CHAPTER 1

Product Overview

The Catalyst 2900 is a fixed-configuration Fast Ethernet switch that provides low density, switched Fast Ethernet for wiring closet and data-center applications. Two available versions each provide virtual LAN (VLAN) networking and layer 2 switching supported by Cisco's Internetwork Operating System (Cisco IOS). You can use the Catalyst 2900 to deploy 10-Mbps Ethernet and 100-Mbps Fast Ethernet connections to existing LAN segments, workstations and servers. The switch architecture includes a single integrated 1.2 gigabit-per-second backplane that supports wire-speed, switched, Fast Ethernet over 10/100BaseTX Category 5 UTP and 100BaseFX fiber-optic cabling.

The Catalyst 2900 is a 2-slot, 14-port, fixed-configuration switch that fits in a standard 19-inch rack. One slot is for the supervisor module, which provides Layer 2 switching, local and remote management, and two Fast Ethernet interfaces. The remaining slot is for a 10/100BaseTX or 100BaseFX module.

Ethernet interfaces are usually used to connect workstations and servers, while Fast Ethernet interfaces connect to workstations, servers, switches, and routers. Multiple Fast Ethernet connections can be used to connect switches on different floors or to create backup links to other switches.

Ethernet and Fast Ethernet interfaces on the Catalyst 2900 can be used to connect network servers and next generation workstations or to interconnect multiple Catalyst 2900 switches, as shown in Figure 1-1, Trunk Configuration example. The products can also be used to expand existing Ethernet networks that need additional capacity.

The use of Layer 2 switching prevents packets sent between two switched ports from being forwarded to other switched ports. Preventing extraneous traffic across switched interfaces increases bandwidth on all networks. Performance can be further enhanced by limiting traffic through the use of virtual local area networks or VLANs. VLANs limit the forwarding of packets to those stations that have been defined as part of the VLAN. VLANs can also be used to provide security barriers, or firewalls, between stations physically connected through the same switch.

Summary of Features

The Catalyst 2900 provides the following features:

- Encoded Address Recognition Logic (EARL)
- Virtual Local Area Network (VLAN)
  - VLAN Trunks and Inter-switch Links (ISL)
  - ISL
  - Dynamic ISL
  - Load Sharing
  - VLAN Trunk Protocol (VTP)
- Embedded Traffic Management Tools:
  - RMON
  - SPAN network monitoring
  - E-SPAN VLAN monitoring
- 10/100 autosensing and auto negotiation
- Load Sharing
- Network Management
  - Supporting Switched Internetwork Management Applications
  - Simple Network Management Protocol (SNMP)
  - Cisco Discovery Protocol (CDP)

Encoded Address Recognition Logic (EARL)

Encoded address recognition logic (EARL) is a custom Catalyst 2900 component similar to the learning bridge or content-addressable memory (CAM) of other types of network switches and routers. The Catalyst 2900 EARL automatically learns source MAC addresses and saves them in a RAM address table with virtual LAN (VLAN) and port information. The EARL uses learned entries as destination addresses (DAs) and directs packets using port information contained in the DAs.

Bus arbitration and EARL are shared among all ports. Together they control the destination of packet transfers and access to the data switching bus.

Virtual Local Area Network (VLAN)

A VLAN on a Catalyst 2900 is essentially a broadcast domain. Only end stations within the VLAN receive packets that are unicast, broadcast, and multicast (flooded) from within the VLAN. A VLAN 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 that are connected through the same switch.

A VLAN can also be described as a group of end stations, independent of physical location, with a common set of requirements. For example, several end stations may be grouped as a department, such as engineering or accounting. If the end stations are located in close proximity to one another, they can be grouped into a LAN segment. If any of the end stations are on a different LAN segment, typically located in different buildings or locations, they can be grouped together into a VLAN that

has all the same attributes as a LAN even though the end stations are not all on the same LAN segment. The information identifying a packet as part of a specific VLAN is preserved across a Catalyst 2900 connection to a router or other switch.

The VLANs on a Catalyst 2900 simplify adding and moving end stations on a network. For example, when an end station is physically moved to a new location, its attributes can be reassigned from a network management station (a console terminal attached to a Catalyst 2900 or through a modem that connects to the console port on the supervisor engine module) via SNMP or the Command Line Interface (CLI). When an end station is moved within the same VLAN, it retains its previously assigned attributes in its new location. When an end station is moved to a different VLAN, the attributes of the new VLAN are applied to the end station, depending upon the security levels in place.

The IP address of a Catalyst 2900 Network Management Processor (NMP) can be assigned to any VLAN. This mobility of the IP address allows a network management station and workstations on any VLAN on a Catalyst 2900 to access directly another Catalyst 2900 on the same VLAN without the use of a router. Only one IP address can be assigned to a Catalyst 2900; therefore, if the IP address is reassigned to a different VLAN, the previous IP address assignment to a VLAN is no longer valid.

VLAN Trunks and Inter-switch Links (ISL)

A trunk is a physical link between two Catalyst 2900s, or between a Catalyst 2900 and routers that carry multiple logical links for VLANs. The Inter-switch Link (ISL) protocol provides a means for the Catalyst 2900 to multiplex up to 1000 VLANs between these switches and routers. Trunks can also be established between a Catalyst 2900 and other Catalyst switches that support the ISL protocol.

ISLs

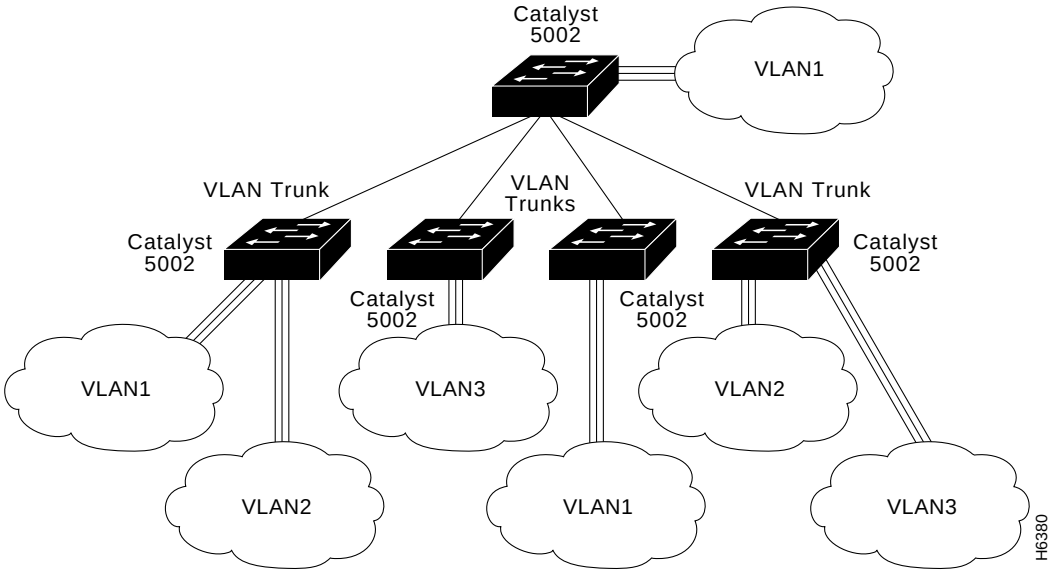
Any Fast Ethernet port can be configured as a trunk. Trunks use Inter-switch link (ISL) protocol to support multiple VLANs. An ISL trunk is like a continuation of the switching backplane. It provides a means for the Catalyst 2900 to multiplex up to 1000 VLANs between switches and routers.

Figure 1-1 shows an example of a trunk configuration.

Dynamic ISL

The Dynamic ISL (DISL) Protocol configures trunk ports between Catalyst 2900s dynamically; it synchronizes the configuration of two interconnected Fast Ethernet interfaces into becoming ISL trunks. DISL Protocol minimizes VLAN trunk configuration procedures because only one end of a link must be configured as a trunk or non-trunk.

Figure 1-1 Trunk Configuration Example



Load Sharing

Load sharing allows VLAN traffic on parallel Fast Ethernet ISL trunks to be split between multiple trunks. By setting STP parameters on a VLAN basis, you can define which VLANs have priority access to a trunk which will use the trunk as a backup when another trunk fails.

In STP, low integer values have the highest priority. Therefore, when you assign spanning tree port priorities that are lower than the default value of 32 to VLANs, the traffic of those VLANs travels on the trunk with the lowest integer value. The spanning tree port priority must be set to the same value at both ends of each trunk on each Catalyst 2900.

For example, Figure 1-2 illustrates two trunks that are connected to the ports of supervisor engine modules on two Catalyst2900s. The port cost of carrying VLAN traffic across these trunks is equal.

- VLANs 8 through 10 are assigned a port priority of 1 on trunk 1
- VLANs 3 through 6 retain their default port priority of 32 on trunk 1
- VLANs 3 through 6 are assigned a port priority of 1 on trunk 2
- VLANs 8 through 10 retain their default port priority of 32 on trunk 2

VLAN traffic is split between the two trunks and increases the throughput capacity and fault tolerance between Catalyst 2900 switches; trunk 1 carries traffic for VLANs 8 through 10, and trunk 2 carries traffic for VLANs 3 through 6. If either trunk fails, the remaining trunk carries the traffic for all of the VLANs. For detailed commands and examples of load sharing, refer to the “Command Reference” portion of this manual.

Caution The port cost of a VLAN must be equal on all parallel trunks when setting port priority for load sharing.

Virtual Trunk Protocol

When new VLANs are added to a Catalyst 2900 in a management domain, VLAN Trunk Protocol (VTP) automatically distributes the information to other trunks of all of the devices in the management domain. This allows VLAN naming consistency and connectivity between all devices in the domain. The VTP is transmitted on all trunk connections, including Inter-switch Link (ISL).

The Catalyst 2900 transmits VTP frames on its trunk ports, broadcasting its management domain name, configuration revision number, and VLAN information it has acquired. Other Catalyst 2900s in the domain use these advertisements to learn about any new VLANs that are configured in the transmitting switch. This process of advertising and learning allows a new VLAN to be created and configured on only one switch in the management domain and be automatically disseminated to all other devices in the domain.

You can have redundancy in a network domain by using multiple VTP servers. Only a few VTP servers are required in a large network. All devices are normally VTP servers in a small network. You can enable VTP transparent mode for devices that cannot or choose not to participate in VTP.

Embedded Traffic Management Tools

The embedded traffic management tools enable you to manage your networks including mirroring traffic on any port or from any VLAN.

Embedded RMON

The Catalyst 2900 provides support for the embedded remote monitoring (RMON) of Ethernet and Fast Ethernet ports. Embedded RMON provides you with visibility into network activity. It enables you to access and monitor remotely the RMON specification RFC 1757 groupings of statistics, historical information, alarms, and events for any port, through SNMP or the TrafficDirector Management application.

The RMON feature monitors network traffic at the link layer of the OSI model without requiring a dedicated monitoring probe or network analyzer. It allows a network manager to analyze network traffic patterns, set up proactive alarms to detect problems before they affect users, identify heavy network users as candidates to move to dedicated or higher speed ports, and perform trend analysis for long-term planning.

The statistics group of the RMON specification maintains utilization and error statistics for the switch that is monitored. Statistics include information about: collisions, cyclic redundancy checks (CRC) and alignment: undersized or oversized packets, jabber, fragments, broadcast, multicast, and unicast messages, and bandwidth utilization.

The history group takes periodic samples from the statistics section and stores them for retrieval, including utilization and error and packet count information.

A system network administrator uses the alarm group to set a sampling interval and threshold for any RMON recorded item. Examples of alarm settings include absolute or relative values, rising or falling thresholds of utilization, packet counts, and CRC errors.

The event group allows events (generated traps) to be logged, printed, and provided to a network manager. The time and date is recorded with each logged event. Network managers use the event group to create customized reports that are based on alarm types.

Extended RMON capabilities are provided through the use of a Cisco SwitchProbe connected to the switch's SPAN port.

SPAN and Network Monitoring

The Switched Port Analyzer (SPAN) enables you to mirror traffic on any port for analysis by a sniffer or RMON probe. The SPAN directs traffic from an Ethernet or Fast Ethernet port or VLAN to an Ethernet or Fast Ethernet monitor port for detailed analysis and troubleshooting. You can monitor a single port or VLAN using a dedicated analyzer, such as a Network General Sniffer or remote monitoring (RMON) probe such as a Cisco SwitchProbe. An RMON probe, such as Cisco's SwitchProbe, enables analysis of the remaining five RMON groups.

E-SPAN VLAN Monitoring

Enhanced SPAN (E-SPAN) enables you to mirror traffic from a VLAN to a port for analysis .

10/100 Autosensing and Autonegotiation

Catalyst 2900 10/100 ports automatically adjust themselves to the Ethernet speed and duplex mode of the attached segment. First, 802.3u is implemented to negotiate the link's speed (10 or 100) and duplex mode (half or full). If the attached device will not autonegotiate, that is, is not 802.3u compliant, the Catalyst 2900 will autosense and configure to the speed and duplex mode of the other device.

Spanning-Tree Protocol

When creating fault-tolerant internetworks, a loop-free path must exist between all nodes in a network. A spanning tree algorithm is used to calculate the best loop-free path throughout a Catalyst 2900 network. Spanning tree packets are sent and received by switches in the network at regular intervals. The packets are not forwarded by the switches participating in the spanning tree, but are instead processed to determine the spanning tree itself. The IEEE 802.1d bridge protocol, called Spanning Tree Protocol (STP), performs this function for Catalyst 2900 switches.

The Catalyst 2900 uses STP on all Ethernet and Fast Ethernet-based virtual local area networks (VLANs). The STP detects and breaks loops by placing some connections in standby mode, which are activated in the event of a failure. A separate STP runs within each configured VLAN, ensuring legal Ethernet topologies throughout the network.

The supported STP states are as follows:

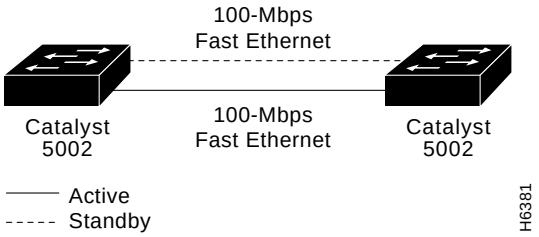
- Disabled
- Forwarding
- Learning
- Listening
- Blocking

The state for each VLAN is initially set by the configuration and later modified by the STP process. After the port-to-VLAN state is set, the 802.1D bridge specification determines whether the port forwards or blocks packets. Ports can be configured immediately to enter STP forwarding mode upon connection instead of the usual sequence of blocking, learning, and then forwarding. This is when immediate server access is required.

Caution Immediate forwarding mode operates correctly on the ports of individual workstations only. It is not recommended for ports connected to switches or other devices that forward messages.

You can design fault-tolerant connections using Ethernet or Ethernet combined with other topologies. Refer to Figure 1-2 for example a Fault Tolerant Ethernet Topology.

Figure 1-2 Fault-Tolerant Fast Ethernet Topology Example



Managing the Network

You can manage your Catalyst 2900 through a console port using either the command line interface (CLI) or other methods for performing network management functions, such as Cisco Discovery Protocol (CDP), Embedded Remote Monitoring (RMON), or Switched Port Analyzer (SPAN). The console port is an EIA/TIA-232 interface which connects to a console terminal or modem.

Through the console port, you can access the CLI or configure a Serial Line Internet Protocol (SLIP) interface directly to access network management functions, such as telnet, ping, or Simple Network Protocol (SNMP).

You can assign the IP address for the Catalyst 2900 to any VLAN. You can direct telnet to access the IP address of the Catalyst 2900 to reach the CLI. You can also use the IP address of the switch to access an SNMP agent.

Note EIA/TIA-232 was known as recommended standard RS-232 before its acceptance as a standard by the Electronics Industry Association (EIA) and Telecommunications Industry Association (TIA).

Supporting Switched Internetwork Management Applications

The Catalyst 2900 supports the following internetwork management applications:

- CiscoView provides you with an intuitive GUI that supports switch configuration, performance monitoring, and troubleshooting.
- TrafficDirector displays embedded remote monitoring (RMON) information through a graphical interface.
- VLANDirector provides a graphical interface that simplifies VLAN adds, moves, and changes. You can also use this application to configure VLAN trunks.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. The SNMP system consists of three parts: SNMP manager, SNMP agent, and Management Information Base (MIB).

Instead of defining a large set of commands, SNMP places all operations in a *get-request*, *get-next-request*, and *set-request* format. For example, an SNMP manager can get a value from an SNMP agent or store a value into that SNMP agent. The SNMP manager can be part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a switch. The SNMP agent can respond to MIB-related queries being sent by the NMS.

Following are basic functions supported by SNMP agents:

- Accessing a MIB variable using the *get-request* or *get-next-request* format—This function is initiated by the SNMP agent as a result of a request for the value of a MIB variable from a network management station. The SNMP agent gets the value of a MIB variable by accessing information stored in the MIB and then responds.
- Setting a MIB variable—This function is also initiated by the SNMP agent as a result of a message from a network management station. The SNMP agent requests that the value of a MIB variable be changed.
- SNMP trap—This function is used to notify a network management station that an extraordinary event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP agent trap message to each of the network management stations as specified in the trap receiver table.

Telnet Client Access

The Catalyst 2900 provides outgoing Telnet functionality from the command line interface; this feature allows a network manager to Telnet from the command line interface of the switch to other devices on the network. Moreover, using Telnet, a network manager can maintain a connection to a Catalyst 2900 while also connecting to another switch or router.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is media- and protocol-independent and runs on all Cisco-manufactured equipment, including routers, bridges, access and communication servers, and switches. With CDP, network management applications can retrieve the device type and SNMP-agent address of neighboring devices. This enables applications to send SNMP queries to neighboring devices.

CDP meets a need created by the existence of lower-level, virtually transparent protocols. CDP allows network management applications to discover dynamically Cisco devices that are neighbors of known devices, in particular, neighbors running lower-layer, transparent protocols. CDP runs on all media that support Subnetwork Access Protocol (SNAP), including LAN and Frame Relay. CDP runs over the data link layer only, not the network layer. Therefore, two systems that support different network layer protocols can learn about each other.

Cached CDP information is available to network management applications. Cisco devices never forward a CDP packet. When new information is received, old information is discarded.

Serial Line Internet Protocol (SLIP)

You can access the Catalyst 2900 command line interface using Serial Line Internet Protocol (SLIP). This protocol is a version of Internet Protocol (IP) that runs over serial links, allowing IP communications through the console port.

Internet Protocols

The Catalyst 2900 uses the following standard internet protocols:

- Address Resolution Protocol (ARP)—used to determine the destination MAC address of a host using its known IP address.
- BOOTP—uses connectionless transport layer User Datagram Protocol (UDP). BOOTP allows the switch (BOOTP client) to get its IP address from a BOOTP server.
- 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.
- Internet Protocol (IP)—suite used to send IP datagram packets between nodes on the Internet.
- Packet internet groper (ping)—used to test the accessibility of a remote site by sending it an ICMP echo request and waiting for a reply.
- Reverse Address Resolution Protocol (RARP)—used to determine an IP address knowing only a MAC address. For example, BOOTP and RARP broadcast requests are used to get IP addresses from a BOOTP or RARPD server.
- Serial Line Internet Protocol (SLIP)—allows IP communication through the console port. SLIP is a version of IP that runs over serial links.
- Simple Network Management Protocol (SNMP)—agents that process requests for network management stations and report exception conditions when they occur. This requires access to information stored in a MIB. For more information, refer to the section, “Supporting MIBs.”
- Transmission Control Protocol (TCP)—a reliable, full-duplex, connection-oriented, end-to-end transport protocol running on top of IP. For example, the Telnet protocol uses the TCP/IP protocol suite.
- Telnet—allows remote access to the command line of a switch over the network (in band). Telnet is a terminal emulation protocol.
- Trivial File Transfer Protocol (TFTP)—used for downloading software updates and configuration files to workgroup switch products.
- The User Datagram Protocol (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.

Supporting MIBs

The Catalyst 2900 supports standard and enterprise-specific MIBs. The following MIBs are supported:

- RFC 1213 (MIB II)
- RFC 1573 (Interfaces MIB)
- RFC 1493 (Bridge MIB)
- RFC 1643 (MIB for Ethernet Interface) (supersedes RFC 1398 (Ethernet MIB))
- RFC 1155-1157 (SNMP v1)
- CISCO-STACK-MIB
- CISCO-CDP-MIB
- CISCO-VTP-MIB

For descriptions, refer to “Appendix C, Workgroup MIB Reference” of this publication for more information.