

7. Layer 2 Features

FDB

VLAN

Spanning Tree

Loopback Detection

Link Aggregation

L2 Multicast Control

LLDP

FDB

Static FDB

Unicast Static FDB

This window is used to view and configure the static unicast forwarding settings on the Switch.

To view the following window, click **L2 Features > FDB > Static FDB > Unicast Static FDB**, as shown below:

Figure 7-1 Unicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
Port	Allows the selection of the port number on which the MAC address entered resides.
VID	Enter the VLAN ID on which the associated unicast MAC address resides.
MAC Address	Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to delete all the entries found in the display table.

Click the **Delete** button to remove the specified entry.

Multicast Static FDB

This window is used to view and configure the multicast static FDB settings. To view the following window, click **L2 Features > FDB > Static FDB > Multicast Static FDB**, as shown below:

VID	MAC Address	Egress Ports

Figure 7-2 Multicast Static FDB window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
VID	Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.
MAC Address	Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX.

Click the **Apply** button to accept the changes made.

Click the **Delete All** button to remove all the entries.

Click the **Delete** button to remove the specific entry.

MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

To view the following window, click **L2 Features > FDB > MAC Address Table Settings**, as shown below:

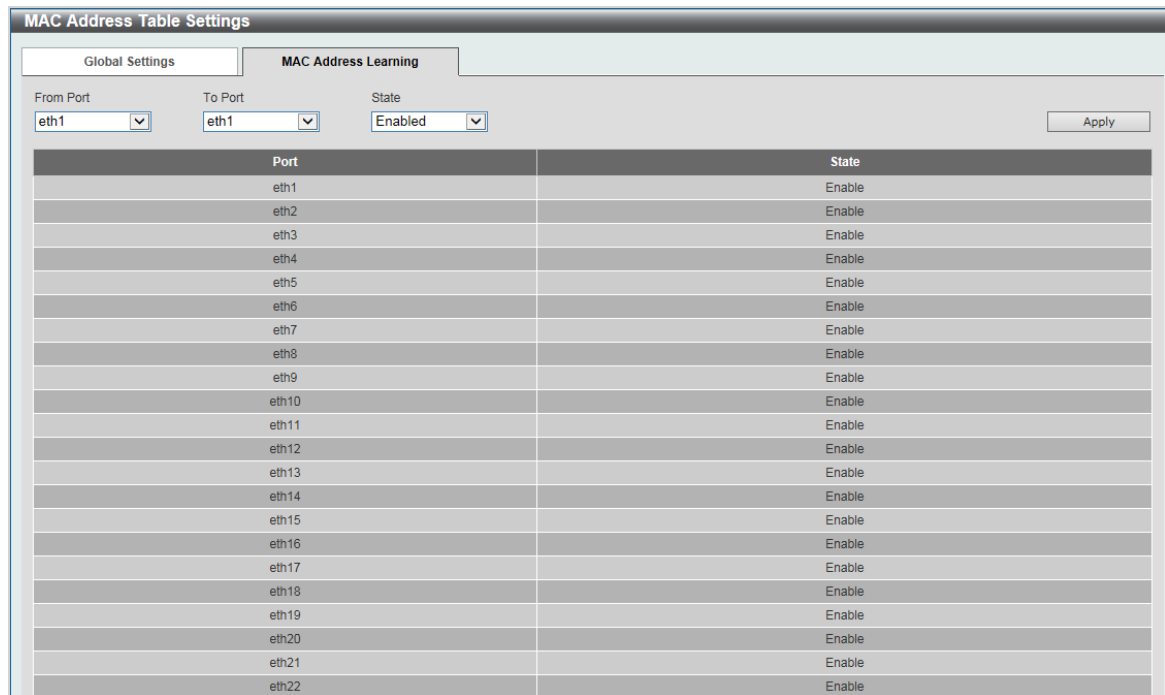
Figure 7-3 MAC Address Table Settings (Global Settings) window

The fields that can be configured are described below:

Parameter	Description
Aging Time	Enter the MAC address table's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

Click the **Apply** button to accept the changes made.

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.



The screenshot shows the 'MAC Address Table Settings' window with the 'MAC Address Learning' tab selected. It features configuration fields for 'From Port' (eth1), 'To Port' (eth1), and 'State' (Enabled), along with an 'Apply' button. Below these is a table listing 22 ports (eth1 to eth22) and their corresponding 'State' (all are 'Enable').

Port	State
eth1	Enable
eth2	Enable
eth3	Enable
eth4	Enable
eth5	Enable
eth6	Enable
eth7	Enable
eth8	Enable
eth9	Enable
eth10	Enable
eth11	Enable
eth12	Enable
eth13	Enable
eth14	Enable
eth15	Enable
eth16	Enable
eth17	Enable
eth18	Enable
eth19	Enable
eth20	Enable
eth21	Enable
eth22	Enable

Figure 7-4 MAC Address Table Settings (MAC Address Learning) window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the range of ports that will be used for this configuration here.
State	Select to enable or disable the MAC address learning function on the ports specified here.

Click the **Apply** button to accept the changes made.

MAC Address Table

This window is used to view the entries listed in the MAC address table.

To view the following window, click **L2 Features > FDB > MAC Address Table**, as shown below:



The screenshot shows the 'MAC Address Table' window. It has a title bar 'MAC Address Table' and a sub-header 'MAC Address Table'. Below is a table with columns: VID, MAC Address, Type, and Port. A 'Clear All' button is located in the top right corner of the table area.

VID	MAC Address	Type	Port
-----	-------------	------	------

Figure 7-5 MAC Address Table window

Click the **Clear All** button to clear all dynamic MAC addresses.

VLAN

802.1Q VLAN

This window is used to view and configure the VLAN settings on this switch.

To view the following window, click **L2 Features > VLAN > 802.1Q VLAN**, as shown below:

Figure 7-6 802.1Q VLAN window

The fields that can be configured for **802.1Q VLAN** are described below:

Parameter	Description
VID List	Enter the VLAN ID list that will be created here.

Click the **Apply** button to accept the changes made.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

Port-based VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click **L2 Features > VLAN > Port-based VLAN**, as shown below:

Figure 7-7 Asymmetric VLAN window

The fields that can be configured are described below:

Parameter	Description
VLAN State	Select this option to enable or disable the Port-based VLAN function.
From Port / To Port	Select the range of ports that will be used for this configuration here.
VLAN Index	VLAN Index is a unique number that identifies a particular VLAN

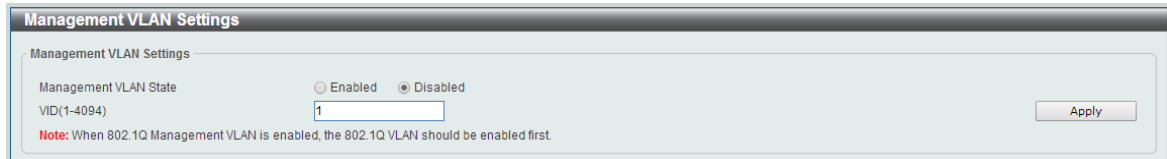
Click the **Apply** button to accept the changes made.

Click the **Delete All** button to delete all the entries found in the display table.

Management VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click **L2 Features > VLAN > Management VLAN**, as shown below:



The screenshot shows the 'Management VLAN Settings' window. It has a title bar 'Management VLAN Settings' and a sub-header 'Management VLAN Settings'. Below this, there is a section for 'Management VLAN State' with two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' button is selected. Below the radio buttons is a text input field for 'VID(1-4094)' containing the number '1'. To the right of the input field is an 'Apply' button. At the bottom, there is a red note: 'Note: When 802.1Q Management VLAN is enabled, the 802.1Q VLAN should be enabled first.'

Figure 7-8 Asymmetric VLAN window

The fields that can be configured are described below:

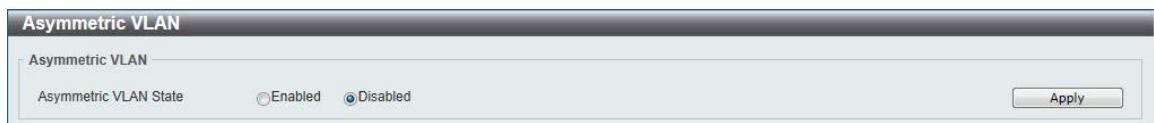
Parameter	Description
Management VLAN State	Select this option to enable or disable the Management VLAN function.
VID	VLAN VID is a unique number (between 1 and 4094) that identifies a particular VLAN.

Click the **Apply** button to accept the changes made.

Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

To view the following window, click **L2 Features > VLAN > Asymmetric VLAN**, as shown below:



The screenshot shows the 'Asymmetric VLAN' window. It has a title bar 'Asymmetric VLAN' and a sub-header 'Asymmetric VLAN'. Below this, there is a section for 'Asymmetric VLAN State' with two radio buttons: 'Enabled' and 'Disabled'. The 'Disabled' button is selected. To the right of the radio buttons is an 'Apply' button.

Figure 7-9 Asymmetric VLAN window

The fields that can be configured are described below:

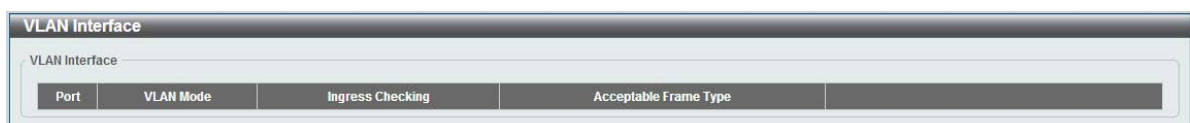
Parameter	Description
Asymmetric VLAN State	Select this option to enable or disable the asymmetric VLAN function

Click the **Apply** button to accept the changes made.

VLAN Interface

This window is used to view and configure VLAN interface settings.

To view the following window, click **L2 Features > VLAN > VLAN Interface**, as shown below:



The screenshot shows the 'VLAN Interface' window. It has a title bar 'VLAN Interface' and a sub-header 'VLAN Interface'. Below this, there is a table with four columns: 'Port', 'VLAN Mode', 'Ingress Checking', and 'Acceptable Frame Type'. The table is currently empty.

Figure 7-10 VLAN Interface window

Click the **View Detail** button to view more detailed information about the VLAN on the specific interface.

Click the **Edit** button to re-configure the specific entry.

After clicking the **VLAN Detail** button, the following page will appear.

VLAN Interface Information	
Port	eth1
VLAN Mode	Hybrid
Native VLAN	1
Hybrid Untagged VLAN	1,
Hybrid Tagged VLAN	-
Ingress Checking	Enabled
Acceptable Frame Type	Admit All

<<Back

Figure 7-11 VLAN Interface Information window

More detailed information about the VLAN of the specific interface is displayed.

Click the **Back** button to return to the previous window.

After click the **Edit** button, the following window will appear. This is a dynamic window that will change when a different **VLAN Mode** was selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

Configure VLAN Interface			
Configure VLAN Interface			
Port	eth1		
VLAN Mode	Access	<input type="checkbox"/> Clone	
Acceptable Frame	Untagged Only	From Port	eth1
Ingress Checking	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	To Port	eth1
VID(1-4094)			
		<<Back Apply	

Figure 7-12 Configure VLAN Interface - Access window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select this option to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

Configure VLAN Interface

Configure VLAN Interface

Port: eth1

VLAN Mode: Hybrid

Acceptable Frame: Admit All

Ingress Checking: ☒ Enabled ☐ Disabled

VID(1-4094):

Action: Untagged

Allowed VLAN Range:

☐ Clone

From Port: eth1

To Port: eth1

<<Back Apply

Figure 7-13 Configure VLAN Interface - Hybrid window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	Select the check box to enable or disable the ingress checking function.
VID	Enter the VLAN ID used for this configuration here. This value must be between 1 and 4094.
Action	Select the action that will be taken here. Options to choose from are Remove , Tagged , and Untagged .
Allowed VLAN Range	Enter the allowed VLAN range information here.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

When **Trunk** is selected as the **VLAN Mode**, the following page will appear.

Configure VLAN Interface

Configure VLAN Interface

Port: eth1

VLAN Mode: Trunk

Acceptable Frame: Admit All

Ingress Checking: ☒ Enabled ☐ Disabled

Action: All

Allowed VLAN Range:

☐ Clone

From Port: eth1

To Port: eth1

<<Back Apply

Figure 7-14 Configure VLAN Interface - Trunk window

The fields that can be configured are described below:

Parameter	Description
VLAN Mode	Select the VLAN mode option here. Options to choose from are Access , Hybrid , and Trunk .
Acceptable Frame	Select the acceptable frame behavior option here. Options to choose from are Tagged Only , Untagged Only , and Admit All .
Ingress Checking	After selecting Trunk as the VLAN Mode the following parameter will be available. Select to enable or disable the ingress checking function.
Action	Select the action that will be taken here. Options to choose from are Remove , Tagged , and Untagged .
Allowed VLAN Range	Enter the allowed VLAN range information here.
From Port / To Port	Select the appropriate port range used for the Clone configuration here.

Click the **Apply** button to accept the changes made.

Click the **Back** button to return to the previous window.

Auto Surveillance VLAN

Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties**, as shown below:

Figure 7-15 Auto Surveillance Properties window

The fields that can be configured for **Global Settings** are described below:

Parameter	Description
Surveillance VLAN	Select this option to enable or disable the surveillance VLAN state
Surveillance VLAN ID	Enter the surveillance VLAN ID. The range is from 2 to 4094.
Surveillance VLAN CoS	Select the priority of the surveillance VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic

	resumes during the aging time, the aging timer will be reset and stop.
--	--

Click the **Apply** button to accept the changes made.

MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

To view the following window, click **L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device**, as shown below:

MAC Settings and Surveillance Device

User-defined MAC Settings | Auto Surveillance VLAN Summary

To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.

Component Type: Video Management Server | Description: 32 chars

MAC Address: 00-01-02-03-00-00 | Mask: | Apply

Total Entries: 3

ID	Component Type	Description	MAC Address	Mask	
1	D-Link Device	IP Surveillance Device	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Delete
2	D-Link Device	IP Surveillance Device	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Delete
3	D-Link Device	IP Surveillance Device	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Delete

Figure 7-16 User -defined MAC Settings window

The fields that can be configured are described below:

Parameter	Description
Component Type	Select the surveillance component type. Options to choose from are Video Management Server , VMS Client/Remote Viewer , Video Encoder , Network Storage , and Other IP Surveillance Device .
Description	Enter the description for the user-defined OUI with a maximum of 8 characters.
MAC Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

After clicking the **Auto Surveillance VLAN Summary** tab, the following page will appear.

MAC Settings and Surveillance Device

User-defined MAC Setting | Auto Surveillance VLAN Summary

Total Entries: 0

Port	Component Type	Description	MAC Address	Start Time
------	----------------	-------------	-------------	------------

Figure 7-17 Auto Surveillance VLAN Summary window

Voice VLAN

Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Global**, as show below:

Figure 7-18 Voice VLAN Global window

The fields that can be configured are described below:

Parameter	Description
Voice VLAN State	Select this option to enable or disable the voice VLAN.
Voice VLAN ID	Enter the voice VLAN ID. The value is range from 2 to 4094.
Voice VLAN CoS	Select the priority of the voice VLAN from 0 to 7.
Aging Time	Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

Click the **Apply** button to accept the changes made for each individual section.

Voice VLAN Port

This window is used to configure the user-defined voice traffic's port.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI**, as show below:

Port	State	Mode
eth1	Disabled	Manual
eth2	Disabled	Manual
eth3	Disabled	Manual
eth4	Disabled	Manual
eth5	Disabled	Manual
eth6	Disabled	Manual
eth7	Disabled	Manual
eth8	Disabled	Manual
eth9	Disabled	Manual
eth10	Disabled	Manual

Figure 7-19 Voice VLAN Port window

The fields that can be configured are described below:

Parameter	Description
From Port / To Port	Select the range of ports that will be used for this configuration here.
State	Select this option to enable or disable the Voice VLAN state of the port.
Mode	Choose the Voice VLAN mode for the port. This can be Auto untagged , Auto Tagged , or Manually configured.

Click the **Apply** button to accept the changes made.

Voice VLAN OUI

This window is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI**, as show below:

Voice VLAN OUI

Voice VLAN OUI

OUI Address: 00-01-E3-00-00-00 Mask: FF-FF-FF-00-00-00 Description: 32 chars **Apply**

Total Entries: 8

OUI Address	Mask	Description	
00-01-E3-00-00-00	FF-FF-FF-00-00-00	Siemens	Delete
00-03-6B-00-00-00	FF-FF-FF-00-00-00	Cisco	Delete
00-09-6E-00-00-00	FF-FF-FF-00-00-00	Avaya	Delete
00-0F-E2-00-00-00	FF-FF-FF-00-00-00	Huawei&3COM	Delete
00-60-B9-00-00-00	FF-FF-FF-00-00-00	NEC&Philips	Delete
00-D0-1E-00-00-00	FF-FF-FF-00-00-00	Pingtel	Delete
00-E0-75-00-00-00	FF-FF-FF-00-00-00	Veritel	Delete
00-E0-BB-00-00-00	FF-FF-FF-00-00-00	3COM	Delete

Figure 7-20 Voice VLAN OUI window

The fields that can be configured are described below:

Parameter	Description
OUI Address	Enter the OUI MAC address.
Mask	Enter the OUI MAC address matching bitmask.
Description	Enter the description for the user-defined OUI with a maximum of 8 characters.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port, the activate time is the latest time saw the device sending the traffic.

To view the following window, click **L2 Features > VLAN > Voice VLAN > Voice VLAN Device**, as show below:

Voice VLAN Device

Voice VLAN Device Table

Port	Voice Device Address	Start Time
------	----------------------	------------

Figure 7-201 Voice VLAN Device window

Spanning Tree

This Switch supports two versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP has been recently introduced to DGS-1100 switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP.

802.1D-2004 Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available.

STP Global Settings

This window is used to view and configure the STP global settings.

To view the following window, click **L2 Features > Spanning Tree > STP Global Settings**, as shown below:

Figure 7-212 STP Global Settings window

The field that can be configured for **Spanning Tree State** is described below:

Parameter	Description
Spanning Tree State	Select this option to enable or disable the STP global state here.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Spanning Tree Mode** are described below:

Parameter	Description
Spanning Tree Mode	Select the STP mode used here. Options to choose from are RSTP , and STP .

Click the **Apply** button to accept the changes made.

The fields that can be configured for **STP Traps** are described below:

Parameter	Description
STP New Root Trap	Select this option to enable or disable the STP new root trap option here.
STP Topology Change Trap	Select this option to enable or disable the STP topology change trap option here.

Click the **Apply** button to accept the changes made.

STP Port Settings

This window is used to view and configure the STP port settings.

To view the following window, click **L2 Features > Spanning Tree > STP Port Settings**, as shown below:



The STP Port Settings window has a title bar 'STP Port Settings'. Below it is a sub-header 'STP Port Settings'. There are three dropdown menus: 'From Port', 'To Port', and 'Port Fast'. The 'Port Fast' dropdown is currently set to 'Network'. An 'Apply' button is on the right. Below the dropdowns is a table with three columns: 'Port', 'Port Fast', and 'State'.

Figure 7-223 STP Port Settings window

The fields that can be configured are described below:

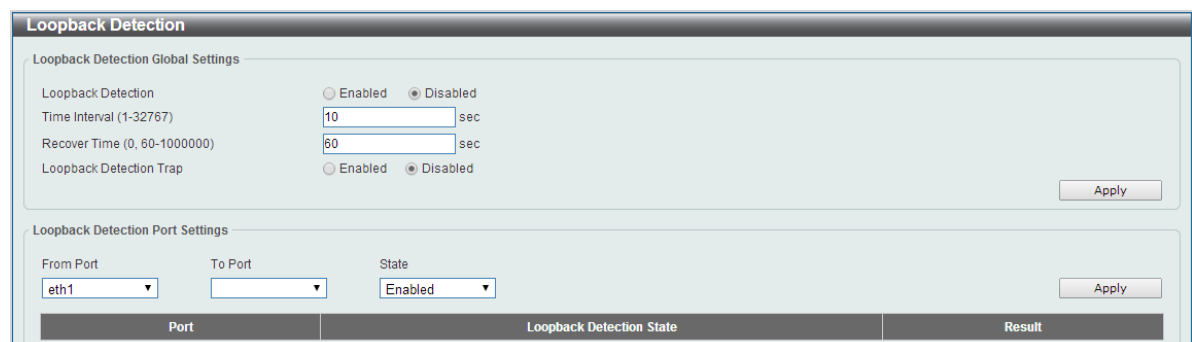
Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Port Fast	Select the port fast option here. Options to choose from are Network , Disabled , and Edge . In the Network mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the Disable mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is Edge .

Click the **Apply** button to accept the changes made.

Loopback Detection

The Loopback Detection (LBD) function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, this signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection port will restart (change to normal state) when the Loopback Detection Recover Time times out. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

To view the following window, click **L2 Features > Loopback Detection**, as shown below:



The Loopback Detection window has a title bar 'Loopback Detection'. Below it is a sub-header 'Loopback Detection Global Settings'. There are three sections: 'Loopback Detection' with radio buttons for 'Enabled' and 'Disabled' (selected), 'Time Interval (1-32767)' with a text box '10' and 'sec', 'Recover Time (0, 60-1000000)' with a text box '60' and 'sec', and 'Loopback Detection Trap' with radio buttons for 'Enabled' and 'Disabled' (selected). An 'Apply' button is on the right. Below this is a sub-header 'Loopback Detection Port Settings'. There are three dropdown menus: 'From Port' (set to 'eth1'), 'To Port', and 'State' (set to 'Enabled'). An 'Apply' button is on the right. Below the dropdowns is a table with three columns: 'Port', 'Loopback Detection State', and 'Result'.

Figure 7-234 Loopback Detection window

The fields that can be configured for **Loopback Detection Global Settings** are described below:

Parameter	Description
Loopback Detection	Select to enable or disable loopback detection. The default is Disabled .
Time Interval	Set a Loop detection Interval between 1 and 32767 seconds. The default is 10 seconds.
Recover Time	Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at 0 seconds, or 60 to 1000000 seconds. Entering 0 will disable the Loop Detection Recover Time. The default is 60 seconds.
Loopback Detection Trap	Select to enable or disable the loopback detection trap state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **Loopback Detection Port Settings** are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
State	Select this option to enable or disable the state of the port.

Click the **Apply** button to accept the changes made.

Note: If Spanning Tree protocol is used, loopback detection will not be available. If Loopback Detection is enabled, the Spanning Tree protocol will not be available.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

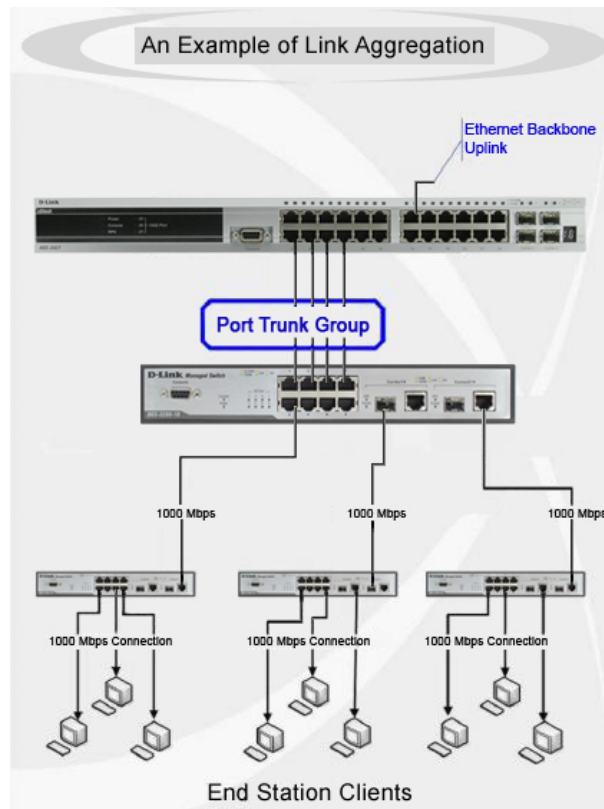


Figure 7-245 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.

This window is used to view and configure the link aggregation settings.

To view the following window, click **L2 Features > Link Aggregation**, as shown below:

Figure 7-256 Link Aggregation window

The fields that can be configured for **Channel Group Information** are described below:

Parameter	Description
From Port / To Port	Select the appropriate port range used for the configuration here.
Group ID	Enter the channel group number here. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.
Mode	<p>Select the mode option here. Options to choose from are On, Active, and Passive. If the mode On is specified, the channel group type is static. If the mode Active or Passive is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.</p> <p>Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p>Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports</p>

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete Member Port** button to remove the specific member port.

Click the **Delete Channel** button to remove the specific entry.

Click the **Channel Detail** button to view more detailed information about the channel.

After clicking the **Channel Detail** button, the following page will be available.

Port Channel

Port Channel Information

Port Channel: 1
Protocol: LACP

Port Channel Detail Information

Port	Working Mode	LACP State	Port Priority	Port Number
eth1	Active	down	255	1

Port Channel Neighbor Information

Port	Partner System ID	Partner PortNo	Partner Working Mode	Partner Port Priority
eth1	00-00-00-00-00-00	0		0

Note:
LACP State:
brdl: Port is attached to an aggregator and bundled with other ports.
indep: Port is in an independent state(not bundled but able to switch data traffic).
hol-stdy: Port is in a hol-standby state.
down: Port is down.

[<<Back](#)

Figure 7-267 Port Channel window

Click the **Back** button to return to the previous window.

L2 Multicast Control

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host.

IGMP Snooping Settings

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings**, as shown below:

Figure 7-278 IGMP Snooping Settings window

The field that can be configured for **Global Settings** is described below:

Parameter	Description
Global State	Select this option to enable or disable IGMP snooping global state.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **VLAN Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping on the VLAN.

Click the **Apply** button to accept the changes made.

The fields that can be configured for **VLAN Querier Status Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping on the VLAN.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

IGMP Snooping Groups Settings

This window is used to configure and view the IGMP snooping static group, and view IGMP snooping group.

To view the following window, click **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings**, as shown below:

Figure 7-281 IGMP Snooping Groups Settings

The fields that can be configured for **IGMP Snooping Static Groups Settings** are described below:

Parameter	Description
VID	Enter a VLAN ID of the multicast group.
Group Address	Enter an IP multicast group address.
From Port / To Port	Select the appropriate port range used for the configuration here.

Click the **Apply** button to accept the changes made.

Click the **Delete** button to remove the specified entry.

Multicast Filtering

This window is used to view and configure the Layer 2 multicast filtering settings.

To view the following window, click **L2 Features > L2 Multicast Control > Multicast Filtering**, as shown below:



Figure 7-292 Multicast Filtering window

The fields that can be configured are described below:

Parameter	Description
Multicast Filter Mode	Select the multicast filter mode here. Options to choose from are Forward Unregistered , and Filter Unregistered . When selecting the Forward Unregistered option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the Filter Unregistered option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to accept the changes made.

LLDP

LLDP Global Settings

LLDP (Link Layer Discovery Protocol) provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices.

This window is used to configure the LLDP global settings.

To view the following window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below:

Figure 7-303 LLDP Global Settings window

The fields that can be configured for **LLDP Global Settings** are described below:

Parameter	Description
LLDP State	Select this option to enable or disable the LLDP feature
LLDP Trap State	Select this option to enable or disable the LLDP trap state.

Click the **Apply** button to accept the changes made.

LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.

To view the following window, click **L2 Features > LLDP > LLDP Neighbor Port Information**, as shown below:

Entity	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description
--------	--------------------	------------	-----------------	---------	------------------

Figure 7-314 LLDP Neighbor Port Information window