

Catalyst 6000 Family Release 5.1CSX and 5.2CSX Supervisor Software

Overview

Release 5.1CSX of the Catalyst® 6000 Family supervisor software introduces support for the Catalyst 6000 Family switches, including the Catalyst 6009 chassis and the Catalyst 6509 chassis, and a variety of Ethernet, Fast Ethernet, and Gigabit Ethernet line cards. Release 5.2CSX runs on all Catalyst 6000 Family Supervisors.

Release 5.2CSX of the Catalyst 6000 Family Supervisor software adds support for high-performance Multilayer Switching Module (MSM) and the six-slot Catalyst 6006 and Catalyst 6506 chassis, as well as providing a maintenance upgrade from the 5.1CSX release. Release 5.1CSX runs on all Catalyst 6000 Family Supervisors.

Features at a Glance

New Hardware Support

Release 5.1CSX

- Catalyst 6009 32-Gbps nine-slot chassis switching platform (WS-C6009)
- Catalyst 6509 256-Gbps nine-slot chassis switching platform (WS-C6509)
- Catalyst 6000 Family Supervisor Engine I with dual-port 1000BaseX uplinks, GBIC (WS-X6K-SUP1-2GE)
- Eight-port Gigabit Ethernet switching module, GBIC (WS-X6408-GBIC)
- 48-port 10/100BaseTX Fast Ethernet switching module, RJ-45 (WS-X6248-RJ-45)
- 24-port 100BaseFX multimode Fast Ethernet switching module, MT-RJ (WS-X6224-100FX-MT)

Release 5.2CSX

- Catalyst 6006 32-Gbps six-slot chassis switching platform (WS-C6006)
- Catalyst 6506 256-Gbps six-slot chassis switching platform (WS-C6506)
- Multilayer switching module (WS-X6302-MSM)
- 48-port 10/100BaseTX Fast Ethernet switching module, telco RJ-21 (WS-X6248-TEL)

New Software Features

Release 5.1CSX

- Multimodule EtherChannel® support
- IP address supernetting
- Quality-of-Service (QoS): port level delay and drop threshold settings
- QoS: 802.1Q classification, drop, and delay thresholds
- 802.1Q to ISL VLAN mapping

All contents are Copyright © 1992--2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Uni-Directional Link Detection (UDLD) for fiber links
- Switch Port Analyzer (SPAN) Enhancements
- HC RMON (high capacity, 64-bit counters)

Release 5.2CSX

- Layer 3 IP/IP multicast switching*
- Layer 3 IPX® Switching**
- IP address Load Balancing on Fast or Gigabit EtherChannel
- IEEE GARP VLAN Registration Protocol (GVRP)
- IEEE GARP Multicast Registration Protocol (GMRP)
- Spanning Tree Protocol (STP) enable/disable per VLAN
- Traceroute MIB

* Use of this feature requires the purchase of the Multilayer switching module. (See ordering information below.)

** Use of this feature requires the purchase of the Multilayer switching module and the IPX feature license. (See ordering information below.)

