1-6, if the uplink of interface1 fails, Monitor Link forcibly switches interface2 to Down state. Then SwitchC detects that a fault occurs on the link between SwitchB and SwitchA. When the uplink of interface1 recovers, Monitor Link unblocks interface2.

Example of Basic Monitor Link Configuration (Major Steps)

NOTE

This section provides only major steps in Smart Link configuration. Here, S9300 V200R001C00 is used as an example.

Create Monitor Link group 2 on SwitchB. Configure GE1/0/1 as the uplink interface and GE2/0/1 as the downlink interface, with the downlink interface number 1.

```
[SwitchB] monitor-link group 2
[SwitchB-mtlk-group2] port gigabitethernet 1/0/1 uplink
[SwitchB-mtlk-group2] port gigabitethernet 2/0/1 downlink 1
```

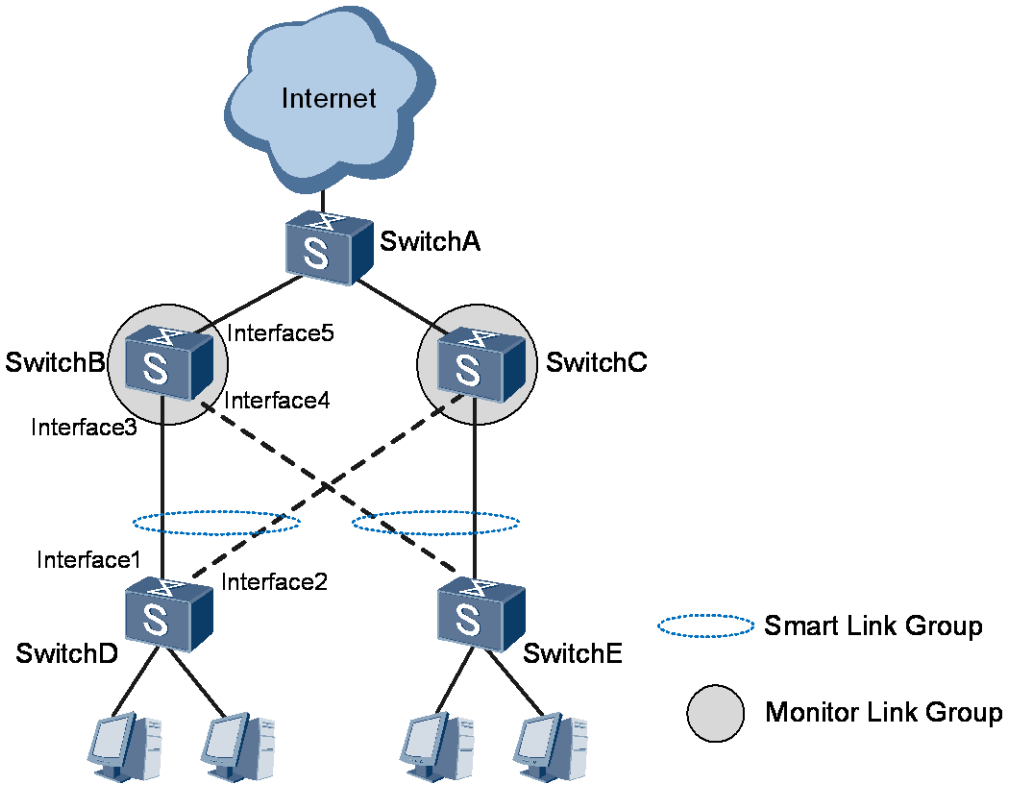
1.7 Applications

1.7.1 Combination of Smart Link and Monitor Link

Smart Link can only detect faults of links directly connected to member interfaces. For example, interface1 and interface2 on SwitchD are configured with Smart Link. As shown in Figure 1-7, Smart Link can only detect the fault of the link between interface1 and SwitchB or between interface2 and SwitchC. If the uplink between SwitchB and SwitchA fails, Smart Link cannot detect this fault so that it does not trigger a switchover, leading to traffic loss.

If you configure Monitor Link on the upstream devices, Smart Link can detect the fault and switch traffic to the standby link quickly. Combination of Smart Link and Monitor Link expands the application scope of Smart Link and allows flexible networking.

