# Content

CHAPTER 1 PORT CONFIGURATION.....1-1

1.1 INTRODUCTION TO PORT.....1-1

1.2 NETWORK PORT CONFIGURATION TASK LIST.....1-1

1.3 PORT CONFIGURATION EXAMPLE.....1-3

1.4 PORT TROUBLESHOOTING.....1-4

CHAPTER 2 PORT ISOLATION FUNCTION CONFIGURATION .....2-1

2.1 INTRODUCTION TO PORT ISOLATION FUNCTION.....2-1

2.2 TASK SEQUENCE OF PORT ISOLATION.....2-1

2.3 PORT ISOLATION FUNCTION TYPICAL EXAMPLES.....2-2

CHAPTER 3 PORT LOOPBACK DETECTION FUNCTION CONFIGURATION.....3-1

3.1 INTRODUCTION TO PORT LOOPBACK DETECTION FUNCTION.....3-1

3.2 PORT LOOPBACK DETECTION FUNCTION CONFIGURATION TASK LIST.....3-2

3.3 PORT LOOPBACK DETECTION FUNCTION EXAMPLE.....3-3

3.4 PORT LOOPBACK DETECTION TROUBLESHOOTING.....3-4

CHAPTER 4 ULDP FUNCTION CONFIGURATION.....4-1

4.1 INTRODUCTION TO ULDP FUNCTION.....4-1

4.2 ULDP CONFIGURATION TASK SEQUENCE.....4-2

4.3 ULDP FUNCTION TYPICAL EXAMPLES.....4-5

4.4 ULDP TROUBLESHOOTING.....4-6

CHAPTER 5 LLDP FUNCTION OPERATION CONFIGURATION

.....5-1

5.1 INTRODUCTION TO LLDP FUNCTION .....5-1

5.2 LLDP FUNCTION CONFIGURATION TASK SEQUENCE .....5-2

5.3 LLDP FUNCTION TYPICAL EXAMPLE .....5-5

5.4 LLDP FUNCTION TROUBLESHOOTING .....5-6

CHAPTER 6 PORT CHANNEL CONFIGURATION .....6-1

6.1 INTRODUCTION TO PORT CHANNEL .....6-1

6.2 BRIEF INTRODUCTION TO LACP.....6-2

6.2.1 Static LACP Aggregation.....6-3

6.2.2 Dynamic LACP Aggregation .....6-3

6.3 PORT CHANNEL CONFIGURATION TASK LIST.....6-4

6.4 PORT CHANNEL EXAMPLES .....6-5

6.5 PORT CHANNEL TROUBLESHOOTING .....6-8

CHAPTER 7 MTU CONFIGURATION.....7-1

7.1 INTRODUCTION TO MTU.....7-1

7.2 MTU CONFIGURATION TASK SEQUENCE.....7-1

# Chapter 1 Port Configuration

**Explanation:**

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

## 1.1 Introduction to Port

Switch contains Cable ports and Combo ports. The Combo ports can be configured as either 1000GX-TX ports or SFP Gigabit fiber ports.

If the user needs to configure some network ports, he/she can use the interface ethernet <interface-list> command to enter the appropriate Ethernet port configuration mode, where <interface-list> stands for one or more ports. If <interface-list> contains multiple ports, special characters such as ';' or '-' can be used to separate ports, ';' is used for discrete port numbers and '-' is used for consecutive port numbers. Suppose an operation should be performed on ports 2,3,4,5 the command would look like: interface ethernet 1/0/2-5. Port speed, duplex mode and traffic control can be configured under Ethernet Port Mode causing the performance of the corresponding network ports to change accordingly.

## 1.2 Network Port Configuration Task List

1. Enter the network port configuration mode
2. Configure the properties for the network ports
   (1) Configure combo mode for combo ports
   (2) Enable/Disable ports
   (3) Configure port names
   (4) Configure port cable types
   (5) Configure port speed and duplex mode
   (6) Configure bandwidth control
   (7) Configure traffic control
   (8) Enable/Disable port loopback function
   (9) Configure broadcast storm control function for the switch
   (10) Configure scan port mode
   (11) Configure rate-violation control of the port
   (12) Configure interval of port-rate-statistics

**1. Enter the Ethernet port configuration mode**

| Command | Explanation |
|---|---|
| Global Mode | |
| **interface ethernet <*interface-list*>** | Enters the network port configuration mode. |

**2. Configure the properties for the Ethernet ports**

| Command | Explanation |
|---|---|
| Port Mode | |
| **media-type {copper \| copper-preferred-auto \| fiber \| sfp-preferred-auto}** | Sets the combo port mode (combo ports only). |
| **shutdown**<br>**no shutdown** | Enables/Disables specified ports. |
| **description <string>**<br>**no description** | Specifies or cancels the name of specified ports. |
| **speed-duplex {auto [10 [100 [1000]] [auto \| full \| half []] \| force10-half \| force10-full \| force100-half \| force100-full \| force100-fx [module-type {auto-detected \| no-phy-integrated \| phy-integrated}] \| {{force1g-half \| force1g-full} [nonegotiate [master \| slave]]}\| force10g-full}**<br>**no speed-duplex** | Sets port speed and duplex mode of 100/1000Base-TX or 100Base-FX ports. The no format of this command restores the default setting, i.e., negotiates speed and duplex mode automatically. |
| **negotiation {on\|off}** | Enables/Disables the auto-negotiation function of 1000Base-FX ports. |
| **bandwidth control <*bandwidth*> [both \| receive \| transmit]**<br>**no bandwidth control** | Sets or cancels the bandwidth used for incoming/outgoing traffic for specified ports. |
| **flow control**<br>**no flow control** | Enables/Disables traffic control function for specified ports. |
| **loopback**<br>**no loopback** | Enables/Disables loopback test function for specified ports. |

| | |
|---|---|
| **strom-control {unicast \| broadcast \| multicast} <packets>** | Enables the storm control function for broadcasts, multicasts and unicasts with unknown destinations (short for broadcast), and sets the allowed broadcast packet number; the no format of this command disables the broadcast storm control function. |
| **port-scan-mode {interrupt \| poll}**<br>**no port-scan-mode** | Configure port-scan-mode as interrupt or poll mode, the no command restores the default port-scan-mode. |
| **rate-violation <200-2000000> [recovery <0-86400>]**<br>**no rate-violation** | Set the max packet reception rate of a port. If the rate of the received packet violates the packet reception rate, shut down this port and configure the recovery time, the default is 300s. The no command will disable the rate-violation function of a port. |
| Global Mode | |
| **port-rate-statistics interval <interval -value>** | Configure statistic interval time of port-rate-statistics. |