Table 1 Release 5.1CSX Software Feature-Function-Benefit Table

Feature	Function	Benefit
MultiModule EtherChannel Support	<ul style="list-style-type: none"> • Up to eight ports may build a channel • Ports within channel may be cross-module 	<ul style="list-style-type: none"> • Allows up to 16 Gbps full duplex (8 Gbps each direction) between switches • Better redundancy for Fast EtherChannel and Gigabit EtherChannel
IP Address Supernetting	<ul style="list-style-type: none"> • Supports variable length subnet masks for switch IP address on sc0 (Classless InterDomain Routing—RFC 1518) 	<ul style="list-style-type: none"> • Allows the administrator to use any subnet mask length required for internal IP addressing scheme
QoS Port Level Delay and Drop Threshold Settings	<ul style="list-style-type: none"> • Provides four user-defined levels of drop threshold management per ingress port • Provides two user-defined levels of drop threshold management for each of two queues per egress port 	<ul style="list-style-type: none"> • Provides a proven mechanism to ensure that higher priority traffic is given preference when a port receives queue fills beyond a user-defined threshold • Provides a proven mechanism to ensure that higher priority traffic is given preference when a port transmit queue fills beyond a user defined threshold due to network congestion on the egress interface
QoS: 802.1p Classification	<ul style="list-style-type: none"> • Allows the switch to set 802.1p class-of-service (CoS) values on traffic received from a specific port • Allows the switch to set 802.1p CoS values on traffic destined to a specific host MAC address or VLAN pair 	<ul style="list-style-type: none"> • Enables network-wide differentiated service levels for different traffic on an ingress port basis • Enables network-wide differentiated service levels for traffic destined to specific hosts or servers
802.1Q to ISL VLAN Mapping	<ul style="list-style-type: none"> • Allows mapping of up to eight 802.1Q VLANs numbered above 1000 to ISL VLANs 	<ul style="list-style-type: none"> • Allows seamless integration between ISL and 802.1Q VLAN numbering
Uni-Directional Link Detection (UDLD) for Fiber Links	<ul style="list-style-type: none"> • UDLD is a new protocol developed by Cisco to detect unidirectional connectivity on network links. • When a unidirectional link is detected, UDLD shuts down the affected port and alerts the user. 	<ul style="list-style-type: none"> • Eliminates a number of difficult-to-troubleshoot network problems on fiber Ethernet links, including spanning-tree topology loops
SPAN (Switch Port Analyzer) Enhancements	<ul style="list-style-type: none"> • Multiple concurrent SPAN Sessions <ul style="list-style-type: none"> – Up to 2 Ingress (RX) or both (RX+TX) SPAN sessions – Up to 4 egress (TX)-only SPAN sessions • SPAN multiple source ports independent of VLAN membership • SPAN multiple VLANs • The SPAN source may now be configured to monitor traffic from multiple VLANs. (Previously it was only possible to SPAN a single VLAN.) 	<ul style="list-style-type: none"> • These enhancements provide a great deal of flexibility in connecting external analysis devices to a Catalyst switch. • Allows use of intrusion detection devices such as Cisco NetRanger® at the same time that a Network Analysis Module or SwitchProbe or other network analyzer is being used on the same switch
High Capacity RMON Counters	<ul style="list-style-type: none"> • Provides 64-bit counters for mini-RMON MIB objects 	<ul style="list-style-type: none"> • Enhances mini-RMON capabilities and allows accurate tracking of high-speed Gigabit Ethernet ports without wrapping counters

Table 2 Release 5.2CSX Software Feature-Function-Benefit Table

Feature	Function	Benefit
Layer 3 IP/IP Multicast Switching	<ul style="list-style-type: none"> 4-6 Mpps Layer 3 switching for IP and IP multicast packets 	<ul style="list-style-type: none"> Provides multigigabit in-the-box Layer 3 switching performance for IP and IP multicast packets Requires Multilayer Switching Module (WS-X6302-MSM)
Layer 3 IPX Switching	<ul style="list-style-type: none"> 4-6 Mpps Layer 3 switching for IPX packets 	<ul style="list-style-type: none"> Provides multigigabit in-the-box Layer 3 switching performance for IPX packets Requires Multilayer Switching Module (WS-X6302-MSM) and IPX feature license (FRC6-MSM-IPX)
IP Address Load Balancing on Fast/Gigabit EtherChannel	<ul style="list-style-type: none"> Option to use source and destination IP address as load balancing scheme for channeling 	<ul style="list-style-type: none"> In some configurations, IP address-based load balancing gives better distribution than MAC address-based
IEEE GVRP	<ul style="list-style-type: none"> GARP VLAN Registration Protocol as specified in 802.1Q 	<ul style="list-style-type: none"> Allows use of standards-based 802.1Q GVRP protocol for configuration of VLANs on a switch Required for full IEEE 802.1Q compliance
IEEE GMRP	<ul style="list-style-type: none"> GARP Multicast Registration Protocol as specified in 802.1p 	<ul style="list-style-type: none"> Supports standards-based 802.1p GMRP protocol for signaling of multicast group membership join and leave requests Required for full IEEE 802.1Q compliance
STP Enable/Disable per VLAN	<ul style="list-style-type: none"> Provides the ability to set spanning tree on or off for a given VLAN, instead of system-wide 	<ul style="list-style-type: none"> Provides better granularity of spanning tree parameters Allows the administrator to better define where spanning tree should be enabled in the network
Traceroute MIB	<ul style="list-style-type: none"> Provides the SNMP MIB object for traceroute 	<ul style="list-style-type: none"> Allows an SNMP-based network management station to poll for traceroute on the switch