Figure 1-7 Smart Link and Monitor Link on one network



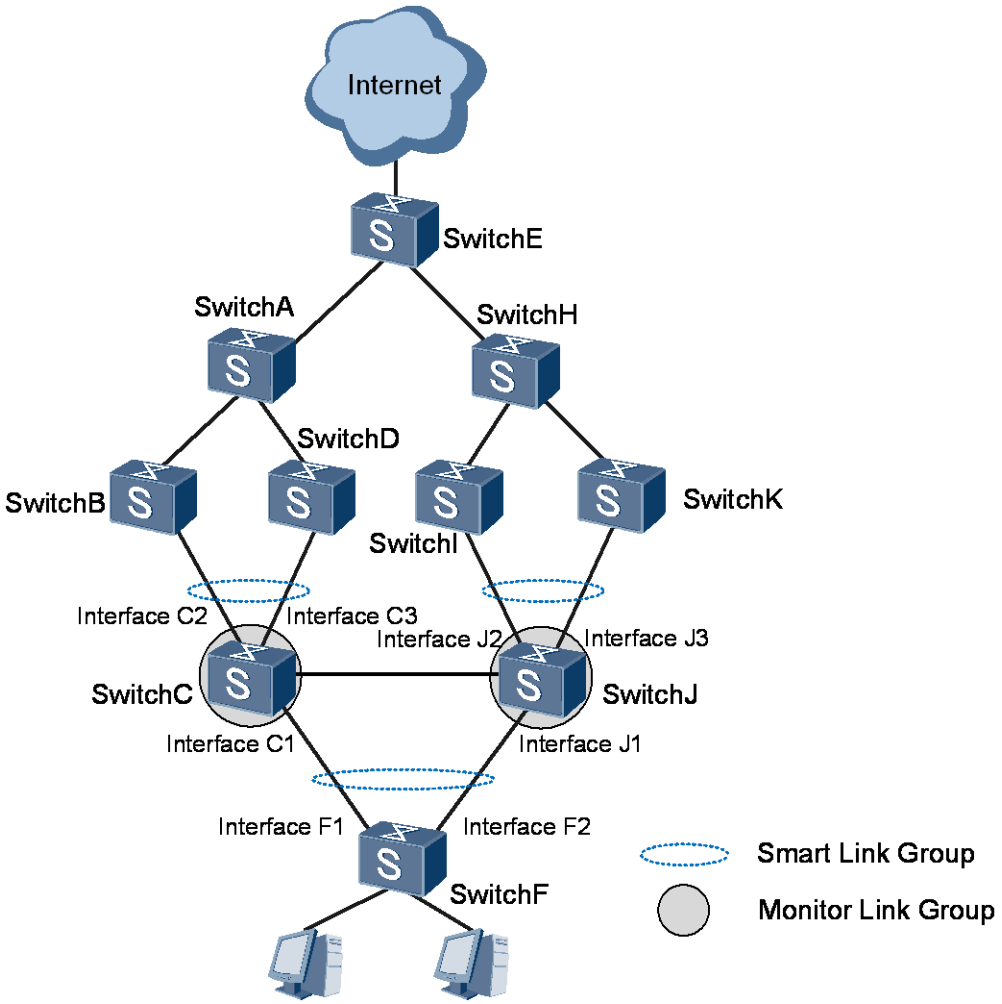
As shown in Figure 1-7, Smart Link is configured on SwitchD and SwitchE. When the link between SwitchB and SwitchD or between SwitchC and SwitchE is faulty, the Smart Link group can detect the fault and switch services to the standby link quickly. To enable SwitchD or SwitchE to detect the fault on the link between SwitchA and SwitchB or between SwitchA and SwitchC, configure Monitor Link on SwitchB and SwitchC.

Use SwitchD and SwitchB for example. A Smart Link group is configured on SwitchD, and interface1 and interface2 are added to this Smart Link group. A Monitor Link group is configured on SwitchB. Interface5 is the uplink interface, and interface3 and interface4 are the downlink interfaces. When the Monitor Link group detects a fault on the uplink, downlink interfaces are shut down forcibly. A switchover is then triggered in the Smart Link group on SwitchD. When the fault on the uplink interface is rectified, downlink interfaces are enabled automatically. In this way, SwitchD can detect the uplink status change.

1.7.2 Cascading of Smart Link and Monitor Link

Figure 1-8 shows cascading networking of Smart Link and Monitor Link. Cascading of Smart Link and Monitor Link improves link backup reliability. A Smart Link group can function as the uplink interface of a Monitor Link group.

