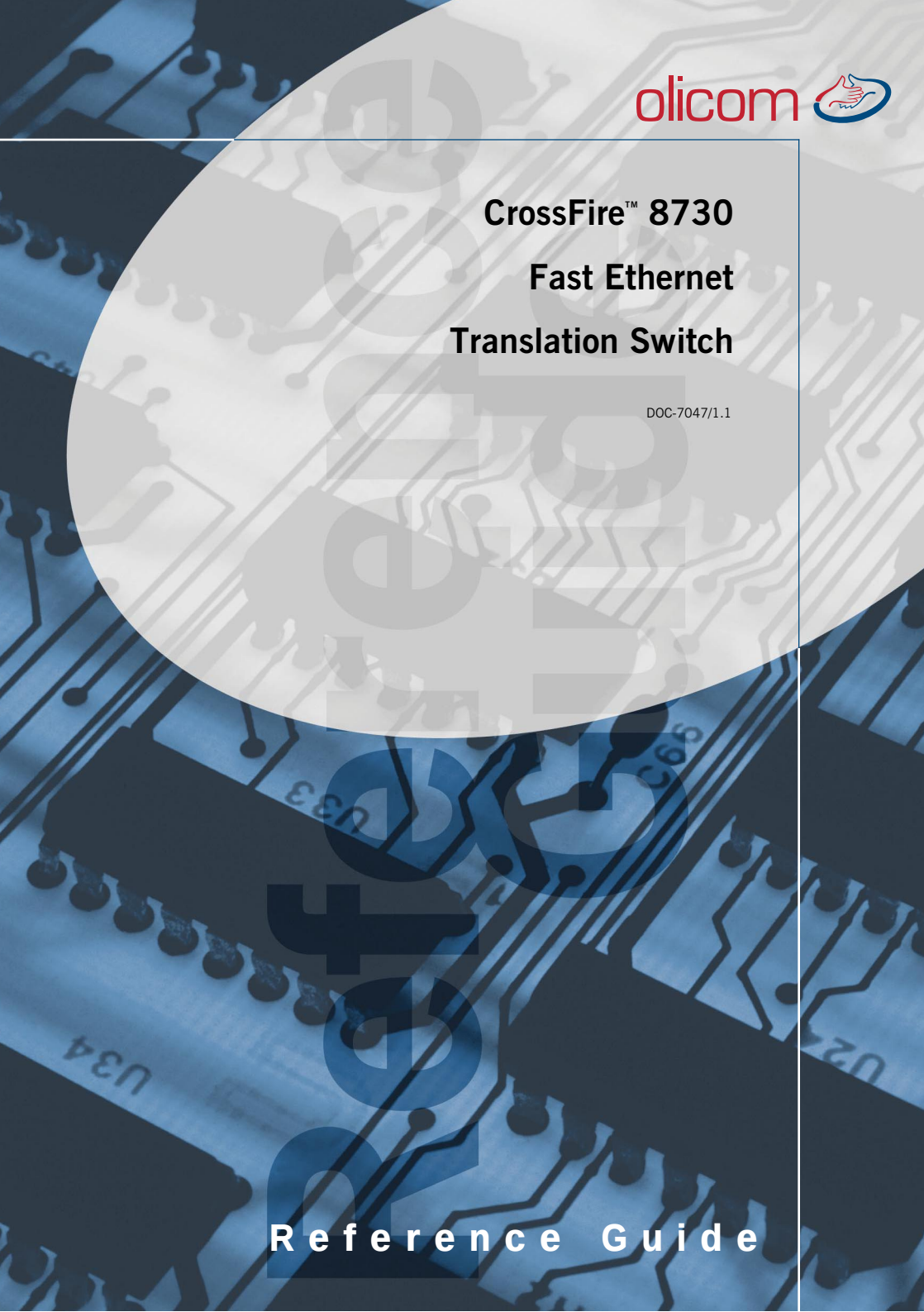
olicom

CrossFire™ 8730

Fast Ethernet

Translation Switch

DOC-7047/1.1



Reference Guide

CrossFire™ 8730
Fast Ethernet Translation Switch

Reference Guide

Trademarks

Copyrights

Publication: DOC-7047 v. 1.1

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Declaration of Conformity

We Olicom A/S
Nybrovej 114
DK-2800 Lyngby
Denmark

declare under our sole responsibility that the product

CrossFire 8730 Fast Ethernet Translation Switch

to which this declaration relates are in conformity with the following standards or other normative documents

EN 50082-1
EN 55022
EN 60950 including Amendments
EN 60825-1

following the provisions of 89/336/EEC Directive and 73/23/EEC Directive.

Modifications

If the device is changed or modified without the express approval of Olicom A/S the user may void his or her authority to operate the equipment.

Safety Notices

Danger: To avoid shock hazard, do not connect or disconnect any cables or perform installation, maintenance, or reconfiguring of the CrossFire 8730 Fast Ethernet Translation Switch during an electrical storm.

Danger: To avoid the possibility of electrical shock, switch power off and unplug the power cord from the outlet before detaching the power cord from the CrossFire 8730 Fast Ethernet Translation Switch.

Danger: Do not open the CrossFire 8730 Fast Ethernet Translation Switch. Dangerous voltages inside.

Danger: To avoid shock hazard the power cord must be connected to a properly wired and earthed receptacle. Any equipment to which the CrossFire 8730 Fast Ethernet Translation Switch will be attached must also be connected to properly wired and earthed receptacles.

Caution:

Observe the following power cable considerations before you begin installation of the CrossFire 8730 Fast Ethernet Translation Switch.

1. The socket outlet shall be installed near the equipment and shall be easily accessible.

2. To prevent electrical shock, the power cord set used must comply with national regulations.

2a. The female receptacle of the cord must meet CEE-22 requirements.

2b. The cord must be UL listed, CSA labelled, and consist of three conductors with a maximum of 15 feet in length.
Type SVT or SJT cord sets shall be used for units which stand on a desk or table. Type SJT cord sets shall be used for units which stand on floor.

2c. The male plug for units operating at 115 VAC shall consist of a parallel blade, grounding type attachment plug rated 15 A, 125 VAC.
The male plug for units operating at 230 VAC shall consist of a tandem blade, grounding type attachment plug rated 15 A, 250 VAC.
The male plug for units operating at 230 VAC (outside of the United States and Canada) shall consist of a grounding type attachment plug rated 15 A, 250 VAC and have the appropriate safety approvals for the country in which the equipment will be installed.

Caution: Support the CrossFire 8730 Fast Ethernet Translation Switch while you are installing the unit to avoid dropping it on the floor or any equipment beneath it in the rack. The CrossFire 8730 Fast Ethernet Translation Switch unit weighs approximately 9.5 kg (20.9 lbs).

Warning: All RJ45 connectors must only be connected to safety extra low voltage (SELV) circuits like local area networking (LAN).

Table of Contents

3. Switch Configuration 41

List of Figures

List of Tables

About this Guide

This reference guide contains information needed to operate the CrossFire™ 8730 Fast Ethernet Translation Switch. The user of this guide is assumed to be a network technician familiar with the installation and operation of networking equipment.

In addition to this reference guide, the CrossFire 8730 Switch is delivered with the *CrossFire 8730 Fast Ethernet Translation Switch Installation Guide* enclosed both as a printed manual and as a pdf file in the package. The installation guide contains information needed to install and get started with the switch.

This reference guide contains the following chapters:

Chapter 1, "Introduction", discusses translation from Token-Ring to Ethernet and lists features and benefits of the switch.

Chapter 2, "Switch Overview", gives an overview of how the switch improves network performance and describes the various features supported on the switch.

Chapter 3, "Switch Configuration", deals with setting up and configuring the switch using a direct console connection.

Chapter 4, "Monitoring the Network from the Statistics Menu", explains how to monitor the switch using the **Statistics** menu through a direct console connection.

Chapter 5, "Monitoring the Network with SNMP", explains how to monitor the switch from a Network Management System using an application that supports Simple Network Management Protocol.

Chapter 6, "Monitoring Port Traffic", explains how to monitor ports on the switch using SwitchProbe.

Chapter 7, "Getting in Touch with Technical Support", lists Olicom's support services such as hotline support, fax support and the support web, as well as other services such as bulletin board service, FTP server and e-mail.

Appendix A, "Abbreviations", lists the abbreviations used in this manual.

Document Conventions

The following conventions are used in this guide:

- HELVETICA NARROW indicates keystrokes, as in "Press ENTER to select the item."
- Items displayed on the screen, such as menus and parameters, are indicated with bold. For example, "Select **Configuration...** in the main menu."

❑

1. Introduction

This chapter discusses translation fromToken-Ring to Ethernet on a general level and lists important features and benefits of the CrossFire 8730 Switch.

For information on the specific physical features of the switch, please refer to the *CrossFire 8730 Fast Ethernet Translation Switch Installation Guide.*

About the CrossFire 8730

The CrossFire 8730 is a simple and inexpensive solution to the challenge of connecting Token-Ring and Ethernet networks, enabling data to quickly and easily flow between the two architectures - at nearly wire speed.

The CrossFire 8730 translates all Token-Ring packets directly into Fast Ethernet frames. This avoids the limitations of proprietary encapsulation techniques.

The CrossFire 8730 supports translational bridging for the key network protocols SNA, IP, IPX, and NetBios. Moreover, all native Token-Ring features, including source routing and IEEE 802.1Q tagged VLAN are supported as well as all network speeds for both standard Token-Ring (16/4 Mbps) and Ethernet (10/100 Mbps).

Also, the CrossFire 8730 supports four different switching modes to provide maximum flexibility in all installation environments. The switching modes are Source Route Switching (SRS), Source Route Bridging (SRB), Source Route Transparent (SRT) and SRT/SRB.

For more information on these features read **Chapter 2, “Switch Overview”**.

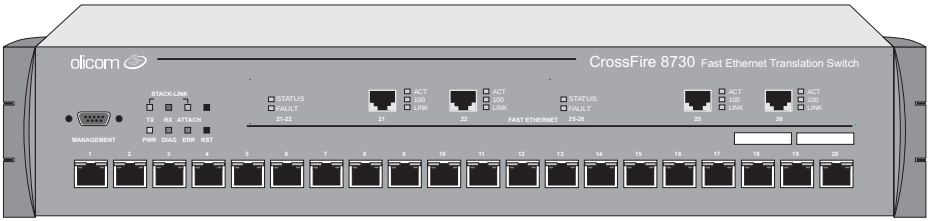


Figure 1. CrossFire 8730 Fast Ethernet Translation Switch

Translation from Token-Ring to Fast Ethernet

The configuration options of the CrossFire 8730 Switch provide for several translation strategies, thereby providing extra flexibility for managers when designing their integrated network. The best option will depend on the current network and the migration strategy.

This section describes a typical migration strategy and gives an example of an application of the CrossFire 8730.

Isolated Ethernet Segments or Servers

As the starting point for migrating a bridged Token-Ring network to Fast Ethernet, the switch could be set up with the four Fast Ethernet ports connected to four isolated Ethernet segments or Fast Ethernet Attached servers. The CrossFire 8730 Switch will make servers and workstations attached to the Fast Ethernet ports appear to be on a single logical Ethernet segment connected to the Token-Ring network through the switch. This configuration will provide a translation bandwidth corresponding to that of four Fast Ethernet ports.

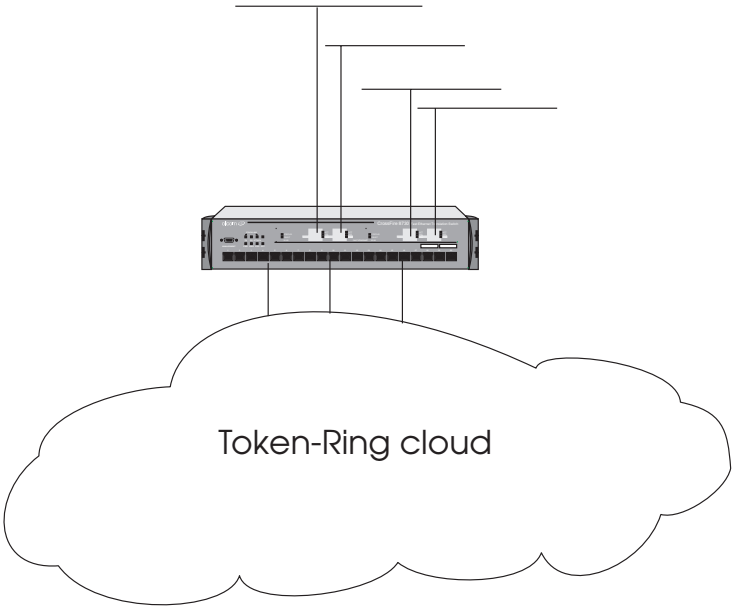


Figure 2. Translation Strategy: Fast Ethernet Ports Operating as 400 Mbps CRF

Application Example

The CrossFire 8730 Fast Ethernet Translation Switch is ideal for situations in which the plan is to connect Token-Ring clients to a Fast Ethernet backbone. It provides switched Token-Ring ports for legacy users and Fast Ethernet ports to connect to a new Fast Ethernet backbone. Translation between Ethernet and Token-Ring is performed within the CrossFire 8730 Switch, making the migration seamless.

The Fast Ethernet backbone can be formed using several CrossFire 8720 Fast Ethernet Backbone Switches or the CrossFire 8710 Fast Ethernet Stackable Switch. This provides a high-performance Ethernet backbone, adds Layer 3 and Layer 4 capabilities to the Ethernet network, and introduces the possibilities of integrating ATM and Gigabit Ethernet.

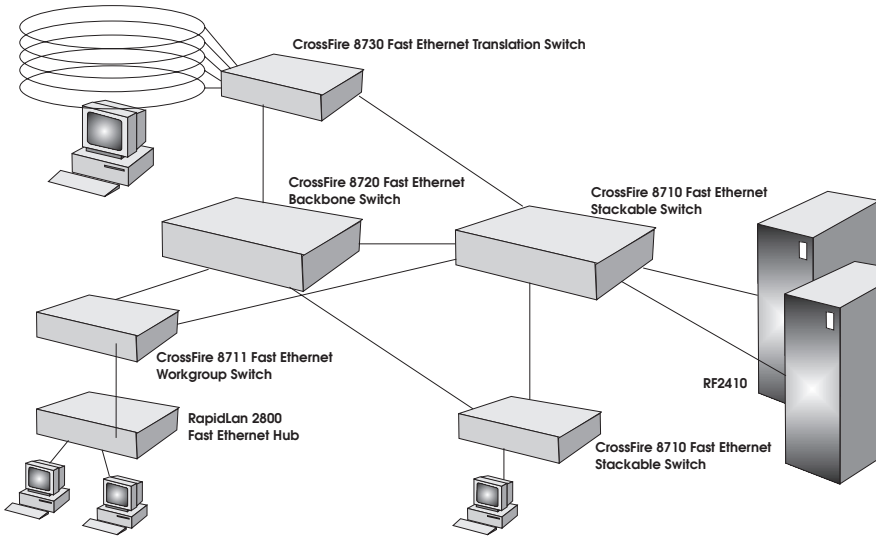


Figure 3. Integrating Ethernet and Token-Ring Networks Using a CrossFire 8730

Benefits of the CrossFire 8730

This section looks into the benefits that can be derived from the technical features of the switch.