Release 5.1CSX Feature Descriptions

Multimodule EtherChannel Support

With software release 5.1CSX, the Catalyst 6000 Family of switches builds additional functionality into the network-proven Cisco technique of port bundling called EtherChannel. EtherChannel provides parallel bandwidth of up to 1600 Mbps (Fast EtherChannel full duplex) or 16 Gbps (Gigabit EtherChannel) between a Catalyst 6000 or 6500 series switch and another switch or host by grouping multiple Fast or Gigabit Ethernet interfaces into single logical transmission paths. Two to eight ports of the same speed and configuration (Gigabit or Fast Ethernet) may be channeled together between neighboring switches or between a switch and a host or server running a compatible channeling protocol.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel within milliseconds. A trap is sent upon a failure identifying the switch, the EtherChannel, and the failed link.

The Catalyst 6000 and 6500 series switches provide the ability to define an EtherChannel composed of ports on separate line cards. This, combined with the fault-tolerant capability of the EtherChannel protocol, has the additional capability of providing extremely rapid recovery in the event of a line card failure.

IP Address Supernetting

IP Supernetting, compatible with classless interdomain routing (CIDR), allows entry of a netmask, instead of a subnet mask, in defining the IP address for switch. Setting the IP address on the switch is required for telnet access to the switch or Simple Network Management Protocol (SNMP) management of the switch.

QoS: Port Level Delay and Drop Threshold Settings

Networks typically operate on a best-effort delivery basis. All traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped. However, network managers are increasingly presented with a variety of bandwidth-hungry applications that compete for limited bandwidth on the enterprise network. These applications have a variety of characteristics. They may be mission-critical legacy applications with a Web interface, online business-critical applications, or newer multimedia-based applications such as desktop videoconferencing, Web-based training, and voice (telephone) over IP. Some of these applications are vital to core business processes, while many are not. It is the network manager's job to ensure that mission-critical application traffic is protected from other bandwidth-hungry applications, while still enabling less critical applications such as desktop videoconferencing.

Enterprises that want to deploy new bandwidth-hungry applications are judging that it is paramount to also ensure the continued success of mission-critical applications over both the LAN and WAN. This can be achieved by defining network policies, which align network resources with business objectives and are enforced by means of QoS mechanisms. Without these QoS controls, nonvital applications can quickly exhaust network resources at the expense of more important ones, such as mission-critical applications, thus compromising business processes and certainly productivity.

The QoS feature on the Catalyst 6000 Family of switches prioritizes network traffic with IEEE 802.1p class-of-service (CoS) values that allow network devices to recognize and deliver high-priority traffic in a predictable manner. When congestion occurs, QoS drops low-priority traffic to allow delivery of high-priority traffic.

Ports can be configured as trusted or untrusted, indicating whether or not to trust the CoS values in received frames to be consistent with network policy. On trusted ports, QoS uses received CoS values. On untrusted ports, QoS replaces received CoS values with the port CoS value.

Each port on the switch has a single receive-queue buffer and four user-defined levels of thresholds for incoming traffic. The receive-queue-drop threshold percentages are configurable, as well the CoS values mapped to each drop threshold. All ports in the switch use the same drop threshold configuration.

The default settings of these thresholds are as follows:

- Using receive-queue-drop threshold 1, the switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 20 percent or more full.
- Using receive-queue-drop threshold 2, the switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 40 percent or more full.
- Using receive-queue-drop threshold 3, the switch drops incoming frames with CoS 4 or 5 when the receive-queue buffer is 75 percent or more full.
- Using receive-queue-drop threshold 4, the switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.