Figure 1-8 Cascading of Smart Link and Monitor Link



As shown in Figure 1-8, the uplink interfaces on SwitchC and SwitchJ are added to Smart Link groups to guarantee reliability. Monitor Link groups are configured on SwitchC and SwitchJ and the Smart Link groups are added to the Monitor Link groups. An active/standby switchover is performed between the downlink interfaces only when both the two uplink interfaces in a Smart Link group are down.

Table 1-1 lists the configuration of Smart Link and Monitor Link.

Table 1-1 Configuration of Smart Link and Monitor Link

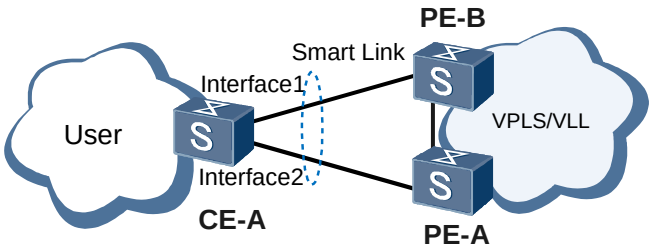
Switch	Smart Link Group		Monitor Link Group	
	Master Interface	Slave Interface	Uplink Interface	Downlink Interface
SwitchC	Interface C2	Interface C3	Smart Link Group Interface C2, Interface C3	Interface C1
SwitchJ	Interface J2	Interface J3	Smart Link Group Interface J2, Interface J3	Interface J1

SwitchF	Interface F1	Interface F2	-

1.7.3 Association Between Smart Link and the VPLS/VLL Module for Fast Link Switchover

When Smart Link is used together with the VPLS/VLL on the network, this function can be configured to enable the VPLS/VLL module to rapidly detect link switching and reduce data packet loss.

Figure 1-9 Association between Smart Link and the VPLS/VLL module



As shown in Figure 1-9, if a CE is dual-homed to a VPLS/VLL network using VLANIF interfaces or Dot1q termination sub-interfaces of PEs, you can associate Smart Link with VPLS/VLL on the corresponding physical interfaces of PEs. When receiving a Flush packet, an interface notifies the VPLS/VLL module. The VPLS/VLL module then clears the MAC addresses in the VSI/VLL bound to the VLANIF interface or sub-interface and sends messages to remote devices, prompting them to update MAC address entries.

1.8 Troubleshooting Cases

1.8.1 Link Switchover Fails in a Smart Link Group

Fault Description

When the active link in a Smart Link group fails, traffic cannot be switched to the standby link.

The possible cause is that data flows are locked on an interface.

Procedure

Step 1 Check the configuration of the Smart Link to see whether data flows are locked on an interface.

Run the **display smart-link group** *group-id* command and check the **Link status** field in the command output to see whether data flows are locked on an interface. If the **Link status** field displays **lock** or **force**, data flows are locked on the master or slave interface. Run the **undo smart-link** { **force** | **lock** } command to unlock data flows.

----End

1.8.2 Monitor Link Group Is Down

Fault Description

The Monitor Link group is always Down.

Procedure

Step 1 Check the status of member interfaces in the Monitor Link group.

Run the **display monitor-link group** *group-id* command to view the **State** field.

- If the **State** field of the interface is **DOWN**, address the interface Down failure.

NOTE

A link fault, a unidirectional OAM connectivity fault, or a failure to establish OAM connections may occur on the uplink interface. The uplink interface is considered as faulty only if the uplink interface is in the Smart Link group and neither of the two interfaces is Active when the Smart Link is enabled or both of the two interfaces are Down when the Smart Link is disabled.

- If the value of the **State** field is **UP**, go to step 2.

Step 2 Check whether member interfaces of the Monitor Link group are added to the service VLAN. Run the **display current-configuration interface** *interface-type interface-number* command in the member interface view to check whether member interfaces of the Monitor Link group are added to the service VLAN. If the interface is not added to the service VLAN, add the interface to the service VLAN.

----End

1.9 FAQ

1.9.1 Can an Eth-Trunk Interface Be Configured as the Master or Slave Interface in a Smart Link Group?

An Eth-Trunk interface can function as the master or slave interface in a Smart Link group. Before configuring an Eth-Trunk interface as the master or slave interface in a Smart Link group, create the Eth-Trunk interface first. Otherwise, no Eth-Trunk interface is available when you run the **port** command in the Smart Link group view.

1.10 Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
STP	Spanning Tree Protocol
RRPP	Rapid Ring Protection Protocol
SMLK	Smart Link
SEP	Smart Ethernet Protection

Acronym and Abbreviation	Full Name
MTLK	Monitor Link