



Product Overview

The Catalyst 6000 family switches facilitate the migration from traditional shared-hub LANs to large-scale, fully integrated internetworks. These switches provide switched connections to individual workstations, servers, LAN segments, backbones, or other switches using a variety of media.

This chapter consists of these sections:

- Supervisor Engine Software, page 1-1
- Supported Software Features, page 1-1
- Supported Internet Protocols, page 1-7
- Supported MIBs, page 1-8

Supervisor Engine Software

The supervisor engine software is factory-installed on every supervisor engine. Some modules (such as ATM modules) require an additional factory-installed software image.

The Catalyst 6000 family switches share a command-line interface (CLI) with which you can configure modules and ports on the switches. For more information, see Chapter 2, “Command-Line Interfaces.” For descriptions of the available CLI commands, refer to the *Catalyst 6000 Family Command Reference* publication.

Supported Software Features

The Catalyst 6000 family switches support these software features:

- Spanning Tree Protocol, page 1-2
- VLANs, page 1-2
- VLAN Trunks, page 1-3
- EtherChannel Port Bundles, page 1-3
- Network Security, page 1-3
- Network Management, page 1-4
- Multicast Services, page 1-5
- Broadcast Suppression, page 1-5
- Administrative Features, page 1-5

- InterVLAN Routing, page 1-6
- Multilayer Switching and NetFlow Data Export, page 1-6
- Access Control Lists, page 1-6
- Quality of Service, page 1-6
- Redundant Supervisor Operation, page 1-7
- Voice-Over-IP, page 1-7

Spanning Tree Protocol

The Spanning Tree Protocol (STP) allows you to create fault-tolerant internetworks that ensure an active, loop-free data path between all nodes in the network. STP uses an algorithm to calculate the best loop-free path throughout a switched network.

The Catalyst 6000 family switches support the following spanning tree enhancements:

- Spanning tree PortFast—PortFast allows a port with a directly attached host to transition to the forwarding state immediately, bypassing the listening and learning states. Additionally, PortFast BPDU guard provides a method for preventing loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. The PortFast BPDU guard option allows for fast convergence in a network while also preventing loops from occurring.
- Spanning tree UplinkFast—UplinkFast provides fast convergence after a spanning tree topology change and achieves load balancing between redundant links using uplink groups. Uplink groups provide an alternate path in case the currently forwarding link fails. UplinkFast decreases spanning tree convergence time for switches that experience a direct link failure.
- Spanning tree BackboneFast—BackboneFast reduces the time needed for the spanning tree to converge after experiencing a topology change caused by an indirect link failure. BackboneFast decreases spanning tree convergence time for any switch that experiences an indirect link failure.

For information on configuring STP, see Chapter 6, “Configuring Spanning Tree.” For information on configuring the STP enhancements, see Chapter 7, “Configuring Spanning Tree PortFast, UplinkFast, and BackboneFast.”

VLANs

A VLAN is an administratively defined broadcast domain that enhances performance by limiting traffic; it allows the transmission of traffic among stations that belong to it and blocks traffic from other stations in other VLANs. VLANs can provide security barriers (firewalls) between end stations on different VLANs within the same switch. Only end stations within the VLAN receive packets that are unicast, broadcast, or multicast (flooded).

These VLAN-related features are also supported on the switches:

- VLAN Trunk Protocol (VTP)—VTP maintains VLAN naming consistency and connectivity between all devices in the VTP management domain. When you add new VLANs on a switch, VTP distributes this information automatically to all the devices in the management domain. VTP is transmitted on all trunk connections, including ISL, 802.1Q, and ATM LAN Emulation (LANE). You can have redundancy in a domain by using multiple VTP servers, through which you can maintain and modify the global VLAN information. Only a few VTP servers are required in a large network.

- GARP VLAN Registration Protocol (GVRP)—GVRP is an industry-standard VLAN management protocol specified in IEEE 802.1p for use in IEEE 802.1Q environments.

For information on configuring VTP, see Chapter 8, “Configuring VTP.” For information on configuring VLANs, see Chapter 9, “Configuring VLANs.” For information on configuring GVRP, see Chapter 11, “Configuring GVRP.”