On the transmit side, each port has a low-priority transmit queue and a high-priority transmit queue. The administrator can configure how the low- and high-priority transmit queues share the total available transmit queue. Each transmit queue has two drop thresholds as follows:

- Frames with CoS 0, 1, 2, or 3 go to the low-priority transmit queue (queue 1).
 - Using transmit-queue 1 drop-threshold 1, when congestion occurs the switch drops frames with CoS 0 or 1 when the low-priority transmit queue buffer is 40 percent full.
 - Using transmit-queue 1 drop-threshold 2, when congestion occurs the switch drops frames with CoS 2 or 3 when the low-priority transmit-queue buffer is 100 percent full.
- Frames with CoS 4, 5, 6, or 7 go to the high-priority transmit-queue (queue 2).
 - Using transmit-queue 2 drop-threshold 1, when congestion occurs the switch drops frames with CoS 4 or 5 when the high-priority transmit-queue buffer is 40 percent full.
 - Using transmit-queue 2 drop-threshold 2, when congestion occurs the switch drops frames with CoS 6 or 7 when the high-priority transmit-queue buffer is 100 percent full.

All ports in the switch use the same transmit-queue and drop-threshold configuration.

QoS 802.1p Classification

QoS evaluates received frames as either classified or unclassified:

- Frames with CoS values are called classified frames.
- Frames without CoS values are called unclassified frames.

On each port, QoS applies the port's CoS value (the default is zero) to unclassified frames or, if the port is untrusted, QoS applies the port's CoS value to all frames.

Before entering the receive queue, all frames have either a received CoS value or the applied port CoS value.

Unclassified frames received on trusted ports and all frames received on untrusted ports may be assigned a CoS value.

In addition, a CoS value may be assigned to all frames, from both trusted and untrusted ports, destined for a particular host destination MAC address and VLAN number value pair.

Mapping 802.1Q VLAN IDs to ISL VLAN IDs

IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved). The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number. This feature allows the administrator to define mappings of 802.1Q VLANs above 1000 to ISL VLANs.

Note: You can map up to eight VLANs. Only one 802.1Q VLAN can be mapped to a specific ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

Uni-Directional Link Detection for Fiber Links

UDLD is a new-link layer protocol developed by Cisco to detect unidirectional connectivity on network links. The UDLD protocol allows devices connected through fiber-optic Ethernet, Fast Ethernet, and Gigabit Ethernet to monitor the physical configuration of the cables and detect when a unidirectional link or a self loop exists. When a link error is detected, UDLD shuts down the affected port and alerts the user.

A unidirectional link occurs when traffic transmitted by one device over a link is received by the neighbor, but traffic from the neighbor is not received. Unidirectional links may cause a variety of problems difficult to troubleshoot, including spanning-tree topology loops.

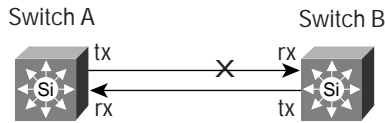
UDLD Hello packets are sent periodically to neighbor devices connected through fiber-optic links to keep each device informed about its neighbors. When a Hello message is received, it is cached and kept in memory for a defined time interval, called holdtime, after which the cache entry is considered stale and is aged out. If a new Hello message is received when a correspondent old cache entry has not been aged out yet, then the old entry is dropped and replaced by the new one with a reset time-to-live timer.

If a switch running the UDLD protocol receives UDLD hello packets from a neighbor switch, but these packets fail to contain the proper UDLD neighbor information, the link is flagged as unidirectional and the port is shut down. Note that for UDLD to work properly, both switches need to be configured for UDLD. If both switches on either side of the fiber optic link are not configured for UDLD, the protocol will not shut down the port. UDLD is configured on either a global or per-port basis. It is supported on all Catalyst 6000 Family switches and will be supported on the Catalyst 5000 Family switches in an upcoming software release. UDLD is disabled globally on the switch by default. Once enabled globally, it will then be enabled on all Ethernet line cards that use fiber media (for example, 100BaseFX, 1000BaseSX, and so on.).

Figures 1-1, 1-2, and 1-3 show examples of link-error conditions UDLD discovers.

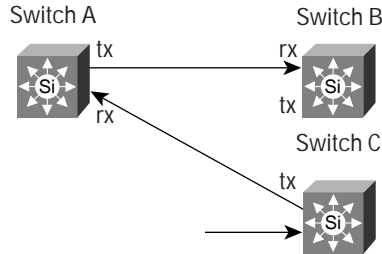
In Figure 1-1, Switch A successfully receives traffic from Switch B on the fiber-optic port. However, due to either a faulty fiber optic cable, a faulty transmitter in Switch A, or receive port failure in Switch B, Switch B does not receive traffic from Switch A on the same port. The UDLD protocol running on Switch A will signal an error condition and disable the port.

Figure 1-1



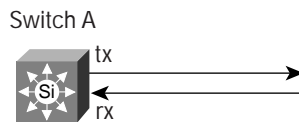
In Figure 1-2, Switch B successfully receives traffic from Switch A on the fiber-optic port. However, due to faulty wiring, Switch A receives traffic from Switch C on this port. The UDLD protocol running on Switch A will signal an error condition and disable the port.

Figure 1-2



In Figure 1-3, Switch A is incorrectly wired for a self loop back to its own port. The UDLD protocol will signal an error condition and disable the port.

Figure 1-3



SPAN Enhancements


The SPAN feature allows the mirroring of network traffic for analysis by a SwitchProbe device or other RMON probe. SPAN mirrors traffic from one or more source ports on the same VLAN to a destination port for analysis.

The Catalyst 6000 Family supports several enhancements to the SPAN capability found in the Cisco Catalyst switches. The first is the ability to support multiple concurrent SPAN sessions, each to a different destination port. The Catalyst 6000 family supports two ingress (RX) or Both (RX and TX) SPAN sessions and up to four egress (TX)-only SPAN sessions. The following SPAN sessions in Table 3 can all be active at the same time.

Table 3 Span Example

	SPAN Source(s)	SPAN Destination	SPAN Direction	Notes
SPAN Session 1:	2/10	6/1	Both	HP probe on port 6/1
SPAN Session 2:	2/11	6/2	RX	HP probe on port 6/2
SPAN Session 3:	3/1, 3/2	7/12	TX	SwitchProbe on port 7/12
SPAN Session 4:	2/1-3/24	8/11	TX	NetRanger on port 8/11
SPAN Session 5:	VLAN_4, VLAN_7	8/12	TX	Sniffer on port 8/12
SPAN Session 6:	VLAN_9	8/10	TX	W&G DA-30 on port 8/10

There can be overlap in the SPAN sources—notice that ports 3/1 and 3/2 are in both the second and third SPAN sessions above.



With the ability to SPAN multiple source ports independent of VLAN membership, it is now possible to select ports in different VLANs.

The SPAN source may now be configured to monitor traffic from multiple VLANs. (Previously it was only possible to SPAN a single VLAN.) For example, the SPAN source can be set to mirror traffic from VLAN 2 and VLAN 3 and send this traffic to the SPAN destination.

Release 5.2CSX Feature Descriptions

Layer 3 IP, IP Multicast, and IPX Switching

With Release 5.2CSX software and the Multilayer Switching Module (MSM), the Catalyst 6000 Family switches now provide Layer 3 switching which enables Catalyst 6000 Family customers to deploy high-performance multiprotocol, multilayer switch services in the backbone distribution of their network to support wiring closet switches. The MSM, which is based on advanced switching ASICs from Cisco, uses Cisco Express Forwarding (CEF) technology to switch packets between subnets and VLANs. It combines sophisticated Cisco IOS® software features with advanced ASIC technology to support wire-speed multiprotocol routing in a compact, manageable platform.

The MSM requires a single slot (with no slot dependency) in any Catalyst 6000 (WS-C6006 and WS-C6009) or Catalyst 6500 (WS-C6506 and WS-C6509) Series platform. The MSM module was designed with fully integrated application specific integrated circuits (ASICs) enabling aggregate throughput of up to six million packets per second for Layer 3 switching (IP, IPX, and IP multicast). Combined with industry-leading Cisco IOS software, the high-performance MSM enables the Catalyst 6000 Family to be particularly effective as a backbone/distribution switch.

