Network Management

You can gather status information and statistical data using the console panels of the Catalyst 3900 or the command line interface of the Catalyst 5000. In addition, the Catalyst Token Ring switches support other forms of network management, including:

- Device Management
- Topology Management
- VLAN Management
- Traffic Management
- Soft Error Management

This chapter provides an overview of the network management support provided with the Catalyst Token Ring switches.

Device Management

Use the following two methods to manage the Catalyst Token Ring switches:

- SNMP-based managers
- RMON

SNMP Management

Most Token Ring switches, including the Catalyst Token Ring switches, can be managed using SNMP. There are several SNMP MIB definitions for Token Ring information and switches. The Catalyst Token Ring switches support the following standard MIBs:

- Network Management of TCP/IP-based Internets, MIB-II (RFC 1213)
- Evolution of Interfaces Group of MIB-II (RFC 1573)
- Definitions of Managed Objects for Bridges (RFC 1493)
- Token Ring Extensions to the Managed Objects for Bridges (RFC 1525)
- IEEE 802.5 Token Ring MIB (RFC 1748)
- RMON MIB/Token Ring Extensions (RFC 1757/1513) partial support
- IEEE 802.5 DTR Concentrator MIB (Catalyst 3900 only)
- IEEE 802.5 DTR MAC MIB (Catalyst 3900 only)

In addition, the Catalyst Token Ring switches support the following Cisco-defined private MIBs:

- Cisco VLAN Trunking Protocol MIB
- Cisco Discovery Protocol MIB

For SNMP-managed switches, it is possible to monitor and configure the switch from a network management application, which typically has a GUI that provides a simulated view of the front and rear panels of the switch.

Cisco provides SNMP-based network management applications that can be used to manage switches. For more information about these applications, see the“Configuring and Managing Token Ring Switches Using Cisco’s Network Management Products” chapter.

RMON Management

RMON is an industry-standard method for providing network statistics monitoring using SNMP. It also collects fault, performance, and configuration statistics. RMON can also be used to supplant traffic analyzers by providing packet capture or tracing data through the switch or on a ring.

In typical SNMP management, the SNMP client has to continuously poll the switch for fault, performance, and configuration information while waiting for the value to change. This causes increased traffic through the network. With RMON, you can have the switch monitor a particular statistic internally and when the statistic reaches a threshold the switch sends a trap to the client. This monitoring method reduces traffic between the SNMP client and the switch.

It is expensive to provide full-packet capture in a Token Ring switch because of the amount of memory required to store the information. Therefore, a solution is to use an internal RMON capability to gather traffic statistics and an external RMON probe for packet capture and higher-layer protocol analysis. The external RMON probe can be connected to the switch via a port mirroring port such as Cisco’s SPAN ports.

As an option, the Catalyst Token Ring switches provide RMON support for statistics, history, alarms, and events. They also provide support for the following groups of the Token Ring extensions to the Remote Network Monitoring MIB (RFC 1513):

- MAC-layer Statistics Group—Collection of MAC-layer statistics kept for each Token Ring interface, such as the total number of MAC packets received and the number of times the port entered a beaconing state.
- Promiscuous Statistics Group—Collection of promiscuous statistics kept for non-MAC packets on each Token Ring interface, such as the total number of good non-MAC frames received that were directed to an LLC broadcast address.
- Token Ring Ring Station Group—The Catalyst Token Ring switches support the ringStationControlTable portion of the Token Ring Ring Station Group. This support allows a Catalyst Token Ring switch to gather segment information from each ring segment to which it is attached. This segment information includes Ring State, Beacon Sender, Beacon NAUN, and Active Monitor MAC Address, as well as Station Order Changes.
- Token Ring Ring Station Order Group—List of the order of stations on the monitored rings.
- Token Ring Ring Station Group—List of ring station entries. An entry exists for each station that is currently or has previously been detected as being physically present on the ring.
- Token Ring Ring Station Config Control Group—List of ring station configuration control entries. Each entry controls the management of stations by a probe. One entry exists in this table for each active station in the ring station table.

You can use an external RMON probe for full RMON support.

Access to RMON data is available only via an SNMP management application that supports RFC 1757 and RFC 1513. You cannot access RMON via the switch's console interface; however, the console statistics provide similar information. For full utilization of RMON data, you should use the traffic management services of CWSI. For more information about CWSI, see the "Configuring and Managing Token Ring Switches Using Cisco's Network Management Products" chapter.

Topology Management

To aid in network management, Cisco developed the Cisco Discovery Protocol (CDP). CDP allows the Catalyst Token Ring switches to establish communication with other models of Cisco equipment. CDP support is provided as part of the Cisco IOS software that runs on many types of Cisco equipment.

CDP is a media- and protocol-independent protocol that is intended to be run on Cisco-manufactured equipment including routers, bridges, access servers, and switches. With CDP, Cisco's network management applications and Cisco devices can learn the device type and the SNMP agent address of neighboring devices. This enables applications to send SNMP queries to neighboring devices.
CDP runs on various media that support the SNAP, including LAN, Frame Relay, and ATM media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

How CDP Works

All Cisco devices transmit CDP packets periodically. These packets advertise a time-to-live value in seconds, which indicates the length of time that the packet must be retained before it can be discarded. CDP packets are sent with a time-to-live value that is nonzero after an interface is enabled and with a time-to-live value of zero immediately before an interface is idled down. This provides for quick state discovery.

All Cisco devices receive CDP packets and cache the information in the packet. The cached information is available to network management. Cisco devices never forward a CDP packet. If any information changes from the last received packet, the new information is cached and the older information is discarded even if its time-to-live value has not yet expired.

CDP Frame Format

CDP is assigned the Cisco HDLC protocol type value 0x2000. A Cisco-proprietary SNAP value enumerates HDLC protocol type values so CDP can run on all media that support SNAP, such as LAN media, Frame Relay, and ATM.

The SNAP format is as follows:
- LLC—0xAAAA03
- Org ID—0x00000C
- HDLC protocol type—0x2000

CDP sends packets on LANs using the multicast address 0100.0CCC.CCCC.

Because CDP does not run on top of any network layer, but rather runs only over the data link layer, two systems that support different network layer protocols can use CDP to learn about each other.

For more information about the format of CDP frames, see the "Frame Formats" appendix.

VLAN Management

To help VLAN management, Cisco developed VTP. As explained in the "VLAN Trunking Protocol" section of the "Token Ring VLANs and Related Protocols" chapter, VTP is used to set up and manage VLANs across an entire management domain. Using VTP, you can configure and manage the VLANs within a management domain from a single switch that is configured to act as a VTP server.

In addition, Cisco provides the following SNMP-based network management applications that can be used to manage VLANs:

- CiscoView, which allows you to configure and manage VLANs remotely.
- VLAN Director, which provides a graphical mapping utility for viewing and configuring VLANs.
- CWSI, which provides traffic management on a per VLAN basis.

For more information about these applications, see the "Configuring and Managing Token Ring Switches Using Cisco's Network Management Products" chapter.

Traffic Management

To help with traffic management, the Catalyst Token Ring switches support the SPAN.

With SPAN, traffic from any port on the switch can be mirrored or copied to another port, which is designated as the SPAN port. You can then connect the SPAN port to an external RMON probe.

This capability allows you to use the internal RMON to determine where problems might exist, and the external RMON to perform detailed problem analysis. For example, if the internal RMON statistics show high traffic on port 5, you can set up an external RMON probe remotely to capture data from port 5 to obtain more information.

Because forwarding to the SPAN port takes place independently of the normal forwarding, switch performance is not impacted.

As an alternative, you can establish a 16-Mbps monitor ring from the centralized data center that connects to all the SPAN ports on Token Ring switches. Then, you can connect the RMON probe or traffic analyzer at the data center, and via software control, the RMON probe can monitor any port on any switch in the network. Central control of remote monitoring is a powerful tool for the network manager.

The Catalyst 3900 and Catalyst 5000 Token Ring module allow you to configure active monitors. An active port monitor allows you to use a customer-supplied trace tool, such as a Network General Sniffer, to monitor only the LLC traffic that is switched by the monitored port. The MAC frames are not monitored.

On the Catalyst 3900, configuring a port to be a SPAN port removes the port from the TrCRF to which it is currently assigned. On the Catalyst 3900, you can also monitor traffic that is processed by an ISL or ATM port on a per-TrCRF basis (monitoring only one TrCRF at a time). You cannot, however, use an ISL or ATM port to monitor other ports.

Caution Using SPAN on more than one switch at a time may overload the monitoring ring. Also monitoring a TrCRF on a high-speed uplink, such as ATM or ISL, may overload the monitoring ring.

Soft Error Management

The Catalyst Token Ring switches perform error detection and isolation by monitoring the Report Soft Error MAC frames generated by stations on each port. Soft errors occur during normal ring operation and do not typically disrupt traffic on the ring. However, soft errors can occur at a rate that could potentially degrade the performance of the ring.

With both the Catalyst 3900 and the Catalyst 5000 series Token Ring module, you can configure soft error thresholds and sampling intervals for a port. During the interval you define, the Catalyst 3900 monitors the stations on the port and if the threshold is exceeded, can be configured to generate a trap indicating the port number and the station on which the threshold was exceeded. If necessary, you can issue a Remove Ring Station MAC frame to remove the station from the ring.

In summary, the Catalyst Token Ring switches:

- Monitor the Report Soft Error MAC frames generated by stations on each port, collect the data from each soft error frame, and generate a trap containing the port number and station on which the user-defined soft error threshold was exceeded.
- Report the soft error monitoring statistics via the console (for the Catalyst 3900), command line interface (for the Catalyst 5000 series Token Ring module), and SNMP.
- Provide the ability to issue a Remove Ring Station MAC frame to remove a station that is reporting a high level of errors or is not authorized to be on a ring.