

Show the transmit power of SFP module.

Mon3(RX PWR):

Show the receiver power of SFP module.

## 3.2 ACL

The GS-2300 series access control list (ACL) is probably the most commonly used object in the firmware. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes, IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8. However, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

### 3.2.1 Ports

The section describes how to configure the ACL parameters (ACE) of the each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Web Interface

To configure the ACL Ports in the web interface:

1. Click Configuration, ACL, then Ports
2. To scroll the specific parameter value to select the correct value for port ACL setting.
3. Click Apply to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
5. After your configuration is complete you can see the counter of the port. Then you could click refresh to update the counter or clear the information.

Figure 3-2.1: The ACL Ports Configuration

ACL Ports Configuration									
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*		<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

Parameter description:

Port:

The logical port for the settings contained in the same row.

Policy ID:

Select the policy to apply to this port. The allowed values are 1 through 8. The default value is 1.

Action:

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID:

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

### 3 Configuration

#### Port Copy:

Select which port frames are copied on. The allowed values are Disabled or a specific port number. The default value is "Disabled".

#### Mirror:

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

#### Logging:

Specify the logging operation of this port. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged.

The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.

#### Shutdown:

Specify the port shut down operation of this port. The allowed values are:

Enabled: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled.

The default value is "Disabled".

#### Counter:

Counts the number of frames that match this ACE.

#### Buttons

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

#### Refresh

Refresh the ACL Port Configuration manually.

#### Clear

Clear the ACL Port Configuration manually.

## 3.2.2 Rate Limiters

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter Level from 1 to 16 allows the user to set rate limiter values and units (pps or kbps).

#### Web Interface

To configure ACL Rate Limiter in the web interface:

1. Click Configuration, ACL, then Rate Limiter
2. Specify the Rate field and the range from 0 to 3276700.
3. Select the unit: pps or kbps.
4. Click Apply to save the settings.
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-2.2: The ACL Rate Limiter Configuration

**ACL Rate Limiter Configuration**

Rate Limiter ID	Rate	Unit
1	1	pps
2	1	pps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Save Reset

Parameter description:

Rate Limiter ID:

The rate limiter ID for the settings contained in the same row.

Rate

The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit:

Specify the rate unit. The allowed values are:

pps: packets per second.

kbps: Kbits per second.

Buttons

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

### 3.2.3 Access Control List

The section describes how to configure Access Control List rules. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs are used for internal protocol and cannot be edited or deleted, the order sequence cannot be changed and the priority is highest

Web Interface

To configure Access Control Lists in the web interface:

## 3 Configuration


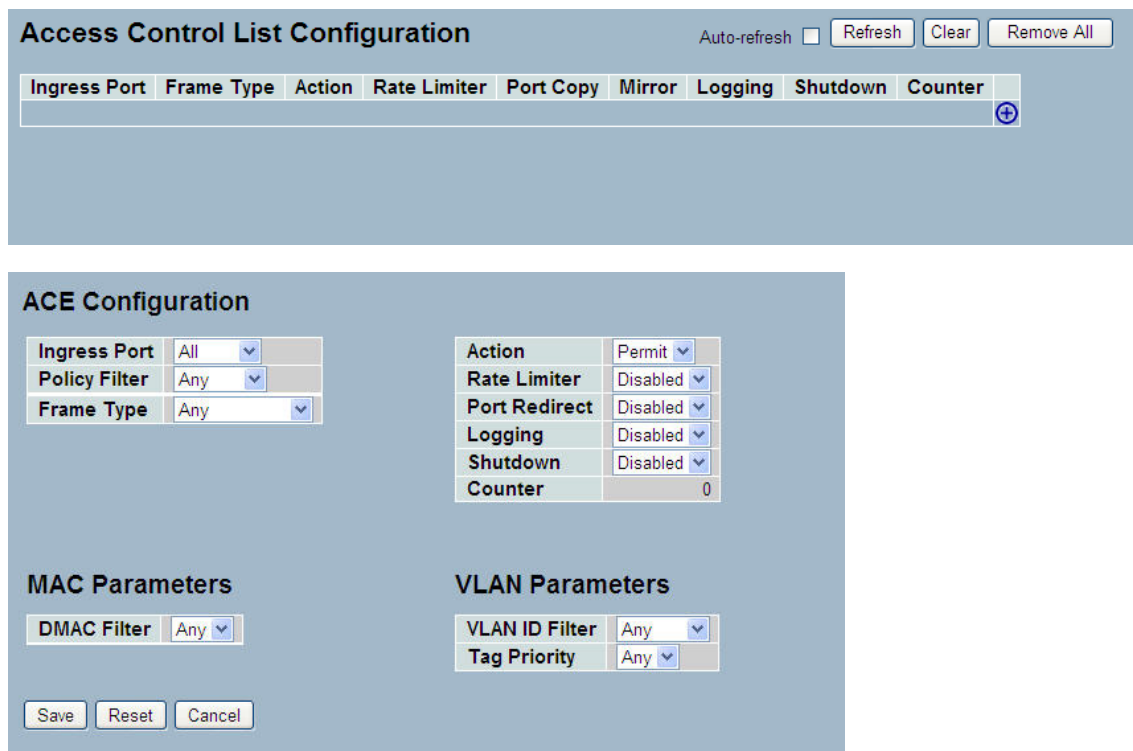

1. Click Configuration, ACL, then Configuration
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list)
3. Specify the parameters of the ACE
4. Click Apply to save the settings.
5. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.
6. When editing an entry on the ACE Configuration page, note that the Items displayed depend on various selections, such as Frame Type and IP Protocol Type. Specify the relevant criteria to be matched for this rule, and set the actions to take when a rule is matched (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Figure 3-2.3: The ACL Rate Limiter Configuration



**Access Control List Configuration** Auto-refresh  Refresh Clear Remove All

Ingress Port	Frame Type	Action	Rate Limiter	Port Copy	Mirror	Logging	Shutdown	Counter
								

**ACE Configuration**

<table style="width: 100%;"> <tr><td>Ingress Port</td><td>All</td></tr> <tr><td>Policy Filter</td><td>Any</td></tr> <tr><td>Frame Type</td><td>Any</td></tr> </table>	Ingress Port	All	Policy Filter	Any	Frame Type	Any	<table style="width: 100%;"> <tr><td>Action</td><td>Permit</td></tr> <tr><td>Rate Limiter</td><td>Disabled</td></tr> <tr><td>Port Redirect</td><td>Disabled</td></tr> <tr><td>Logging</td><td>Disabled</td></tr> <tr><td>Shutdown</td><td>Disabled</td></tr> <tr><td>Counter</td><td>0</td></tr> </table>	Action	Permit	Rate Limiter	Disabled	Port Redirect	Disabled	Logging	Disabled	Shutdown	Disabled	Counter	0
Ingress Port	All																		
Policy Filter	Any																		
Frame Type	Any																		
Action	Permit																		
Rate Limiter	Disabled																		
Port Redirect	Disabled																		
Logging	Disabled																		
Shutdown	Disabled																		
Counter	0																		

<p><b>MAC Parameters</b></p> <table style="width: 100%;"> <tr><td>DMAC Filter</td><td>Any</td></tr> </table>	DMAC Filter	Any	<p><b>VLAN Parameters</b></p> <table style="width: 100%;"> <tr><td>VLAN ID Filter</td><td>Any</td></tr> <tr><td>Tag Priority</td><td>Any</td></tr> </table>	VLAN ID Filter	Any	Tag Priority	Any
DMAC Filter	Any						
VLAN ID Filter	Any						
Tag Priority	Any						

Save Reset Cancel

Parameter description:

Ingress Port:

Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type:

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

Ethernet type: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

Action:

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter:

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Copy:

Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

Mirror:

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging:

Indicates the logging operation of the ACE. Possible values are:

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

Please note that the System Log memory size and logging rate is limited.

Shutdown:

Indicates the port shut down operation of the ACE. Possible values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

Counter:

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

- ⊕: Inserts a new ACE before the current row.
- ✎: Edits the ACE row.
- ⬆: Moves the ACE up the list.
- ⬇: Moves the ACE down the list.
- ✖: Deletes the ACE.
- ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings.

MAC Parameter:

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP.)

### 3 Configuration

Specify the source MAC filter for this ACE.

Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)

Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

Specify the destination MAC filter for this ACE.

Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

Buttons

Save – Click to save changes.

Reset – Click to undo any changes made locally and revert to previously saved values.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the ACL configuration manually

Clear

Clear the ACL configuration.

Remove All

Remove all ACL configurations from the table.

#### 3.2.4 ACL Status

The section describes how to show the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

Web Interface

To display the ACL status in the web interface:

1. Click Configuration, ACL, then ACL status
2. If you want to auto-refresh the information then you need to activate "Auto-refresh".
3. Click "Refresh" to refresh the ACL Status

Figure 3-2.4: The ACL Status

ACL Status										
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict	
IP Management	All	ARP	Permit	Disabled	Disabled	Yes	No	198	No	
IP Management	All	IPv4/UDP 68 DHCP Server	Permit	Disabled	Disabled	Yes	No	0	No	

Parameter description:

User:

Indicates the ACL user.

Ingress Port:

Indicates the ingress port of the ACE. Possible values are:

Any: The ACE will match any ingress port.

Policy: The ACE will match ingress ports with a specific policy.

Port: The ACE will match a specific ingress port.

Frame Type:

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

Action:

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Rate Limiter:

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Copy:

Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.

Mirror:

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

CPU:

Forward packet that matched the specific ACE to CPU.

CPU Once:

Forward first packet that matched the specific ACE to CPU.

Counter:

## 3 Configuration

The counter indicates the number of times the ACE was hit by a frame.

Conflict:

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the ACL status information manually.

## 3.3 Aggregation

You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

### 3.3.1 Static Trunk

The Aggregation Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation.

#### 3-3.1.1 Static Trunk

Ports using Static Trunk as their trunk method can choose their unique Static GroupID to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

Web Interface

To configure the Trunk Aggregation Hash mode and Aggregation Group in the web interface:

1. Click Configuration, Static Trunk, and then Aggregation Mode Configuration.
2. Activate to enable or disable the aggregation mode function.

Activate Aggregation Group ID and Port members

3. Click Apply to save the setting
4. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-3.1.1: The Aggregation Mode Configuration



### Aggregation Mode Configuration

**Hash Code Contributors**

Source MAC Address

Destination MAC Address

IP Address

TCP/UDP Port Number

### Aggregation Group Configuration

Group ID	Port Members																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
24	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
25	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
26	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Parameter description:

Hash Code Contributors

Source MAC Address:

The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address:

The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address:

The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number:

The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Aggregation Group Configuration

Locality:

Indicates the aggregation group type. This field is only valid for switches.

Global: The group members may reside on different units. The device supports two 8-port global aggregations.

Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.

Group ID:

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members:

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Buttons

Save – Click to save changes.

## 3 Configuration

Reset – Click to undo any changes made locally and revert to previously saved values.

### 3.3.2 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

#### 3-3.2.1 Configuration

This page allows the user to inspect the current LACP port configurations, and possibly change them as well. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group.

#### Web Interface

To configure the Trunk Aggregation LACP parameters in the web interface:

1. Click Configuration, Aggregation, LACP, Configuration
2. Activate to enable or disable the LACP on the port.
3. Select the Key parameter: Auto or specific value. Default is Auto.
4. Select the Role: Active or Passive. Default is Active.
5. Click Apply to save the settings
6. If you want to cancel the setting then you need to click the reset button. It will revert to previously saved values.

Figure 3-3.2.1: The LACP Port Configuration (GS-2310P)

Port	LACP Enabled	Key		Role
*	<input type="checkbox"/>	<>		<>
1	<input type="checkbox"/>	Auto		Active
2	<input type="checkbox"/>	Auto		Active
3	<input type="checkbox"/>	Auto		Active
4	<input type="checkbox"/>	Auto		Active
5	<input type="checkbox"/>	Auto		Active
6	<input type="checkbox"/>	Auto		Active
7	<input type="checkbox"/>	Auto		Active
8	<input type="checkbox"/>	Auto		Active
9A	<input type="checkbox"/>	Auto		Active
10A	<input type="checkbox"/>	Auto		Active
9B	<input type="checkbox"/>	Auto		Active
10B	<input type="checkbox"/>	Auto		Active

Apply    Reset

Parameter description:

Port:

The switch port number.

LACP Enabled:

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs.

Key: