



Turn It On

Power Up

Turn on all these features to leverage the full value of Cisco routers and switches.

- Protective QoS Features
 - Control Plane Policing (CoPP)
 - Network-Based Application Recognition (NBAR)
- VRF-Lite/Multi-VRF CE
- Advanced VPN Services:
 - Dynamic Multipoint VPN (DMVPN)
 - Group Encrypted Transport (GET VPN)
- Catalyst Integrated Security Features (CISF)
- **Spanning-Tree Protocol (STP) Toolkit**
- Encapsulated Remote Switched Port Analyzer (ERSPAN)
- Dynamic Intelligent Routing Solutions
 - IP Service-Level Agreement (IPSLA)
 - Optimized Edge Routing (OER)
 - Embedded Event Manager (EEM)

To help you get the most functionality, value and ROI from your Cisco routers and switches, we want to ensure you're aware of the many powerful features residing within. Our **Turn it On** program is designed to empower Federal agencies like yours to take full advantage of Cisco's powerful core networking solutions to maximize your productivity, efficiency and technology investment.

Spanning-Tree Protocol (STP) Toolkit

Spanning-Tree Protocol (STP) provides the functionality necessary for a Layer 2 Ethernet network to function properly, including path redundancy and prevention of undesirable forwarding loops. Its algorithms automatically recalculate topology and activate standby redundant paths to ensure the network remains up and running at maximum efficiency. But while STP behavior should be deterministic by definition, it often isn't due to changes on user-controlled edge switches, unidirectional link failures, etc.

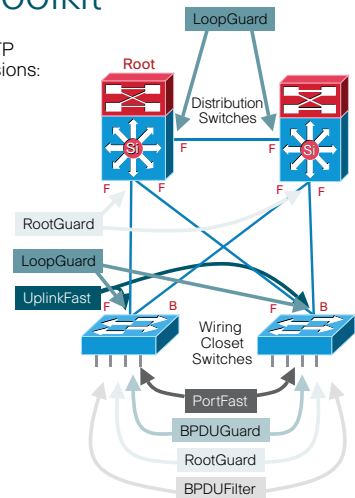
The answer to maximize STP performance is Cisco's STP Toolkit. This advanced suite of tools makes it easy to add layer 2 hardening on Cisco's Catalyst enterprise LAN switches, which use STP (the IEEE 802.1D and 802.1w bridge protocols) on Ethernet port-based VLANs. The result is dramatically improved stability and performance of the basic STP algorithm, and the best part is all these features are already built into your Cisco switch. All you have to do is turn them on.

Cisco Spanning Tree Toolkit

To improve performance of the basic IEEE 802.1D STP algorithm, Cisco has introduced a number of extensions:

- **PortFast***: Bypass listening-learning phase for access port(s)
- **UplinkFast**: Three to five seconds convergence after link failure
- **LoopGuard***: Prevents alternate or root port from becoming designated in absence of BPDUs
- **RootGuard***: Prevents external switches from becoming root
- **BPDUGuard***: Disable PortFast-enabled port if a BPDU is received
- **BPDUFILTER***: Do not send or receive BPDUs on PortFast-enabled ports
- **BackboneFast**: Cuts convergence time by Max_Age for indirect failure

(* Also Supported with MST and Rapid PVST+)



Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches.

To learn about enabling additional Cisco features, visit www.cisco.com/go/turniton.



Powerful Functionality

Cisco's Spanning-Tree Protocol Toolkit delivers a comprehensive spectrum of useful, easy-to-administer functions that greatly improve STP performance and stability.

PortFast

Advantages

- Causes a Layer 2 LAN access port to enter the forwarding state immediately, bypassing the listening and learning states.
- When configured for PortFast, a port is still running STP and can immediately transition to the blocking state if necessary.
- Can be enabled on trunk ports.
- Can have an operational value that is different from the configured value.

Notes

- Should only be used on access ports.
- Should only be used when connecting a single end-station to avoid creating a network loop.
- Enabling on a port connected to a switch might create a temporary bridging loop.

BPDUGuard

Advantages

- When enabled, shuts down a port that receives a BPDU (Bridge Protocol Data Unit).
- Provides a secure response to invalid configurations, because the administrator can manually put the port back in service.
- When configured at the interface level, shuts the port down as soon as the port receives a BPDU, regardless of PortFast configuration.

Notes

- In a valid configuration, PortFast-enabled ports do not receive BPDUs. Reception of a BPDU by a PortFast-enabled port signals an invalid configuration.
- When enabled globally, BPDUGuard applies to all interfaces that are in an operational PortFast state.

BPDUFilter

Advantages

- Prevents a port from sending or receiving BPDUs.

Notes

- Can be configured on a per-port basis.
- When configured globally, applies to all operational PortFast ports.
- When an operational PortFast port receives a BPDU it immediately loses its operational PortFast status, BPDU filtering is automatically disabled on the port, and STP resumes sending BPDUs on the port.
- Explicitly configuring PortFast BPDU filtering on a port that is not connected to a host can result in bridging loops.
- If a port configuration is not set to the default configuration, the PortFast setting will not affect PortFast BPDU filtering.

UplinkFast

Advantage

- Provides fast convergence after a direct link failure and can achieve load balancing between redundant Layer 2 links using uplink groups.

Notes

- Most useful in wiring-closet switches.
- When enabled, affects all VLANs on the Catalyst 6500 series switch.
- Cannot be configured on an individual VLAN.
- The IEEE 802.1w "rapid" STP enhancements include this feature.

RootGuard

Advantages

- Prevents a port from becoming root port or blocked port.
- When a RootGuard-configured port receives a superior BPDU, the port immediately goes to the root-inconsistent (blocked) state.

BackboneFast

Advantages

- Initiated when a root port or blocked port on a network device receives inferior BPDUs from its designated bridge.
- Provides fast failover when an indirect link failure occurs.

Notes

- Operates correctly only when enabled on all network devices in the network.
- Not supported on Token Ring VLANs.
- Is supported for use with third-party network devices.

LoopGuard

Advantages

- Helps prevent bridging loops that could occur because of a uni-directional link failure on a point-to-point link.
- When enabled globally, applies to all point-to-point ports on the system.
- Detects root ports and blocked ports and ensures they keep receiving BPDUs from the designated port on the segment.
- When enabled, if a root or blocked port stops receiving BPDUs from its designated port, it transitions to the loop-inconsistent blocking state.

- Can be enabled on a per-port basis.
- When enabled, it is automatically applied to all active instances or VLANs to which that port belongs.
- When disabled for specified ports, moves all loop-inconsistent ports to the listening state.
- When enabled on an EtherChannel (link bundle) and the first link becomes unidirectional, it blocks the entire channel until the affected port is removed from the channel.

Notes

- Cannot enable on PortFast ports, Dynamic VLAN ports, or RootGuard-enabled switches.
- Does not affect UplinkFast or BackboneFast operation.
- Must be enabled on point-to-point links only.
- When LoopGuard blocks the first port in an EtherChannel, no BPDUs will be sent over the channel even if other ports in channel bundle are operational.
- Port Aggregation Protocol enforces uniform LoopGuard configuration on all ports in the channel group.

Contact your Cisco Systems Engineer for more information and assistance in turning on the full functionality of your Cisco routers and switches. To learn about enabling additional Cisco features, visit www.cisco.com/go/turniton.