Key Benefits

Industry-Leading Layer 3 with Cisco IOS Software

The MSM supports feature-rich IP, IPX, and IP multicast Layer 3 switching without sacrificing the performance required in a scalable backbone/distribution platform. This unique combination of performance and flexibility enables customers to integrate the Catalyst 6000 Family into existing Cisco IOS network configurations while at the same time scaling their backbone capacity to gigabit speeds. Routing protocols supported in the MSM module include:

- Enhanced IGRP (EIGRP)
- Interior Gateway Routing Protocol (IGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP) Versions I and II
- Static routes
- Route redistribution

Additional Cisco IOS Protocols Supported in the Catalyst 6000 Family MSM Module Include:

- Hot Standby Router Protocol (HSRP)
- Internet Group Management Protocol (IGMP) Versions I and II
- Dynamic Host Configuration Protocol (DHCP) Relay
- Cisco Group Management Protocol (CGMP)
- Internet Control Message Protocol (ICMP)
- Gateway Discovery Protocol (GDP)
- ICMP Router Discovery Protocol (IRDP)
- Bootstrap Protocol (BOOTP) Relay
- Protocol Independent Multicast (PIM) (sparse and dense mode)

Wire-Speed IPX Support

The Catalyst 6000 Family MSM module is also a full-featured IPX router. The MSM provides basic services such as Novell network RIP and Service Advertising Protocols (SAPs), Novell Enhanced IGRP, and route distribution among all of these protocols. In addition, the MSM supports the following features to scale Novell networks:

- Get Nearest Server (GNS) response filtering and round-robin GNS support
- Novell RIP
- SAP, protocol, and NetBIOS name filtering
- Equal-cost path loadsharing
- Variable RIP and SAP timers
- Novell NetBIOS type 20 propagation support for legacy applications that continue to be mission critical
- Novell-compliant IPX ping utility

IP Address Load Balancing on Fast and Gigabit EtherChannel

EtherChannel distributes frames across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

On the Catalyst 6000 Family of switches, EtherChannel frame distribution can use either MAC addresses or IP addresses and either source or destination or both source and destination addresses. The selected mode applies to all EtherChannel configured ports on the switch.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is only going to a single MAC address (a router, for example), using the destination MAC address always chooses the same link in the channel; using source addresses or IP addresses may result in better frame distribution.

The ability to configure EtherChannel frame distribution by IP address is only available on Rev-A Supervisor boards on the Catalyst 6000 and 6500 switches. To determine the revision of your Supervisor, use the “show module” command. If the display shows the “Sub-Type” to be “L2 Switching Engine II WS-F6020A,” then EtherChannel frame distribution by IP address is configurable on your switch and the default is to use source and destination IP addresses.

Trace Route MIB

Trace Route is helpful in locating routing issues on a distant gateway. If the local routing tables are correct on locally administered routers, distant routers under another administration may be the cause of incorrectly routed or dropped data packets. Trace Route will give a general location of where the packet is getting lost. Once a packet is handed to the next gateway, it is that gateway’s responsibility to see to it that the packet continues on correctly to the final destination. The Catalyst 6000 Family of switches now add support the SNMP management information base (MIB) for Trace Route.

Spanning Tree Protocol Enable or Disable per VLAN

The ability to enable or disable Spanning Tree per VLAN is the latest Cisco enhancement to the Spanning Tree protocol.

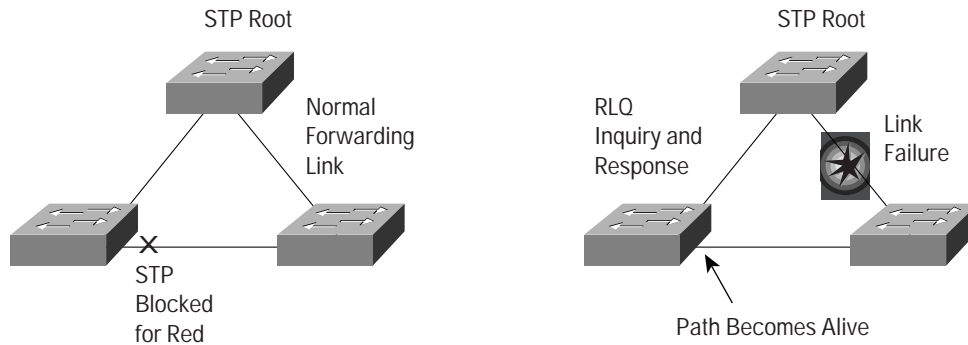
STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path must exist at Layer 2 between two stations. STP operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The Catalyst 6000 and 6500 series switches use STP (IEEE 802.1D bridge protocol) on all Ethernet VLANs. When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. In STP, an algorithm calculates the best loop-free path throughout a Catalyst switched network. The switches send and receive spanning-tree packets at regular intervals. The switches do not forward the packets, they use the packets to identify a loop-free path. The default configuration has STP enabled for all VLANs.

Multiple active paths between stations cause loops in the network. If a loop exists in the network, you might receive duplicate messages. When loops occur, some switches see stations on both sides of the switch. This condition confuses the forwarding algorithm and allows duplicate frames to be forwarded.

To provide path redundancy, STP defines a tree that spans all switches in an extended network. STP forces certain redundant data paths into a standby (blocked) state. If one network segment in the STP becomes unreachable, or if STP costs change, the spanning-tree algorithm reconfigures the spanning-tree topology and reestablishes the link by activating the standby path as shown in Figure 2-1.

Figure 2-1 Spanning Tree Convergence



In addition to the enhancements Cisco has made to the Spanning Tree Protocol (PortFast, UplinkFast, BackboneFast), the Catalyst 6000 and 6500 Series switches now have the ability to enable or disable STP on a per-VLAN basis. Previous to this, STP had to be either enabled or disabled on the entire switch. This enhancement allows the administrator to better define where the Spanning Tree Protocol should operate in the network. For example, VLANs that are architected without the possibility of multiple redundant links (that is, loop) might have improved stability when STP is disabled.

Note that STP is enabled by default on all VLANs and on all newly created VLANs.

Useful References

- Catalyst 6000 Family Overview
<http://cco/warp/public/cc/cisco/mkt/switch/cat/6000/index.shtml>
- Catalyst 6000 Family Documentation
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>
- Catalyst 6000 Multilayer Switching Module
http://cco/warp/public/cc/cisco/mkt/switch/cat/6000/prodlit/c60fm_ds.htm
- Catalyst 6000 Family Release Notes
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/index.htm>

System Requirements for 5.1CSX

- Release 5.1CSX software runs on all Cisco Catalyst 6000 Family Supervisors.

System Requirements for 5.2CSX

- Release 5.2CSX software runs on all Cisco Catalyst 6000 Family Supervisors.

Ordering Information

The IP/IP multicast and IPX Layer 3 switching feature sets are combined in a single image for the MSM Cisco IOS Release 12.0(1a)WX5(6d). This image requires the 5.2CSX release or higher running on the Supervisor. Please upgrade the Supervisor to the 5.2CSX image or higher before installing the MSM in the chassis. Use of Layer 3 IPX switching on the MSM requires purchase of the IPX feature set license. Use of mini-RMON on the Catalyst 6000 and 6500 Series switches requires the purchase of the RMON agent license. One IPX feature set software license is required for each MSM that will be enabled to Layer 3 switch IPX traffic (that is, a chassis with dual MSMs does require two licenses). Only one RMON agent license is required per chassis (that is, a chassis with redundant supervisors does *not* require two licenses). Licensing is based on the honor system.

Table 4 Part Numbers

Product Number	Description
Release 5.2CSX Feature Set License	
SFC6K-SUP-5.2.1	Catalyst 6000 Supervisor Flash Image, Release 5.2(1)
SFC6-MSM-12.0.1W	Catalyst 6000 MSM IP/IP-Multicast Routing Feature Set
FR6-MSM-IPX	Catalyst 6000 MSM IPX Feature Set License
Mini-RMON Agent Licenses	
WS-C6X06-EMS-LIC	Catalyst 6X06 RMON Agent License
WS-C6X09-EMS-LIC	Catalyst 6X09 RMON Agent License

Customers can download Release 5.2CSX Supervisor software from Cisco Connection Online (CCO) in the Software Image Library. Customers who are unable to download the files electronically can order a software kit with 3.5-inch IBM formatted floppy disks by contacting Cisco at 408 526-4000 or, in North America, call 800 553-NETS (6387).



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe s.a.r.l.
Parc Evolic, Batiment L1/L2
16 Avenue du Quebec
Villebon, BP 706
91961 Courtaboeuf Cedex
France
<http://www-europe.cisco.com>
Tel: 33 1 69 18 61 00
Fax: 33 1 69 28 83 26

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Connection Online Web site at <http://www.cisco.com/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela