CHAPTER 3

Concepts

This chapter explains the following concepts that you need to understand to effectively configure and manage your Catalyst 2820 or 1900.

- Address learning
- Forwarding, filtering, and flooding
- Switching modes
- Securing ports
- Full-duplex 100BaseTX or 100BaseFX
- Flooding controls
- Port monitoring
- Remote monitoring (RMON)
- Virtual LANs (VLANs)

Address Learning

With multiple Media Access Control (MAC) address support on all ports, you can connect individual workstations, repeaters, switches, routers, or other network devices to any switch port.

The Catalyst 2820 and 1900 maintain an address table associating the address of each device with the port on which it resides.

The Catalyst 2820 and 1900 can automatically learn the source address of packets received on each port. The switch then adds these dynamic addresses and associated port numbers to the address table. As stations are added or removed from the network, the switch

automatically updates the address table by adding new entries and aging out ones currently not in use. Dynamic addressing simplifies the management of the switch and requires no configuration.

A network administrator can also manually enter addresses into the address table. These static addresses do not age and must be added or removed by the administrator. Static addressing also allows for a measure of security in that access to a port can be restricted. See the “Securing Ports” section in this chapter for more information.

Forwarding, Filtering, and Flooding

The Catalyst 2820 and 1900 forward, filter, and flood packets in accordance with the IEEE 802.1d specification. Each switch transfers, or forwards, packets between any combination of ports based on the destination address of the received packet. By maintaining an address table that determines which port the address resides on, the switch is able to forward the packet only to that port. If the destination address resides on the port the packet was received from, the packet is filtered and not forwarded.

If a destination address is not known by the switch, it sends (floods) the packet to all ports. This ensures that the packet will arrive at its destination even when the switch does not know on which port the destination address resides. The Catalyst 2820 and 1900 can also flood multicast and broadcast packets. There are times when it can be useful to disable flooding. See the “Flooding Controls” section in this chapter for more information.

The Catalyst 2820 and 1900 also support source-port filtering. This enhanced filtering capability only forwards packets to destinations when received on specified ports. Packets to these destinations received on other ports are filtered. These destinations are referred to as restricted static addresses. See the “Port Addressing” section in the “Out-of-Band Management” chapter for more information. If you are using SNMP, see the “Standard MIBs and MIB Extensions” section in the “In-Band Management” chapter.

Switching Modes

The switching mode determines how quickly the Catalyst 2820 or 1900 can forward a packet and, therefore, how much latency the packet will experience. Latency is the delay between the time a packet is received on one port and the time it is transmitted from the appropriate destination port. Selecting a switching mode is often a choice between enhanced error checking and lower latency.

The Catalyst 2820 and 1900 offer three switching modes:

- FastForward (the default)
- FragmentFree
- Store-and-Forward

FastForward and FragmentFree are two forms of *cut-through* switching. You can define the switching mode on the System Menu of the management console, as described in the "System Configuration" section of the "Out-of-Band Management" chapter. You can also use the appropriate MIB objects listed in the "Standard MIBs and MIB Extensions" section of the "In-Band Management" chapter.

FastForward

FastForward offers the lowest level of latency by immediately forwarding a packet after receiving the destination address. Because FastForward starts forwarding before the entire packet is received, there can be times when packets are relayed with errors. Although the destination network adapter discards the faulty packet upon receipt, the superfluous traffic can be deemed unacceptable. Packets forwarded with errors can be reduced by using the FragmentFree option. In FastForward mode, latency is measured first-bit-received to first-bit-transmitted or FIFO.

FragmentFree

FragmentFree switching filters out collision fragments, the majority of packet *errors*, before forwarding begins. In a properly functioning network, collision fragments must be less than 64 bytes. Anything greater than 64 bytes is a valid packet and is usually received

without error. FragmentFree switching waits until the received packet has been determined not to be a collision fragment before forwarding the packet. In FragmentFree mode, latency is measured as FIFO.

Store-and-Forward

The third switching mode supported by the Catalyst 2820 and 1900 is the traditional Store-and-Forward mode. Complete packets are stored and checked for errors prior to transmission. In Store-and-Forward mode, latency is measured last-bit-received to first-bit-transmitted or LIFO. This does not include the time it takes to receive the entire packet, which can vary, according to packet size, from 65 microseconds to 1.3 milliseconds. Store-and-Forward is the most error-free form of switching, but the forwarding latency is higher than either of the two cut-through switching modes, as shown in Table 3-1.

Table 3-1 Catalyst 2820 and 1900 Switching Latencies

Switching Mode	10 Mbps to 10 Mbps	10 Mbps to 100 Mbps	100 Mbps to 100 Mbps	100 Mbps to 10 Mbps
FastForward (FIFO)[1]	31 microsec	–	7 microsec	7 microsec
FragmentFree (FIFO)	70 microsec	–	9 microsec	10 microsec
Store-and-Forward (LIFO)[2]	7 microsec	7 microsec	3 microsec	3 microsec

1. First In, First Out
2. Last In, First Out

Note Although Table 3-1 shows Store-and-Forward experiencing the lowest latency, the figures do not include the time it takes to receive the packet, which varies according to the packet size.

Selecting a Switching Mode

FastForward is the default switching mode and provides the lowest latency packet switching. If your attached networks experience a significant number of collisions, you can use FragmentFree to eliminate the chance of forwarding collision fragments. If you are experiencing frame check sequence (FCS) or alignment errors, use Store-and-Forward to ensure that packets with errors are filtered and not propagated to the rest of the network.

You select a switching mode for the entire switch; the chosen switching mode is then applied to traffic flowing between all ports with the following exceptions:

- Store-and-Forward is always used for transfers from 10-Mbps to 100-Mbps ports.
- Store-and-Forward is always used for broadcast packets; multicast packets can be Store-and-Forward or the switching mode set for the switch.

To define the switching mode with the management console, refer to the "System Configuration" section of the "Out-of-Band Management" chapter for more information. You can also define the switching mode in-band using any SNMP-compatible management station. Refer to the *Catalyst 2820 Series and Catalyst 1900 Series MIB Reference Manual* for a description of the MIB objects. The switching mode is set with the MIB objects listed in Table 6-1 in the "In-Band Management" chapter.

Securing Ports

Secured ports restrict the use of a port to a user-defined group of stations. The number of devices on a secured port can range from 1 to 132. The addresses for the devices on a secure port are statically assigned by an administrator or *sticky-learned*. Sticky learning takes place when the address table for a port that is set as secured does not contain a full complement of static addresses. The port sticky-learns the source address of incoming packets and automatically assigns them as static addresses.

Secured ports generate address-security violations under the following conditions:

- When the address table of a secured port is full and the address of an incoming packet is not found in the table
- When an incoming packet has a source address statically assigned to another port

When a security violation occurs, the port can be suspended or disabled, as described in the "Port Status" section in this chapter, and SNMP traps can be generated. You can also choose to ignore the violation and keep the port enabled. What action is taken by the switch is defined by the administrator using the MIB objects listed in Table 6-1 in the "In-Band Management" chapter or with the menu described in the "System Configuration" section in the "Out-of-Band Management" chapter.

Note To fully secure a port, you must also disable flooding to the port. See the "Flooding Controls" section in this chapter for more information.

Applications of Secured Ports

There are several reasons to secure ports. Address security can be used to ensure that only members of a workgroup have access to the switch on a given port. When you assign static addresses to a secure port, the switch does not forward any packets with source addresses outside the group. Secured ports used in conjunction with VLANs allow for a completely secure switch.

The private Ethernet configuration is also an application of secured ports. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port.

See the "Port Addressing" section in the "Out-of-Band Management" chapter for more on securing ports with the management console. If you are using SNMP, Table 6-1 in the "In-Band Management" chapter lists the MIB objects used for securing ports.

Port Status

Port status is a system-wide indicator of the state of a port. A port's status can change in response to security violations, by management intervention, or by actions of the Spanning-Tree Protocol. At any given time, each switch port will be in one of three states:

Enabled	The port is active and receiving and transmitting packets.
Suspended	The port is not active but will be automatically returned to the enabled state when the condition causing its suspension is removed.
Disabled	The port is inactive and must be manually returned to an enabled state.

No packets are forwarded to or from a disabled or suspended port. However, suspended ports do monitor incoming packets to look for an activating condition. If a linkbeat returns, for example, a port suspended due to linkbeat failure returns to the enabled state.

Full-Duplex 100BaseT

You can configure a Catalyst 2820 or Catalyst 1900 to provide full-duplex operation on switched 100BaseT ports for up to 200 Mbps of bandwidth. Full duplex is the simultaneous transmission and reception of 100-Mbps streams.

Note As both ends of the link must be configured for full duplex, a full-duplex port cannot be connected to a repeater.

A likely full-duplex scenario would be to connect a 100BaseT port to a server with a 100BaseT adapter configured for full duplex. You could also connect it to another switch or router configured for full-duplex operation. 100BaseFX full-duplex links can span distances of up to 2 kilometers.

See the “Port Configuration” section in the “Out-of-Band Management” chapter for instructions on configuring ports for full-duplex. If you are using SNMP, Table 6-1 in the “In-Band Management” chapter lists the MIB objects required to configure full-duplex operation.

Port Monitoring

The design of the Catalyst 2820 and 1900 has the added security feature of precluding eavesdropping or monitoring of traffic destined for other ports. However, there are times when you might want to use a Remote Monitoring (RMON) probe or sniffer to examine traffic on some or all of the switch ports. Port-monitoring mode is provided for this purpose.

Port-monitoring mode forwards traffic from ports that are assigned to a capture list to the port designated as the monitor port. The sniffer can then be used on this port. The capture list can include any number of ports, from none to all 27. To enable port-monitoring mode with the management console, see the “Monitoring Configuration” section in the “Out-of-Band Management” chapter. If you are using SNMP, the MIB objects for configuring port monitoring are listed in Table 6-1 in the “In-Band Management” chapter.

Remote Monitoring

The Catalyst 2820 and 1900 support four RMON groups as defined by RFC 1757. As recommended by the RFC, default statistics and history rows are created automatically when you start the system. You can obtain information about these four groups using any SNMP management application. The four supported RMON groups are described in Table 3-2.

Table 3-2 RMON Groups and Their Functions

Group Name	Description
Statistics	Collects statistics for a specific interface. For example, you could use this group to determine how many error packets have been seen on a given port. By default, two rows of statistics are established, one for each high-speed port.
History	Collects statistics within a given interval for a specific interface. By default, two rows of statistics are established for each high-speed port. One is a long-term interval–30 minutes–and the other is short term, 30 seconds.
Alarm	Generates an alarm according to user-defined thresholds. You could, for example, set off an alarm when CRC errors exceeded a predefined limit.
Event	Generates traps and log entries based on the configuration of alarm entries.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) allows network managers to obtain an accurate picture of the network at any time. By gathering information about the types of devices in the network, the links between those devices, and the number of interfaces within each device, CDP enables network management applications to display a graphical topology map of the network. Detailed information about the connections between devices is also available.

For more information about enabling CDP, see the “CDP Configuration Status” section of the “Out-of-Band Management” chapter.

Flooding Controls

Flooding is the forwarding of multicast and unicast packets with unknown destination addresses to all ports. Also, broadcast packets are always forwarded to all ports. In certain applications, this flooding might be unnecessary and undesirable. Note that when you create a VLAN, all traffic—including broadcast traffic—is kept within the boundaries of the VLAN, regardless of whether flooding controls are used.

Unicast Filtering

When a Catalyst 2820 or 1900 receives a unicast packet with a destination address that it has not learned, the default is to flood it to all ports. However, on ports with only statically assigned addresses or single stations attached, there are no unknown destinations, and flooding serves no purpose. You can disable flooding in this case on a per-port basis.

If there is only one port connected to a larger network, you can also forward all packets with unknown unicast addresses to that port. This port, the Network Port, is explicitly defined and cannot be secured. It also does not learn addresses.

The Network Port configuration is for a switch that has only one network connection; all the other switch ports must be connected to end stations. Because address aging drops learned addresses from the address table, assigning a Network Port can cause a loss of connectivity to idle end stations. You can overcome this by increasing the address aging time for the switch to a value higher than the ARP-cache aging time set for routers and end stations on the segment.

Use the “System Configuration” menu described in the “Out-of-Band Management” chapter to define a port as the Network Port and to change the address aging time for the switch. See the “Port Addressing” section in the “Out-of-Band Management” chapter for more information on disabling the flooding of packets to individual ports.

Multicast Registration and Filtering

When a Catalyst 2820 or 1900 receives a multicast or broadcast packet, the default is to flood it to all ports. You can use the switch’s management console or SNMP to register multicast addresses and list the ports these packets are to be forwarded to. You can also disable the normal flooding of unregistered multicast packets on a per-port basis. Besides reducing unnecessary traffic, these features open up the possibility of using multicast packets for dedicated groupcast applications such as broadcast video. See the “Multicast Registration” section in the “Out-of-Band Management” chapter for more information about registering multicast addresses with the management console. If you are using SNMP, the MIB objects for configuring this function are listed in Table 6-1 in the “In-Band Management” chapter.

Cisco Group Management Protocol

Cisco Group Management Protocol (CGMP) reduces the unnecessary flooding of IP multicast packets. The switch receives data via the CGMP from a Cisco router identifying clients that should receive certain IP multicast packets. With this information, the switch limits the transmission of the IP multicast packets to those clients in the group. See the "Port Configuration" section in the "Out-of-Band Management" chapter for information about configuring CGMP.

Broadcast Storm Control

A broadcast storm is an increase in the number of broadcast packets coming from a given port. Forwarding these packets can cause the network to slow down or time out. To avoid this, broadcast storm control enables you to set a threshold for the number of broadcast packets that can be received from a port before forwarding is blocked. A second threshold is defined to determine when to re-enable the normal forwarding of broadcast packets.

VLANs

The Catalyst 2820 and 1900 support up to four intraswitch VLANs. This capability allows ports on the switch to be grouped into separate logical networks. Unicast, broadcast, and multicast packets are forwarded (and flooded) only to those stations within a VLAN, creating a virtual firewall between VLANs. A port can be assigned to a VLAN using the switch's management console or in-band using any SNMP-compatible management station.

Because a VLAN is considered a separate logical network, it contains its own bridge MIB information and supports its own implementation of some of the features described in this section, including Spanning-Tree Protocol.

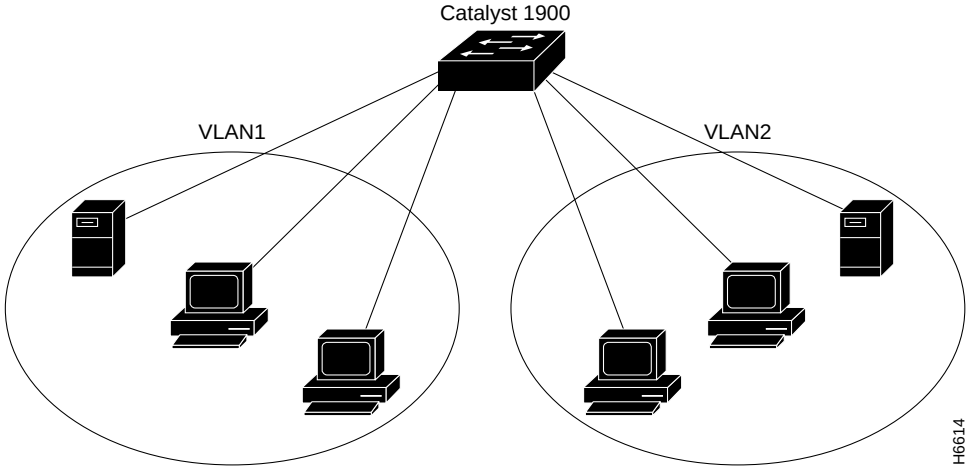
One VLAN, the management VLAN, can be assigned an IP address. Other VLANs must use a port connected to a router to communicate with ports in the management VLAN.

Configuring Simple VLANs

Figure 3-1 illustrates a simple VLAN configuration that groups workstations attached to a Catalyst 1900, ports 1 through 12, and a server attached to port A, into VLAN1. Workstations attached to ports 13 through 24 are grouped with a server attached to port B into VLAN2. The traffic on one VLAN is completely isolated from the other's traffic.

See the "Virtual LAN Configuration" section in the "Out-of-Band Management" chapter for details on assigning ports to VLANs. If you are using SNMP, the MIB objects for configuring this function are listed in Table 6-1 in the "In-Band Management" chapter.

Figure 3-1 Workgroups Defined as VLANs

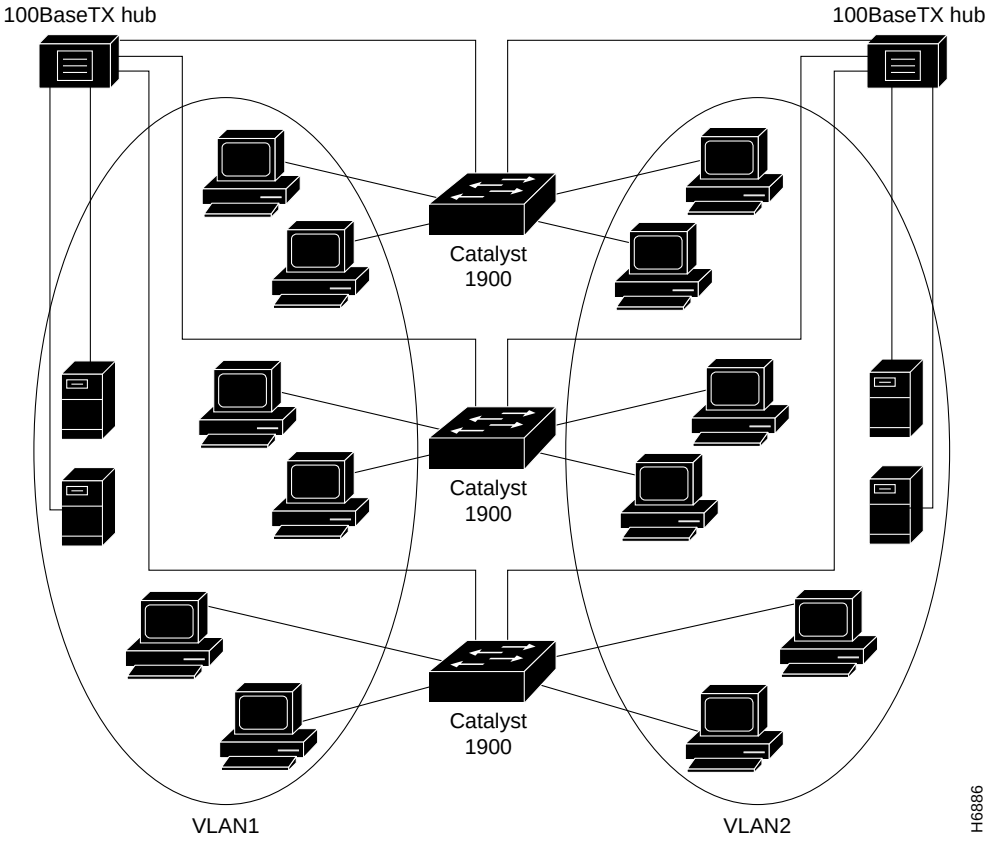


VLANs Spanning Multiple Switches

VLANs spanning multiple Catalyst 2820s or 1900s require a dedicated port on each switch for each VLAN interconnection. The configuration in Figure 3-2 shows two VLANs spanning multiple Catalyst 1900s. In this example, ports A and B on each switch provide the link to interconnect VLAN1 and VLAN2, respectively. An external 100BaseT hub (or FDDI concentrator) then connects each link to form the overall VLAN. If one or more of

the switched 100BaseT ports on the Catalyst 1900 are used for other connections, or if more than two VLANs span multiple Catalyst 1900s, a dedicated 10BaseT port on each switch is required to interconnect the VLANs.

Figure 3-2 VLANs Spanning Multiple Switches



Spanning-Tree Protocol

Spanning-Tree Protocol is a standardized mechanism for maintaining a network of multiple bridges or switches. As part of the IEEE 802.1d standard, Spanning-Tree Protocol interoperates with compliant bridges and switches from other vendors. It transparently reconfigures bridges when the topology changes to avoid the creation of loops and to establish redundant paths in the event of lost connections. All 27 ports are included in Catalyst 2820 and 1900 Spanning-Tree Protocol support, and management of Spanning-Tree Protocol is through the standard bridge MIB.

Note Each Catalyst 2820 and 1900 VLAN is treated as a separate bridge, and a separate instance of the bridge MIB is applied to each VLAN. See the "*Catalyst 2820 Series and Catalyst 1900 Series MIB Reference Manual*" for information on how to access different instances of the bridge MIB on the same switch.

Port Fast Spanning-Tree Protocol

The Port Fast option is a simplified version of the Spanning-Tree Protocol that eliminates several of the normal spanning-tree states. The pre-forwarding states are bypassed to more quickly bring ports into the forwarding states. Port Fast is enabled on a per-port basis. It is recommended for end-station attachments only. See the "Port Configuration" section in the "Out-of-Band Management" chapter for more information.

Using Spanning-Tree Protocol to Support Redundant Connectivity

You can create a redundant backbone with Spanning-Tree Protocol by connecting two of the switch's ports to another device or to two different devices. Spanning-Tree Protocol will automatically disable one port but enable it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is always disabled. If the speed of the two links is the same, the port priority and port ID are added together and the link with the lowest value is disabled.

Spanning-Tree Protocol and Accelerated Address Aging

Dynamic addresses are aged and dropped from the address table after a configurable period of time. The default for aging dynamic addresses is 5 minutes. A reconfiguration of the spanning tree, however, can cause many station locations to change. Because this could mean that many stations were unreachable for 5 minutes or more, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when Spanning-Tree Protocol reconfigures. This parameter is described in the "Spanning-Tree Configuration" section in the "Out-of-Band Management" chapter. If you are using SNMP, Table 6-5 in the "In-Band Management" chapter lists the MIB objects used to configure this function.