

The Key value incurred by the port, range 1-65535. The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.

Role:

The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).

Buttons

Save – Click to save changes.

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

3-3.2.2 System Status

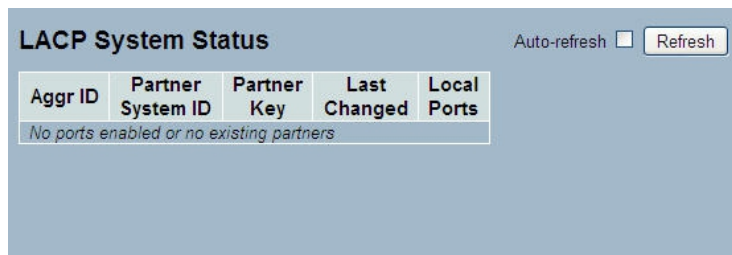
This section describes the LACP System Status which is provided when LACP is configured on the switch.

Web Interface

To display the LACP System status in the web interface:

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

Figure 3-3.2.2: The LACP System Status



Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

Parameter description:

Aggr ID:

The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Partner System ID:

The system ID (MAC address) of the aggregation partner.

Partner Key:

The Key that the partner has assigned to this aggregation ID.

Last changed:

The time since this aggregation changed.

Local Ports:

Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Auto-refresh:

To activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the LACP System status information manually.

3 Configuration

3-3.2.3 Port Status

This section describes the LACP Status which is provided when LACP is configured on the switch.

Web Interface

To display the LACP Port status in the web interface:

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

Figure 3-3.2.3: The LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-

Parameter description:

Port:

The switch port number.

LACP:

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile its LACP status is disabled.

Key:

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID:

The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.

Partner System ID:

The partner's System ID (MAC address).

Partner Port:

The partner's port number connected to this port.

Auto-refresh:

To activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the LACP port status information manually.

3-3.2.4 Port Statistics

This section describes the LACP Statistics which are provided when LACP is configured on the switch.

Web Interface

To display the LACP Port statistics in the web interface:

1. Click Configuration, Aggregation, LACP, Port Statistics
2. If you want to auto-refresh the information then you need to activate "Auto refresh".

3. Click "Refresh" to refresh the LACP Statistics.

Figure 3-3.2.4: The LACP Statistics

LACP Statistics					
Port	LACP Received	LACP Transmitted	Discarded		
			Unknown	Illegal	
1	0	0	0	0	
2	0	0	0	0	
3	0	0	0	0	
4	0	0	0	0	
5	0	0	0	0	

Parameter description:

Port:

The switch port number.

LACP Received:

Shows how many LACP frames have been received at each port.

LACP Transmitted:

Shows how many LACP frames have been sent from each port.

Discarded:

Shows how many unknown or illegal LACP frames have been discarded at each port.

Auto-refresh:

To activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the LACP port statistics information manually.

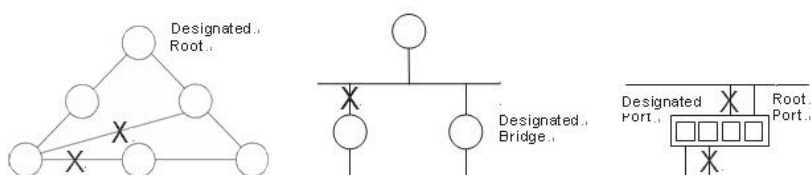
Clear:

Clear the LACP port statistics information manually.

3.4 Spanning Tree

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



3 Configuration

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

3.4.1 Bridge Settings

The section describes how to configure the Spanning Tree Bridge and STP System settings. It allows you to configure STP System settings which are used by all STP Bridge instances in the Switch.

Web Interface

To configure the Spanning Tree Bridge Settings parameters in the web interface:

1. Click Configuration, Spanning Tree, Bridge Settings
2. Select the parameters and enter available values of parameters in the blank field in Basic Settings
3. Activate to enable or disable the parameters and enter available value of parameters in the blank field in Advanced settings
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.1: The STP Bridge Configuration

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	128
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save Reset

Parameter description:

Basic Settings

Protocol Version:

The STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority:

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Forward Delay:

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age:

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.

Maximum Hop Count:

This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count:

The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings**Edge Port BPDU Filtering:**

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard:

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery:

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout:

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Save – Click to save changes.

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

3.4.2 MSTI Mapping

When you implement a Spanning Tree protocol on the switch that the bridge instance the CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. Due to the reason that you need to set the list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)

This section describes how the user can inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Mapping parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Mapping
2. Specify the configuration identification parameters in the field
3. Specify the VLANs Mapped blank field.
4. Click Apply to save the setting
5. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.2: The MSTI Configuration

3 Configuration

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	<input type="text" value="00-40-c7-74-00-d1"/>
Configuration Revision	<input type="text" value="0"/>

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	<input type="text"/>
MSTI2	<input type="text"/>
MSTI3	<input type="text"/>
MSTI4	<input type="text"/>
MSTI5	<input type="text"/>
MSTI6	<input type="text"/>
MSTI7	<input type="text"/>

Parameter description:

Configuration Identification

Configuration Name:

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision:

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI:

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

VLANs Mapped:

The list of VLANs mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs

Buttons

Save – Click to save changes.

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

3.4.3 MSTI Priorities

When you implement a Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier

This section show how the user can inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree MSTI Priorities parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Priorities
2. Scroll the Priority maximum is 240. Default is 128.
3. Click "Save" to save the settings.
4. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.3: The MSTI Configuration

MSTI	Priority
CIST	128
MSTI1	128
MSTI2	128
MSTI3	128
MSTI4	128
MSTI5	128
MSTI6	128
MSTI7	128

Save Reset

Parameter description:

MSTI:

The bridge instance. The CIST is the default instance, which is always active.

Priority:

Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

Buttons

Save – Click to save changes.

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

3.4.4 CIST Ports

When you implement a Spanning Tree protocol on the switch that the bridge instance. You need to configure the CIST Ports. The section describes how the user to inspect to inspect the current STP CIST port configurations, and possibly change them as well.

Web Interface

To configure the Spanning Tree CIST Ports parameters in the web interface:

1. Click Configuration, Spanning Tree, CIST Ports
2. Set the parameters of the CIST Aggregated Port Configuration.
3. Enable or disable the STP, then set the parameters of the CIST normal Port configuration.
4. Click Apply to save the settings.
5. If you want to cancel the settings then you need to click the Reset button. It will revert to previously saved values.

3 Configuration

Figure 3-4.4: The STP CIST Port Configuration (GS-2310P)

STP CIST Port Configuration									
CIST Aggregated Port Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True
CIST Normal Port Configuration									
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9A	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10A	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9B	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10B	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Apply Reset

Parameter description:

Port:

The switch port number of the logical STP port.

STP Enabled:

Controls whether STP is enabled on this switch port.

Path Cost:

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority:

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

operEdge (state flag):

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge:

Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge:

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role:

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN:

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard:

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point

Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

Save – Click to save changes.

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

3.4.5 MSTI Ports

The section describes how to view and change the current STP MSTI port configurations.

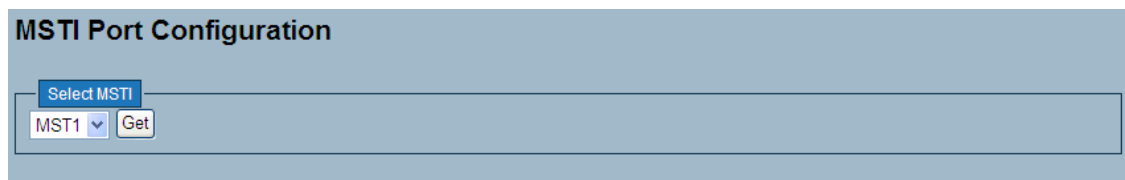
An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

Web Interface

To configure the Spanning Tree MSTI Port Configuration parameters in the web interface:

1. Click Configuration, Spanning Tree, MSTI Ports
2. Select the MST1 or other MSTI Port
3. Click Get to set the detail parameters of the MSTI Ports.
4. Set all parameters of the MSTI Port configuration.
5. Click Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-4.5: The MSTI Port Configuration (GS-2310P)



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128
5	Auto	128
6	Auto	128
7	Auto	128
8	Auto	128
9A	Auto	128
10A	Auto	128
9B	Auto	128
10B	Auto	128

Apply Reset

Parameter description:

Port:

The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost:

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority:

Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).