## 1.3 Port Configuration Example

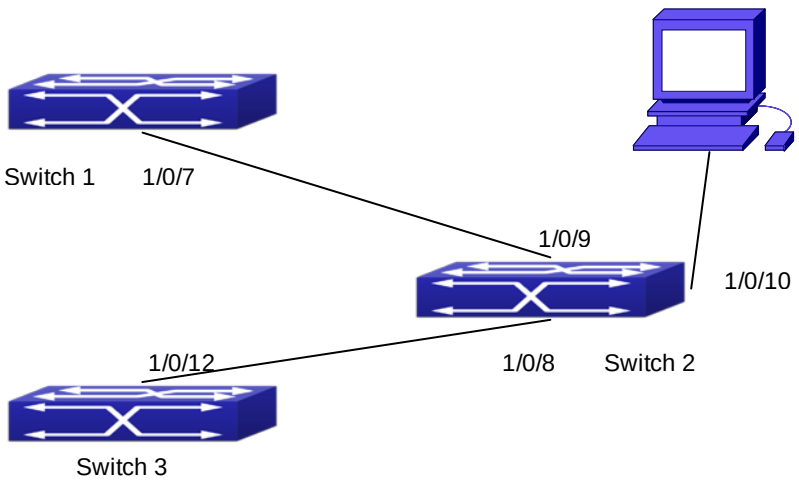


Fig 1-1 Port Configuration Example

No VLAN has been configured in the switches, default VLAN1 is used.

| Switch | Port | Property |
|---|---|---|
| Switch1 | 1/0/7 | Ingress bandwidth limit: 50 M |

| | | |
|---|---|---|
| Switch2 | 1/0/8 | Mirror source port |
| | 1/0/9 | 100Mbps full, mirror source port |
| | 1/0/10 | 1000Mbps full, mirror destination port |
| Switch3 | 1/0/12 | 100Mbps full |

The configurations are listed below:

**Switch1:**

Switch1(config)#interface ethernet 1/0/7

Switch1(Config-If-Ethernet1/0/7)#bandwidth control 50000 both

**Switch2:**

Switch2(config)#interface ethernet 1/0/9

Switch2(Config-If-Ethernet1/0/9)#speed-duplex force100-full

Switch2(Config-If-Ethernet1/0/9)#exit

Switch2(config)#interface ethernet 1/0/10

Switch2(Config-If-Ethernet1/0/10)#speed-duplex force1g-full

Switch2(Config-If-Ethernet1/0/10)#exit

Switch2(config)#monitor session 1 source interface ethernet 1/0/8;1/0/9

Switch2(config)#monitor session 1 destination interface ethernet 1/0/10

**Switch3:**

Switch3(config)#interface ethernet 1/0/12

Switch3(Config-If-Ethernet1/0/12)#speed-duplex force100-full

Switch3(Config-If-Ethernet1/0/12)#exit

# 1.4 Port Troubleshooting

Here are some situations that frequently occurs in port configuration and the advised solutions:

- ☞ Two connected fiber interfaces won't link up if one interface is set to auto-negotiation but the other to forced speed/duplex. This is determined by IEEE 802.3.
- ☞ The following combinations are not recommended: enabling traffic control as well as setting multicast limiting for the same port; setting broadcast, multicast and unknown destination unicast control as well as port bandwidth limiting for the same port. If such combinations are set, the port throughput may fall below the expected performance.

# Chapter 2 Port Isolation Function Configuration

## 2.1 Introduction to Port Isolation Function

Port isolation is an independent port-based function working in an inter-port way, which isolates flows of different ports from each other. With the help of port isolation, users can isolate ports within a VLAN to save VLAN resources and enhance network security. After this function is configured, the ports in a port isolation group will be isolated from each other, while ports belonging to different isolation groups or no such group can forward data to one another normally. No more than 16 port isolation groups can a switch have.

## 2.2 Task Sequence of Port Isolation

1. Create an isolate port group
2. Add Ethernet ports into the group
3. Specify the flow to be isolated
4. Display the configuration of port isolation

**1. Create an isolate port group**

| Command | Explanation |
|---|---|
| Global Mode | |
| **isolate-port group *<WORD>***<br>**no isolate-port group *<WORD>*** | Set a port isolation group; the no operation of this command will delete the port isolation group. |

**2. Add Ethernet ports into the group**

| Command | Explanation |
|---|---|
| Global Mode | |
| **isolate-port group *<WORD>* switchport interface [ethernet] *<IFNAME>***<br>**no isolate-port group *<WORD>* switchport interface [ethernet]** | Add one port or a group of ports into a port isolation group to isolate, which will become isolated from the other ports in the group; the no operation of this command will |

| | |
|---|---|
| ***<IFNAME>*** | remove one port or a group of ports out of a port isolation group. |

**3. Specify the flow to be isolated**

| Command | Explanation |
|---|---|
| Global Mode | |
| **isolate-port apply [<l2\|l3\|all>]** | Apply the port isolation configuration to isolate layer-2 flows, layer-3 flows or all flows. |

**4. Display the configuration of port isolation**

| Command | Explanation |
|---|---|
| Admin Mode and global Mode | |
| **show isolate-port group [ *<WORD>* ]** | Display the configuration of port isolation, including all configured port isolation groups and Ethernet ports in each group. |

## 2.3 Port Isolation Function Typical Examples

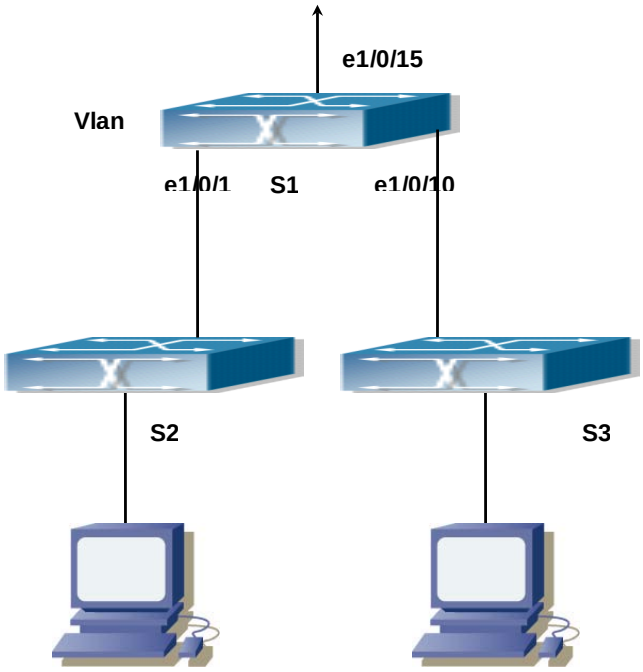


Fig 2-1 Typical example of port isolation function

The topology and configuration of switches are showed in the figure above, with e1/0/1, e1/0/10 and e1/0/15 all belonging to VLAN 100. The requirement is that, after port isolation is enabled on switch S1, e1/0/1 and e1/0/10 on switch S1 can not communicate with each other, while both of them can communicate with the uplink port e1/0/15. That is, the communication between any pair of downlink ports is disabled while that between any downlink port and a specified uplink port is normal. The uplink port can communicate with any port normally.

The configuration of S1:

Switch(config)#isolate-port group test

Switch(config)#isolate-port group test switchport interface ethernet 1/0/1;1/0/10

# Chapter 3 Port Loopback Detection Function Configuration

## 3.1 Introduction to Port Loopback Detection Function

With the development of switches, more and more users begin to access the network through Ethernet switches. In enterprise network, users access the network through layer-2 switches, which means urgent demands for both internet and the internal layer 2 Interworking. When layer 2 Interworking is required, the messages will be forwarded through MAC addressing the accuracy of which is the key to a correct Interworking between users. In layer 2 switching, the messages are forwarded through MAC addressing. Layer 2 devices learn MAC addresses via learning source MAC address, that is, when the port receives a message from an unknown source MAC address, it will add this MAC to the receive port, so that the following messages with a destination of this MAC can be forwarded directly, which also means learn the MAC address once and for all to forward messages.

When a new source MAC is already learnt by the layer 2 device, only with a different source port, the original source port will be modified to the new one, which means to correspond the original MAC address with the new port. As a result, if there is any loopback existing in the link, all MAC addresses within the whole layer 2 network will be corresponded with the port where the loopback appears (usually the MAC address will be frequently shifted from one port to another ), causing the layer 2 network collapsed. That is why it is a necessity to check port loopbacks in the network. When a loopback is detected, the detecting device should send alarms to the network management system, ensuring the network manager is able to discover, locate and solve the problem in the network and protect users from a long-lasting disconnected network.

Since detecting loopbacks can make dynamic judgment of the existence of loopbacks in the link and tell whether it has gone, the devices supporting port control (such as port isolation and port MAC address learning control) can maintain that automatically, which will not only reduce the burden of network managers but also response time, minimizing the effect caused loopbacks to the network.

# 3.2 Port Loopback Detection Function Configuration

# Task List

1. Configure the time interval of loopback detection
2. Enable the function of port loopback detection
3. Configure the control method of port loopback detection
4. Display and debug the relevant information of port loopback detection
5. Configure the loopback-detection control mode (automatic recovery enabled or not)

**1. Configure the time interval of loopback detection**

| Command | Explanation |
|---|---|
| Global Mode | |
| **loopback-detection interval-time <*loopback*> <*no-loopback*>**<br>**no loopback-detection interval-time** | Configure the time interval of loopback detection. |

**2. Enable the function of port loopback detection**

| Command | Explanation |
|---|---|
| Port Mode | |
| **loopback-detection specified-vlan <vlan-*list*>**<br>**no loopback-detection specified-vlan <vlan-*list*>** | Enable and disable the function of port loopback detection. |

**3. Configure the control method of port loopback detection**

| Command | Explanation |
|---|---|
| Port Mode | |
| **loopback-detection control {shutdown \|block\| learning}**<br>**no loopback-detection control** | Enable and disable the function of port loopback detection control. |

**4. Display and debug the relevant information of port loopback detection**

| Command | Explanation |
|---|---|
| Admin Mode | |

| | |
|---|---|
| **debug loopback-detection**<br>**no debug loopback-detection** | Enable the debug information of the function module of port loopback detection. The no operation of this command will disable the debug information. |
| **show loopback-detection [interface <*interface-list*>]** | Display the state and result of the loopback detection of all ports, if no parameter is provided; otherwise, display the state and result of the corresponding ports. |

**5. Configure the loopback-detection control mode (automatic recovery enabled or not)**

| Command | Explanation |
|---|---|
| Global Mode | |
| **loopback-detection control-recovery timeout <0-3600>** | Configure the loopback-detection control mode (automatic recovery enabled or not) or recovery time. |

## 3.3 Port Loopback Detection Function Example


Fig 3-1 Typical example of port loopback detection

As shown in the above configuration, the switch will detect the existence of loopbacks in the network topology. After enabling the function of loopback detection on the port

connecting the switch with the outside network, the switch will notify the connected network about the existence of a loopback, and control the port on the switch to guarantee the normal operation of the whole network.

The configuration task sequence of SWITCH:

Switch(config)#loopback-detection interval-time 35 15

Switch(config)#interface ethernet 1/0/1

Switch(Config-If-Ethernet1/0/1)#loopback-detection special-vlan 1-3

Switch(Config-If-Ethernet1/0/1)#loopback-detection control block

If adopting the control method of block, MSTP should be globally enabled. And the corresponding relation between the spanning tree instance and the VLAN should be configured.

Switch(config)#spanning-tree

Switch(config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1

Switch(Config-Mstp-Region)#instance 2 vlan 2

Switch(Config-Mstp-Region)#

## 3.4 Port Loopback Detection Troubleshooting

The function of port loopback detection is disabled by default and should only be enabled if required.

# Chapter 4 ULDP Function Configuration

## 4.1 Introduction to ULDP Function

Unidirectional link is a common error state of link in networks, especially in fiber links. Unidirectional link means that only one port of the link can receive messages from the other port, while the latter one can not receive messages from the former one. Since the physical layer of the link is connected and works normal, via the checking mechanism of the physical layer, communication problems between the devices can not be found. As shown in Graph, the problem in fiber connection can not be found through mechanisms in physical layer like automatic negotiation.