VLAN Trunks

You can extend VLANs from one switch to another, or from a switch to a router, using VLAN trunks. To verify the trunking capabilities of a particular port, see the hardware documentation for your switch or use the **show port capabilities** command.

You can split VLAN traffic between parallel trunks. By setting spanning tree parameters on a per-VLAN basis, you can define which VLANs are active on a trunk and which use the trunk as a backup if the primary trunk fails.

For information on configuring trunks, see the following sections:

- For information on configuring ISL and 802.1Q Ethernet VLAN trunks, see Chapter 10, “Configuring Ethernet VLAN Trunks.”
- For information on configuring ATM LANE, refer to the *ATM Software Configuration and Command Reference—Catalyst 5000 Family and Catalyst 6000 Family Switches* publication.

EtherChannel Port Bundles

EtherChannel port bundles allow you to create high-bandwidth connections between two switches or a switch and a router by grouping multiple ports into a single logical transmission path.

For information on configuring EtherChannel, see Chapter 5, “Configuring EtherChannel.”

Network Security

The Catalyst 6000 family switches support these network security features:

- Local, RADIUS, TACACS+, and Kerberos authentication—You can control access to the switch using any combination of these authentication methods. For information on configuring authentication, see Chapter 15, “Switch Access: Using Authentication, Authorization and Accounting.”
- Secure port filtering—You can block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of a station attempting to access the port is different from the configured or learned MAC address. For information on secure port filtering, see Chapter 29, “Configuring Port Security.”
- IP permit list—You can restrict incoming Telnet and SNMP access to a limited list of IP addresses. For information on the IP permit list, see Chapter 28, “Configuring IP Permit List.”

Network Management

The Catalyst 6000 family switches offer network management and control through the CLI or through alternative methods, such as CWSI and SNMP. The switch software supports these network management features:

- **SNMP**—This protocol facilitates the exchange of management information between network devices. Catalyst 6000 family switches support these SNMP types and enhancements:
 - **SNMP**—Simple Network Management Protocol, a Full Internet Standard
 - **SNMP v2C**—Community-based administrative framework for Version 2 of SNMP
 - **SNMP v3**—Community-based administrative framework for Version 3 of SNMP
 - **SNMP trap message enhancements**—Additional information with certain SNMP trap messages, including spanning tree topology change and configuration change notifications.

For information on SNMP, see Chapter 30, “Configuring SNMP.”

- **Remote Monitoring (RMON)**—This protocol allows network monitors and console systems to exchange network monitoring data. The following RMON enhancements are supported:
 - **Extended RMON alarms**—RMON alarms for all MIB objects supported by the Catalyst 6000 family switch SNMP agent.
 - **RMON2 configuration group**—The RMON2 configuration group trap destinations MIB defined in RFC 2021. When you generate a trap, it is sent to all the hosts configured in the `sysTrapReceiverTable` and the `trapDestTable`, and is registered at the given User Datagram Protocol (UDP) port.

For information on RMON, see Chapter 31, “Configuring RMON.”

- **Switched Port Analyzer (SPAN)**—SPAN allows you to monitor traffic on any port for analysis by a network analyzer or RMON probe. Remote SPAN (RSPAN) allows you to remotely monitor any port or VLAN from any other switch in the network. For information on SPAN and RSPAN, see Chapter 32, “Configuring SPAN and RSPAN.”
- **System message logs**—You can redirect system error messages and output from asynchronous events such as an interface transition, to a virtual terminal, internal buffers, or a UNIX host running a syslog server. The syslog format is compatible with 4.3 BSD UNIX. For information on system message logging, see Chapter 21, “Configuring System Message Logging.”
- **Switch TopN reports**—This feature allows you to generate a report showing metrics for port utilization, broadcasts, multicasts, unicasts, and errors. Reports are available through either SNMP or the CLI. The Switch TopN Reports utility cannot be used to generate reports on the Multilayer Switch Feature Card (MSFC), Multilayer Switch Module (MSM), or ATM ports. For information on switch TopN reports, see Chapter 33, “Using Switch TopN Reports.”

For a list of MIBs supported on the Catalyst 6000 family switches, see the “Supported MIBs” section on page 1-8. For additional information, refer to the “*Enterprise MIB User Quick Reference*,” on Cisco Connection Online (<http://www.cisco.com>).

Multicast Services

Multicasting saves bandwidth by forcing the network to replicate packets only when necessary and by allowing hosts to join and leave groups dynamically. These multicast services are supported:

- Internet Group Management Protocol (IGMP) snooping—IGMP snooping manages multicast traffic. The switch software examines IP multicast packets and makes forwarding decisions based on their content. Multicast traffic is forwarded only to ports with attached hosts interested in receiving the multicast traffic. IGMP snooping is supported only with specific hardware.
- GARP Multicast Registration Protocol (GMRP)—GMRP is an industry-standard multicast group membership protocol specified in 802.1p.
- Router Group Management Protocol (RGMP)—Multicast routers receive all multicast data traffic unless they are configured to do otherwise. RGMP enables a switch to reduce network congestion by forwarding multicast data traffic to only those routers that are configured to receive it.

For information on configuring multicast services, see Chapter 34, “Configuring Multicast Services.”

Broadcast Suppression

Broadcast suppression controls excessive broadcast traffic in the network. You can limit the number of broadcasts from switch ports to prevent congestion caused by broadcast storms. For information on configuring broadcast suppression, see Chapter 26, “Configuring Broadcast Suppression.”

Administrative Features

These administrative features are supported:

- Multiple default IP gateways—You can configure up to three default IP gateways to provide redundancy. In the event that the primary gateway is not reachable, the switch uses the secondary default IP gateways in the order in which they were configured. For information on configuring default gateways, see Chapter 3, “Configuring the Switch IP Address and Default Gateway.”
- Domain Name System (DNS)—This protocol resolves IP addresses to host names. In addition, a Catalyst 6000 family switch populates the system name string based on the switch IP address-to-host name mapping in DNS. For information on configuring default gateways, see Chapter 22, “Configuring DNS.”
- Cisco Discovery Protocol (CDP)—This protocol discovers and learns information about neighboring Cisco devices on the network. Network management applications can use CDP to retrieve the device type and SNMP-agent address of neighboring devices so the applications can send SNMP queries to neighboring devices. For information on configuring default gateways, see Chapter 23, “Configuring CDP.”
- Network Time Protocol (NTP)—This protocol time-synchronizes switches by downloading the system time from an NTP server. Synchronization allows events to be correlated when system logs are created and other time-specific events occur. For information on configuring default gateways, see Chapter 25, “Configuring NTP.”

InterVLAN Routing

InterVLAN routing allows network devices in different VLANs to communicate with one another. There are two ways to do interVLAN routing on Catalyst 6000 family switches:

- MSM—For information on configuring interVLAN routing using the MSM, refer to the *Multilayer Switch Module Installation and Configuration Note*.
- MSFC—For information on configuring interVLAN routing using the MSFC, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

Multilayer Switching and NetFlow Data Export

Multilayer Switching (MLS) scales Layer 3 performance to high-performance link speeds by extending the MLS concept introduced in Cisco IOS software to LAN switching hardware. MLS requires a Catalyst 6000 family switch with an MSFC. NetFlow Data Export allows you to export MLS flow information to an RMON probe for analysis.

Three MLS feature sets are supported:

- IP unicast MLS
- IP multicast MLS
- IPX unicast MLS

For more information, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

Access Control Lists

Supported access control lists (ACLs) are as follows:

- IOS ACLs require the MSFC
- VLAN ACLs (VACLs) require the Policy Feature Card (PFC)
- Quality of service (QoS) ACLs require the MSFC and PFC

For information on configuring these ACLs, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

Quality of Service

Typically, networks operate on a *best-effort* delivery basis, which means that 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.

QoS uses classification, marking, policing, and scheduling to transmit traffic from the switch in a predictable manner. For information on configuring QoS, see Chapter 35, “Configuring Quality of Service.”

Redundant Supervisor Operation

Catalyst 6000 family switches support an optional redundant supervisor engine. You can install two supervisor engines in slots 1 and 2 of the chassis. When the switch powers up, the supervisor engine that comes up first enters active mode, while the second supervisor engine enters standby mode.

Both supervisor engines must have the same feature cards:

- L2 Switching Engine I WS-F6020 or L2 Switching Engine II WS-F6020A
- MSFC
- PFC

All network management functions occur on the active supervisor engine. The console port on the standby supervisor engine is inactive. The uplink ports on the standby supervisor engine are active and can be used as normal switch ports.

If the active supervisor engine detects a major problem, it resets itself and the standby supervisor engine seamlessly becomes the active supervisor engine.

For information on how supervisor engine redundancy works, see Chapter 16, “Configuring Redundant Supervisor Engines.”

Voice-Over-IP

Telephony systems built on an IP network instead of the traditional circuit-switched Private Branch Exchange (PBX) are called IP PBX systems. For information on how to configure your Catalyst 6000 family switch for Voice-over-IP networking, see Chapter 36, “Configuring a Voice-over-IP Network.”

Supported Internet Protocols

The Catalyst 6000 family switches support these standard Internet protocols:

- Address Resolution Protocol (ARP)—Determines the destination MAC address of a host using its known IP address.
- Bootstrap Protocol (BOOTP)—Allows the switch (BOOTP client) to retrieve its IP address from a BOOTP server. BOOTP uses connectionless transport layer User Datagram Protocol (UDP).
- Dynamic Host Configuration Protocol (DHCP)—Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
- Internet Control Message Protocol (ICMP)—Allows hosts to send error or control messages to other hosts. ICMP is a required part of IP. For example, the **ping** command uses ICMP echo requests to test if a destination is alive and reachable.
- IP—Sends IP datagram packets between nodes on the Internet. IP is a protocol suite.
- ping—Tests the accessibility of a remote site by sending an ICMP echo request and waiting for a reply.
- Reverse Address Resolution Protocol (RARP)—Determines an IP address knowing only a MAC address. For example, BOOTP, DHCP, and RARP broadcast requests are used to get IP addresses from a BOOTP, DHCP, or RARP server.
- SLIP—Allows IP communications over the administrative interface. SLIP is a version of TCP/IP that runs over serial links.

- **SNMP**—Processes requests for network management stations and reports exception conditions when they occur. These agents require access to information stored in a MIB. (For more information, see the “Network Management” section on page 1-4.)
- **TCP**—Transports full-duplex, connection-oriented, end-to-end packets running on top of IP. For example, Telnet uses the TCP/IP protocol suite.
- **Telnet**—Allows remote access to the administrative interface of a switch over the network (in band). Telnet is a terminal emulation protocol.
- **Trivial File Transfer Protocol (TFTP)**—Downloads software updates and configuration files to workgroup switch products.
- **UDP**—Allows an application (such as an SNMP agent) on one system to send a datagram to an application (a network management station using SNMP) on another system. UDP uses IP to deliver datagrams. UDP/IP protocol suites are used by TFTP and SNMP.

Supported MIBs

Catalyst 6000 family switches support these standard and private MIBs:

- BRIDGE-MIB (RFC 1493)
- CISCO-CDP-MIB
- CISCO-COPS-CLIENT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAGP-MIB
- CISCO-PIB-MIB
- CISCO-PROCESS-MIB
- CISCO-QOS-MIB
- CISCO-RMON-CONFIG-MIB
- CISCO-RSVP-MIB
- CISCO-STACK-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SWITCH-ENGINE-MIB
- CISCO-SYSLOG-MIB
- CISCO-VLAN-BRIDGE-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- HC-RMON-MIB.my

- IF-MIB (RFC 1573)
- RFC 1213 (MIB II)
- RMON MIB (RFC 1757)
- RMON2-MIB (probeInformationGroup, trapDestTable from RFC 2021)
- SMON-MIB

For information about MIBs, refer to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

