Spanning Tree Protocol (STP) Interface Settings Configuration on Sx500 Series Stackable Switches

Objective

Spanning Tree Protocol (STP) is a network protocol that prevents the occurrence of loops in the topology. These loops cause switches to forward traffic an infinite amount of times. This causes the network to flood and use its resources which reduces network efficiency.

STP interface settings are used to increase efficiency of STP on a per port basis. The edge port function fast link increases the speed of STP convergence by setting a port to a forwarding state when a device is connected. The Root Guard and Bridge Protocol Data Unit (BPDU) Guard are used to control the STP topology. This extra control in the topology prevents any occurrence of bridge loops.

This article explains how to configure STP interface settings on the Sx500 Series Stackable Switches.

Applicable Devices
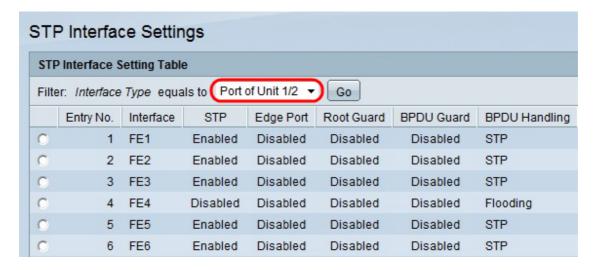
• Sx500 Series Stackable Switches

Software Version

• v1.2.7.76

STP Interface Settings

Note: Before the configuration of the STP Interface Settings, the user should choose the Classic STP mode of operation. Refer to the article *Spanning Tree Protocol (STP) Configuration on Sx500 Series Stackable Switches* for more information.

Step 1. Log in to the web configuration utility to choose **Spanning Tree > STP Interface Settings**. The *STP Interface Settings* page opens:

STP Interface Settings

STP Interface Setting Table

Filter: *Interface Type* equals to **Port of Unit 1/2** ▼ [Go]

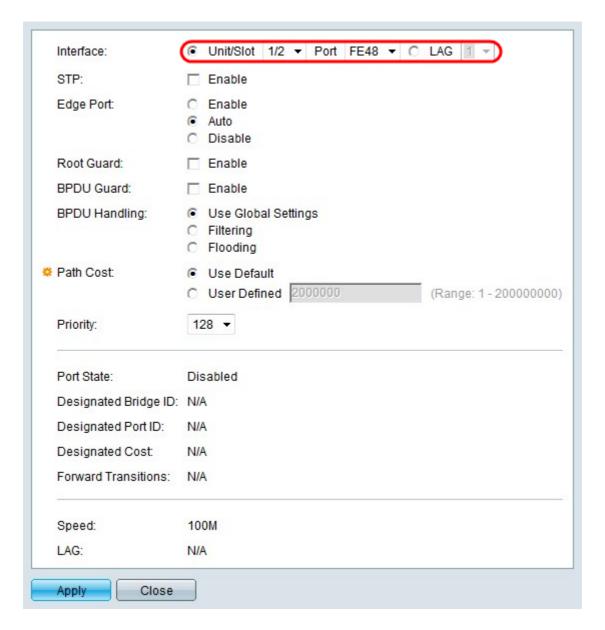|	Entry No.	Interface	STP	Edge Port	Root Guard	BPDU Guard	BPDU Handling
○	1	FE1	Enabled	Disabled	Disabled	Disabled	STP
○	2	FE2	Enabled	Disabled	Disabled	Disabled	STP
○	3	FE3	Enabled	Disabled	Disabled	Disabled	STP
○	4	FE4	Disabled	Disabled	Disabled	Disabled	Flooding
○	5	FE5	Enabled	Disabled	Disabled	Disabled	STP
○	6	FE6	Enabled	Disabled	Disabled	Disabled	STP

Step 2. Choose the type of interface you wish to edit from the Interface Type drop-down list.

Step 3. Click **Go** to show only ports or LAGs on the page.

○	41	FE41	Enabled	Disabled	Disabled	Disabled	STP
○	42	FE42	Enabled	Disabled	Disabled	Disabled	STP
○	43	FE43	Enabled	Disabled	Disabled	Disabled	STP
○	44	FE44	Enabled	Disabled	Disabled	Disabled	STP
○	45	FE45	Enabled	Disabled	Disabled	Disabled	STP
○	46	FE46	Enabled	Disabled	Disabled	Disabled	STP
○	47	FE47	Enabled	Disabled	Disabled	Disabled	STP
●	48	FE48	Enabled	Disabled	Disabled	Disabled	STP
○	49	GE3	Enabled	Disabled	Disabled	Disabled	STP
○	50	GE4	Enabled	Disabled	Disabled	Disabled	STP

[Copy Settings...]   [Edit...]

Step 4. Click the radio button of the port or LAG that is connected to the other switch and click **Edit**. The *Edit STP Interface* window appears:
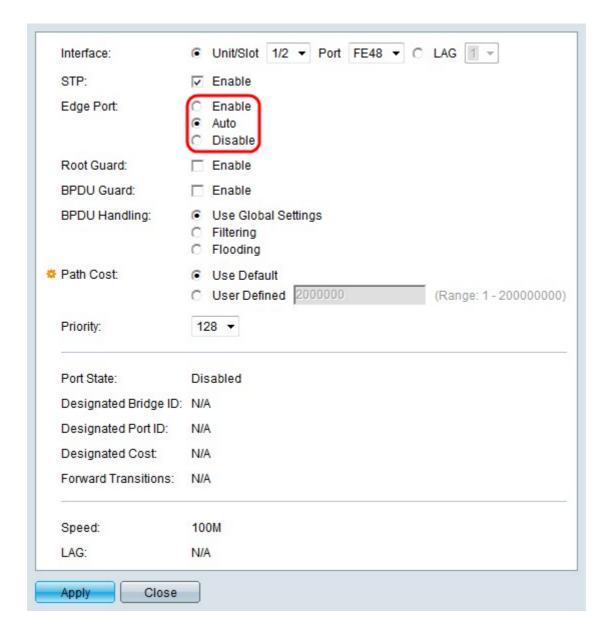
Step 5. (Optional) Click the radio button that corresponds to the desired interface type in the Interface field.

• Unit/Slot — From the Unit/Slot drop-down lists choose the appropriate Unit/Slot. The unit identifies whether the switch is active or a member in the stack. The slot identifies which switch is connected to which slot (slot 1 is SF500 and slot 2 is SG500). If you are unfamiliar with the terms used, check out Cisco Business: Glossary of New Terms.

– Port — From the Port drop-down list, choose the appropriate port to configure.

• LAG — Choose on which LAG the STP is advertised from the LAG drop-down list. A Link Aggregate Group (LAG) is used to link multiple ports together. LAGs multiply bandwidth, increase port flexibility, and provide link redundancy between two devices to optimize port usage.

Step 6. Check **Enable** in the STP field to enable STP on the interface.
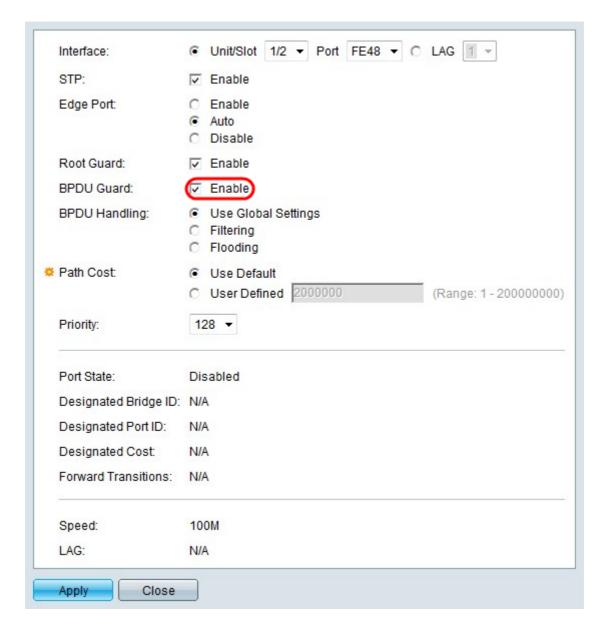
Step 7. Click the radio button that corresponds to the desired use of fast link in the Edge Port field. Fast link is used to automatically set a port to forwarding state when the port links up. Fast link optimizes the STP convergence.

• Enable — Immediately enables fast link.

• Auto — Waits to enable fast link until a few seconds after the interface becomes active so that loops can be resolved first.
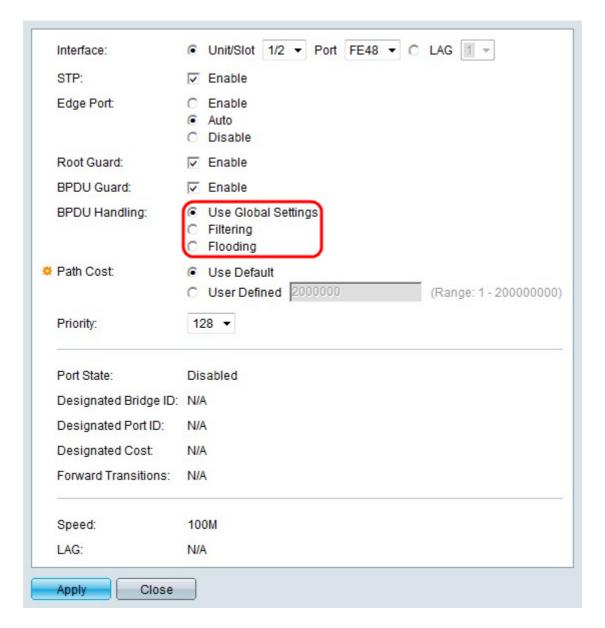
• Disable — Disables fast link.

Step 8. (Optional) Check **Enable** in the Root Guard field to enable Root Guard on the interface. This option allows you to enforce the placement of the root bridge in the network. Root Guard does not allow new connected devices to become the root bridge, which would affect the STP topology.

Note: The root guard should be configured only on the interfaces that go out of the root bridge.
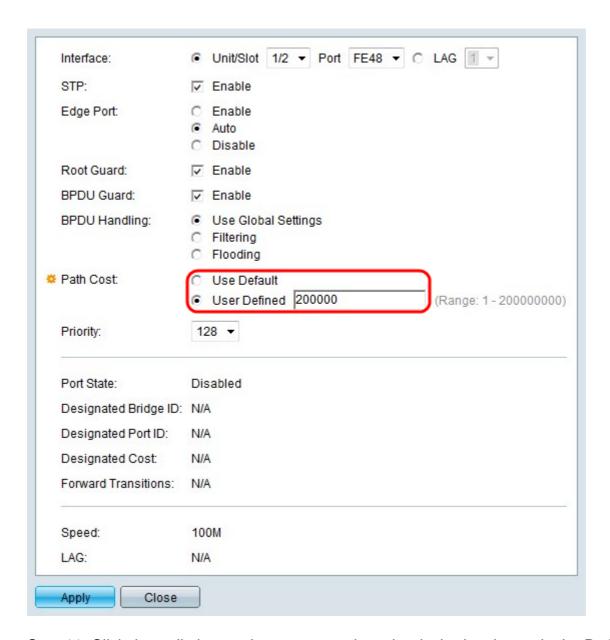
Step 9. (Optional) Check **Enable** in the BPDU Guard field to enable Bridge Protocol Data Unit (BPDU) Guard on the interface. BPDU Guard allows the user to enforce the STP domain borders on the interface and to keep the active topology predictable. Devices that are connected to an interface that have BPDU enabled cannot affect the STP topology. When the switch receives a BPDU on the interface with BPDU Guard enabled, the interface is disabled and an SNMP trap is generated.

Note: The BPDU guard should be enabled on interfaces where port fast is enabled and not on any other interface.
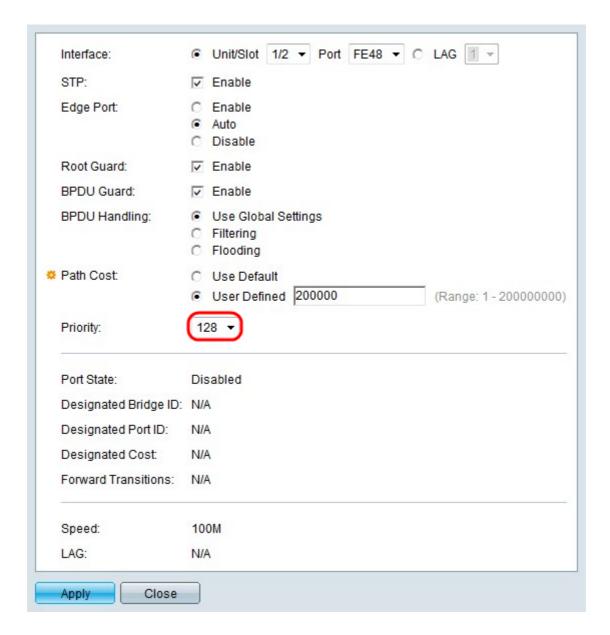
Step 10. Click the radio button that corresponds to the desired option in the BPDU Handling field. This determines how BPDU packets are managed when STP is disabled on the interface. BPDUs are used to transmit STP information.

• Use Global Settings — Uses the settings that are defined on the *STP Status and Global Settings* page.

• Filtering — On the ports where portfast is enabled, BPDU Filtering is enabled to prevent BPDUs from being sent or processed on one or more switch ports.

• Flooding— The BPDU packets are forwarded by all interfaces when STP is disabled on the interface.

Step 11. Click the radio button that corresponds to the desired path cost in the Path Cost field. The path cost is the port contribution to the root path.

• Use Default — Use the default cost generated by the system.

• User Defined — Enter a value for the path cost in the User Defined field. The path cost should be chosen with respect to the interface through which packets are sent out. An interface with a lower path cost is chosen as the outgoing interface.

Step 12. From the Priority drop-down list choose the priority value of the interface. The priority value determines port choice when a bridge has two ports connected in a loop. The lower the value, the higher the priority the port has on the bridge.

The following fields display statistics of the interface.

• Port State — Current state of the specified port.

  – Disabled — STP is disabled. The port forwards traffic while learning MAC addresses.

  – Blocking — The port is currently blocked, and cannot forward traffic.

  – Listening — The port cannot forward traffic, and cannot learn MAC addresses.

  – Learning — Ports in this state can learn new MAC addresses, but still cannot send data frames.

  – Forwarding — Ports in this state can now send and receive data frames and send and receive BPDUs.

• Designated Bridge ID — The bridge priority and MAC address of the designated bridge.

• Designated Port ID — The priority and interface of the selected port.

• Designated Cost — The cost of the port that is part of the STP topology. Ports with lower costs are less likely to be blocked if STP detects loops.

• Forward Transitions — How many times the port has changed from the blocking state to the forwarding state.

• Speed — The speed of the port.

• LAG — The LAG to which the port belongs. The LAG settings override port settings.

Step 13. Click **Apply**.