Buttons

Save – Click to save changes.

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

3.4.6 Bridge Status

After you complete the MSTI Port configuration the you could to ask the switch display the Bridge Status. The section provides a status overview of all STP bridge instances. The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Web Interface

To display the STP Bridges status in the web interface:

1. Click Configuration, Spanning Tree, STP Bridges
2. If you want to auto-refresh the information then you need to activate "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

Figure 3-4.6: The STP Bridges status

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80-00-00:40:C7:74:00:C9	80-00-00:40:C7:74:00:C9	-	0	Steady	-

Parameter description:

MSTI:

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID:

The Bridge ID of this Bridge instance.

Root ID:

The Bridge ID of the currently elected root bridge.

Root Port:

The switch port currently assigned the root port role.

Root Cost:

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag:

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last:

The time since last Topology Change occurred.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh:

Refresh the STP Bridges status information manually.

3.4.7 Port Status

After you complete the STP configuration you could ask the switch to display the STP Port Status. It displays the STP CIST port status for physical ports of the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, STP Port Status
2. If you want to auto-refresh the information then you need to activate "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

Figure 3-4.7: The STP Port status

3 Configuration

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-

Parameter description:

Port:

The switch port number of the logical STP port.

CIST Role:

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, Backup Port, RootPort, DesignatedPort Disabled.

CIST State:

The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the STP Port status information manually.

3.4.8 Port Statistics

After you complete the STP configuration then you could to let the switch display the STP Statistics. The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the currently selected switch.

Web Interface

To display the STP Port status in the web interface:

1. Click Configuration, Spanning Tree, Port Statistics
2. If you want to auto-refresh the information then you need to activate "Auto-refresh".
3. Click "Refresh" to refresh the STP Bridges.

Figure 3-4.8: The STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Parameter description:

Port:

The switch port number of the logical STP port.

MSTP:

The number of MSTP Configuration BPDU's received/transmitted on the port.

RSTP:

The number of RSTP Configuration BPDU's received/transmitted on the port.

STP:

The number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN:

The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.

Discarded Unknown:

The number of unknown Spanning Tree BPDU's received (and discarded) on the port.

Discarded Illegal:

The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Auto-refresh:

Activate the auto-refresh to refresh the information automatically.

Refresh

Refresh the STP Statistics information manually.

Clear

Clear the STP Statistics information manually.

3.5 IGMP Snooping

IGMP Snooping is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch which supports IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

3.5.1 Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

Web Interface

To configure the IGMP Snooping parameters in the web interface:

1. Click Configuration, IGMP Snooping, Basic Configuration
2. Activate to select enable or disable which Global configuration

3 Configuration

3. Activate which port wants to become a Router Port or enable/ disable the Fast Leave function.
4. Set the Throttling parameter.
5. Click Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values.

Figure 3-5.1: The IGMP Snooping Configuration (GS-2310P)

IGMP Snooping Configuration

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Apply Reset

Parameter description:

Snooping Enabled:

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding enabled:

Enable unregistered IPMCv4 traffic flooding.

IGMP SSM Range:

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)

Proxy Enabled:

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port:

It shows the physical Port index of switch.

Router Port:

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave:

Enable the fast leave on the port.

Throttling:

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save – Click to save changes.

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

3.5.2 VLAN Configuration

The section describes the VLAN configuration setting process integrated with IGMP Snooping function. For each setting page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

Web Interface

To configure the IGMP Snooping VLAN in the web interface:

1. Click Configuration, IGMP Snooping, VLAN Configuration
2. Activate to select enable or disable Snooping, IGMP Querier
3. Specify the parameters in the blank field.
4. Click the refresh to update the data or click << or >> to display previous entry or next entry.
5. Click Apply to save the setting
6. If you want to cancel the setting then you need to click the Reset button. It will revert to previously saved values

Figure 3-5.2: The IGMP Snooping VLAN Configuration.

VLAN ID	Snooping Enabled	IGMP Querier	Compatibility	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-	-	-	-	-	-

Parameter description:

VLAN ID:

It displays the VLAN ID of the entry.

Snooping Enabled:

Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.

IGMP Querier:

A router sends IGMP Query messages onto a particular link. This Router is called the Querier. Enable the IGMP Querier in the VLAN.

Compatibility:

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.