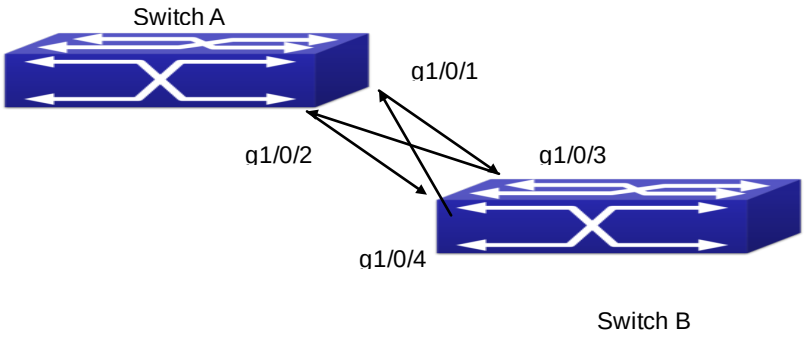


Fig 4-1 Fiber Cross Connection

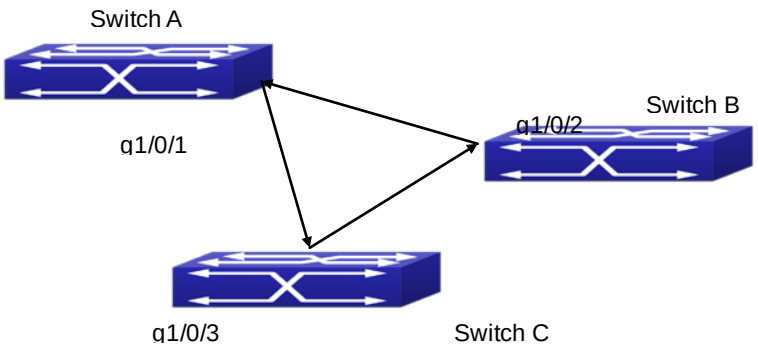

Fig 4-2 One End of Each Fiber Not Connected

This kind of problem often appears in the following situations: GBIC (Giga Bitrate Interface Converter) or interfaces have problems, software problems, hardware becomes unavailable or operates abnormally. Unidirectional link will cause a series of problems, such as spinning tree topological loop, broadcast black hole.

ULDP (Unidirectional Link Detection Protocol) can help avoid disasters that could happen in the situations mentioned above. In a switch connected via fibers or copper Ethernet line (like ultra five-kind twisted pair), ULDP can monitor the link state of physical links. Whenever a unidirectional link is discovered, it will send warnings to users and can disable the port automatically or manually according to users' configuration.

The ULDP of switches recognizes remote devices and check the correctness of link connections via interacting ULDP messages. When ULDP is enabled on a port, protocol state machine will be started, which means different types of messages will be sent at different states of the state machine to check the connection state of the link by exchanging information with remote devices. ULDP can dynamically study the interval at which the remote device sends notification messages and adjust the local TTL (time to live) according to that interval. Besides, ULDP provides the reset mechanism, when the port is disabled by ULDP, it can check again through reset mechanism. The time intervals of notification messages and reset in ULDP can be configured by users, so that ULDP can respond faster to connection errors in different network environments.

The premise of ULDP working normally is that link works in duplex mode, which means ULDP is enabled on both ends of the link, using the same method of authentication and password.

## 4.2 ULDP Configuration Task Sequence

1. Enable ULDP function globally
2. Enable ULDP function on a port
3. Configure aggressive mode globally
4. Configure aggressive mode on a port
5. Configure the method to shut down unidirectional link
6. Configure the interval of Hello messages
7. Configure the interval of Recovery
8. Reset the port shut down by ULDP
9. Display and debug the relative information of ULDP

**1. Enable ULDP function globally**

| Command | Explanation |
|---|---|

| | |
|---|---|
| Global configuration mode | |
| **uldp enable**<br>**uldp disable** | Globally enable or disable ULDP function. |

**2. Enable ULDP function on a port**

| Command | Explanation |
|---|---|
| Port configuration mode | |
| **uldp enable**<br>**uldp disable** | Enable or disable ULDP function on a port. |

**3. Configure aggressive mode globally**

| Command | Explanation |
|---|---|
| Global configuration mode | |
| **uldp aggressive-mode**<br>**no uldp aggressive-mode** | Set the global working mode. |

**4. Configure aggressive mode on a port**

| Command | Explanation |
|---|---|
| Port configuration mode | |
| **uldp aggressive-mode**<br>**no uldp aggressive-mode** | Set the working mode of the port. |

**5. Configure the method to shut down unidirectional link**

| Command | Explanation |
|---|---|
| Global configuration mode | |
| **uldp manual-shutdown**<br>**no uldp manual-shutdown** | Configure the method to shut down unidirectional link. |

**6. Configure the interval of Hello messages**

| Command | Explanation |
|---|---|
| Global configuration mode | |
| **uldp hello-interval <*integer*>**<br>**no uldp hello-interval** | Configure the interval of Hello messages, ranging from 5 to 100 seconds. The value is 10 seconds by default. |

**7. Configure the interval of Recovery**

| Command | Explanation |
|---|---|
| Global configuration mode | |

| | |
|---|---|
| **uldp recovery-time <*integer*>**<br>**no uldp recovery-time <*integer*>** | Configure the interval of Recovery reset, ranging from 30 to 86400 seconds. The value is 0 second by default. |

**8. Reset the port shut down by ULDP**

| Command | Explanation |
|---|---|
| Global configuration mode or port configuration mode | |
| **uldp reset** | Reset all ports in global configuration mode;<br>Reset the specified port in port configuration mode. |

**9. Display and debug the relative information of ULDP**

| Command | Explanation |
|---|---|
| Admin mode | |
| **show uldp [interface ethernet IFNAME]** | Display ULDP information. No parameter means to display global ULDP information. The parameter specifying a port will display global information and the neighbor information of the port. |
| **debug uldp fsm interface ethernet <*IFname*>**<br>**no debug uldp fsm interface ethernet <*IFname*>** | Enable or disable the debug switch of the state machine transition information on the specified port. |
| **debug uldp error**<br>**no debug uldp error** | Enable or disable the debug switch of error information. |
| **debug uldp event**<br>**no debug uldp event** | Enable or disable the debug switch of event information. |
| **debug uldp packet {receive\|send}**<br>**no debug uldp packet {receive\|send}** | Enable or disable the type of messages can be received and sent on all ports. |
| **debug uldp {hello\|probe\|echo\|unidir\|all} [receive\|send] interface ethernet <*IFname*>**<br>**no debug uldp {hello\|probe\|echo\|unidir\|all} [receive\|send] interface ethernet <*IFname*>** | Enable or disable the content detail of a particular type of messages can be received and sent on the specified port. |

## 4.3 ULDP Function Typical Examples

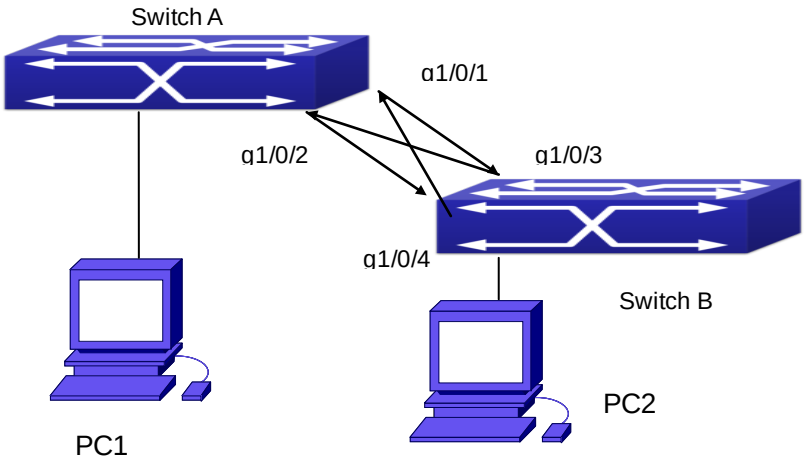


Fig 4-3 Fiber Cross Connection

In the network topology in Graph, port g1/0/1 and port g1/0/2 of SWITCH A as well as port g1/0/3 and port g1/0/4 of SWITCH B are all fiber ports. And the connection is cross connection. The physical layer is connected and works normally, but the data link layer is abnormal. ULDP can discover and disable this kind of error state of link. The final result is that port g1/0/1, g1/0/2 of SWITCH A and port g1/0/3, g1/0/4 of SWITCH B are all shut down by ULDP. Only when the connection is correct, can the ports work normally (won't be shut down).

Switch A configuration sequence:

SwitchA(config)#uldp enable

SwitchA(config)#interface ethernet 1/0/1

SwitchA(Config-If-Ethernet1/0/1)#uldp enable

SwitchA(Config-If-Ethernet1/0/1)#exit

SwitchA(config)#interface ethernet 1/0/2

SwitchA(Config-If-Ethernet1/0/2)#uldp enable

Switch B configuration sequence:

SwitchB(config)#uldp enable

SwitchB(config)#interface ethernet1/0/3

SwitchB(Config-If-Ethernet1/0/3)#uldp enable

SwitchB(Config-If-Ethernet1/0/3)#exit

SwitchB(config)#interface ethernet 1/0/4

SwitchB(Config-If-Ethernet1/0/4)#uldp enable

As a result, port g1/0/1, g1/0/2 of SWITCH A are all shut down by ULDP, and there is

notification information on the CRT terminal of PC1.

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/1 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/1 shut down!

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/2 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/2 shutted down!

Port g1/0/3, and port g1/0/4 of SWITCH B are all shut down by ULDP, and there is notification information on the CRT terminal of PC2.

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/3 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/3 shutted down!

%Oct 29 11:09:50 2007 A unidirectional link is detected! Port Ethernet1/0/4 need to be shutted down!

%Oct 29 11:09:50 2007 Unidirectional port Ethernet1/0/4 shutted down!

## 4.4 ULDP Troubleshooting

Configuration Notice:

- ☞ In order to ensure that ULDP can discover that the one of fiber ports has not connected or the ports are incorrectly cross connected, the ports have to work in duplex mode and have the same rate.
- ☞ If the automatic negotiation mechanism of the fiber ports with one port misconnected decides the working mode and rate of the ports, ULDP won't take effect no matter enabled or not. In such situation, the port is considered as "Down".
- ☞ In order to make sure that neighbors can be correctly created and unidirectional links can be correctly discovered, it is required that both end of the link should enable ULDP, using the same authentication method and password. At present, no password is needed on both ends.
- ☞ The hello interval of sending hello messages can be changed (it is10 seconds by default and ranges from 5 to 100 seconds) so that ULDP can respond faster to connection errors of links in different network environments. But this interval should be less than 1/3 of the STP convergence time. If the interval is too long, a STP loop will be generated before ULDP discovers and shuts down the unidirectional connection port. If the interval is too short, the network burden on the port will be increased, which means a reduced bandwidth.
- ☞ ULDP does not handle any LACP event. It treats every link of TRUNK group (like Port-channel, TRUNK ports) as independent, and handles each of them respectively.

- ULDP does not compact with similar protocols of other vendors, which means users can not use ULDP on one end and use other similar protocols on the other end.
- ULDP function is disabled by default. After globally enabling ULDP function, the debug switch can be enabled simultaneously to check the debug information. There are several DEBUG commands provided to print debug information, such as information of events, state machine, errors and messages. Different types of message information can also be printed according to different parameters.
- The Recovery timer is disabled by default and will only be enabled when the users have configured recovery time (30-86400 seconds).
- Reset command and reset mechanism can only reset the ports automatically shut down by ULDP. The ports shut down manually by users or by other modules won't be reset by ULDP.

# Chapter 5 LLDP Function Operation Configuration

## 5.1 Introduction to LLDP Function

Link Layer Discovery Protocol (LLDP) is a new protocol defined in 802.1ab. It enables neighbor devices to send notices of their own state to other devices, and enables all ports of every device to store information about them. If necessary, the ports can also send update information to the neighbor devices directly connected to them, and those neighbor devices will store the information in standard SNMP MIBs. The network management system can check the layer-two connection state from MIB. LLDP won't configure or control network elements or flows, but only report the configuration of layer-two. Another content of 802.1ab is to utilizing the information provided by LLDP to find the conflicts in layer-two. IEEE now uses the existing physical topology, interfaces and Entity MIBs of IETF.

To simplify, LLDP is a neighbor discovery protocol. It defines a standard method for Ethernet devices, such as switches, routers and WLAN access points, to enable them to notify their existence to other nodes in the network and store the discovery information of all neighbor devices. For example, the detail information of the device configuration and discovery can both use this protocol to advertise.

In specific, LLDP defines a general advertisement information set, a transportation advertisement protocol and a method to store the received advertisement information. The device to advertise its own information can put multiple pieces of advertisement information in one LAN data packet to transport. The type of transportation is the type length value (TLV) field. All devices supporting LLDP have to support device ID and port ID advertisement, but it is assumed that, most devices should also support system name, system description and system performance advertisement. System name and system description advertisement can also provide useful information for collecting network flow data. System description advertisement can include data such as the full name of the advertising device, hardware type of system, the version information of software operation system and so on.

802.1AB Link Layer Discovery Protocol will make searching the problems in an enterprise network an easier process and can strengthen the ability of network management tools to discover and maintain accurate network topology structure.

Many kinds of network management software use "Automated Discovery" function to

trace the change and condition of topology, but most of them can reach layer-three and classify the devices into all IP subnets at best. This kind of data are very primitive, only referring to basic events like the adding and removing of relative devices instead of details about where and how these devices operate with the network.

Layer 2 discovery covers information like which devices have which ports, which switches connect to other devices and so on, it can also display the routs between clients, switches, routers, application servers and network servers. Such details will be very meaningful for schedule and investigate the source of network failure.

LLDP will be a very useful management tool, providing accurate information about network mirroring, flow data and searching network problems.

## 5.2 LLDP Function Configuration Task Sequence

1. Globally enable LLDP function
2. Configure the port-based LLDP function switch
3. Configure the operating state of port LLDP
4. Configure the intervals of LLDP updating messages
5. Configure the aging time multiplier of LLDP messages
6. Configure the sending delay of updating messages
7. Configure the intervals of sending Trap messages
8. Configure to enable the Trap function of the port
9. Configure the optional information-sending attribute of the port
10. Configure the size of space to store Remote Table of the port
11. Configure the type of operation when the Remote Table of the port is full
12. Display and debug the relative information of LLDP

**1. Globally enable LLDP function**

| Command | Explanation |
|---|---|
| Global Mode | |
| **lldp enable**<br>**lldp disable** | Globally enable or disable LLDP function. |

**2. Configure the port-base LLDP function switch**

| Command | Explanation |
|---|---|
| Port Mode | |
| **lldp enable**<br>**lldp disable** | Configure the port-base LLDP function switch. |

**3. Configure the operating state of port LLDP**

| Command | Explanation |
|---|---|
| Port Mode | |
| **lldp mode (send\|receive\|both\|disable)** | Configure the operating state of port LLDP. |

**4. Configure the intervals of LLDP updating messages**

| Command | Explanation |
|---|---|
| Global Mode | |
| **lldp tx-interval <*integer*>**<br>**no lldp tx-interval** | Configure the intervals of LLDP updating messages as the specified value or default value. |

**5. Configure the aging time multiplier of LLDP messages**

| Command | Explanation |
|---|---|
| Global Mode | |
| **lldp msgTxHold <*value*>**<br>**no lldp msgTxHold** | Configure the aging time multiplier of LLDP messages as the specified value or default value. |

**6. Configure the sending delay of updating messages**

| Command | Explanation |
|---|---|
| Global Mode | |
| **lldp transmit delay <*seconds*>**<br>**no lldp transmit delay** | Configure the sending delay of updating messages as the specified value or default value. |

**7. Configure the intervals of sending Trap messages**

| Command | Explanation |
|---|---|
| Global Mode | |
| **lldp notification interval <*seconds*>**<br>**no lldp notification interval** | Configure the intervals of sending Trap messages as the specified value or default value. |

**8. Configure to enable the Trap function of the port**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |

| | |
|---|---|
| **lldp trap <*enable*\|*disable*>** | Enable or disable the Trap function of the port. |

**9. Configure the optional information-sending attribute of the port**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |
| **lldp transmit optional tlv [portDesc] [sysName] [sysDesc] [sysCap]**<br>**no lldp transmit optional tlv** | Configure the optional information-sending attribute of the port as the option value of default values. |

**10. Configure the size of space to store Remote Table of the port**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |
| **lldp neighbors max-num < *value* >**<br>**no lldp neighbors max-num** | Configure the size of space to store Remote Table of the port as the specified value or default value. |

**11. Configure the type of operation when the Remote Table of the port is full**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |
| **lldp tooManyNeighbors {discard \| delete}** | Configure the type of operation when the Remote Table of the port is full. |

**12. Display and debug the relative information of LLDP**

| Command | Explanation |
|---|---|
| Admin, Global Mode | |
| **show lldp** | Display the current LLDP configuration information. |
| **show lldp interface ethernet <*IFNAME*>** | Display the LLDP configuration information of the current port. |
| **show lldp traffic** | Display the information of all kinds of counters. |
| **show lldp neighbors interface ethernet < *IFNAME* >** | Display the information of LLDP neighbors of the current port. |
| **show debugging lldp** | Display all ports with LLDP debug enabled. |
| Admin Mode | |

| | |
|---|---|
| **debug lldp**<br>**no debug lldp** | Enable or disable the DEBUG switch. |
| **debug lldp packets interface ethernet** ***<IFNAME>***<br>**no debug lldp packets interface ethernet** ***<IFNAME>*** | Enable or disable the DEBUG packet-receiving and sending function in port or global mode. |
| Port configuration mode | |
| **clear lldp remote-table** | Clear Remote-table of the port. |

## 5.3 LLDP Function Typical Example

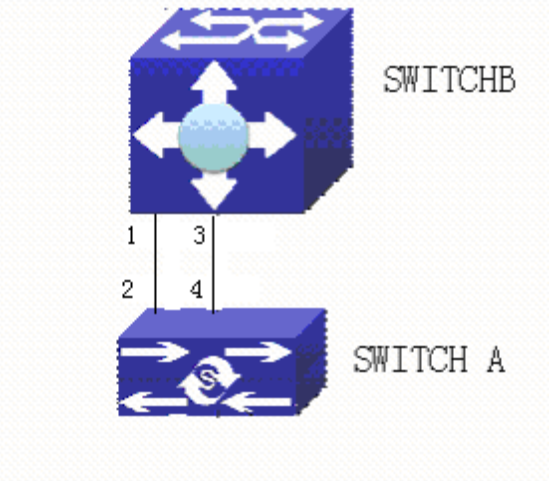


Fig 5-1 LLDP Function Typical Configuration Example

In the network topology graph above, the port 1,3 of SWITCH B are connected to port 2,4 of SWITCH A. Port 1 of SWITCH B is configured to message-receiving-only mode, Option TLV of port 4 of SWITCH A is configured as portDes and SysCap.

SWITCH A configuration task sequence:

SwitchA(config)# lldp enable

SwitchA(config)#interface ethernet 1/0/4

SwitchA(Config-If-Ethernet1/0/4)#lldp transmit optional tlv portDesc sysCap

SwitchA(Config-If-Ethernet1/0/4)exit

SWITCH B configuration task sequence:

SwitchB(config)#lldp enable

SwitchB(config)#interface ethernet1/0/1

SwitchB(Config-If-Ethernet1/0/1)#lldp mode receive

SwitchB(Config-If-Ethernet1/0/1)#exit

## 5.4 LLDP Function Troubleshooting

- LLDP function is disabled by default. After enabling the global switch of LLDP, users can enable the debug switch "**debug lldp**" simultaneously to check debug information.
- Using "show" function of LLDP function can display the configuration information in global or port configuration mode.

# Chapter 6 Port Channel Configuration

## 6.1 Introduction to Port Channel

To understand Port Channel, Port Group should be introduced first. Port Group is a group of physical ports in the configuration level; only physical ports in the Port Group can take part in link aggregation and become a member port of a Port Channel. Logically, Port Group is not a port but a port sequence. Under certain conditions, physical ports in a Port Group perform port aggregation to form a Port Channel that has all the properties of a logical port, therefore it becomes an independent logical port. Port aggregation is a process of logical abstraction to abstract a set of ports (port sequence) with the same properties to a logical port. Port Channel is a collection of physical ports and used logically as one physical port. Port Channel can be used as a normal port by the user, and can not only add network's bandwidth, but also provide link backup. Port aggregation is usually used when the switch is connected to routers, PCs or other switches.

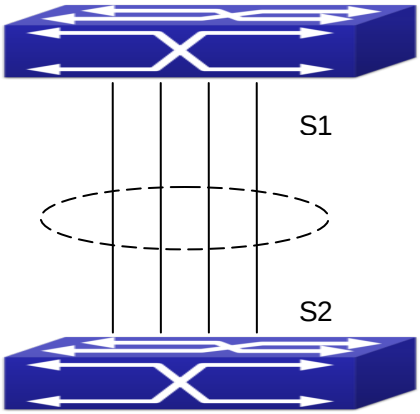


Fig 6-1 Port aggregation

As shown in the above, S1 is aggregated to a Port Channel, the bandwidth of this Port Channel is the total of all the four ports. If traffic from S1 needs to be transferred to S2 through the Port Channel, traffic allocation calculation will be performed based on the source MAC address and the lowest bit of target MAC address. The calculation result will decide which port to convey the traffic. If a port in Port Channel fails, the other ports will undertake traffic of that port through a traffic allocation algorithm. This algorithm is carried out by the hardware.

Switch offers two methods for configuring port aggregation: manual Port Channel creation and LACP (Link Aggregation Control Protocol) dynamic Port Channel creation.

Port aggregation can only be performed on ports in full-duplex mode.

For Port Channel to work properly, member ports of the Port Channel must have the same properties as follows:

- ☞ All ports are in full-duplex mode.
- ☞ All Ports are of the same speed.
- ☞ All ports are Access ports and belong to the same VLAN or are all TRUNK ports, or are all Hybrid ports.
- ☞ If the ports are all TRUNK ports or Hybrid ports, then their “Allowed VLAN” and “Native VLAN” property should also be the same.

If Port Channel is configured manually or dynamically on switch, the system will automatically set the port with the smallest number to be Master Port of the Port Channel. If the spanning tree function is enabled in the switch, the spanning tree protocol will regard Port Channel as a logical port and send BPDU frames via the master port.

Port aggregation is closely related with switch hardware. Switch allow physical port aggregation of any two switches, maximum 128 groups and 8 ports in each port group are supported.

Once ports are aggregated, they can be used as a normal port. Switch have a built-in aggregation interface configuration mode, the user can perform related configuration in this mode just like in the VLAN and physical interface configuration mode.

## 6.2 Brief Introduction to LACP

LACP (Link Aggregation Control Protocol) is a kind of protocol based on IEEE802.3ad standard to implement the link dynamic aggregation. LACP protocol uses LACPDU (Link Aggregation Control Protocol Data Unit) to exchange the information with the other end.

After LACP protocol of the port is enabled, this port will send LACPDU to the other end to notify the system priority, the MAC address of the system, the priority of the port, the port ID and the operation Key. After the other end receives the information, the information is compared with the saving information of other ports to select the port which can be aggregated, accordingly, both sides can reach an agreement about the ports join or exit the dynamic aggregation group.

The operation Key is created by LACP protocol according to the combination of configuration (speed, duplex, basic configuration, management Key) of the ports to be aggregated.

After the dynamic aggregation port enables LACP protocol, the management Key is 0 by default. After the static aggregation port enables LACP, the management Key of the port is the same with the ID of the aggregation group.

For the dynamic aggregation group, the members of the same group have the same operation Key, for the static aggregation group, the ports of Active have the same operation Key.

The port aggregation is that multi-ports are aggregated to form an aggregation group, so as to implement the out/in load balance in each member port of the aggregation group and provides the better reliability.

## 6.2.1 Static LACP Aggregation

Static LACP aggregation is enforced by users configuration, and do not enable LACP protocol. When configuring static LACP aggregation, use “on” mode to force the port to enter the aggregation group.

## 6.2.2 Dynamic LACP Aggregation

1. The summary of the dynamic LACP aggregation

Dynamic LACP aggregation is an aggregation created/deleted by the system automatically, it does not allow the user to add or delete the member ports of the dynamic LACP aggregation. The ports which have the same attribute of speed and duplex, are connected to the same device, have the same basic configuration, can be dynamically aggregated together. Even if only one port can create the dynamic aggregation, that is the single port aggregation. In the dynamic aggregation, LACP protocol of the port is at the enable state.

2. The port state of the dynamic aggregation group

In dynamic aggregation group, the ports have two states: selected or standby. Both selected ports and standby ports can receive and send LACP protocol, but standby ports can not forward the data packets.

Because the limitation of the max port number in the aggregation group, if the current number of the member ports exceeds the limitation of the max port number, then the system of this end will negotiates with the other end to decide the port state according to the port ID. The negotiation steps are as follows:

Compare ID of the devices (the priority of the system + the MAC address of the system). First, compare the priority of the systems, if they are same, then compare the MAC address of the systems. The end with a small device ID has the high priority.

Compare the ID of the ports (the priority of the port + the ID of the port). For each port in the side of the device which has the high device priority, first, compare the priority of the ports, if the priorities are same, then compare the ID of the ports. The port with a small port ID is selected, and the others become the standby ports.

In an aggregation group, the port which has the smallest port ID and is at the selected

state will be the master port, the other ports at the selected state will be the member port.

## 6.3 Port Channel Configuration Task List

1. Create a port group in Global Mode
2. Add ports to the specified group from the Port Mode of respective ports
3. Enter port-channel configuration mode
4. Set load-balance method for port-group
5. Set the system priority of LACP protocol
6. Set the port priority of the current port in LACP protocol
7. Set the timeout mode of the current port in LACP protocol

**1. Creating a port group**

| Command | Explanation |
|---|---|
| Global Mode | |
| **port-group <*port-group-number*>**<br>**no port-group <*port-group-number*>** | Create or delete a port group. |

**2. Add physical ports to the port group**

| Command | Explanation |
|---|---|
| Port Mode | |
| **port-group <*port-group-number*> mode {active \| passive \| on}**<br>**no port-group** | Add the ports to the port group and set their mode. |

**3. Enter port-channel configuration mode.**

| Command | Explanation |
|---|---|
| Global Mode | |
| **interface port-channel <*port-channel-number*>** | Enter port-channel configuration mode. |

**4. Set load-balance method for port-group**

| Command | Explanation |
|---|---|
| Aggregation port configuration mode | |
| **load-balance {src-mac \| dst-mac \| dst-src-mac \| src-ip \| dst-ip \| dst-src-ip}** | Set load-balance for port-group. |

**5. Set the system priority of LACP protocol**

| Command | Explanation |
|---|---|
| Global mode | |
| **lacp system-priority <*system-priority*>**<br>**no lacp system-priority** | Set the system priority of LACP protocol, the no command restores the default value. |

**6. Set the port priority of the current port in LACP protocol**

| Command | Explanation |
|---|---|
| Port mode | |
| **lacp port-priority <*port-priority*>**<br>**no lacp port-priority** | Set the port priority in LACP protocol. The no command restores the default value. |

**7. Set the timeout mode of the current port in LACP protocol**

| Command | Explanation |
|---|---|
| Port mode | |
| **lacp timeout {short \| long}**<br>**no lacp timeout** | Set the timeout mode in LACP protocol. The no command restores the default value. |

# 6.4 Port Channel Examples

Scenario 1: Configuring Port Channel in LACP.

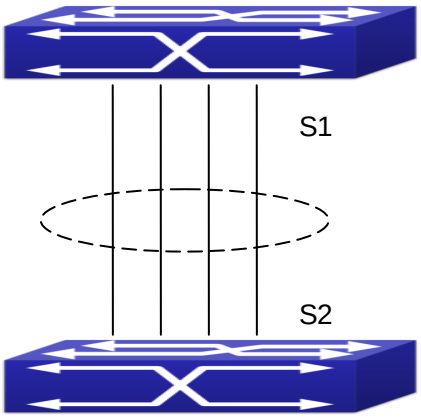

Fig 6-2 Configure Port Channel in LACP

The switches in the description below are all switch and as shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with active mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with passive mode. All the ports should be connected with cables.

**The configuration steps are listed below:**

Switch1#config
Switch1(config)#interface ethernet 1/0/1-4
Switch1(Config-If-Port-Range)#port-group 1 mode active
Switch1(Config-If-Port-Range)#exit
Switch1(config)#interface port-channel 1
Switch1(Config-If-Port-Channel1)#

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2(Config-If-Ethernet1/0/6)#port-group 2 mode passive
Switch2(Config-If-Ethernet1/0/6)#exit
Switch2(config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode passive
Switch2(Config-If-Port-Range)#exit
Switch2(config)#interface port-channel 2
Switch2(Config-If-Port-Channel2)#

**Configuration result:**

Shell prompts ports aggregated successfully after a while, now ports 1, 2, 3, 4 of S1 form an aggregated port named “Port-Channel1”, ports 6, 8, 9, 10 of S2 form an aggregated port named “Port-Channel2”; can be configured in their respective aggregated port mode.

Scenario 2: Configuring Port Channel in ON mode.

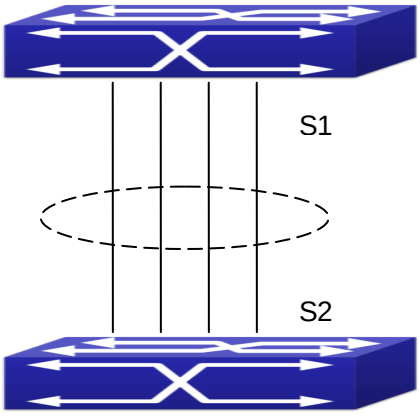


Fig 6-3 Configure Port Channel in ON mode

As shown in the figure, ports 1, 2, 3, 4 of S1 are access ports and add them to group1 with “on” mode. Ports 6, 8, 9, 10 of S2 are access ports and add them to group2 with “on” mode.

**The configuration steps are listed below:**

Switch1#config
Switch1(config)#interface ethernet 1/0/1
Switch1(Config-If-Ethernet1/0/1)#port-group 1 mode on
Switch1(Config-If-Ethernet1/0/1)#exit
Switch1(config)#interface ethernet 1/0/2
Switch1 (Config-If-Ethernet1/0/2)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/2)#exit
Switch1 (config)#interface ethernet 1/0/3
Switch1 (Config-If-Ethernet1/0/3)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/3)#exit
Switch1 (config)#interface ethernet 1/0/4
Switch1 (Config-If-Ethernet1/0/4)#port-group 1 mode on
Switch1 (Config-If-Ethernet1/0/4)#exit

Switch2#config
Switch2(config)#port-group 2
Switch2(config)#interface ethernet 1/0/6
Switch2 (Config-If-Ethernet1/0/6)#port-group 2 mode on
Switch2 (Config-If-Ethernet1/0/6)#exit
Switch2 (config)#interface ethernet 1/0/8-10
Switch2(Config-If-Port-Range)#port-group 2 mode on
Switch2(Config-If-Port-Range)#exit

**Configuration result:**

Add ports 1, 2, 3, 4 of S1 to port-group1 in order, and we can see a group in “on” mode is completely joined forcedly, switch in other ends won’t exchange LACP PDU to complete aggregation. Aggregation finishes immediately when the command to add port 1/0/2 to port-group 1 is entered, port 1 and port 2 aggregate to be port-channel 1, when port 1/0/3 joins port-group 1, port-channel 1 of port 1 and 2 are ungrouped and re-aggregate with port 3 to form port-channel 1, when port 1/0/4 joins port-group 1, port-channel 1 of port 1, 2 and 3 are ungrouped and re-aggregate with port 4 to form port-channel 1. (It should be noted that whenever a new port joins in an aggregated port group, the group will be ungrouped first and re-aggregated to form a new group.) Now all four ports in both S1 and S2 are aggregated in “on” mode and become an aggregated port respectively.

## 6.5 Port Channel Troubleshooting

If problems occur when configuring port aggregation, please first check the following for causes.

- ☞ Ensure all ports in a port group have the same properties, i.e., whether they are in full-duplex mode, forced to the same speed, and have the same VLAN properties, etc. If inconsistency occurs, make corrections.
- ☞ Some commands cannot be used on a port in port-channel, such as arp, bandwidth, ip, ip-forward, etc.

# Chapter 7 MTU Configuration

## 7.1 Introduction to MTU

So far the Jumbo (Jumbo Frame) has not reach a determined standard in the industry (including the format and length of the frame). Normally frames sized within 1519-9000 should be considered jumbo frame. Networks with jumbo frames will increase the speed of the whole network by 2% to 5%. Technically the Jumbo is just a lengthened frame sent and received by the switch. However considering the length of Jumbo frames, they will not be sent to CPU. We discard the Jumbo frames sent to CPU in the packet receiving process.

## 7.2 MTU Configuration Task Sequence

1. Configure enable MTU function

**1. Configure enable MTU function**

| Command | Explanation |
|---|---|
| Global Mode | |
| **mtu [<mtu-value>]**<br>**no mtu enable** | Enable the receiving/sending function of MTU frame. The no command disables sending and receiving function of MTU frames. |