TP-LINK®
The Reliable Choice

Configuration Guide

Managing Physical Interface

T Series Product

CONTENTS

1 Physical Interface

1.1 Overview

Interfaces of a device are used to exchange data and interact with other network devices. Interfaces are classified into physical interfaces and logical interfaces.

- Physical interfaces are the ports on the front panel or rear panel of the switch.
- Logical interfaces are manually configured and do not physically exist, such as loopback interfaces and routing interfaces.

This chapter introduces the configurations for physical interfaces.

1.2 Supported Features

The switch supports the following features about physical interfaces:

Basic Parameters

You can configure port status, speed mode, duplex mode, flow control and other basic parameters for ports.

Port Mirror

This function allows the switch to forward packet copies of the monitored ports to a specific monitoring port. Then you can analyze the copied packets to monitor network traffic and troubleshoot network problems.

Port Security

You can use this feature to limit the number of MAC addresses that can be learned on each port, thus preventing the MAC address table from being exhausted by the attack packets.

Port Isolation

You can use this feature to restrict a specific port to send packets to only the ports in the forward-port list that you configure.

Loopback Detection

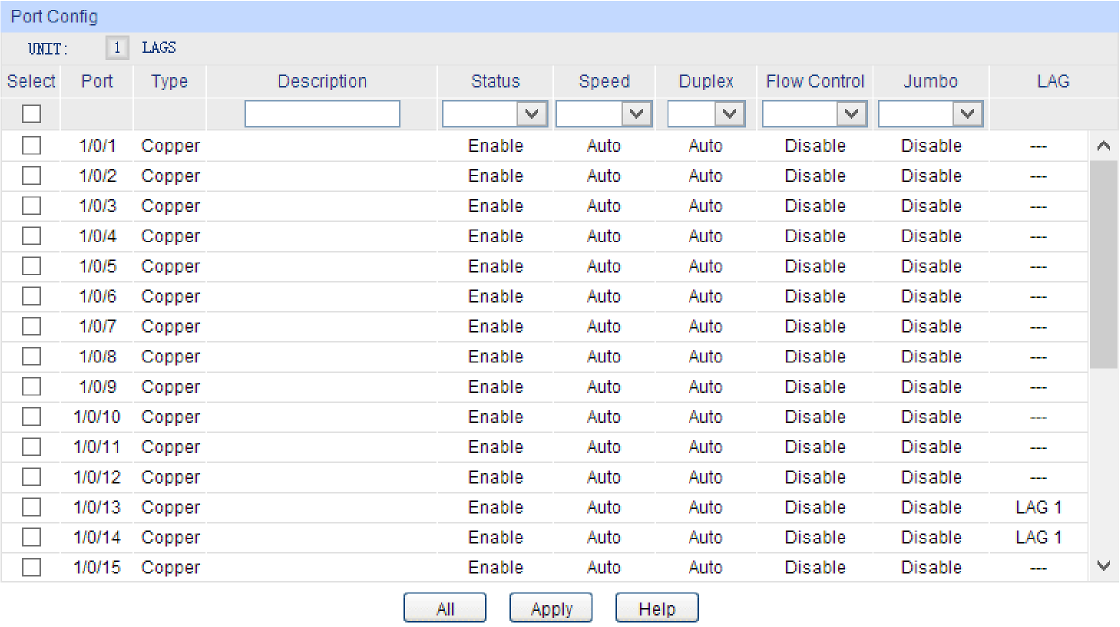
This function allows the switch to detect loops in the network. When a loop is detected on a port, the switch will display an alert on the management interface and further block the corresponding port according to your configurations.

2 Basic Parameters Configurations

2.1 Using the GUI

Choose the menu **Switching > Port > Port Config** to load the following page.

Figure 2-1 Configuring Basic Parameters



Port Config

UNIT: 1 LAGS

Select	Port	Type	Description	Status	Speed	Duplex	Flow Control	Jumbo	LAG
□									
□	1/0/1	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/2	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/3	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/4	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/5	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/6	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/7	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/8	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/9	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/10	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/11	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/12	Copper		Enable	Auto	Auto	Disable	Disable	---
□	1/0/13	Copper		Enable	Auto	Auto	Disable	Disable	LAG 1
□	1/0/14	Copper		Enable	Auto	Auto	Disable	Disable	LAG 1
□	1/0/15	Copper		Enable	Auto	Auto	Disable	Disable	---

Follow these steps to set basic parameters for ports:

Select and configure your desired ports or LAGs. Then click **Apply** to make the settings effective.

UNIT:1/LAGS:	Click **1** to configure physical ports. Click **LAGS** to configure LAGs.
Type:	Displays the port type. **Copper** indicates an Ethernet port, and **SFP** or **SFP+** indicates a fiber port.
Description:	Give a port description for identification.
Status:	With this option enabled, the port forwards packets normally. Otherwise, the port discards all the received packets. By default, it is enabled.
Speed:	Select the appropriate speed mode for the port. When **Auto** is selected, the port autonegotiates speed mode with the connected device. The default setting is **Auto**. This value is recommended if both ends of the line support auto-negotiation.
Duplex:	Select the appropriate duplex mode for the port. There are three options: **Half**, **Full** and **Auto**. When **Auto** is selected, the port autonegotiates duplex mode with the connected device. The default setting is **Auto**.
Flow Control:	With this option enabled, the switch synchronizes the data transmission speed with the peer device, thus avoiding the packet loss caused by congestion. By default, it is disabled.
Jumbo:	With this option enabled, the port can send jumbo frames. The default MTU (Maximum Transmission Unit) size for frames received and sent on all ports is 1518 bytes. For the port with Jumbo enabled, the MTU size is up to 9216 bytes, thus allowing the port to send jumbo frames. By default, it is disabled.

Note：

We recommend that you set the ports on both ends of a link as the same speed and duplex mode.

2.2 Using the CLI

Follow these steps to set basic parameters for the ports.

Step 1	**configure** Enter global configuration mode.
Step 2	**interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***]** Enter interface configuration mode.

Step 3

Configure basic parameters for the port:

description *string*

Give a port description for identification.

string: Content of a port description, ranging from 1 to 16 characters.

shutdown
no shutdown

Use **shutdown** to disable the port, and use **no shutdown** to enable the port. When the status is enabled, the port can forward packets normally, otherwise it will discard the received packets. By default, all ports are enabled.

speed { 10 | 100 | 1000 | 10000 | auto **}**

Set the appropriate speed mode for the port.

10 | 100 | 1000 | 10000 | auto: Speed mode of the port. The options are subject to your actual product. The device connected to the port should be in the same speed and duplex mode with the port. When auto is selected, the speed mode will be determined by auto negotiation.

duplex { auto | full | half **}**

Set the appropriate duplex mode for the port.

auto | full | half: Duplex mode of the port. The device connected to the port should be in the same speed and duplex mode with the port. When auto is selected, the duplex mode will be determined by auto negotiation.

flow-control

Enable the switch to synchronize the data transmission speed with the peer device, avoiding the packet loss caused by congestion. By default, this feature is disabled.

jumbo

Change the MTU (Maximum Transmission Unit) size on the port to support jumbo frames. The default MTU size for frames received and sent on all ports is 1518 bytes. For the port with Jumbo enabled, the MTU size is up to 9216 bytes, thus allowing the port to send jumbo frames.

Step 4

end

Return to privileged EXEC mode.

Step 5

copy running-config startup-config

Save the settings in the configuration file.

The following example shows how to implement the basic configurations of port1/0/1, including setting a description for the port, making the port autonegotiate speed and duplex with the neighboring port, and enabling the flow-control and jumbo feature:

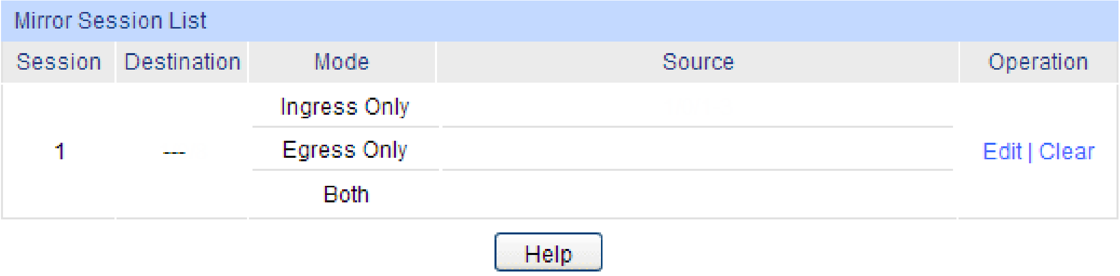
```
Switch#configure

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

Switch(config-if)#no shutdown
Switch(config-if)#description router connection

Switch(config-if)#speed auto

Switch(config-if)#duplex auto

Switch(config-if)#flow-control

Switch(config-if)#jumbo

Switch(config-if)#show interface configuration gigabitEthernet 1/0/1

Port      State     Speed   Duplex   FlowCtrl   Jumbo   Description

----      -----     -----   ------   --------   -----   -----------

Gi1/0/1   Enable    Auto    Auto     Enable     Enable  router connection

Switch(config-if)#end

Switch#copy running-config startup-config
```

3 Port Mirror Configurations

3.1 Using the GUI

Choose the menu **Switching** > **Port** > **Port Mirror** to load the following page.

Figure 3-1 Mirror Session List

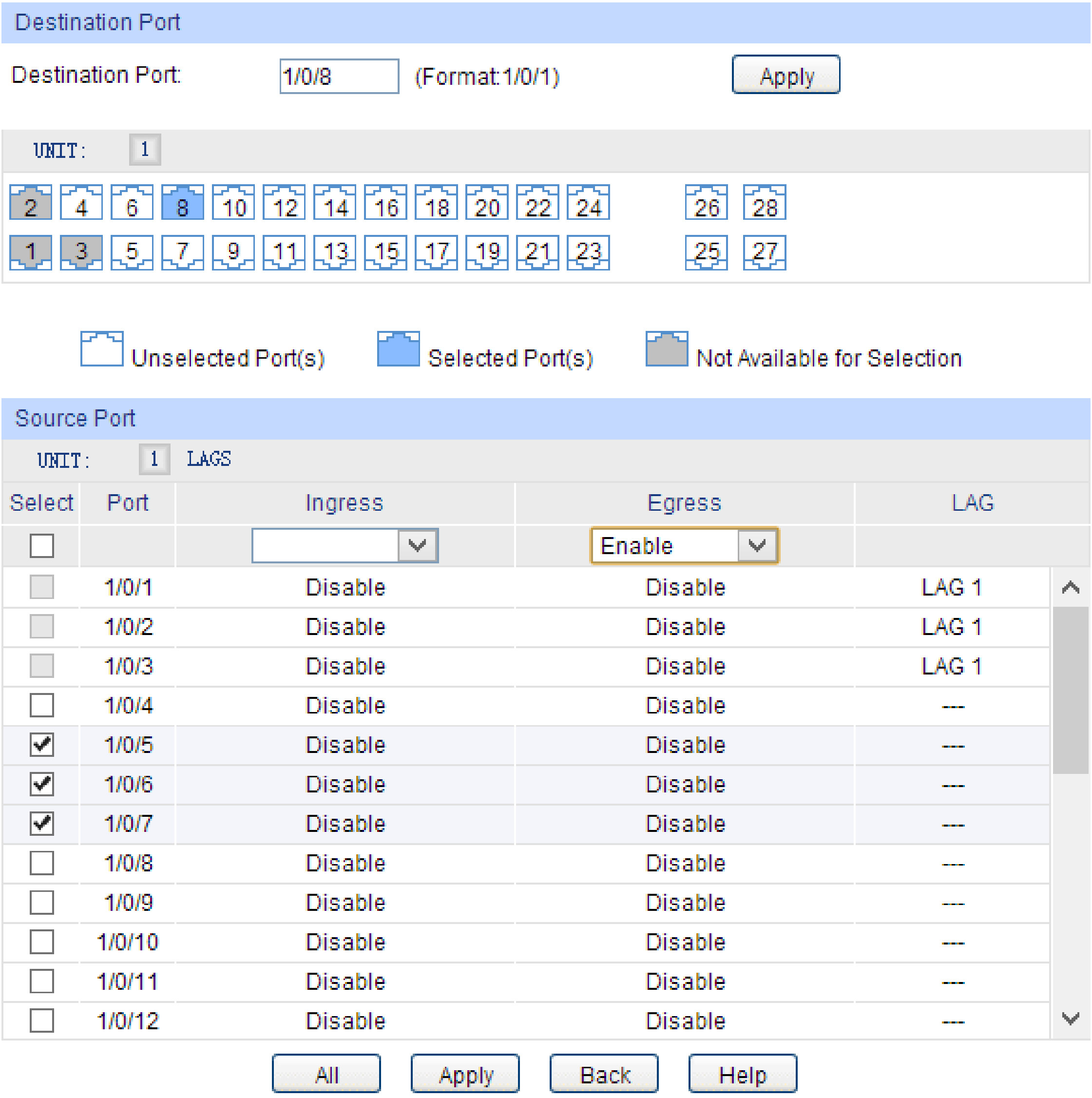


Mirror Session List

Session	Destination	Mode	Source	Operation
1	---	Ingress Only		Edit | Clear
		Egress Only		
		Both		

The above page displays a mirror session, and no more session can be created. Click **Edit** to configure this mirror session on the following page.

Figure 3-2 Configuring Port Mirror



Destination Port

Destination Port: 1/0/8 (Format:1/0/1)

Source Port

UNIT: 1 LAGS

Select	Port	Ingress	Egress	LAG
□			Enable	
□	1/0/1	Disable	Disable	LAG 1
□	1/0/2	Disable	Disable	LAG 1
□	1/0/3	Disable	Disable	LAG 1
□	1/0/4	Disable	Disable	---
☑	1/0/5	Disable	Disable	---
☑	1/0/6	Disable	Disable	---
☑	1/0/7	Disable	Disable	---
□	1/0/8	Disable	Disable	---
□	1/0/9	Disable	Disable	---
□	1/0/10	Disable	Disable	---
□	1/0/11	Disable	Disable	---
□	1/0/12	Disable	Disable	---

Follow these steps to configure Port Mirror:

1) In the **Destination Port** section, specify a monitoring port for the mirror session, and click **Apply**.

2) In the **Source Port** section, select one or multiple monitored ports for configuration. Then set the parameters and click **Apply** to make the settings effective.

UNIT:1/LAGS:	Click **1** to select physical ports. Click **LAGS** to select LAGs.
Ingress:	With this option enabled, the packets received by the monitored port will be copied to the monitoring port. By default, it is disabled.
Egress:	With this option enabled, the packets sent by the monitored port will be copied to the monitoring port. By default, it is disabled.

Note:

- The member port of an LAG cannot be set as a monitoring port or monitored port.
- A port cannot be set as the monitoring port and monitored port at the same time.

3.2 Using the CLI

Follow these steps to configure Port Mirror.

Step 1	**configure** Enter global configuration mode.
Step 2	**monitor session** *session_num* **destination interface { fastEthernet** *port* **| gigabitEthernet** *port* **| ten-gigabitEthernet** *port* **}** Enable the port mirror function and set the monitoring port. *session_num*: The monitor session number. It can only be specified as 1. *port*: The monitoring port number. You can specify only one monitoring port for the mirror session.
Step 3	**monitor session** *session_num* **source interface { fastEthernet** *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **| port-channel** *port-channel-id* **}** *mode* Set the monitored ports. *session_num*: The monitor session number. It can only be specified as 1. *port-list*: List of monitored port. It is multi-optional. *mode*: The monitor mode. There are three options: **rx**, **tx** and **both**: **rx**: The incoming packets of the monitored port will be copied to the monitoring port. **tx**: The outgoing packets of the monitored port will be copied to the monitoring port. **both**: Both of the incoming and outgoing packets on monitored port can be copied to the monitoring port.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to copy the received and transmitted packets on port 1/0/1,2,3 to port 1/0/10.

```
Switch#configure

Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/10

Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/1-3 both

Switch(config)#show monitor session

Monitor Session:        1

Destination Port:       Gi1/0/10
```

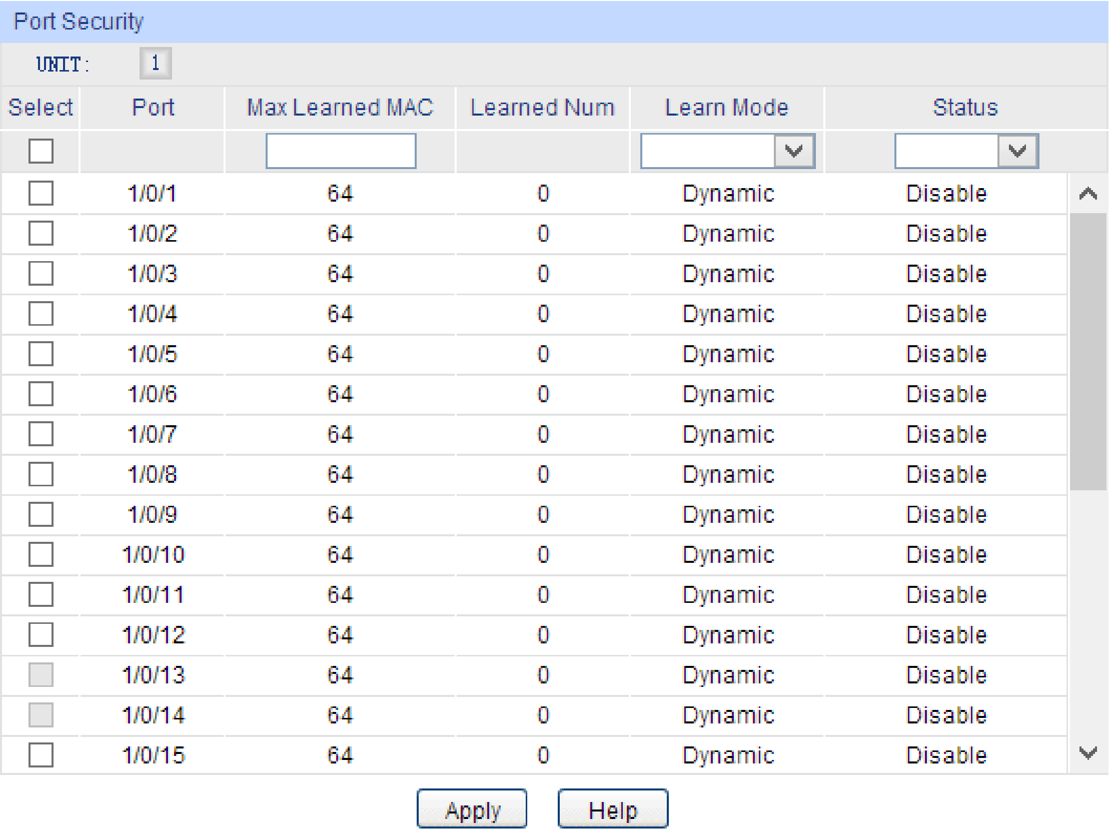
```
Source Ports(Ingress):   Gi1/0/1-3

Source Ports(Egress):    Gi1/0/1-3

Switch(config-if)#end

Switch#copy running-config startup-config
```

4 Port Security Configurations

4.1 Using the GUI

Choose the menu **Switching** > **Port** > **Port Security** to load the following page.

Figure 4-1 Port Security



Port Security

UNIT: 1

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
□					
□	1/0/1	64	0	Dynamic	Disable
□	1/0/2	64	0	Dynamic	Disable
□	1/0/3	64	0	Dynamic	Disable
□	1/0/4	64	0	Dynamic	Disable
□	1/0/5	64	0	Dynamic	Disable
□	1/0/6	64	0	Dynamic	Disable
□	1/0/7	64	0	Dynamic	Disable
□	1/0/8	64	0	Dynamic	Disable
□	1/0/9	64	0	Dynamic	Disable
□	1/0/10	64	0	Dynamic	Disable
□	1/0/11	64	0	Dynamic	Disable
□	1/0/12	64	0	Dynamic	Disable
□	1/0/13	64	0	Dynamic	Disable
□	1/0/14	64	0	Dynamic	Disable
□	1/0/15	64	0	Dynamic	Disable

Follow these steps to configure Port Security:

1) Select one or multiple ports for security configuration.

2) Specify the maximum number of the MAC addresses that can be learned on the port, and then select the learn mode of the MAC addresses.

Max Learned MAC: Specify the maximum number of MAC addresses that can be learned on the port. When the learned MAC address number reaches the limit, the port will stop learning. The default value is 64.

Learned Num: Displays the number of MAC addresses that have been learned on the port.

Learn Mode:

Select the learn mode of the MAC addresses on the port. Three modes are provided:

Dynamic: The switch will delete the MAC addresses that are not used or updated within the aging time. It is the default setting.

Static: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted.

Permanent: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted.

3) Select the status of the port security feature.

Status:

Select the status of Port Security. Three kinds of status can be selected:

Drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned.

Forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned.

Disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.

4) Click **Apply** to make the settings effective.

Note:

- Port Security cannot be enabled on the member port of a LAG, and the port with Port Security enabled cannot be added to a LAG.
- On one port, Port Security and 802.1X cannot be enabled at the same time.

4.2 Using the CLI

Follow these steps to configure Port Security:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***]** Enter interface configuration mode.

Step 3	**mac address-table max-mac-count { [max-number** *num***] [mode** { dynamic | static | permanent } **] [status** { forward | drop | disable } **] }** Enable the port security feature of the port and configure the related parameters. *num*: The maximum number of MAC addresses that can be learned on the port. It ranges from 0 to 64. The default value is 64. **mode**: Learn mode of the MAC address. There are three modes: dynamic: The switch will delete the MAC addresses that are not used or updated within the aging time. static: The learned MAC addresses are out of the influence of the aging time and can only be deleted manually. The learned entries will be cleared after the switch is rebooted. permanent: The learned MAC address is out of the influence of the aging time and can only be deleted manually. The learned entries will be saved even the switch is rebooted. **status**: Status of port security feature. By default, it is disabled. drop: When the number of learned MAC addresses reaches the limit, the port will stop learning and discard the packets with the MAC addresses that have not been learned. forward: When the number of learned MAC addresses reaches the limit, the port will stop learning but send the packets with the MAC addresses that have not been learned. disable: The number limit on the port is not effective, and the switch follows the original forwarding rules. It is the default setting.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the maximum number of MAC addresses that can be learned on port 1/0/1 as 30 and configure the mode as permanent and the status as drop:

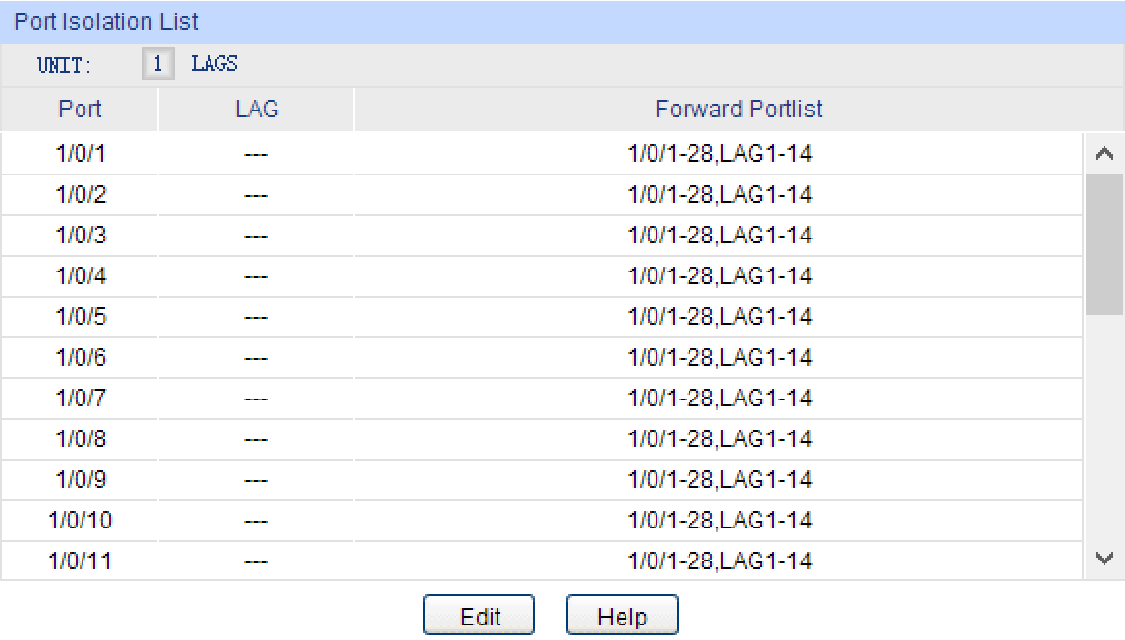
```
Switch#configure

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

Switch(config-if)#mac address-table max-mac-count max-number 30 mode permanent status drop

Switch(config-if)#show mac address-table max-mac-count interface gigabitEthernet 1/0/1

Port        Max-learn      Current-learn    Mode        Status

----        ---------      -----------      ------      ------

Gi1/0/1     30             0                permanent   drop

Switch(config-if)#end

Switch#copy running-config startup-config
```

5 Port Isolation Configurations

5.1 Using the GUI

Choose the menu **Switching** > **Port** > **Port Isolation** to load the following page.

Figure 5-1 Port Isolation List



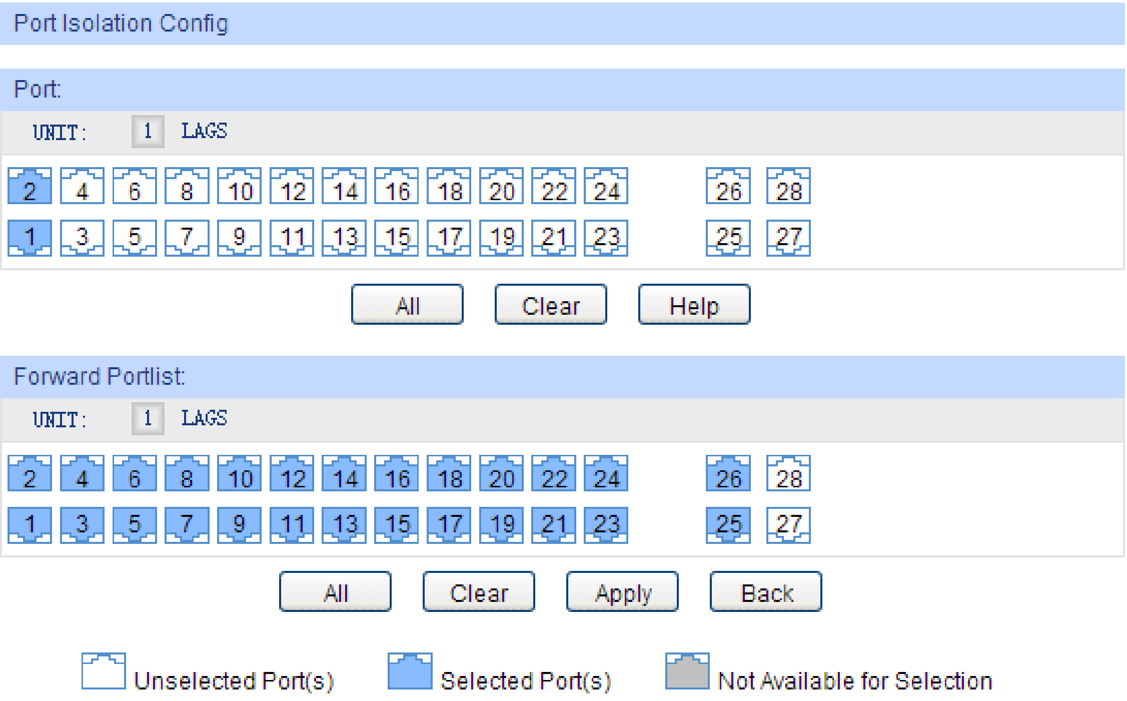
Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/1-28,LAG1-14
1/0/2	---	1/0/1-28,LAG1-14
1/0/3	---	1/0/1-28,LAG1-14
1/0/4	---	1/0/1-28,LAG1-14
1/0/5	---	1/0/1-28,LAG1-14
1/0/6	---	1/0/1-28,LAG1-14
1/0/7	---	1/0/1-28,LAG1-14
1/0/8	---	1/0/1-28,LAG1-14
1/0/9	---	1/0/1-28,LAG1-14
1/0/10	---	1/0/1-28,LAG1-14
1/0/11	---	1/0/1-28,LAG1-14

The above page displays the port isolation list. Click **Edit** to configure Port Isolation on the following page.

Figure 5-2 Port Isolation



Follow these steps to configure Port Isolation:

1) In the **Port** section, select one or multiple ports to be isolated.

2) In the **Forward Portlist** section, select the forward ports or LAGs which the isolated ports can only communicate with. It is multi-optional.

3) Click **Apply** to make the settings effective.

5.2 Using the CLI

Follow these steps to configure Port Isolation:

Step 1	**configure** Enter global configuration mode.
Step 2	**interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***]** Enter interface configuration mode.
Step 3	**port isolation { [fa-forward-list** *fa-forward-list* **] [gi-forward-list** *gi-forward-list***] [ten-gi-forward-list** *ten-gi-forward-list* **] [po-forward-list** *po-forward-list* **] }** Specify ports or LAGs to the forward list of the specific port which can only communicate with the forward ports or LAGs. It is multi-optional. *fa-forward-list/gi-forward-list/ten-gi-forward-list*: The list of Ethernet ports. *po-forward-list*: The list of LAGs.

Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to add ports 1/0/1-3 and LAG 4 to the forward list of port 1/0/5:

```
Switch#configure

Switch(config)#interface gigabitEthernet 1/0/5

Switch(config-if)#port isolation gi-forward-list 1/0/1-3 po-forward-list 4

Switch(config-if)#show port isolation interface gigabitEthernet 1/0/5

Port       LAG     Forward-List

----       ---     -----------------------

Gi1/0/5    N/A     Gi1/0/1-3,Po4

Switch(config-if)#end

Switch#copy running-config startup-config
```

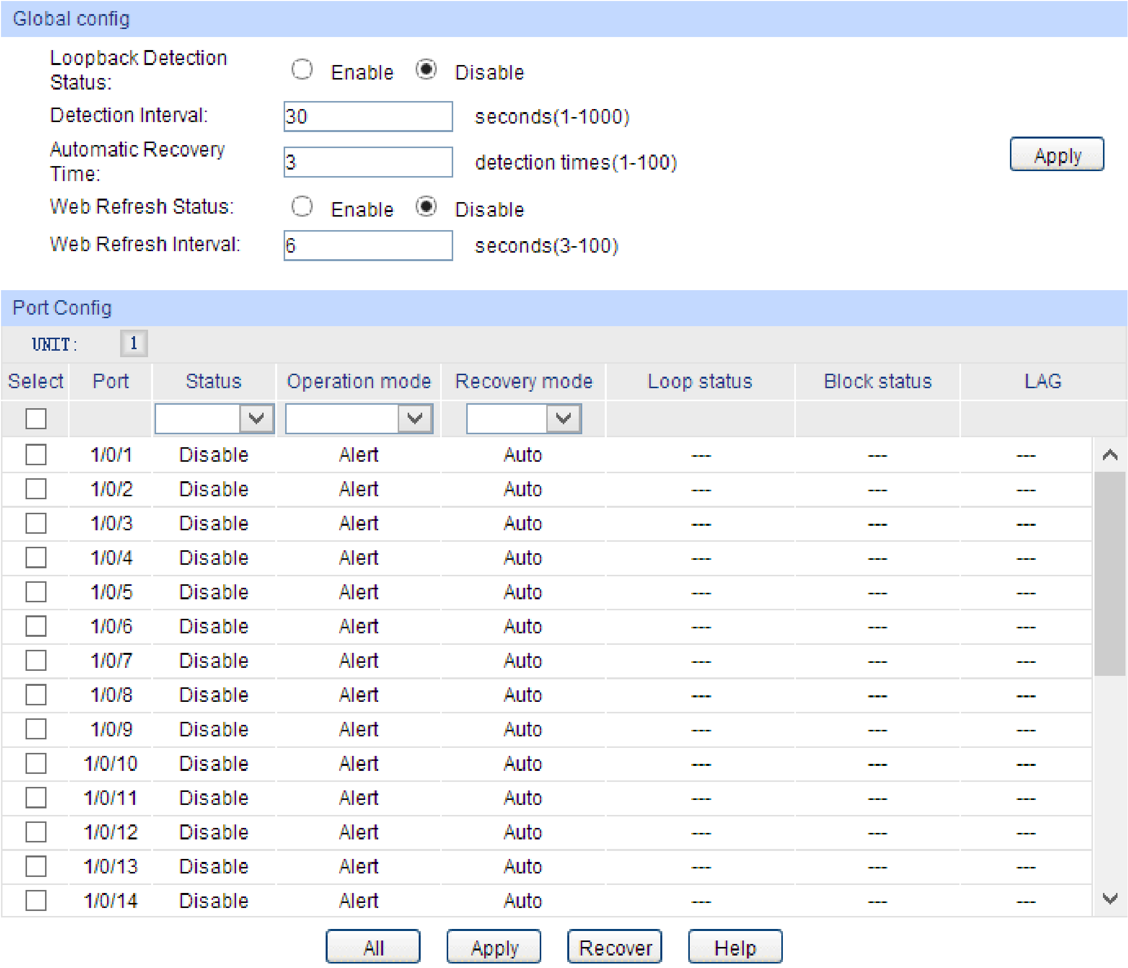
6 Loopback Detection Configurations

6.1 Using the GUI

To avoid broadcast storm, we recommend that you enable storm control before loopback detection is enabled. For detailed introductions about storm control, refer to *Managing QoS*.

Choose the menu **Switching > Port > Loopback Detection** to load the following page.

Figure 6-1 Loopback Detection



Global config

Loopback Detection Status: ○ Enable ● Disable

Detection Interval: 30 seconds(1-1000)

Automatic Recovery Time: 3 detection times(1-100)

Web Refresh Status: ○ Enable ● Disable

Web Refresh Interval: 6 seconds(3-100)

Port Config

UNIT: 1

Select	Port	Status	Operation mode	Recovery mode	Loop status	Block status	LAG
□							
□	1/0/1	Disable	Alert	Auto	---	---	---
□	1/0/2	Disable	Alert	Auto	---	---	---
□	1/0/3	Disable	Alert	Auto	---	---	---
□	1/0/4	Disable	Alert	Auto	---	---	---
□	1/0/5	Disable	Alert	Auto	---	---	---
□	1/0/6	Disable	Alert	Auto	---	---	---
□	1/0/7	Disable	Alert	Auto	---	---	---
□	1/0/8	Disable	Alert	Auto	---	---	---
□	1/0/9	Disable	Alert	Auto	---	---	---
□	1/0/10	Disable	Alert	Auto	---	---	---
□	1/0/11	Disable	Alert	Auto	---	---	---
□	1/0/12	Disable	Alert	Auto	---	---	---
□	1/0/13	Disable	Alert	Auto	---	---	---
□	1/0/14	Disable	Alert	Auto	---	---	---

Follow these steps to configure loopback detection:

1) In the **Global Config** section, enable loopback detection and configure the global parameters. Then click **Apply**.

Loopback Detection Status:	Enable loopback detection globally.
Detection Interval:	Set the interval of sending loopback detection packets. The value ranges from 1 to 1000 seconds and the default value is 30 seconds.
Automatic Recovery Time:	Set the recovery time globally, after which the blocked port in Auto Recovery mode can automatically recover to normal status. It should be integral times of detection interval. The value ranges from 1-100 and is 3 by default.
Web Refresh Status:	With this option enabled, the switch refreshes the web timely. By default, it is disabled.
Web Refresh Interval:	If you enabled web refresh, set the refresh interval between 3 and 100 seconds. The default value is 6 seconds.

2) In the **Port Config** section, select one or multiple ports for configuration. Then set the parameters and click **Apply** to make the settings effective.

Status:	Enable loopback detection for the port.
Operation Mode:	Select the operation mode when a loopback is detected on the port: **Alert**: The switch will display alerts. It is the default setting. **Port Based**: In addition to displaying alerts, the switch will block the port on which the loop is detected.
Recovery Mode:	If you select **Port Based** as the operation mode, you also need to configure the recovery mode for the blocked port: **Auto**: The blocked port will automatically recover to normal status after the automatic recovery time. It is the default setting. **Manual**: You need to manually release the blocked port. Click the **Recovery** button to release the selected port.

3) View the loopback detection information on this page.

Loop Status:	Displays whether a loop is detected on the port.
Block Status:	Displays whether the port is blocked.

6.2 Using the CLI

Follow these steps to configure Loopback Detection:

Step 1	**configure** Enter global configuration mode.
Step 2	**loopback-detection** Enable the loopback detection feature globally. By default, it is disabled.

Step 3	**loopback-detection interval** *interval-time* Set the interval of sending loopback detection packets which is used to detect the loops in the network. *interval-time*: The interval of sending loopback detection packets. It ranges from 1 to 1000 seconds. By default, the value is 30 seconds.
Step 4	**loopback-detection recovery-time** *recovery-time* Set the recovery time, after which the blocked port in Auto Recovery mode can automatically recover to normal status. *recovery-time*: It is integral times of detection interval, ranging from 1 to 100. The default value is 3.
Step 5	**interface [fastEthernet** *port* **| range fastEthernet** *port-list* **| gigabitEthernet** *port* **| range gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port* **| range ten-gigabitEthernet** *port-list***]** Enter interface configuration mode.
Step 6	**loopback-detection** Enable loopback detection of the port. By default, it is disabled.
Step 7	**loopback-detection config [process-mode {** alert | port-based **}] [recovery-mode {** auto | manual **}]** Set the process mode when a loopback is detected on the port. There are two modes: alert: The switch will only display alerts when a loopback is detected. It is the default setting. port-based: In addition to displaying alerts, the switch will block the port on which the loop is detected. Set the recovery mode for the blocked port. There are two modes: auto: After the recovery time, the blocked port will automatically recover to normal status and restart to detect loops in the network. manual: The blocked port can only be released manually. You can use the command 'loopback-detection recover' to recover the blocked port to normal status.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to enable loopback detection globally (keeping the default parameters):

```
Switch#configure

Switch(config)#loopback-detection

Switch(config)#show loopback-detection global

 Loopback detection global status : enable

 Loopback detection interval : 30 s
 Loopback detection recovery time : 3 intervals

Switch(config-if)#end

Switch#copy running-config startup-config
```

The following example shows how to enable loopback detection of port 1/0/3 and set the process mode as alert and recovery mode as auto:

```
Switch#configure

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode alert recovery-mode auto

Switch(config-if)#show loopback-detection interface gigabitEthernet 1/0/3

 Port      Enable    Process Mode     Recovery Mode     Loopback    Block    LAG

 ----      ------   ------------     -------------     --------    -----    ------

 Gi1/0/3   enable   alert            auto              N/A          N/A      N/A

Switch(config-if)#end

Switch#copy running-config startup-config
```

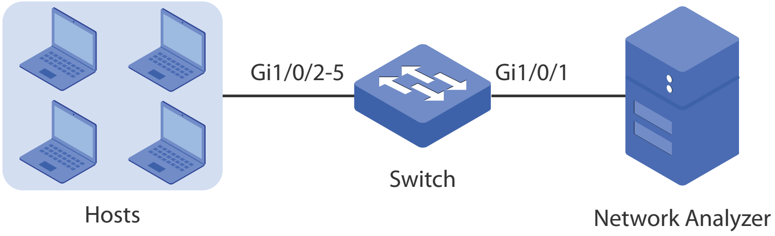
7 Configuration Examples

7.1 Example for Port Mirror

7.1.1 Network Requirements

As shown below, several hosts and a network analyzer are directly connected to the switch. For network security and troubleshooting, the network manager needs to use the network analyzer to monitor the data packets from the end hosts.

Figure 7-1 Network Topology



7.1.2 Configuration Scheme

To implement this requirement, you can configure port mirror to copy the packets from ports 1/0/2-5 to port 1/0/1. The overview of configuration is as follows:

1) Specify ports 1/0/2-5 as the source ports, allowing the switch to copy the packets from the hosts.

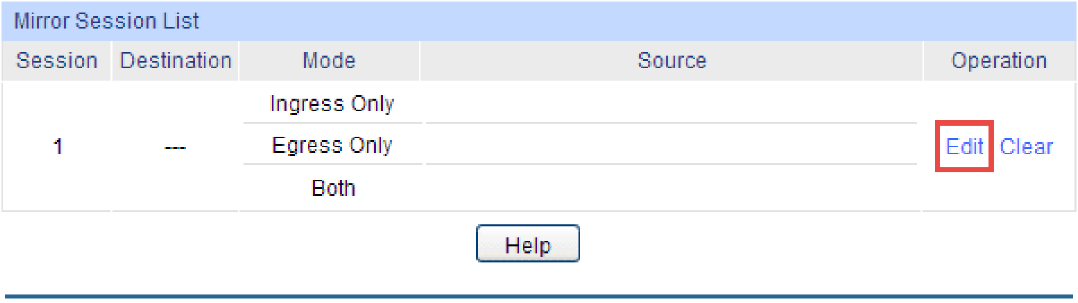
2) Specify port 1/0/1 as the destination port so that the network analyzer can receive mirrored packets from the hosts.

Exampled with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.1.3 Using the GUI

1) Choose the menu **Switching** > **Port** > **Port Mirror** to load the following page. It displays the information of the mirror session.

Figure 7-2 Mirror Session List

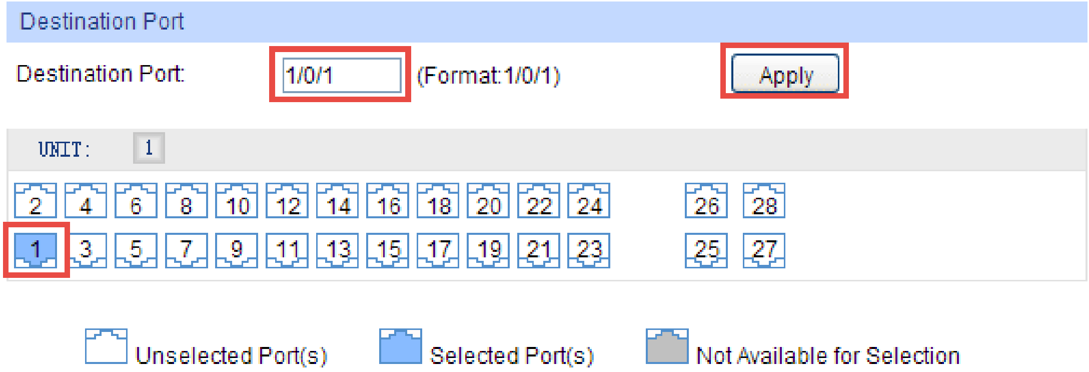


Mirror Session List

Session	Destination	Mode	Source	Operation
1	---	Ingress Only Egress Only Both		Edit Clear

2) Click **Edit** on the above page to load the following page. In the **Destination Port** section, select port 1/0/1 as the monitoring port and click **Apply**.

Figure 7-3 Destination Port Configuration

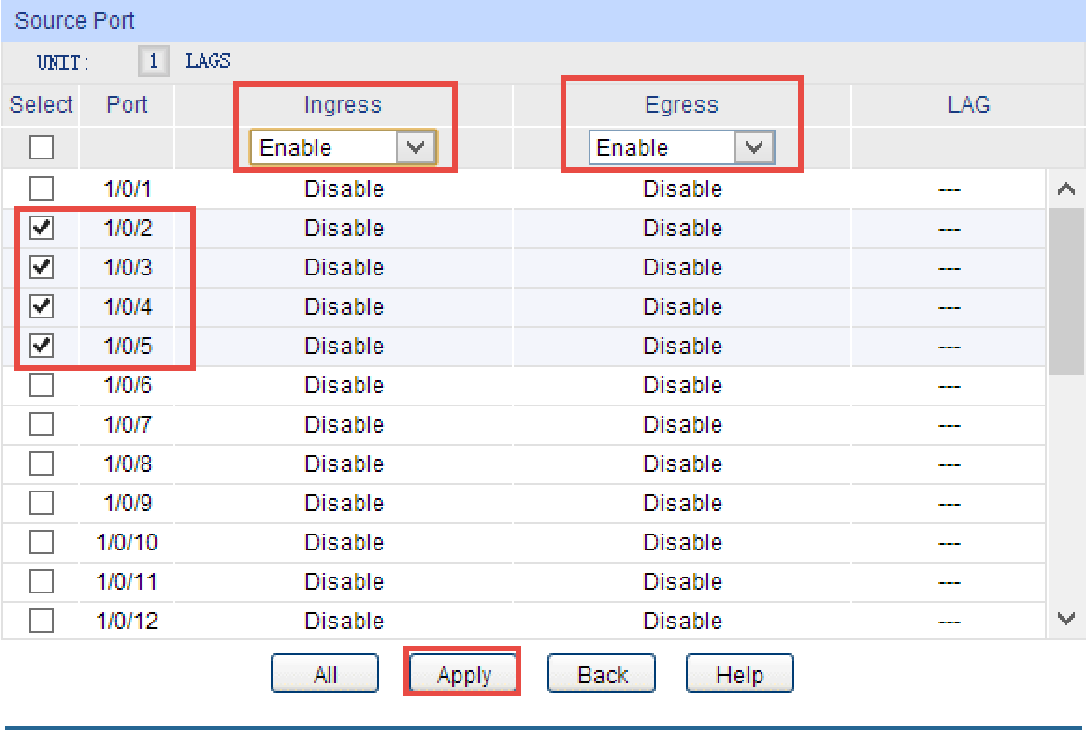


Destination Port

Destination Port: 1/0/1 (Format:1/0/1)

3) In the **Source Port** section, select ports 1/0/2-5 as the monitored ports, and enable **Ingress** and **Egress** to allow the received and sent packets to be copied to the monitoring port. Then click **Apply.**

Figure 7-4 Source Port Configuration



Source Port

UNIT: 1 LAGS

Select	Port	Ingress	Egress	LAG
□		Enable	Enable	
□	1/0/1	Disable	Disable	---
☑	1/0/2	Disable	Disable	---
☑	1/0/3	Disable	Disable	---
☑	1/0/4	Disable	Disable	---
☑	1/0/5	Disable	Disable	---
□	1/0/6	Disable	Disable	---
□	1/0/7	Disable	Disable	---
□	1/0/8	Disable	Disable	---
□	1/0/9	Disable	Disable	---
□	1/0/10	Disable	Disable	---
□	1/0/11	Disable	Disable	---
□	1/0/12	Disable	Disable	---

4) Click **Save Config** to make the settings effective.

7.1.4 Using the CLI

```
Switch#configure

Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/1

Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/2-5 both

Switch(config)#end

Switch#copy running-config startup-config
```

Verify the Configuration

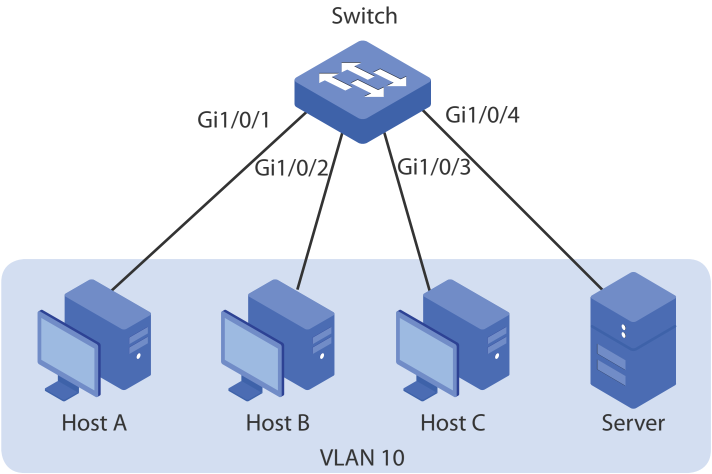
```
Switch#show monitor session 1

Monitor Session:          1

Destination Port:         Gi1/0/1

Source Ports(Ingress):   Gi1/0/2-5

Source Ports(Egress):    Gi1/0/2-5
```

7.2 Example for Port Isolation

7.2.1 Network Requirements

As shown below, three hosts and a server are connected to the switch and all belong to VLAN 10. With the VLAN configuration unchanged, Host A is not allowed to communicate with the other hosts except the server, even if the MAC address or IP address of Host A is changed.

Figure 7-5 Network Topology



7.2.2 Configuration Scheme

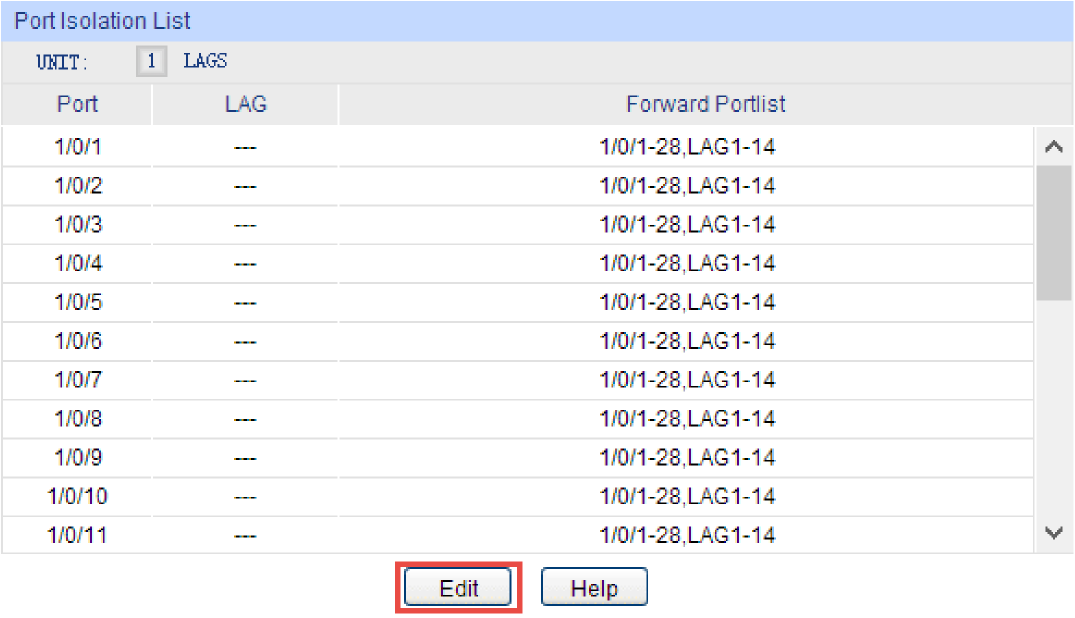
You can configure port isolation to implement the requirement. Set 1/0/4 as the only forwarding port for port 1/0/1, thus forbidding Host A to forward packets to the other hosts.

Exampled with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.2.3 Using the GUI

1) Choose the menu **Switching > Port > Port Isolation** to load the following page. It displays the port isolation list.

Figure 7-6 Port Isolation List



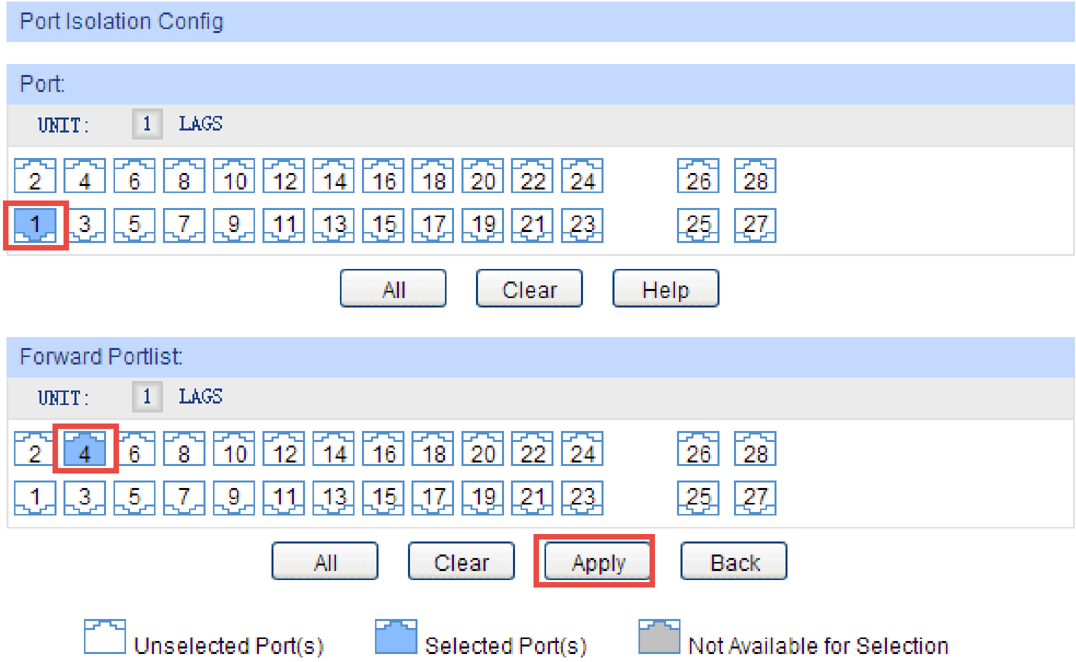
Port Isolation List

UNIT: 1 LAGS

Port	LAG	Forward Portlist
1/0/1	---	1/0/1-28,LAG1-14
1/0/2	---	1/0/1-28,LAG1-14
1/0/3	---	1/0/1-28,LAG1-14
1/0/4	---	1/0/1-28,LAG1-14
1/0/5	---	1/0/1-28,LAG1-14
1/0/6	---	1/0/1-28,LAG1-14
1/0/7	---	1/0/1-28,LAG1-14
1/0/8	---	1/0/1-28,LAG1-14
1/0/9	---	1/0/1-28,LAG1-14
1/0/10	---	1/0/1-28,LAG1-14
1/0/11	---	1/0/1-28,LAG1-14

2) Click **Edit** on the above page to load the following page. Select port 1/0/1 as the isolated port, and select port 1/0/4 as the forwarding port. Click **Apply**.

Figure 7-7 Port Isolation Configuration



Port Isolation Config

Port:

UNIT: 1 LAGS

Forward Portlist:

UNIT: 1 LAGS

□ Unselected Port(s) 🟦 Selected Port(s) ▨ Not Available for Selection

3) Click **Save Config** to make the settings effective.

7.2.4 Using the CLI

```
Switch#configure

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

Switch(config-if)#port isolation gi-forward-list 1/0/4

Switch(config-if)#end

Switch#copy running-config startup-config
```

Verify the Configuration

```
Switch#show port isolation interface

Port      LAG    Forward-List

----      ---    ------------

Gi1/0/1   N/A    Gi1/0/4

Gi1/0/2   N/A    Gi1/0/1-28,Po1-14

Gi1/0/3   N/A    Gi1/0/1-28,Po1-14

......
```

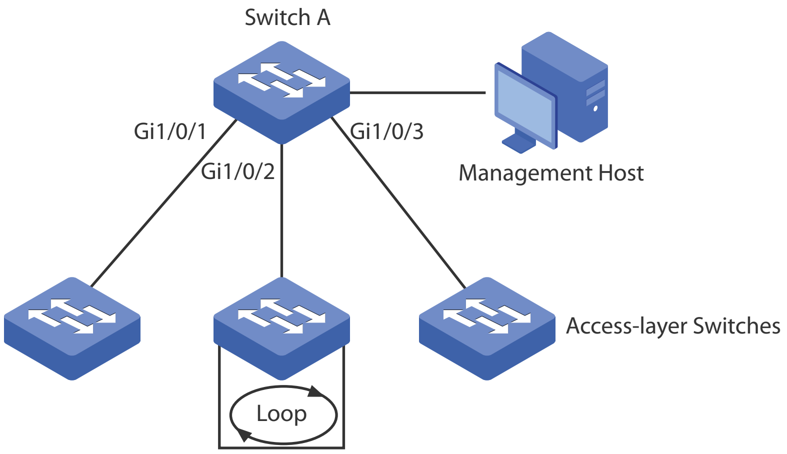
7.3 Example for Loopback Detection

7.3.1 Network Requirements

As shown below, Switch A is a convergence-layer switch connecting several access-layer switches. Loops can be easily caused in case of misoperation on the access-layer switches. If there is a loop on an access-layer switch, broadcast storms will occur on Switch A or even in the entire network, creating excessive traffic and degrading the network performance.

To reduce the impacts of broadcast storms, users need to detect loops in the network via Switch A and timely block the port on which a loop is detected.

Figure 7-8 Network Topology



7.3.2 Configuration Scheme

Enable loopback detection on ports 1/0/1-3 and configure SNMP to receive the notifications. For detailed instructions about SNMP, refer to *Managing SNMP*. Here we introduce how to configure loopback detection and monitor the detection result on the management interface of the switch.

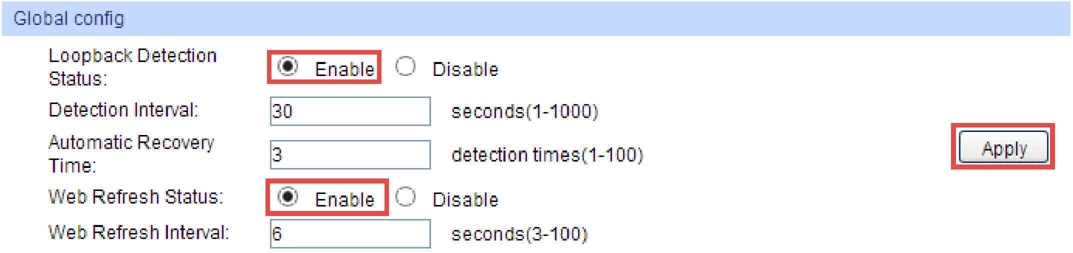
Exampled with T2600G-28TS, the following sections provide configuration procedure in two ways: using the GUI and using the CLI.

7.3.3 Using the GUI

1) Choose the menu **Switching** > **Port** > **Loopback Detection** to load the configuration page.

2) In the **Global Config** section, enable loopback detection and web refresh globally. Keep the default parameters and click **Apply**.

Figure 7-9 Global Configuration

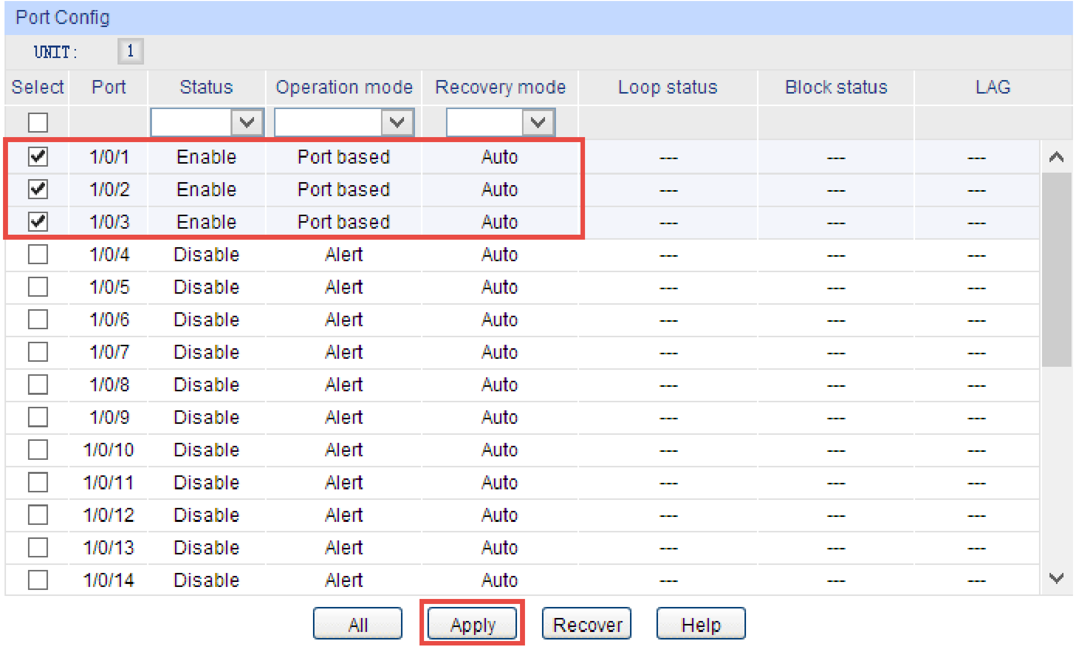


Global config

Loopback Detection Status:	● Enable ○ Disable	
Detection Interval:	30	seconds(1-1000)
Automatic Recovery Time:	3	detection times(1-100)
Web Refresh Status:	● Enable ○ Disable	
Web Refresh Interval:	6	seconds(3-100)

3) In the **Port Config** section, enable ports 1/0/1-3, select the operation mode as **Port based** so that the port will be blocked when a loop is detected, and keep the recovery mode as **Auto** so that the port will recover to normal status after the automatic recovery time. Click **Apply**.

Figure 7-10 Port Configuration



Port Config

UNIT: 1

Select	Port	Status	Operation mode	Recovery mode	Loop status	Block status	LAG
□							
☑	1/0/1	Enable	Port based	Auto	---	---	---
☑	1/0/2	Enable	Port based	Auto	---	---	---
☑	1/0/3	Enable	Port based	Auto	---	---	---
□	1/0/4	Disable	Alert	Auto	---	---	---
□	1/0/5	Disable	Alert	Auto	---	---	---
□	1/0/6	Disable	Alert	Auto	---	---	---
□	1/0/7	Disable	Alert	Auto	---	---	---
□	1/0/8	Disable	Alert	Auto	---	---	---
□	1/0/9	Disable	Alert	Auto	---	---	---
□	1/0/10	Disable	Alert	Auto	---	---	---
□	1/0/11	Disable	Alert	Auto	---	---	---
□	1/0/12	Disable	Alert	Auto	---	---	---
□	1/0/13	Disable	Alert	Auto	---	---	---
□	1/0/14	Disable	Alert	Auto	---	---	---

4) Monitor the detection result on the above page. The **Loop status** and **Block status** are displayed on the right side of ports.

7.3.4 Using the CLI

1) Enable loopback detection globally and configure the detection interval and recovery time.

```
Switch#configure

Switch(config)#loopback-detection

Switch(config)#loopback-detection interval 30

Switch(config)#loopback-detection recovery-time 3
```

2) Enable loopback detection on ports 1/0/1-3 and set the process mode and recovery mode.

```
Switch(config)#interface gigabitEthernet 1/0/1

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode port-based recovery-mode auto

Switch(config-if)#exit

Switch(config)#interface gigabitEthernet 1/0/2

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode port-based recovery-mode auto
Switch(config-if)#exit

Switch(config)#interface gigabitEthernet 1/0/3

Switch(config-if)#loopback-detection

Switch(config-if)#loopback-detection config process-mode port-based recovery-mode auto

Switch(config-if)#end

Switch#copy running-config startup-config
```

Verify the Configuration

Verify the global configuration:

```
Switch#show loopback-detection global

Loopback detection global status : disable

Loopback detection interval      : 30 s

Loopback detection recovery time : 3 intervals
```

Verify the loopback detection configuration on ports:

```
Switch#show loopback-detection interface

Port     Enable    Process Mode    Recovery Mode    Loopback    Block    LAG

----     ------    ----------      ------------     --------    -------  ------

Gi1/0/1  enable    port-based      auto             N/A         N/A      N/A

Gi1/0/2  enable    port-based      auto             N/A         N/A      N/A

Gi1/0/3  enable    port-based      auto             N/A         N/A      N/A
```

8 Appendix: Default Parameters

Default settings of Switching are listed in th following tables.

Table 8-1 Configurations for Ports

Parameter	Defualt Setting
Port Config	
Type	Copper
Status	Enable
Speed	Auto
Duplex	Auto
Flow Control	Disable
Jumbo	Disable
Port Mirror	
Ingress	Disable
Egress	Disable
Port Security	
Max Learned MAC	64
Learned Num	0
Learned Mode	Dynamic
Status	Disable
Loopback Detection	
Loopback Detection Status	Disable
Detection Interval	30 seconds
Automatic Recovery Time	3 detection times
Web Refresh Status	Disable
Web Refresh Interval	6 seconds
Port Status	Disable

Parameter	Defualt Setting
Operation mode	Alert
Recovery mode	Auto