Translational Switching

Feature	Description	Benefit
High-speed translation between Fast Ethernet and Token-Ring	Translates frames between Token-Ring and Fast Ethernet at nearly line speed	Fast and efficient integration of Token-Ring and Fast Ethernet networks
Next-generation switch architecture	Full-featured switching for maximum performance and compatibility	Segment legacy LAN to improve performance until migration is complete.
IEEE 802.1Q tagged VLAN support over the Fast Ethernet link	Industry standard that enables frames belonging to different VLANsto be carried over the same physical link	Translation to Fast Ethernet
Support for IP multicasting	Transmissions from a single source can be delivered to several subscribing participants.	Avoids unnecessary broadcasting to provide an efficient use of bandwidth.
Support for IP fragmentation	Provides tight compatibility with IP-based networks	Ensures fast, simple connections between IP, Token-Ring and Ethernet networks
NetBios Address Translation	Provides tight compatibility for networks using NetBios	Ensures fast, efficient performance

Table 1. Translational Switching Benefits

Multiple Bridging Modes

Feature	Function	Benefit
Transparent and Source Route Switching (SRS)	Switching is based on MAC addresses only. Learns MAC addresses and source routing route descriptors of Source Route Bridges attached to local switch ports.	Allows easy installation in environments with no need for Source Route Bridging.
Source Route Bridging (SRB)	The switch ports may be grouped into logical rings. The switch acts as a standard multiport Source Route Bridge between logical rings. Non Source Route frames (NSR) are not forwarded outside the logical ring.	Allows easy installation in existing Token-Ring networks where Source Route Bridges are used. Allows easy replacement of bridges with switches.
Source Route Transparent Bridging (SRT)	NSR frames are forwarded between Logical Rings based on MAC address. Source Route frames are forwarded as by SRB.	Allows the mix of source route and non source route protocols in the network.
SRT/SRB	Combines the SRT and SRB modes.	Allows the use of duplicate MAC addresses when running in SRT. Ports with duplicate MAC addresses are reachable only via source routing. Duplicate MAC addresses are typically found in installations utilizing SNA gateways and/or front-ends.

Table 2. Benefits of the Multiple Bridging Modes

Token-Ring Port Operation Modes

Each port can be independently configured to one of the following operating modes.

Feature	Function	Benefit
Half-duplex concentrator port	Port behaves like an active MAU port for classical Token-Ring.	Connects to a single station in half-duplex mode. Compatible with older adapters.
Half-duplex station emulation	The Token-Ring port is connected to a port on a MAU.	Connects to classical Token-Ring segments with multiple stations in existing installations.
Full-duplex concentrator port	Connects to a single station in full-duplex.	Allows high-performance station and server connection and allows high performance server attachments with up to 97% improvement over a half-duplex Token-Ring connection.
Full-duplex station emulation.	Connects to another switch in full-duplex mode.	Allows easy connection between switches.
RI/RO-like connection on Token-Ring ports 19 and 20	Allows connection of the RI/RO port from a MAU or CAU directly to the switch.	Enables easy integration into existing installations.
Automatic port sensing of operating mode	The port senses automatically which mode to operate in.	Makes installation easier and faster.
Auto-configuration	All Token-Ring and Ethernet switch ports automatically sense connection speed and duplex mode.	Easy, plug and play installation

Table 3. Benefits of Token-Ring Port Operation Modes

Feature	Function	Benefit
Congestion control	The size of each port's output queue is monitored. In case of congestion the queue size is adjusted through frame priority adjustment and frame purging.	Minimizes the effect of congestion on output ports

Table 3. Benefits of Token-Ring Port Operation Modes

Fast Ethernet Port Operation Modes

Each port can be independently configured to one of the following operating modes:

Feature	Function	Benefit
Half-duplex 10 Mbps	Switch-to-switch, switch-to-workstation or switch-to-HUB connection.	Compatibility with older adapters in half-duplex mode.
Half-duplex 100 Mbps	Switch-to-switch, switch-to-workstation or switch-to-HUB connection.	Allows high performance connection in half-duplex mode.
Full-duplex 10 Mbps	Switch-to-switch or switch-to-workstation connection.	Compatibility with older adapters in full-duplex mode.
Full-duplex 100 Mbps	Switch-to-switch or switch-to-workstation connection.	Allows high performance server or switch connection in full duplex mode.

Table 4. Benefit of Ethernet Port Operation Modes

Three Switching Modes

Note that the Fast Ethernet ports always use the *Store and Forward* mode.

Feature	Function	Benefit
Cut-Through for Token-Ring.	Switches with minimum and constant latency, approximately 35 µs	Lowest possible switch-latency, which means optimal response time for end-users.
Store and Forward for both Token-Ring and Fast Ethernet.	Each packet is forwarded only after the entire packet has been received by the switch. This is used for data transfer between LAN segments of different speeds or for LAN segments with a high error rate.	Does not propagate errors to other segments.
Auto (Adaptive Cut-Through) for Token-Ring.	Cut-through switching that checks for error packets. If a port's errors exceed a user-defined threshold then the port switches to store and forward.	Same speed as cut-through switching, but with built-in adaptation to errors which means that bandwidth is effectively preserved

Table 5. Benefits of the Switching Modes

Spanning Tree Protocol

Feature	Function	Benefit
IEEE 802.1D	Allows redundant network paths to be defined in both SRB and transparent switching configurations. Enables Spanning Tree to be implemented on both Ethernet and Token-Ring networks, as well as IBM Spanning Tree on the Token-Ring side.	No single point of failure. The duplicate STP modes allow operation in both transparent and source route bridging modes. Easy compatibility with existing Ethernet and Token-Ring installations
IBM for Token-Ring only.	When in SRB/SRT mode, a combination of IBM spanning tree and IEEE 802.1D is used.	Same as above, and in addition ensures compatibility in IBM SRB installations.

Table 6. Spanning Tree Protocol Benefits

Management

Feature	Function	Benefit
SNMP	Can be configured and managed using SNMP management station.	Allows integration into any SNMP-based management environment.
VLAN support	Ensures the availability of a high number of switched, port based, VLANs for an enterprise network.	Eases network-wide administration by enabling ports to be grouped together in a logical way. Provides performance and security control. Enables effective broadcast control. Improves and simplifies adds, moves, and changes in the network.
HP OpenView for Windows Additional Network Management applications available for Unix platforms: *HP OpenView NNM for HP- UX* and *Tivoli TME 10 NetView for AIX*	Full Graphical HP OpenView for Windows management application.	Allows full graphical integration into HP OpenView management environments.
Telnet management	Allows management from a any LAN station via Telnet.	Makes management flexible by enabling management from any station.
VT100 management	Allows out-of-band management from an external VT100 type terminal connected directly or via a modem.	Enables management of switches in remote locations.

Table 7. Management Benefits

Network Monitoring

Feature	Function	Benefit
RMON support	Support for Token-Ring specific remote monitoring.	Enables collection and analysis of enhanced traffic-management data.
Passive Port Monitoring	All traffic flowing on the monitored port is copied to the monitoring port (the monitoring port is a true copy of the monitored port).	Eases the management task by making it easy to collect Token-Ring statistics with a special passive network analyzer.
Active Port Monitoring	All traffic switched to and from the monitored port is also sent to the monitoring port (the order and timing of frames on the monitoring port can be different).	Eases the management task by making it easy to collect network statistics and carry out protocol analysis. Active monitoring respects the MAC protocol, allowing the use of a standard network analyzer.
Built-in port counters	Many MAC layer, error, and frame forwarding counters are collected per port	Provides a detailed picture of port traffic.
Port Mirroring	Allows any port to be used for connecting a network analyzer. Can then duplicate traffic n any other port to troubleshoot attached segments.	Greatly simplifies system management and facilitates collection of network statistics.

Table 8. Network Monitoring Benefits

Filtering

Feature	Function	Benefit
MAC address	Allows filtering based on frame source and destination MAC addresses.	Preserves available network bandwidth by restricting traffic from propagating beyond the needed limits. Enables enhanced network security policies to be established.
Logical Link Control (LLC): DSAP/SNAP	Allows filtering based on LLC parameters DSAP (Destination Source Access Point) and SNAP (Subnetwork Access Protocol).	Same as above.

Table 9. Filtering Benefits

Connectivity Options

Feature	Function	Benefit
CrossLink high-speed inter-switch connection for Token-Ring (up to 256 Mbps using eight ports)	Allows switches to be interconnected using 1-8 Token-Ring ports.	Provides easy and scalable switch inter connection.
Stackable: **3 possibilities:** **A. 2 switch stack** **B. 5 switch stack** **C. 8 switch stack**	Stack Products Needed: A. 2 x 8630 B. 1 x 8635 and 4 x 8630 C. 1 x 8300 and 8 x 8630	Allows several switches to be stacked, accommodating switch scalability up to 160 switched Token-Ring ports and 32 Fast Ethernet ports.
Optional redundant power supply	Up to six switches can receive backup power from one CrossFire 8310 Redundant Power supply, fully equipped with six CrossFire 8311 power supply units. (Note that CrossFire 8311 is **not** hot-swappable.)	Gives a high degree of resilience to power supply failures when used in critical applications.

Table 10. Connectivity Benefits

❑

2. Switch Overview

This chapter explains how the CrossFire 8730 Fast Ethernet Translation Switch improve network performance.

How the CrossFire 8730 Works

The switch contains the following main elements, as listed below:

- Switching Bus—the architecture of the switch centers around the AXIS bus, a 520 Mbps switching fabric through which all switched ports communicate. The AXIS bus is a partially asynchronous time division multiplexed bus used for switching packets between heterogeneous LAN modules.
- Token-Ring Ports—each port can attach to a classical Token-Ring segment or to a dedicated station. Now users running basic applications are able to share bandwidth, and users running bandwidth-intensive applications can receive their own dedicated 16 Mbps port. Each dedicated port can also be set up in full-duplex communication mode, so that each 16 Mbps port doubles to 32 Mbps.
- Fast Ethernet Ports— each port can attach to a 10/100 Mbps Fast Ethernet network or Fast Ethernet station.
- Stack Link Module—the switch supports a stack link module that can be used to connect two switches in a back-to-back configuration. Alternatively, up to five switches can be connected together using and internal stacker module, and up to eight switches can be connected together using the stack link module and an additional switch stack unit. By connecting switches together through the stack link module, the switches virtually combine to form a single unit, providing scalability, simplified management, and enhanced performance.

Multiple Simultaneous Conversations

A limitation of a shared media LAN is that it supports only one packet at a time. The CrossFire 8730 improve data throughput by supporting multiple, simultaneous, full-duplex conversations. By using High-Speed bus switching technology, the switch creates multiple data paths. These switched connections between LAN segments last only for the duration of a byte transmission. New connections are made “on-the-fly” between different ports on the switch for the next byte.

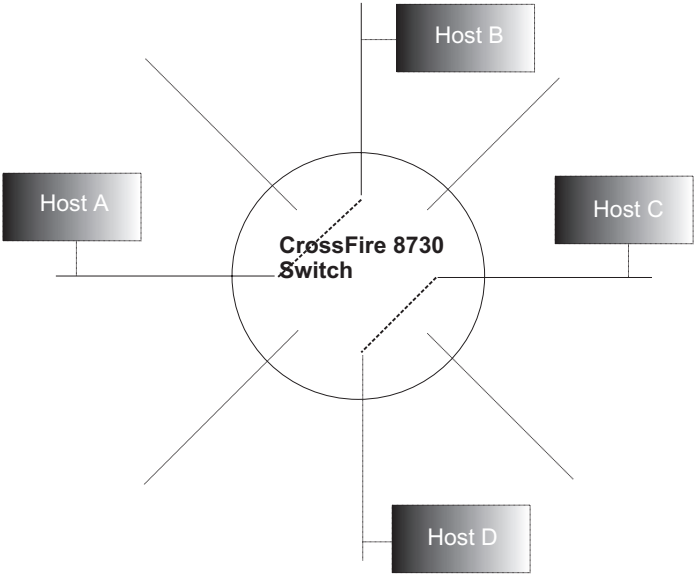


Figure 4. Multiple Conversations Through a CrossFire 8730

For example, as shown in Figure 4, while host A is transmitting a byte to host B, the switch connects only the lines from A to B since there is no need to send packets to all other ports. At the same time, a second switching circuit can connect host C to host D. The result: Two packets are sent simultaneously.

Note: The switch transmits broadcast and multicast packets on several switch ports simultaneously.

The increase in throughput is directly proportional to the number of physical LAN segments that are interconnected through the switch. A switch with 20 ports interconnected provides up to ten concurrent paths. With ten simultaneous Token-Ring conversations, the switch creates 160 Mbps throughput in half-duplex mode, or 320 Mbps throughput in full-duplex mode.

A single segment can be dedicated to a single host or shared by several. To optimize throughput, high-speed servers can be given dedicated switch ports.

By transporting Token-Ring packets simultaneously, the CrossFire 8730 boosts overall network throughput.

Address Management

At power up, the system address tables do not contain any information. Whenever a switch receives a packet with an unknown source or destination address, it learns the new source address and stores its location in coming port in the address table. If the destination address is unknown it sends the packet to all ports that can receive data from the incoming port. When the response packet comes back, the switch will learn the responder's location and adds it to the address table. Once the address table entries are created, the switch uses these learned address to switch all subsequent packets to the port where the destination address is located.

The system address table maintains up to 10,000 entries. Each Token-Ring port address table maintains 5,500 active addresses (each port address table is shared by four ports, as follows: 1-4, 5-8, 9-12, 13-, etc.). If an address has not been active for a configurable aging time, it is removed from the table. Each Fast Ethernet port maintains up to 15,000 active addresses. Unlike Token-Ring ports, that need local and transparent addresses only, a Fast Ethernet port must know all the active addresses in the network.

Multiple Bridging Modes

The CrossFire 8730 supports four different switching modes to provide maximum flexibility in all installation environments. The switching modes are Source Route Switching (SRS), Source Route Bridging (SRB), Source Route Transparent (SRT) and SRT/SRB. The switch operates on two levels (BRF and CRF) as outlined below.

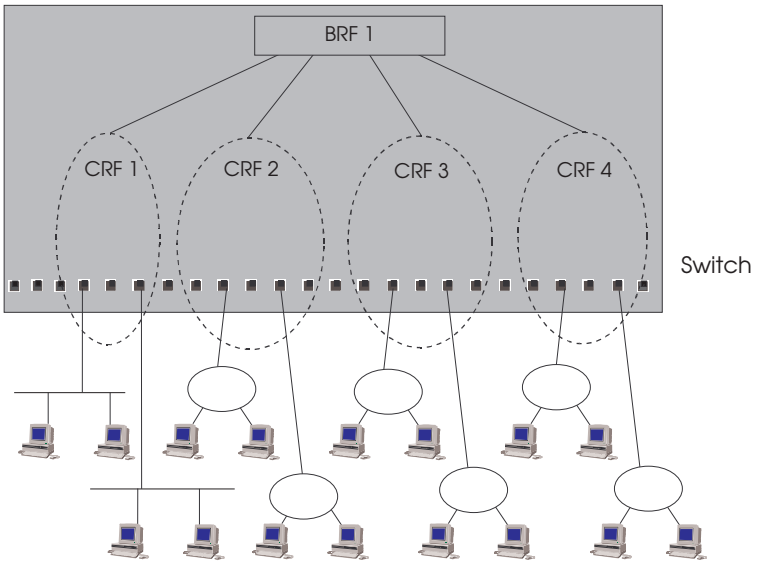


Figure 5. Typical Configuration with Switches Using Multiple Bridging Modes

The switch bridging modes are founded on the concept of Logical Rings (LR) or Logical Segments in Ethernet. The Logical Ring is represented on the switch by the DTR (IEEE 802.5r) standard's Concentrator Relay Function (CRF). A Logical Ring may consist of interconnected CRFs on different switches.

Each port on the switch belongs to a CRF, which is a logical grouping of ports within the switch. A CRF can consist of any number of ports within a switch or a switch stack. The ports within a CRF do not have to be adjacent.

The Logical Rings and, subsequently, the CRFs, are assigned an unique ring number each when the switch performs source routing functions. The bridging is performed through the logical entity of the Bridge Relay Function (BRF).

The CRF communicates via a logical, virtual port with the Bridge Relay Function, which functions as a multiport (virtual) bridge between the Logical Rings. The switch can support up to 63 logical rings.

There are two levels of relay functions supported by the switch. The first level is the TrCRF (Token-Ring Concentrator Relay Function) to which the ports are assigned. The second level is the TrBRF (Token-Ring Bridge Relay Function). This is the parent relay function to which TrCRFs are assigned. The switch maintains certain configuration information and management statistics on a per BRF/CRF basis. Therefore, when you access VLAN-specific switch configuration or management screens (such as the **Current Spanning Tree Information** screen), you will be prompted to specify the desired TrBRF for TrCRF.

For specific information for the Fast Ethernet ports, see "Fast Ethernet Bridging Modes" on page 23.

Source Route Switching (SRS)

This mode is used between ports comprising a Logical Ring.

SRS switching combines the normal transparent bridge function with the ability to forward frames based on source route information to locally attached source-route bridges. The switch does not otherwise act as a source route bridge. For non source-routed packets, the switch decision is based upon destination MAC Addresses. For source-routed packets, it is based on the source-route information combined with the destination MAC address.

The switch learns MAC addresses and source-routing route descriptors of Source Route Bridges attached to local switch ports.

Parallel paths are eliminated via the IEEE 802.1D Spanning Tree Protocol.

Source Route Bridging (SRB)

The BRF acts as a multiport Source Route Bridge between CRFs with the following characteristics:

- Each Logical Ring has a different ring number
- Source Route Frames are forwarded between the Logical Rings by the Bridge Relay Function based on the route information field
- Non-source-route frames are not forwarded between logical rings
- The Bridge Relay Function has a single bridge number and multiple ring numbers (one per Logical Ring)

SRS is used between the ports of each logical ring. The Bridge Relay Function runs the IBM Spanning Tree Protocol to eliminate parallel paths with other source-route bridges. The IEEE 802.1D Spanning Tree Protocol is still used with each logical ring. Duplicate MAC addresses are allowed **only** if they are on different Logical Rings.

Source Route Transparent (SRT)

The BRF can combine transparent switching with Source Route Bridging. Non source-routed packets are switched across logical rings by transparent bridging. Source-routed frames are switched across logical rings by Source-Route Bridging and within each logical ring by Source-Route Switching.

The Bridge Relay Function runs the IEEE 802.1D Spanning Tree Protocol. Duplicate MAC addresses are **not** allowed.

SRT/SRB

This is a special mode combining SRT and the SRB switching modes. Each Logical Ring will operate either in SRT mode or in SRB mode. Transparent bridging will only take place between logical rings in SRT mode. Source-route bridging will take place between all logical rings.

The purpose of the SRT/SRB mode is to allow duplicate MAC addresses to be used when in SRT mode. The ports on which the duplicate MAC addresses reside can be reached only by source routing.

The Bridge Relay Function runs the IBM Spanning Tree Protocol on the SRB logical rings to eliminate parallel paths with all source route bridges. It runs IEEE 802.1D Spanning Tree Protocol on the SRT logical rings to eliminate parallel paths with other SRT bridges. The two resulting spanning trees are joined together.

The IEEE 802.1D Spanning Tree Protocol is still used to eliminate parallel paths within each logical ring whether it is SRB or SRT.

The benefit of the SRT/SRB mode is that it allows part of the network to be run in SRT mode to accommodate applications that do not support source routing, while still supporting duplicate MAC addresses on a number of SRB ports (for example, for SNA gateway applications).

Filtering

Filtering is important for a LAN switch. Filters can be used to reduce broadcast traffic, block certain protocols and provide security functions.

The switch provides filters for:

- Destination or source MAC addresses
- Destination service access point (DSAP)
- Subnetwork Access Protocol (SNAP) type

Each protocol filter can be applied on a per-port basis for both input and output traffic. This feature allows certain protocols to be blocked from certain ports. For example, filters can be established to allow only Systems Network Architecture (SNA) traffic to flow to ports with SNA gateways.

Source and destination MAC address filtering can be applied to all incoming frames. The MAC address filters act in one of three ways:

- Block destination address at a specific port—this prevents the specified port from sending frames to a specified destination.
- Allow destination address at specific ports—this indicates that the specified port must send frames to the specified destinations **only**.
- Force destination address to a specific port—this allows forwarding to a unicast address that has not been learned. It can also be used to limit the forwarding of Multicast addresses to a subset of ports. This last filter applies to non-source-routing frames **only**.

Congestion Control

At regular intervals, the switch CPU inspects the queues on all Token-Ring output ports. If a queue size is above a certain threshold, the port is instructed to:

- Set the transmit priority for low priority frames to a specified high level
- Delete old frames from the queue until it reaches a specified size

When the queue size again comes below a normal threshold size the port is instructed to set the transmit priority back to the normal level.

Three Switching Modes

Cut-Through

In this mode the switch starts forwarding the packet to the output port as soon as the destination address or the source-route of the incoming packet has been resolved. This technique ensures very low latency, typically in the range of 30-100 µs. However, if errors occur on the input port during the reception of a packet, the error will still be forwarded to the output port. Note that cut-through can only be used in transmissions between ports which operate at 16 Mbps.

This mode is only supported by the Token-Ring ports.

Store and Forward

In this mode, the switch receives the total packet from the input port, checks it for any errors and then starts forwarding the packet to the destination port. This technique will ensure that no faulty packets are transmitted by output port. The negative impact however, is higher latency, typically in the range of 40–2,000 µs depending on the packet size. Though slower than cut-through mode, this is still much faster that conventional bridges.

The Fast Ethernet ports support this mode only.

Auto (Adaptive Cut-Through)

This is a technique whereby the switch will automatically swap between store-and-forward and cut-through modes based on an error threshold. If the number of received faulty packets is low, then cut-through mode is used; if the number of faulty packets is high, the store and forward mode is used. This provides optimized performance but introduces variable latency.

Fast Ethernet

The following sections up to page 32 provides information about Fast Ethernet and various network scenarios.

Fast Ethernet Ports

The Fast Ethernet ports are configured much like Token-Ring ports, and generally appear in all tables where Token-Ring ports appear.

Fast Ethernet Virtual Ports and VLAN Tagging

For general information on VLAN support, see page 35.

Unlike Token-Ring ports, the Fast Ethernet ports can function as trunk ports. This means that they can carry traffic belonging to all of the possible 63 VLANs over the same physical cable connection.

Frames from different VLANs are distinguished by means of standard IEEE 802.1Q frame tags. The tag is inserted in the Ethernet frame after the frame header before transmission on the Fast Ethernet port, and subsequently recognized and removed when the frame is received.

To identify the VLAN to which the frame belongs, the frame tag makes use of a VLAN identifier that uniquely identifies the BRF. It also contains a 3 bit priority field (described in section “Virtual Port Configuration” on page 41.)

Each Fast Ethernet port can be assigned to several CRFs, but there can be only one per BRF/VLAN. A virtual port is created for each CRF to which the Fast Ethernet port is assigned. All virtual ports but one must be tagged (i.e., a single virtual port can be left untagged).

Note that a Fast Ethernet port with a single untagged virtual port is functionally equivalent to an ordinary Token-Ring port. This is also the default configuration, with the virtual port in ethcrf-default.

Virtual Port Restriction

A Fast Ethernet port can have only one virtual port in each VLAN. This follows from the nature of VLAN tagging. Otherwise it would not be possible to distinguish frames from two virtual ports in the same VLAN, since they would have the same VLAN identifier.

Ring Number Restriction

All CRFs in which a Fast Ethernet port has virtual ports must have the same ring number. Thus, the ring number is a “per-port” parameter and not a “per-virtual-port” parameter. If this were not the case, the meaning of the RIF would be

ambiguous and depend on the VLAN to which the frame was sent. It would thus be incomprehensible to equipment that does not understand VLAN tags.

Fast Ethernet Port Operation Modes

Each Fast Ethernet port may operate in one of the following modes:

- **Half-duplex**
  In this mode the port offers a 10 Mbps or 100 Mbps connection from the switch to another switch, a workstation, or a hub.
- **Full-duplex**
  In this mode the port offers a 10 Mbps or 100 Mbps connection from the switch to another switch or a workstation.

Fast Ethernet Bridging Modes

For general information on the bridging modes, see “Multiple Bridging Modes” on page 17.

Source Route Switching (SRS)

SRS is the default mode of operation. This mode is also restored after a NVRAM reset of the switch. In this mode, all Fast Ethernet ports are in the same CRF. Frames are switched between ports based only on MAC addresses. In this mode, the spanning tree algorithm is disabled by default. If more than one Fast Ethernet port is used to connect to the Ethernet cloud, the IEEE Spanning Tree Protocol should be enabled on the CRF.

Source Route Transparent (SRT)

Note: SRT is the suggested mode of operation.

If multiple CRFs are used on a switch, all Fast Ethernet links to the same Ethernet cloud should be grouped into one CRF. If the spanning tree protocol is to be used, enable the STP (spanning tree protocol) on the CRF and BRF. The CRF’s STP should be set to IEEE; the BRFs’ STP should be set to Based on Bridging mode or IEEE.

Note that this translational CRF is used only on the Token-Ring side and is used to route source-routed Token-Ring frames toward the Ethernet cloud. See Figure 6.

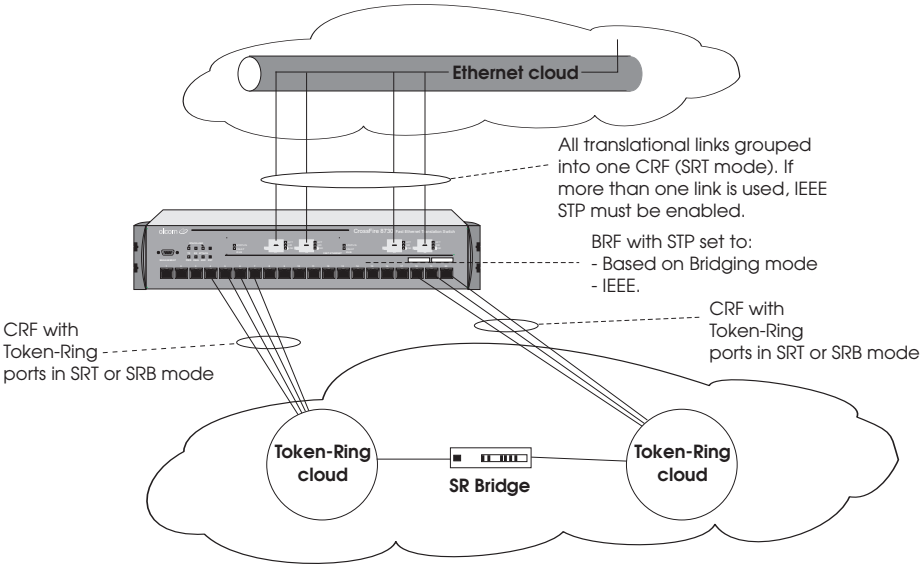


Figure 6. Source Route Transparent Bridging (SRT) Mode

Source Route Bridging (SRB)

Note: SRT is the suggested mode of operation.

If multiple CRFs are used on a switch, all Fast Ethernet links to the same Ethernet cloud should be grouped into one CRF. If a CRF is created in SRB Bridging mode and Spanning Tree is to be used, IEEE STP must be manually configured on the BRF and CRF.

Note that this translational CRF is used only on the Token-Ring side and is used to route source-routed Token-Ring frames toward the Ethernet cloud. See Figure 7.

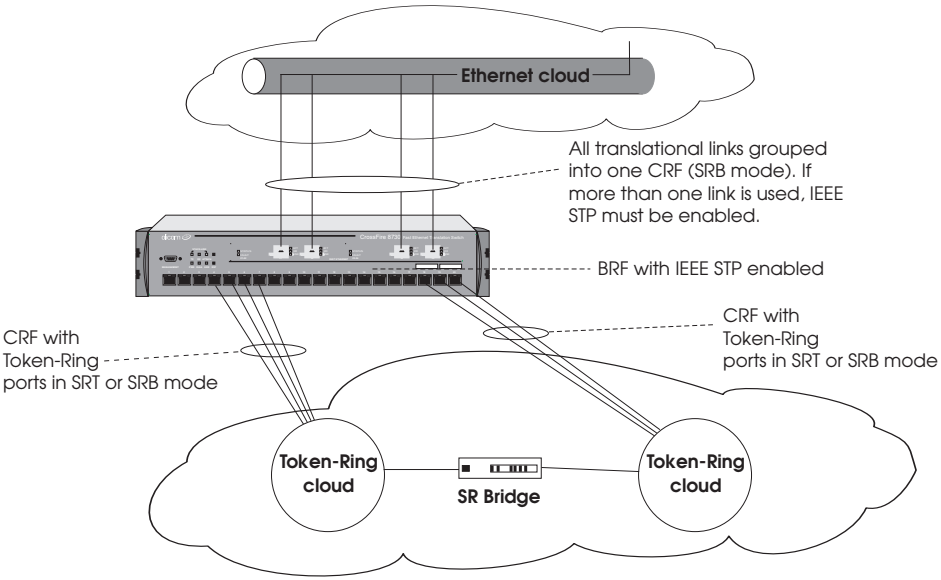


Figure 7. Source Route Bridging (SRB) Mode

Redundant Connections to Fast Ethernet Network

A connection to the Ethernet cloud can be made using several Fast Ethernet ports from multiple switches. Fast Ethernet ports connected from one switch to the same Ethernet cloud should be grouped into one common CRF with an assigned LAN segment number. From each switch, one CRF can be connected to the same Ethernet cloud.

Redundant connections between source-routed and transparent networks may cause ARE frame duplication and infinite ARE frame loops as a result of discarding source routing information during translation from Token-Ring to Ethernet format. There are, however, solutions to both problems:

- Infinite frame loops are eliminated by using a common LAN segment number for the entire Ethernet cloud or by proper Spanning Tree configuration. The recommended CRF number is 4095.
- Frame duplication is eliminated by a proper STP configuration allowing only one link between the Token-Ring cloud and the Ethernet to be forwarding.

See the next section “Network Scenarios—Preventing Frame Duplication and Looping” on page 26 for details.

Network Scenarios—Preventing Frame Duplication and Looping

This section discusses preventing frame duplication and frame looping in networks.

Preventing Frame Duplication

The ARE duplication problem can occur only in a configuration with redundant Fast Ethernet ports in different switches (as in the configuration that follows).

It is assumed that the network consists of a physically connected Ethernet cloud and a physically connected Token-Ring cloud. The two clouds are then connected by a number of links that implement translational bridging. See Figure 8. below.

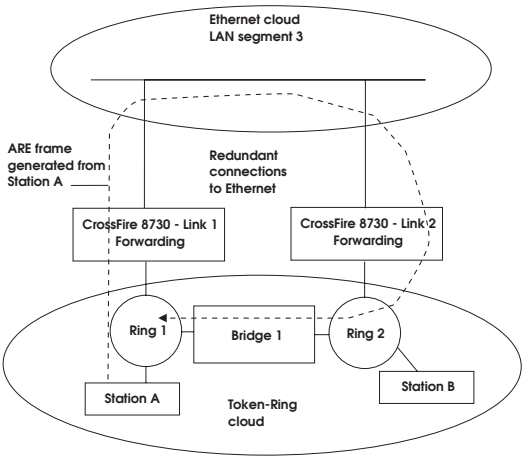


Figure 8. Preventing Frame Duplication

In a pure Token-Ring network, an All Routes Explorer (ARE) frame generated from Station A traverses all rings only one time based on a Routing Information Field (RIF) expanded by each source-routed bridge. In this example, both Fast Ethernet links are in the forwarding state. An ARE frame originating in Ring1 may go through the Ethernet cloud and come back to Ring 2. Because the RIF is lost when passing through the Ethernet cloud, LAN segment 1 is no longer included in the new RIF and the frame will be forwarded by Bridge 1 from Ring 2 back to Ring 1. This results in frame duplication – after visiting Ring 1 again, the frame will be discarded by the Fast Ethernet ports connected to Ring 1.

This issue can be resolved by making sure that only one Fast Ethernet port can be in the forwarding state.

Preventing Frame Looping

The previous network scenario was free of the ARE looping issue because the entire Ethernet cloud had the same LAN Segment number.

In the next scenario, the Fast Ethernet ports have different LAN segment numbers. In this configuration, an infinite loop is created in addition to the frame duplication issue.

Station A sends an ARE frame to Ring1 – ex. IP ARP with destination MAC being Broadcast. This frame is converted to a transparent broadcast and sent on Ethernet link 1. The frame is then received by the Fast Ethernet port on link 2 and sent as an ARE frame to Ring 2 – note that the RIF does not contain LAN Segment 4. The ARE frame is then forwarded by Bridge 1 and link 1 back to the Ethernet, and so on. See Figure 9. below.

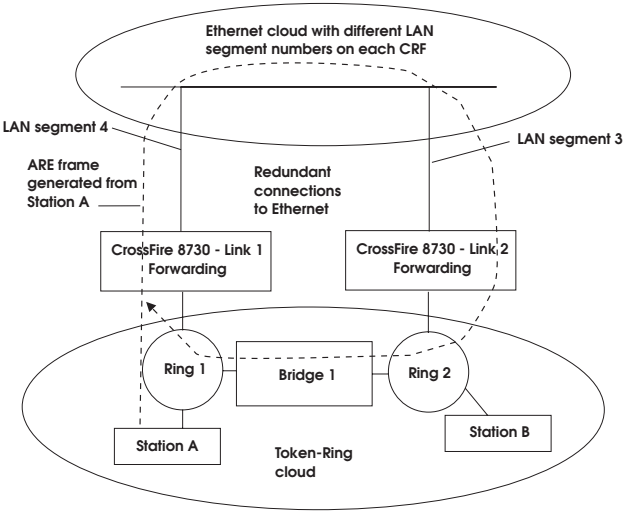


Figure 9. Frame Looping

This loop can be resolved by making sure that only one Fast Ethernet link can be in the forwarding state or by using the same LAN segment number for all Fast Ethernet links.

Using two different LAN segment numbers has some interesting advantages. If the Ethernet cloud becomes physically separated into two parts (see below), both parts can still communicate via the Token-Ring cloud. If the Ethernet cloud is not split and the root of the spanning tree is on the Token-Ring side, there might be a loss of connectivity between Ethernet stations depending on the CRF numbers configured.

To avoid those hazardous situations, follow the recommendations in section “Spanning Tree Configuration for Fast Ethernet” below.

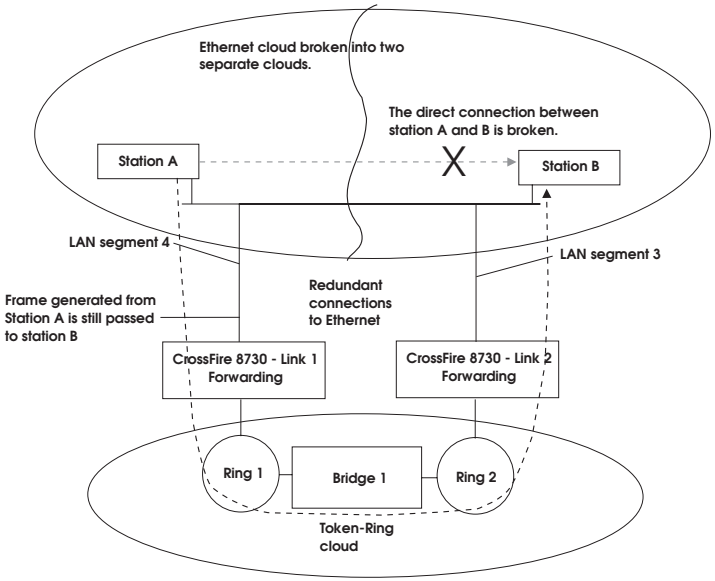


Figure 10. Preventing Frame Looping

Spanning Tree Configuration for Fast Ethernet

Running the IEEE Spanning Tree Protocol (STP) will create a single spanning tree covering the entire network. Depending on the topology and configured path costs, there will be one or more forwarding links between the two clouds.

If there are multiple Fast Ethernet links in multiple switches, the path costs on these links should be selected such that only one forwards. This will prevent ARE duplication and the looping problem.

Normally this can be achieved by assigning very large path costs on both sides of the Fast Ethernet links such that at most one can be forwarding. The Fast Ethernet ports provides support for STP cost manipulation which does not require cost configuration on both sides of the link.

For each CRF of Fast Ethernet ports connected to the same Ethernet cloud, a connection attribute can be assigned (see “TS Connection” on page 56):

- ***Primary* connection** – for a main connection to the Ethernet cloud (default value for each CRF). This connection is always forwarding if active.
- ***Secondary 1*** – for a backup connection to the Ethernet cloud. This connection is always blocking if the primary is active.

- ***Secondary 2*** – for a second backup connection to the Ethernet cloud. This connection is always blocking if *Primary* or *Secondary 1* are active.

Each CRF of Fast Ethernet ports connected to the same Ethernet cloud must have a different connection attribute set. See Figure 11.

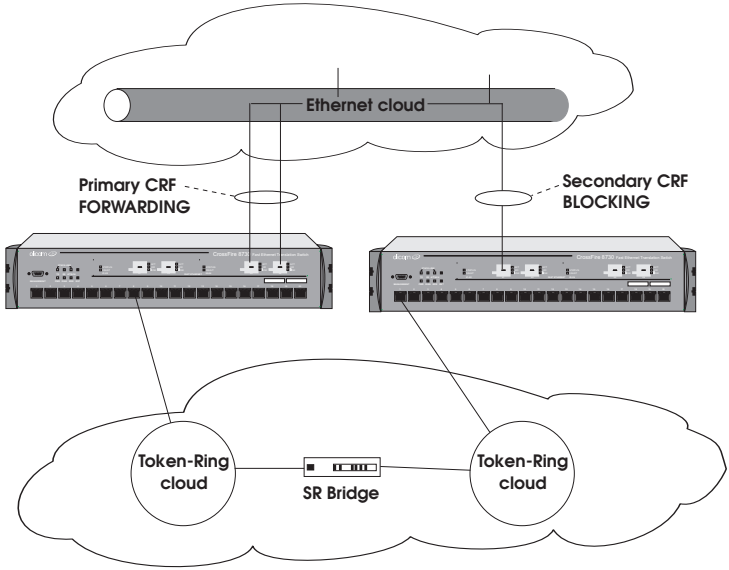


Figure 11. Spanning Tree Configuration

The described spanning tree configuration results in exactly one forwarding link between Ethernet and Token-Ring clouds, additional links becoming stand-by. For customers migrating from Token-Ring to Ethernet it is recommended over time to physically split the Token-Ring cloud into disjoint networks to increase bandwidth between Token-Ring and Ethernet.

Figure 12. below illustrates a network with two physically disjointed Ethernet clouds. Each switch in the configuration has one primary connection to one of the two Ethernet clouds and one secondary connection to the other cloud.

This way redundancy for both Ethernet clouds is provided, while at the same time the traffic load between the Token-Ring and Ethernet clouds is split between the two switches.

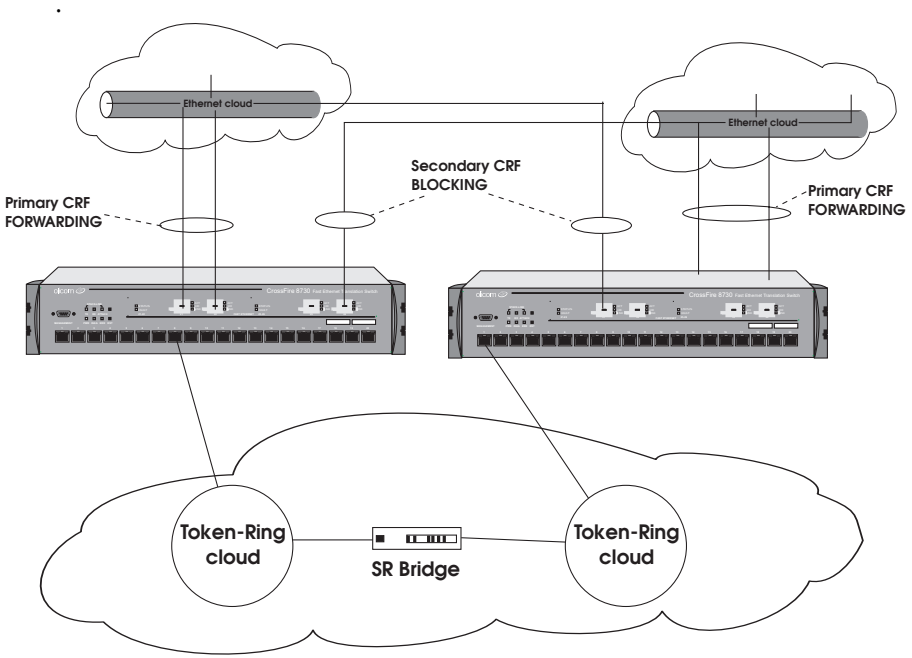


Figure 12. Two Separate Ethernet Clouds

Note: The CRF connection attribute can be set from the console or via ClearSight.

Technical Background

For each CRF with a Fast Ethernet port, the spanning tree protocol should be enabled. For SRT CRF, the default STP algorithm is IEEE 802.1D. Only this spanning tree algorithm can be used for Fast Ethernet ports.

A Fast Ethernet port has its own LAN segment number and recognizes source routing. However, the Fast Ethernet port is an element of a transparent network and frames are passed through only in forwarding state. This restriction is applied to all frames, including ARE and specifically routed frames.

Only one link of a CRF at a time may become forwarding. To achieve this, the spanning tree costs of the internal BRF to CRF link will be modified according to the CRF connection attribute. The BRF to CRF link is a virtual internal link and exists only for spanning tree purposes.

The spanning tree cost of each primary connection remains unmodified.

Note that in the *Secondary 1* and *Secondary 2* connections, different values are added to the cost of the internal BRF to CRF link in order to make sure that

Secondary 1 will become forwarding first, when the primary connection fails. The *Secondary 2* connection is chosen only after the *Secondary 1* connection.

Cost modification of BRF to CRF link:

- For the *Secondary 1* connection, a value of 20,000 will be added to the cost of the internal BRF to CRF link.
- For the *Secondary 2* connection, a value of 40,000 will be added to the cost of the internal BRF to CRF link

In the picture below, the CrossFire 8730 Switch 2 and Ethernet Switch 2 know that the root path cost seen from the secondary link is 20,000 bigger, than the root path cost of the primary link seen by the CrossFire 8730 Switch 1 and Ethernet Switch 1. This means that the secondary link will be blocked on the internal CRF to BRF link.

If the spanning tree costs are configured manually for backup connection to Ethernet, each connection attribute should be set to *Primary* and then spanning tree costs must be changed on each side of the backup link.

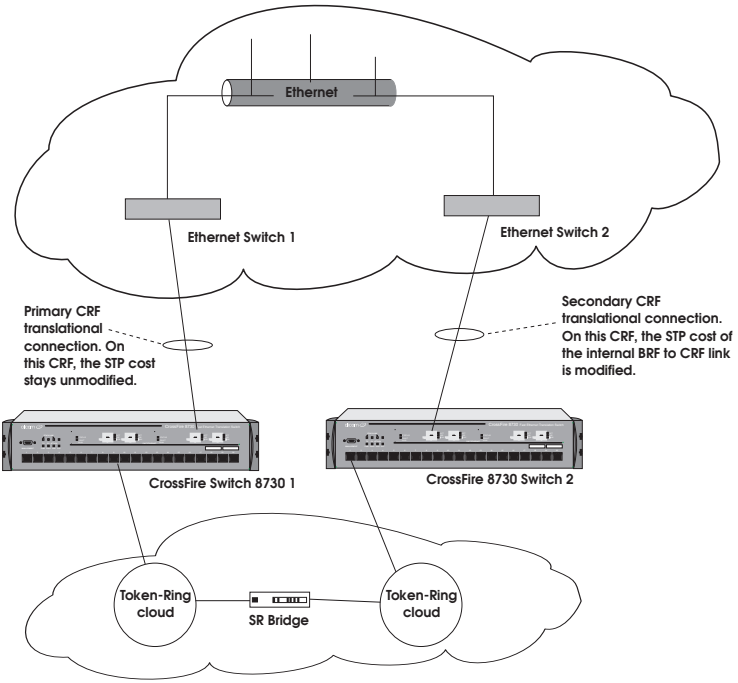


Figure 13. STP BPDU Cost Modification

Token-Ring

The following sections “Token-Ring Port Operation Modes”, “RI/RO-Like Connection”, “Transmission Priority Queues”, and “CrossLink Connections” contains information that only applies to the Token-Ring ports.

Token-Ring Port Operation Modes

Each Token-Ring port may operate in one of the following modes:

- **Half-duplex concentrator port**
  The port behaves like an active MAU port for classical Token-Ring. Connects to a single station in half-duplex mode. This is also known as Token Passing (TKP) port mode.
- **Half-duplex station emulation**
  The port is connected to a port on a MAU. Connects to a classical Token-Ring segment with multiple stations. This is also known as Token Passing (TKP) station mode.
- **Full-duplex concentrator port**
  Connects to a single station or to another switch in full-duplex mode. This is also known as Transmit Immediate (TXI) port mode.
- **Full-duplex station emulation**
  Connects to another Token-Ring switch. This is also known as Transmit Immediate (TXI) station mode.
- **RI/RO-like connection**

The mode of operation can be configured manually or sensed automatically with the exception of RI/RO, when equipment is connected to the port. The media speed (4 or 16 Mbps) can also be manually configured or automatically sensed in all port modes.

RI/RO-Like Connection

On CrossFire 8730, a RI/RO-like connection is available on ports 19 and 20.

This feature allows the switch to connect to CAU/LAM systems using the RI/RO connections thus providing a RI/RO-like functionality. This enables the switch to be easily installed in existing Token-Ring networks.

A loop-back function has been implemented on these ports so that if the port is disabled or the switch is powered off there will not be a break in the attached main ring. This means that attaching a cable from the RI port of a MAU port to one of the two switch ports in effect joins the primary and the backup ring in a MAU/CAU main ring system. Connecting the other end of the RI/RO connection to the other

switch port, *creates redundant paths* because the two switch ports are connected to the same segment. *Therefore, the IEEE Spanning-Tree Protocol (STP) must be enabled*, which will place one port in forward and the other in blocked mode. If there is a break in the main ring, the STP will place both ports in forward mode, and all MACs on both segments will be relearned.

If a switch port has been configured to RI/RO mode, it will automatically sense whether the port has been connected to RI or RO of the MAU.

Note: It is not possible to automatically verify whether an UTP/STP port has been connected according to the configuration. Any errors, such as attaching port 19 or 20 to a normal MAU port when the CrossFire 8730 port has been configured for RI/RO, will cause a complete disruption of the ring to which the port is attached. Therefore, be careful when using the RI/RO feature.

Transmission Priority Queues

To address the needs of delay-sensitive data, such as multimedia, the Token-Ring ports of the switch have two transmit queues, a high-priority queue and a low-priority queue.

The queue for a frame is determined by the value of the priority field in the frame control (FC) byte. If FC priority is above a configurable level (default 3), the frame is put into the high-priority queue. If an output port becomes congested, you can dynamically configure the port to transmit all frames at high priority regardless of the FC byte contents.

Enabled FC modification on Fast Ethernet virtual ports preserves frame priority during translation between Ethernet 802.1Q Tagged frames and Token Ring frames.

CrossLink Connections

Two switch stacks or switches may be interconnected by a number of parallel Token-Ring connections (up to 256 Mbps using eight Token-Ring ports). The traffic between the switches will be shared between the connections.

Spanning Tree Protocol Support

The CrossFire 8730 supports the spanning tree protocols most often used in both Ethernet and Token-Ring topologies. The switch supports IEEE 802.1D Spanning Tree for all Ethernet ports, and both IEEE 802.1D Spanning Tree and IBM Spanning Tree Protocols for Token-Ring ports. This makes it easy to integrate the switch into most existing Token-Ring and Fast Ethernet installations.

For more information on spanning tree, see “Spanning Tree Configuration for Fast Ethernet” on page 28 and “Spanning Tree Protocol” on page 64.

IBM initially supported only Source Route Bridging (SRB) in its bridges, so most Token-Ring networks were built to use it. The main consideration for SRB implementations in switches is the spanning-tree algorithm for spanning tree explorers (STEs). IBM originally implemented a form of the Institute of Electrical and Electronics Engineers (IEEE) spanning-tree algorithm. This algorithm, commonly referred to as the IBM spanning tree, limits the STE frames to one copy per destination ring. Some SRB implementations have also implemented the IEEE Spanning Tree Protocol to be compatible with SRT bridges. The IEEE Spanning Tree Protocol is not compatible with the IBM Spanning Tree Protocol.

VLAN Support

The virtual LAN (VLAN) concept creates a virtual switch within a physical switch. Frames are not forwarded between VLANs unless directed via a router or layer-3 switch.

The CrossFire 8730 provides the following VLAN functionality:

- No frames are forwarded between ports belonging to different VLANs.
- Each VLAN may be assigned a separate IP address.
- Spanning Tree determination is executed independently within each VLAN.

VLANs on the Token-Ring Side

On the Token-Ring side, VLANs are set up on a per-port basis. This means that all stations connected to a port must be part of the same VLAN. VLAN tagging is not used.

IEEE 802.1Q tagged VLANs entering the switch from the Fast Ethernet side are translated into port-based VLANs on the Token-Ring side (and vice-versa).

Port groups on different VLANs may be assigned the same ring number, but ring numbers must be unique within the same VLAN.

VLANs on the Fast Ethernet Side

On the Fast Ethernet side, IEEE 802.1Q VLAN tagging is applied. This enables traffic from several Token-Ring port-based VLANs to pass over a single Fast Ethernet link. Furthermore, Q-tagged VLAN information is able to travel further into the network so VLAN information will be preserved by all equipment that supports Q-tagging, regardless of the manufacturer or topology.

IEEE 802.1Q tagged VLANs entering the switch from the Fast Ethernet side are translated into port-based VLANs on the Token-Ring side (and vice-versa).

The following figure illustrates an example of a VLAN with a CrossFire 8730 Switch.

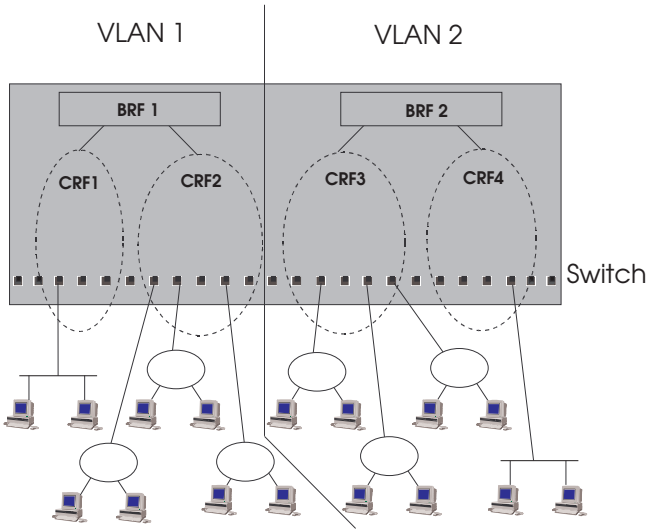


Figure 14. A Switch Configured with Two VLANs

Management

SNMP

The switch can be managed via a SNMP manager. It supports ten Management Information Bases (MIBs). Six of the MIBs are standard MIBs, which are defined by RFCs and are included with most SNMP management applications. Four of the MIBs are proprietary and are provided on the disk that accompanies the switch. SNMP management is supported via IP.

The following MIBs are supported:

Specification	MIB
RFC1213	SNMP MIB II
RFC1493	Bridge MIB
RFC1525	SR Bridge MIB
RFC1573	Evolution of the Interfaces Group of MIB-II
RFC1757/1513	RMON MIB/TR extensions - only partial support
RFC1749/1748	IEEE 802.5 MIB
DTR MIB	IEEE 802.5r MIB
DTR MAC MIB	IEEE 802.5r MIB
Olicom	oc8600 unit MIB
	oc8660 unit MIB
Olicom/Cisco	VTP MIB

Table 11. Supported MIBs

Most user configurable variables will be supported in either the standard MIBs or the proprietary MIB. Configuration settings, such as port attributes, and operational information, such as address tables, are fully accessible through SNMP. Certain other settings, such as passwords and console settings, cannot be viewed or modified via SNMP for security reasons.

Switch Manager for HP OpenView for Windows

The Switch Manager is an application that runs under HP OpenView for Windows. It provides an intuitive graphical user interface (GUI) that displays a chassis physical view and supports configuration, performance monitoring, and troubleshooting.

This application is included with the switch.

For information about Switch Manager on other platforms, please contact your local Olicom sales representative.

Telnet Management and VT100 Management (Console)

The Console Management function may be accessed out-of-band via the TIA/EIA-232-F (i.e. RS-232) port labelled MANAGEMENT or in-band via Telnet.

IBM LAN Network Manager

The switch does **not** support management by the IBM LAN Network Manager, but it will allow LAN Network Manager LLC frames to flow through the switch so that communication to existing LNM manageable hubs and source route bridges will be maintained.

Some error reporting functions and ring map functions might be lost for the rings attached to through the switch, because a Token-Ring Switch will not (and should not) forward MAC frames, but only LLC frames between ports.

RMON Support

RMON is an industry-standard method for providing network statistics monitoring using SNMP. It also collects fault, performance, and configuration statistics. It can monitor continuously, even when communication with the management station is not possible or efficient. RMON can then notify the management station when an exceptional condition occurs.

In typical SNMP management, the SNMP client has to continuously poll the switch for fault, performance, and configuration information, 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 statistics reaches a threshold, the switch will send a trap to the client. This monitoring method reduces traffic between the SNMP client and the switch.

The following groups are supported in RFC-1513 Token-Ring Extensions RMON MIB

- The Token-Ring Mac-Layer Statistics Group
- The Token-Ring Promiscuous Statistics Group
- The Token-Ring Mac-Layer History Group
- The Token-Ring Promiscuous History Group
- The Token-Ring Ring Station Group (SETs not supported)
- The Token-Ring Ring Station Order Group.

The Following Groups are supported in RFC-1757 RMON MIB for both Token-Ring and Fast Ethernet ports.

- The Statistics Group (group 1)
- The History Control Group (group 2)
- The Event Group (group 9)
- The Alarm Group (group 3)

Full RMON support for a selected subset of ports is implemented by an external RMON Probe.

Note: Remember to enable **RMON Statistics** on the **SNMP Configuration** menu.

Note: 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 console interface of the switch.

Built-in Port Counters

The switch supports a wide range of port counters, which enables you to obtain a detailed overview of the port traffic. The counters give a comprehensive overview in the areas of:

- MAC Layer Counters
- MAC Layer Error Counters
- Frame Forwarding Counters

Stackable Architecture

A CrossFire 8730 switch can be stacked together with other CrossFire 8730 switches and with switches from the CrossFire 8600 series in any desired combination to provide uplinks like ATM, HSTR, and Fast Ethernet. For more information on stacking, refer to the CrossFire 8600 Series documentation.

Optional Redundant Power Supply

The switch has an input for a backup power supply. It is compatible with the CrossFire 8310 Redundant Power Supply Chassis, which can supply backup power for up to six switches, when up to six CrossFire 8311 Redundant Power Supply Units are installed in the chassis. This gives a high degree of resilience to power supply failures. The switch will start using the external power supply if the internal supply fails. The switch monitors the power source and informs the network management system which supply is in use.

The CrossFire 8300 Switch Stacker also accommodates an optional switch matrix 8301, which includes a redundant power supply, ensuring the highest degree of resilience in the stack of switches.

Caution: The redundant power supply unit CrossFire 8311 is **not** hot-swappable. Both the CrossFire 8311 unit and the switch **must be off** before connecting or disconnecting the DC power cable.

❑

3. Switch Configuration

This chapter explains how to modify the switch configuration via the menus and screens in the switch console interface. To access the interface, a VT100 console can be attached to the switch directly or via a modem connection. The switch configuration can also be modified from a remote VT100 console via a telnet session.

For information on how to connect a VT100 console directly to the switch, please refer to the *CrossFire 8730 Fast Ethernet Translation Switch Installation Guide*, Chapter 4, “Switch Access”.

General Guidelines

To work within the console menus and screens, follow these guidelines:

- To select an item on a screen or a menu, highlight it by using the arrow keys and then press ENTER. If you need to specify additional information for that item—for example, selecting **Yes** or **No** or supplying a *value*—a prompt appears on the screen.
- In most cases, new values are saved when you select **Return**.
- The **More** item means there is more information than what is displayed on that screen. Selecting **More** and pressing ENTER displays the next screen of information.
- **Port** refers to the number of a specific port on a switch.
- **Index** refers to the numerical order of a list.
- To return to the main menu from any screen, press CTRL-P. Note that any changes made to the screen you were in will not be saved when you do this. To return to the greeting screen, press CTRL-B.
- To refresh the console screen, press CTRL-L.
- If you are administering switches in a stack, many of the console screens will prompt for a box number. Enter the number of the box you want to administer.
- The “VLAN” term in connection with CRF is discussed on page 35.
- The terms “Virtual LAN” and “domain” are interchangeable.
- The console automatically returns to the greeting screen after five minutes of inactivity. Five minutes is the default value. The time can be changed at the **Console Configuration** menu as explained later in this chapter.

  To open the **Console Configuration** menu from the main menu, select **Configuration... → Console Configuration...**.
- For protection against inadvertent or unauthorized access to configuration screens, you may establish a password that users must enter at the greeting screen. If no password is configured, just press ENTER and the main menu is presented. To establish a password, see the section “Password Menu” on page 116.

  To open the **Password** menu, select **Configuration... → Password...**.

Navigating within the Menus

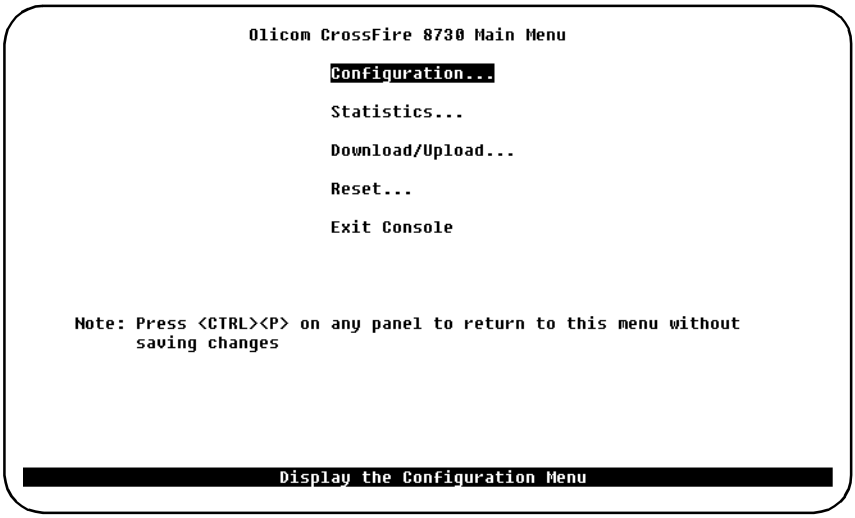
Use the arrow keys (also referred to as cursor keys) to highlight an item on the screen or menu.

- Items that end with three dots, opens another screen or menu. Pressing the ENTER key on such an item will display the new screen or menu.
- If the item on the screen is a command, such as **Reset**, pressing the ENTER key will execute the command.

Unless specified differently, all the screens and menus are accessed in the same way.

The following section describes the items on the main menu.

Main Menu



Configuration...

Displays the **Configuration** menu, which enables you to view and set the switch configuration parameters. A detailed explanation of the configuration submenus starts on on page 45.

Statistics...

Displays the **Statistics** menu for the switch. Explanations of screens in the **Statistics** menu are in Chapter 4, “Monitoring the Network from the Statistics Menu” on page 135.

Download/Upload...

Displays the **Download/Upload** menu that is explained starting from page 125.

Reset...

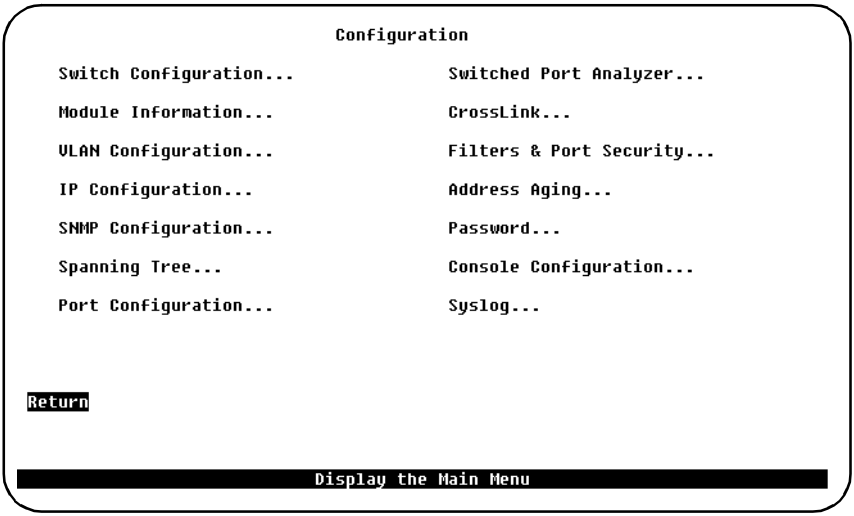
Displays the **Reset** menu that is explained in this chapter starting from page 130.

Exit Console

Highlighting this command and pressing ENTER will return the console to the greeting screen (on a Telnet session, this will cause the session to close).

Configuration Menu

Open this menu by selectiong **Configuration...** in the main menu.
From the **Configuration** menu you can view and set the switch configuration parameters.



Detailed descriptions and of the submenus and screens these items open follows below in this chapter.

Configuration Overview for the Fast Ethernet Ports

To configure the Fast Ethernet ports, follow general steps listed below:

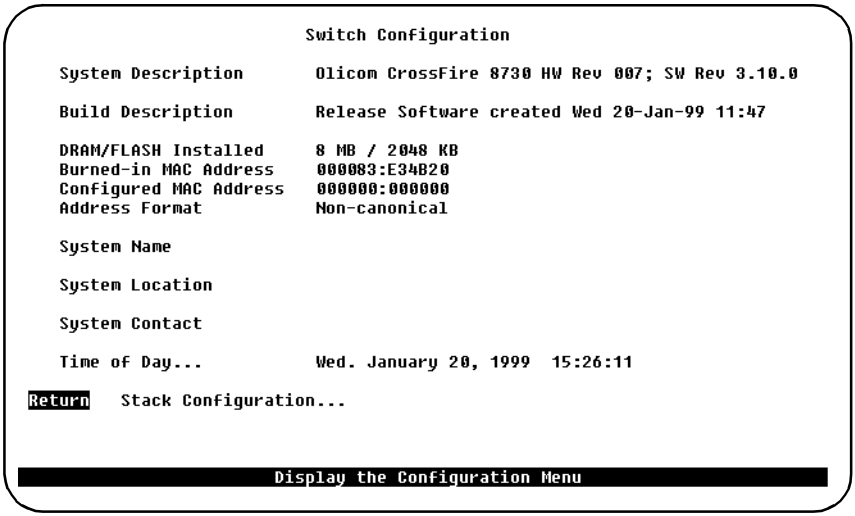
- Determine which VLANs the Fast Ethernet ports should connect.
- Determine which VLAN, if any, should be untagged.
- Configure the Fast Ethernet VLAN ID for all the BRFs that should be tagged.
- Make sure that each Fast Ethernet VLAN ID matches that of the Fast Ethernet equipment in the other end.
- Assign CRFs to the Fast Ethernet port, thereby creating one virtual port in each VLAN. Possibly create new CRFs to make sure that the CRFs do not have conflicting ring numbers, as discussed in section “Ring Number Restriction” above.
- Configure the virtual ports, in particular the tagging mode. The relevant configuration menus are described in detail in the following sections.

Configure the translational bridging parameters for each Virtual Port.

Switch Configuration Screen

To open this screen from the main menu, select **Configuration → Switch Configuration**.

Use this screen to view system information and to view or change the system name, location, contact, and time of day. To add or change the system name, location, contact or time of day, use the arrow keys to highlight the field and press the ENTER key. A prompt appears near the bottom of the screen for entering text for that field. Pressing ENTER again enters that text.



The following sections explain the fields in the **Switch Configuration** screen.

System Description

Name and model of this switch. Information in this field cannot be changed.

Burned-in MAC Address

The factory-assigned base MAC address of the switch. Information in this field cannot be changed.

Configured MAC Address

The MAC address that is currently in use, or, if a new MAC address has been configured, the MAC address that will be used after the next boot. If a locally administered address is assigned to the switch, this field displays that address. Otherwise, the field displays *000000:000000*. To assign a locally administered address, select this field, and enter the new address. Note that the switch occupies this, the base MAC address, and the next 96 addresses.

All usage of MAC-Addresses in the switch is based upon one address. This address is denoted the Switch Base address and can be either Burned-in (The factory assigned Universal Administrated Address UAA) or configured (the Local Administrated Address LAA). To configure a LAA address, use the **Switch Configuration** screen from a console session or an SNMP based management tool. Note that a restart is necessary when changing the base MAC address.

The greeting screen on the console will always show the current active Switch base Address.

The switch reserves 31 addresses for ports.

The Token-Ring ports on a switch will be assigned MAC addresses using the following scheme:

- BASE Module port 1- 20 will be assigned Switch Base Address + port number

OR:

- A Token-Ring port will be assigned a MAC address, which is Switch Base Address + the port number displayed on the port configuration screen (or interface table for SNMP).

  This MAC address is used for the Token-Ring MAC protocol, and for the spanning tree protocol.

The switch reserves 63 addresses for TrBRF (VLAN).

Each VLAN has an attached Bridge relay function (TrBRF) and a Management entity (IP-protocol stack), and consequently it needs a MAC Address. In the switch, these two logical units use the same address, however this address must be unique in the network. This is ensured by assigning MAC address to TrBRF's from the Switch Base Address + 32 (0x20) and upwards. The switch is designed in such a way, that it operates with 63 active or preferred VLAN's, implying that 63 MAC addresses need to be reserved for TrBRF.

Summarizing, each CrossFire 8730 reserve: Switch Base Address + 31 Addresses for Token-Ring ports + 63 MAC Addresses for TrBRFs = 95, which is rounded up to 96 or hexadecimal 0x60.

The MAC address of the default TrBRF (brf-default) will always be the switch base address + 32. If the switch operates in a stack, only one of the switches will operate the bridge relay function. Hence the MAC address of the default TrBRF will be the base address of the stackmaster + 32. The stackmaster is determined by software, when the stack consists of two switches back to back and by the port numbers in 8300/8635 stack configurations.

There is no simple rule to find the MAC address of other TrBRF, but it is always within the range described, as follows:

- Stack Master Base Address + 32 < TrBRF MAC Address < Stack Master Base Address + 95.

  A TrBRF (VLAN) MAC address is assigned, when the VLAN becomes preferred (i.e. it has an assigned port in the actual switch or stack of switches) by selecting the lowest available MAC address above Stack Master Base Address + 32.

If management (SNMP or TELNET) contact with the switch is lost (e.g. because ports are moved from one TrBRF to another) it is suggested, that a terminal is connected to the OBM port of the switch stack, and the IP Configuration menu is entered. From here, it is possible to read the MAC address of the management entity (TrBRF).

Address Format

Display format used for MAC addresses (canonical or non-canonical). Canonical format is typically used in Ethernet networks and is also known as least significant bit first. Non-canonical is typically used in Token-Ring networks and is also known as most significant bit first.

System Name

Any name you choose to assign to the switch (on a TCP/IP network, it could be the IP hostname).

System Location

Physical location of the switch.

System Contact

Person to contact if questions should arise.

DRAM Installed

Amount (in MB) of dynamic memory installed. Information in this field cannot be changed.

Flash Memory Installed

Amount (in KB) of flash memory installed. Information in this field cannot be changed.

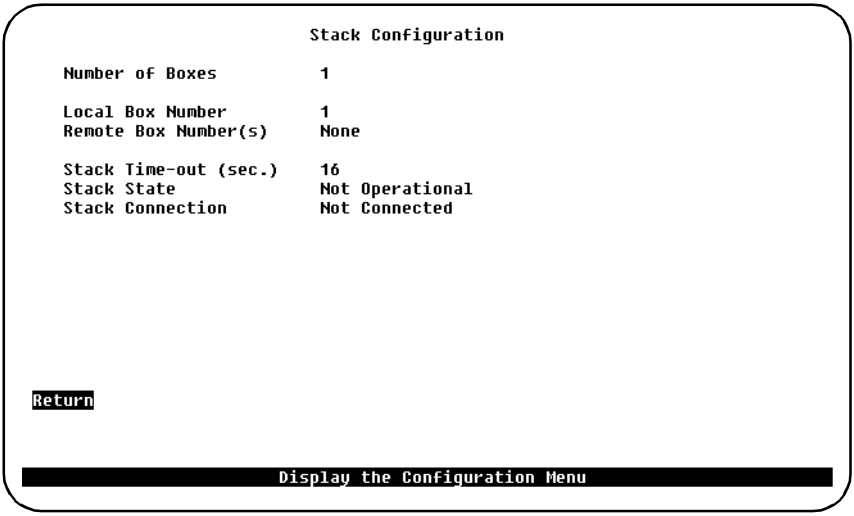
Time of Day

An internal clock is used to calculate total time of operation and time of day. To adjust the time, select this item, press ENTER, then enter the month, day, hour, or minute.

Note: If you cannot set the **Time of Day**, the lithium battery may need replacing. If this is the case, contact your local reseller.

Stack Configuration Screen

To open this screen from the main menu, select **Configuration → Switch Configuration → Stack Configuration**.



The following information is displayed on this screen:

Number of Boxes

Number of switches currently participating in the stack. Information in this field cannot be changed.

Local Box Number

Number assigned to the switch to which the console is connected. The local box is also the source of the information displayed on this screen. Information in this field cannot be changed.

Remote Box Number(s)

Number of switches (in addition to this one) in the stack. Information in this field cannot be changed.

Stack Time-out

If a switch goes off line, the length of time (in seconds) during which the stack tries to reestablish communication with the switch. The default is 16 seconds.

Stack State

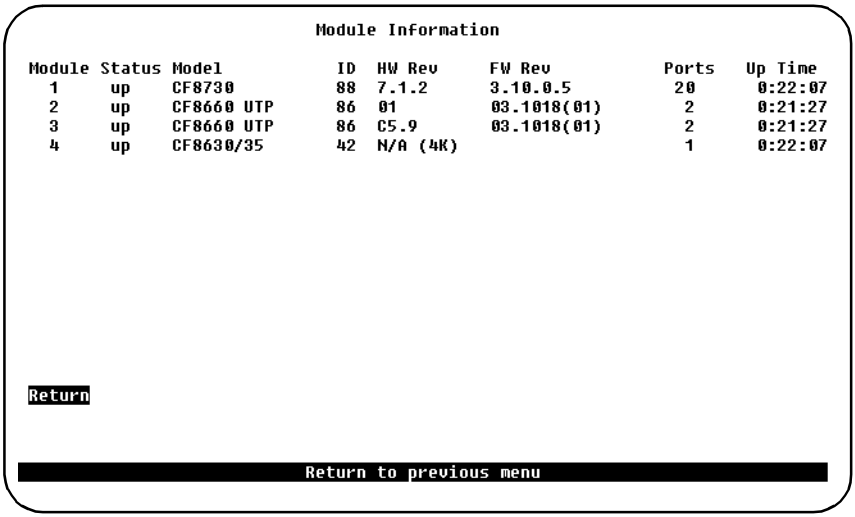
Whether the CrossFire Switch Stacker is operational (CrossFire 8630 or CrossFire 8635). Information in this field cannot be changed.

Stack Connection

Whether the CrossFire 8300 Switch Stacker is connected. Information in this field cannot be changed.

Module Information Screen

To open this screen from the main menu, select **Configuration → Module Information**.



This screen shows information about the different modules that the switch consists of:

Module

Module number. The basic switch is listed as module 1. The Fast Ethernet ports 21 and 22 are listed as module 2 and ports 25 and 26 are listed as module 3. The stack port is listed as module 4.

Status

Whether the module is up, down, or the slot is empty.

Model

Type of module. The CrossFire switch is listed for the base switch. For this module as well as for others, this field displays the product number.

Board ID

Identifier of the board in decimal.

HW Rev

Hardware revision level.

FW Rev

Firmware revision level. On modules with Token-Ring ports, this is the MAC mode revision level.

Ports

Number of ports on the module.

Up Time

Amount of time (in hours, minutes, and seconds) that the module has been up (since the last reset).

You cannot change the information that appears on this screen.

VLAN Configuration

The Virtual LAN feature can be used to partition a switch or a stack of switches into several Virtual LANs, each containing its own set of ports (the terms *Virtual LAN* and *domain* are interchangeable). Packets are forwarded only between ports belonging to the same. The benefit of Virtual LAN is to restrict access from one segment to another, either for security purposes or to reduce intersegment traffic. Figure 15 illustrates a switch with four VLANs.

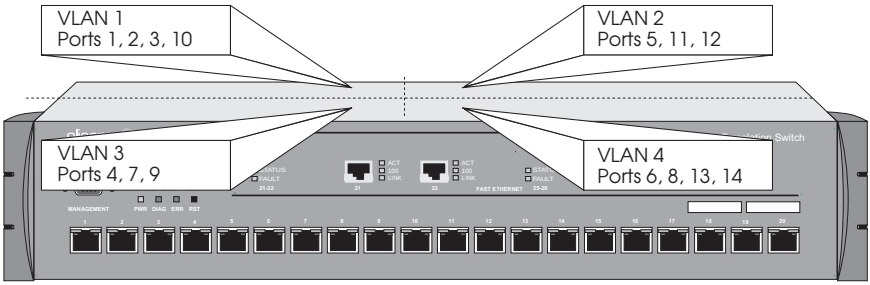


Figure 15. Switch with Four VLANs

To set up domains using the VLAN Configuration menu, specify the ports belonging to the domains, then set up the IP configurations, trap configuration (trap receivers are associated with a set of VLANs and a receiver IP address) and STP configurations specific to the appropriate VLANs. If you have already supplied configuration information using the main configuration menus, that information applies to VLAN “default”. Virtual LANs affects other switch features in the following ways:

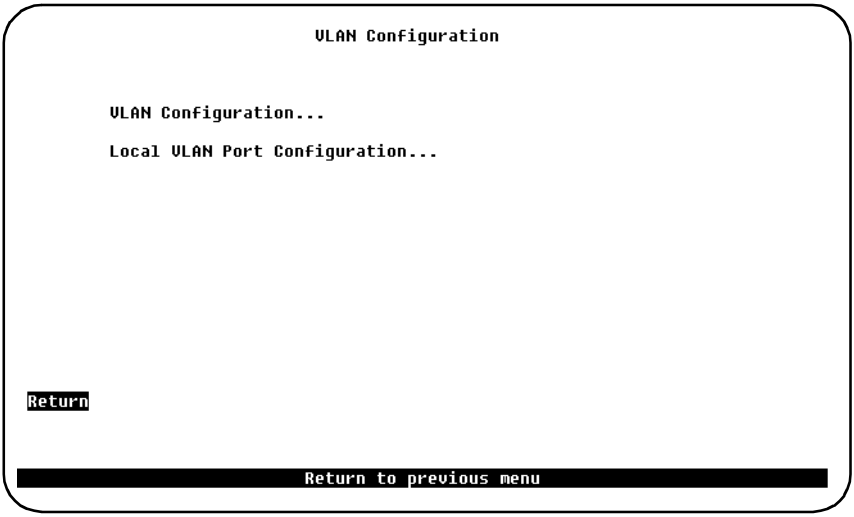
- *Spanning Tree Protocol (STP).* If you are using STP in a certain domain, you must supply STP information for that domain. The STP software treats ports on other domains as nonexistent. Domains do not affect port priorities and port costs. You set these parameters using the STP Configuration menu that you select from the main Configuration menu.
- *SNMP trap tables*. Each domain appears to the network management system as a physically different Token-Ring switch unit. Certain MIB II objects and proprietary objects are domain-sensitive, while others are not. For a list of domain-sensitive objects, see Chapter 4, “Monitoring the Network from the Statistics Menu”.
- *IP.* You may give each domain an IP address, subnet mask, and gateway address definition.

- *Address filters.* Domains have no effect on address filters. For example, suppose you create two domains: one containing ports 1–8 and the other ports 9–16. If you add an address filter to ports 7, 8, 9, and 10, the filter will work properly even though it applies to ports in other domains.
- *CrossLink.* All the Token-Ring ports in a single CrossLink must belong to the same CRF. Therefore, the console software prevents you from defining a CrossLink connection that includes ports in different CRFs. It also prevents you from assigning the Token-Ring ports in an existing CrossLink to different CRFs.

VLAN Configuration Menu

To open this screen from the main menu, select **Configuration → VLAN Configuration.**

See the section “VLAN Support” on page 35 for a discussion of VLANs.

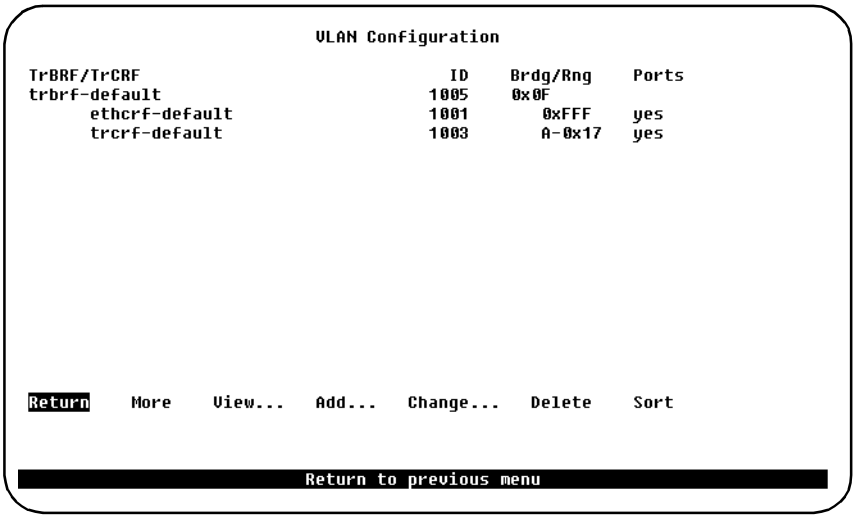


Information on the various submenus follows in the next two subsections.

VLAN Configuration Screen

To open this screen from the main menu, select **Configuration → VLAN Configuration → VLAN Configuration.**

Use the this screen to define and administer BRFs and CRFs in the switch.



TrBRF/TrCRF

ASCII name associated with the BRF or CRF.

ID

Numeric ID.

Brdg/Rng

Bridge/Ring numbers.

Ports

Port numbers.

Return

Returns to the previous menu.

More

Scrolls or refreshes the display.

View...

Zooms in a VLAN.

Add...

Prompts for a new ID and brings up the **VLAN Parameter Configuration** screen.

Change...

Prompts for a numeric ID of a BRF or CRF to change and brings up the **VLAN Parameter Configuration** screen.

Delete

Lets you delete a BRF or CRF. You cannot delete a BRF if there are CRFs assigned to it, or a CRF if there are ports assigned to it.

Sort

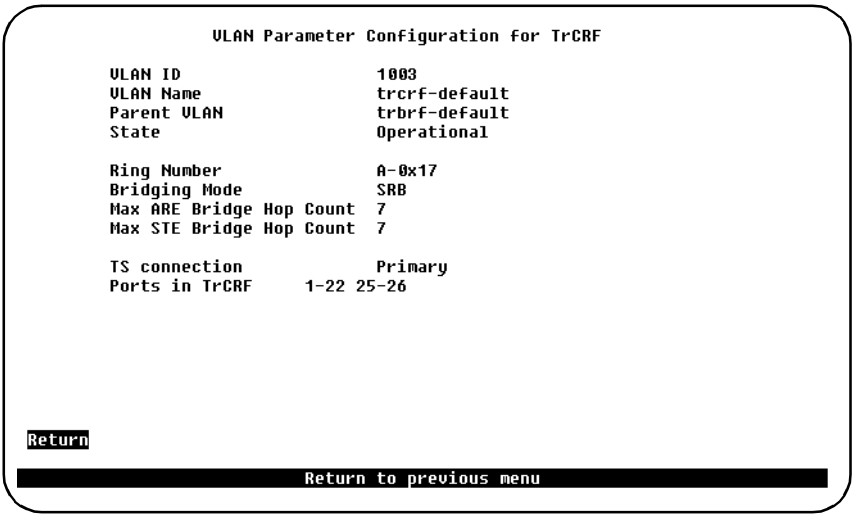
Sorts VLANs by Parent-Child relationship, or by VLAN-ID.

VLAN Parameter Configuration for TrCRF Screen

To open this screen, do the following:

1. From the main menu, select **Configuration → VLAN Configuration → VLAN Configuration.**
2. Select **View...**, **Add...,** or **Change...**
3. When prompted, enter the VLAN ID for the TrCRF.

Use this screen to add or change a CRF. Note that the *trcrf-default* cannot be deleted. Also, the *trcrf-default* cannot be assigned to other BRFs.



The following information is displayed on this screen:

VLAN ID

Numeric ID of the CRF. Possible values are *1* through *1005*. Values *1002* through *1005* and *1* are reserved for the default CRFs and BRFs.

VLAN Name

ASCII name associated with the CRF. Up to 32 characters are allowed.

Parent VLAN

Parent to which the CRF belongs.

State

Current state of the CRF. Possible values are *Operational* and *Suspended.* CRFs in operational state are functional. CRFs in suspended state do not pass packets. The default is operational.

Ring Number

Logical ring number assigned to this CRF. Possible hexadecimal values are *auto* and *OX001* through *OXFFF*. The default is *auto*, meaning that the ring number will be learned. If the ring number has been learned, the learned ring number will be prefixed with *A*.

Note: Forwarding of frames between CRFs in SRB mode is only possible, if the CRFs know their ring numbers. If you are running the switch in an environment without other bridges/switches, learning of ring numbers is not possible. Hence manual configuration of ring numbers is required.

Bridging Mode

Bridging mode for this CRF. Possible values are *SRB* and *SRT*. The default is *SRB*.

Max ARE Bridge Hop Count

Maximum number of hops for all-routes explorer (ARE) frames. Possible values are *1* through *13*. The default is *7*.

Max STE Bridge Hop Count

Maximum number of hops for spanning tree explorer (STE) frames. Possible values are *1* through *13.* The default is *7*.

TS Connection

This parameter displays the connection attribute assigned to the selected CRF of Fast Ethernet ports that are connected to the Ethernet cloud. The connection attribute can be one of the following:

- *Primary* connection - for a main connection to the Ethernet cloud (default value for each CRF). This connection is always forwarding if active.

- *Secondary 1* - for a backup connection to the Ethernet cloud. This connection is always blocking if *Primary* is active.
- *Secondary 2* - for a second backup connection to the Ethernet cloud. This connection is always blocking if *Primary* or *Secondary 1* are active.

Each CRF of Fast Ethernet ports connected to the same Ethernet cloud must have a different connection attribute set.

Ports in TrCRF

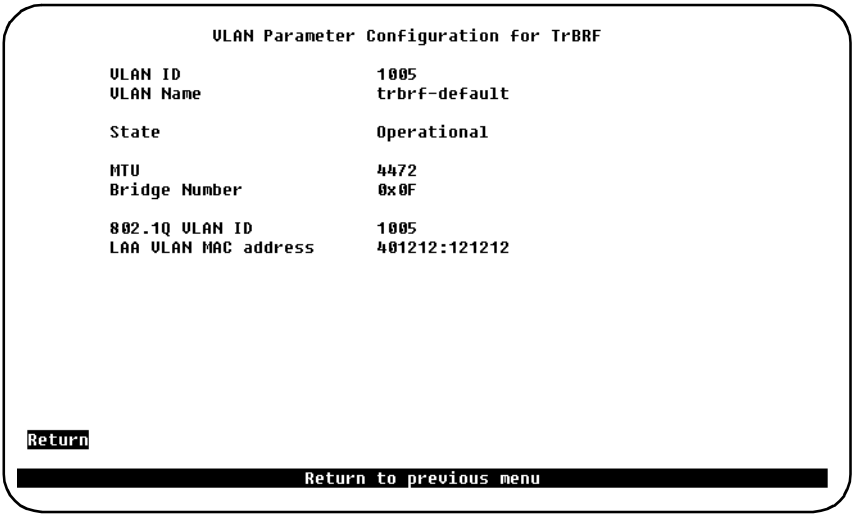
This parameter lists the ports assigned to the CRF.

VLAN Parameter Configuration for TrBRF Screen

To open this screen, do the following:

1. From the main menu, select **Configuration → VLAN Configuration → VLAN Configuration.**
2. Select **View...**, **Add...** or **Change...**
3. When prompted, enter the VLAN ID for the TrBRF.

Use the this screen to add or change a BRF. Note that the *trbrf-default* cannot be deleted. Also, the *trbrf-default* cannot be assigned new BRFs. The BRF screen is shown below.



The following information is displayed on this screen:

VLAN ID

Numeric ID of the BRF. Possible values are *1* through *1005*. Values *1002* through *1005* and *1* are reserved for the default BRFs and CRFs.

VLAN Name

ASCII name associated with the BRF. Up to 32 characters are allowed.

State

Current state of the BRF. Possible values are Operational and Suspended. BRFs in operational state are functional. BRFs in suspended state do not pass packets. The default is operational.

MTU

Maximum Transfer Unit of the BRF (maximum size of the information field in transmitted packets). Possible values are *1,500*, *4,472* (default), *8,144*, and *17,800*. The actual value used depends also on the value configured for the port (the smaller value is used).

These values correspond to maximum frame size values of *1,548*, *4,546* (default), *9,236*, and *18,192* respectively.

The actual value used depends on the value configured for the ports (the smaller value is used).

Bridge Number

Source-routing bridge number for this BRF. Possible hexadecimal values are *0* through *F*. The default is *F*.

802.1Q VLAN ID

The 802.1Q VLAN ID is the value that is inserted in the IEEE 802.1Q frame tags. It is entered as a decimal value between 1 and 4094.

The 802.1Q VLAN ID should not be confused with the existing VLAN ID, which is a number chosen by the user and used by the switch to index CRFs and BRFs. By default, however, the 802.1Q VLAN ID is set to the same value as the VLAN ID.

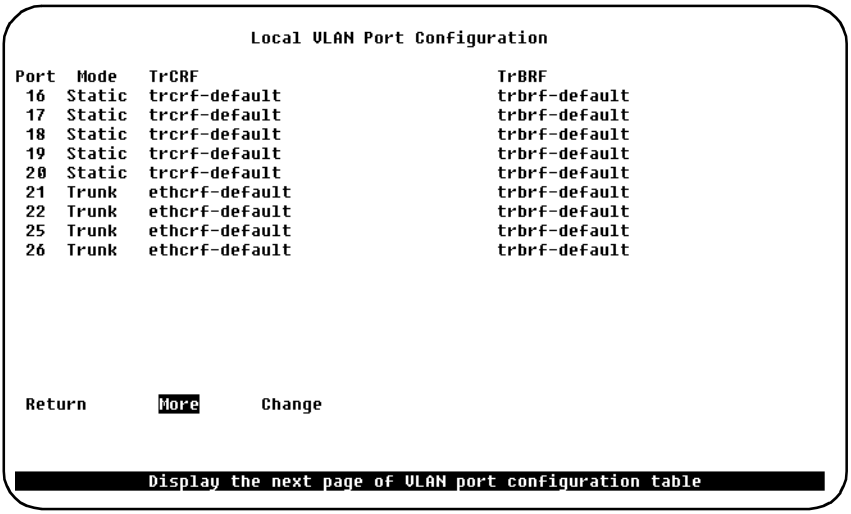
LAA VLAN MAC Address

This parameter makes it possible to assign an Local Administrated Address used for IP communication to the selected VLAN. You will have to reset the switch before the new value takes effect. The selected value is only used for IP (and SNMP over MAC), not for Spanning Tree.

Local VLAN Port Configuration Screen

To open this screen from the main menu, select **Configuration → VLAN Configuration → Local VLAN Port Configuration.**

This screen is used to view and edit current port assignments to CRFs.



Port

The port number.

Mode

VLAN mode of the port. Possible values are *Static* and *Trunk*.

The Fast Ethernet ports will appear as trunk ports in the **Local VLAN Port Configuration**. This means that more than one CRF can be assigned to the Fast Ethernet ports. Note, however, the virtual port restriction described above.

TrCRF

CRF to which the port is currently assigned. By default, all ports are assigned to trcrf-default.

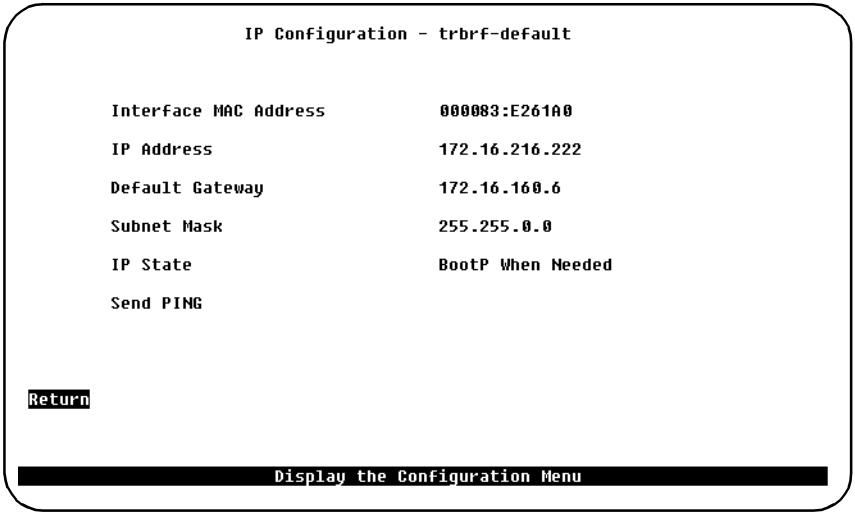
TrBRF

Parent BRF of the CRF to which the port is currently assigned. The default is *trbrf-default*.

IP Configuration Screen

To open this screen from the main menu, select **Configuration → IP Configuration.** Then select the TrBRF to display the screen.

This screen is used to view or change IP information associated with a BRF, such as the IP address, subnet mask, or IP state, or to send PINGs.



Interface MAC Address

Displays the MAC address assigned to this BRF.

IP Address

Displays the current IP address of the selected TrBRF. To change it, highlight the field and press ENTER.

Default: *192.0.2.1*

Default Gateway

Displays the current gateway address. The default is the IP address of the gateway or router through which information must pass to get to the network management application.

Default: *0.0.0.0*

Subnet Mask

Displays the current subnet mask.

Default: *0.0.0.0*

IP State

Display the following choices by highlighting **IP State** and pressing ENTER:

- *IP Disabled*
- *BootP When Needed*
- *BootP Always*

Then highlight one of these choices and press ENTER. The meaning of these values are as described below:

- *IP Disabled*—When a VLAN is IP-disabled, it will not process any IP or ARP packets it receives. This means that no IP-SNMP, Ping, Telnet, or ARP Packets will be responded to when received.

Note: Sending a Ping from an IP-disabled VLAN or a VLAN whose IP address is *0.0.0.0* is not possible.

- *BootP When Needed*—In this state, the switch will send out BootP requests in the VLAN until the IP address becomes different from *0.0.0.0* or *192.0.2.1*.

  BootP When Needed is the factory-set default. A switch for which NVRAM is not initialized (for instance, a new switch out of the box or on a bootup after NVRAM is cleared) or one whose NVRAM is corrupted and unreadable, will always attempt to use BootP the first time.

- *BootP Always*—In this state, IP is enabled for the VLAN but will not function fully on boot until a BootP reply has been received. If a non-zero IP address is stored in NVRAM for a given VLAN in this state when booted, it is cleared to *0.0.0.0* since it would never be used.

Note: For the default TrBRF the value is *BootP when Needed*. For all the other VLANs the default is *IP Disabled*

Send PING

Prompts you to enter an IP address (IP address must be entered and the IP subnet mask must be set). The system then sends a PING to that address. Note that if you have just set the IP address, you must press ENTER and select the menu again before a PING can be sent.

BootP Requests and Parameters

When using BootP to determine its IP address, the switch repeats BootP requests at regular intervals, beginning at one second each and eventually decreasing to every five minutes over time until it receives a valid reply. If the IP display for the VLAN is accessed from the console (or via Telnet from another VLAN) during that time, the switch may cease using BootP if the parameters are set (on display exit) in such a way that BootP would no longer be necessary - for instance, if the IP state is switched from *BootP Always* to *IP-Disabled* or if an IP address different from *0.0.0.0* or *192.0.2.1* is specified in any IP state.

Once the switch has stopped sending BootP requests on a VLAN, it does not restart sending requests on that VLAN and does not recognize BootP responses on that VLAN unless the switch is reset.

Besides the switch's IP address, several other parameters in a BootP response are also recognized and recorded in NVRAM, when received in the same response:

- Default Gateway (see note below)
- Subnet Mask
- TFTP Bootfile Name
- TFTP Server Address (only recognized if the Bootfile name is present)

One other parameter, the TFTP VLAN, is inferred whenever a TFTP Bootfile name is present in the BootP response. That is, if the switch receives a BootP response that specifies a TFTP Bootfile name, the switch automatically records the VLAN on which the response was received as the TFTP VLAN number. Therefore, the bootfile name should not be specified on a VLAN from which the TFTP server cannot be accessed, either directly or through the VLAN’s default gateway (if one exists). More information on TFTP is available under the section "TFTP" on page 127 in this chapter.

Note: The default gateway accepted is the first one in the list of routers whose net/subnet address is the same as that of the IP address specified. If no routers are specified or if none qualify, the gateway address for the VLAN will be zeroed out and recorded as such in NVRAM when the IP screen is exited.

SNMP Configuration Menu

The next menu item in the **Configuration** menu is **SNMP Configuration...**. This item opens a menu that is explained in Chapter 5, “Monitoring the Network with SNMP”.

The next section describes the Spanning Tree Protocol and the STP menus that you can access from the **Configuration** menu.

Spanning Tree Protocol

The spanning tree protocol (STP) is a bridge-to-bridge link management protocol that provides path redundancy while preventing undesirable loops. To provide path redundancy, spanning tree protocol defines a tree that spans all switches and bridges in the extended network. If one of the network segments in the tree becomes inaccessible, STP reconfigures itself to reestablish the links. To prevent loops, STP selects just one switch port as the designated path to the root, assigning it the Forwarding, or active state. It assigns all other ports the blocking, or standby, state. A port in the blocking state does not forward any transmitted frames in any direction.

Note: In the VLAN STP configuration menu, for the selection of port priority/port path cost, select only the ports which are part of the current VLAN. Do not configure ports in other VLANs.

The path cost indicates the relative speed of the segment: The higher the speed of the segment, the lower the path cost. Switches and bridges in the network attempt to determine the path to the route with the lowest path cost. IEEE 802.1D recommends that you assign path costs using the following formula:

Path cost = 1000 / LAN speed in Mbps

If two ports to the root have the same path cost, the STP device selects the one with the highest priority (lowest value), an arbitrary value that you assign. To block traffic on a particular segment, assign it low port priority (high value)

If more ports have the same priority value assigned, the lowest port number will be selected.

IEEE 802.1D Spanning Tree Protocol (STP)

When the IEEE 802.1D Spanning Tree Protocol is active, a port within that domain will require several seconds to make the transition from the blocking state to the forwarding state, when the port is initially activated (e.g. joins an existing ring or activates a dedicated link.) Some client or server applications may attempt to establish session activity during this time, resulting in error messages indicating a connection failure. These applications should be configured to wait at least 30 seconds after the LAN link is active, before attempting to establish session activity. This delay can be reduced by modifying the 802.1D Spanning Tree Protocol default parameters.

If STP is enabled on a dedicated port, and a station is attached to it, it takes at least 30 seconds for the port to transition Down → Listening → Learning → Forwarding.

The IPX client and server stations may have given up before then. And the first many PINGs get lost.

In general, STP should not be enabled on ports, which are intended for dedicated stations. Shared media do not have the same problem, because the port will stay attached to the Hub, even though all stations have closed.

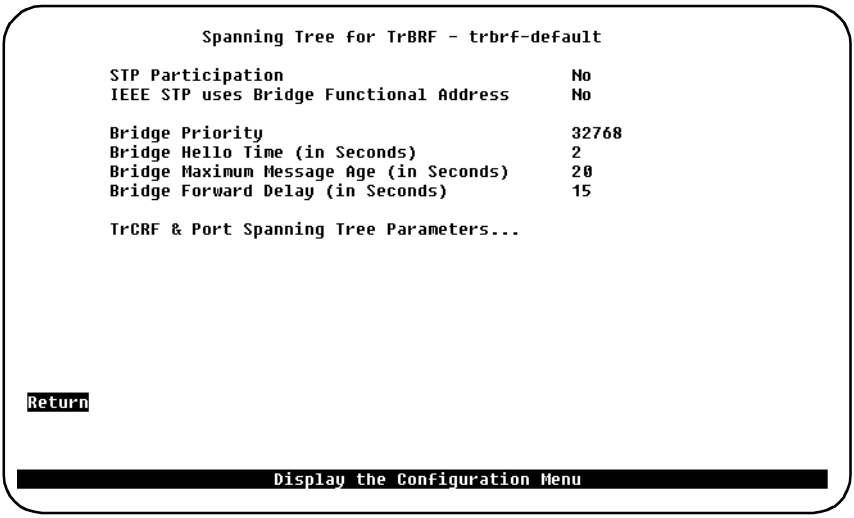
Another reason for not enabling STP on dedicated ports is, that the whole network will go into Topology Change state each time a station opens or closes. This will cause the whole network to use short aging timers, so all address tables will be trashed. The result is a lot of unknown station broadcasts, before the tables converge again.

To disable STP on a port, select the STP Mode *Forwarding* for this port. Refer to the "STP Mode" parameter on page 71.

Spanning Tree for TrBRF Screen

To open this screen from the main menu, do the following:

1. Select **Configuration → Spanning Tree. A** list containing available TrBRF VLANs appears.
2. Choose a TrBRF from the list. The **Spanning Tree for TrBRF** screen will now appear. From this screen you can go on to select TrCRFs and ports associated with the BRF for modification (**TrCRF & Port Spanning Tree Parameters...**).



STP Participation

Whether this TrBRF participates in the spanning tree protocol and, if so, the

protocol to be used. Possible values are *No, IEEE, IBM*, and *Base on Bridging Mode*. The default is *No*.

- If **STP Participation** is set to *No*, then all TrCRFs with this TrBRF as a parent will be set to forwarding mode. You can then override this by blocking a particular TrCRF.
- If **STP Participation** is set to *IEEE* or *IBM*, then the selected protocol will be used to determine the forwarding/blocked mode of the TrCRFs that are configured with an STP mode of *auto*.
- If **STP Participation** is set to *Base on Bridging Mode*, then the spanning tree protocol used is based on the bridging mode of the TrCRF. If the bridging mode is SRB, the IBM Spanning Tree Protocol is used. If the bridging mode is SRT, the IEEE 802.1D Spanning Tree Protocol is used.

For a particular TrCRF the protocols selected here can be overridden. See the **STP Mode** parameter in the section "Spanning Tree for TrCRF Screen" on page 67.

IEEE STP Uses Bridge Functional Address

- *Yes*: Sets IEEE Spanning Tree to use the Bridge Functional Address.
- *No*: Sets IEEE Spanning Tree to use the standard IEEE STP Address.

Bridge Priority

Enter a priority value for this switch. The bridge with the lowest priority value in an STP becomes the root. (To change individual port priorities, enter the **Port Spanning Tree Parameters** screen.)

Range: *0–65535*
Default: *32768*

Bridge Hello Time (in Seconds)

Enter a time between configuration messages when this switch is root. The minimum value may not be less than 1. The maximum may not be more than the lower of 10 or **Switch Maximum Message Age**/2–1. The upper range limit that appears reflects the value currently selected for **Switch Maximum Message Age**.

Default: *2*

Bridge Maximum Message Age (in Seconds)

Enter the maximum message age advertised when this switch is root. The minimum value may not be less than the higher of 6 or (2 x (**Switch Hello Time** + 1)). The maximum may not be more than the lower of 40 or (2 x (**Switch Forward Delay** – 1)). The range limits that appear reflect the values currently selected for **Switch Hello Time** and **Switch Forward Delay**.

Default: *20*

Bridge Forward Delay (in Seconds)

Enter the time the switch waits between transitions from listening to learning, and from learning to forwarding. The minimum may not be less than the larger of *4* or ((**Switch Maximum Message Age** / 2) +1). The maximum may not be higher than 30. The lower range limit that appears reflects the value currently selected for **Switch Maximum Age**.

Default: *15*

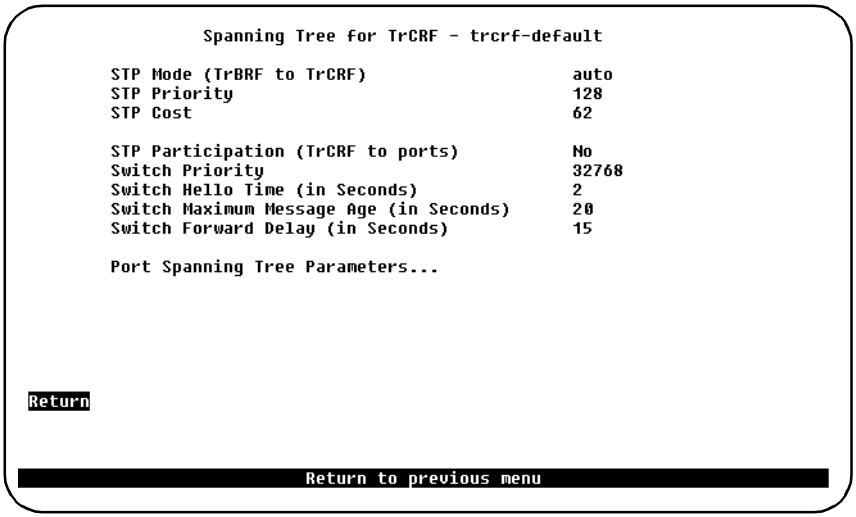
TrCRF & Port Spanning Tree Parameters...

If you select the **TrCRF & Port Spanning Tree Parameters** item, you will be presented with a screen listing the TrCRFs that have the current TrBRF as parent. From this screen, you can select a TrCRF and modify the TrCRF and/or port parameters as desired.

Spanning Tree for TrCRF Screen

To open this screen from the main menu, do the following:

1. Select **Configuration → Spanning Tree.** A list containing available TrBRF VLANs appears.
2. Choose a TrBRF to open the **Spanning Tree for TrBRF** screen and then select the **TrCRF & Port Spanning Tree Parameters...** item.
3. A screenwill appear displaying the TrCRFs that have the currently selected TrBRF as parent. When you select a TrCRF from this list, the **Spanning Tree for TrCRF screen** is displayed.



STP Mode (TrBRF to TrCRF)

Determines the mode of the internal port from this TrCRF to its TrBRF. Possible values are *auto, forwarding, blocked*. If the parent TrBRF is participating in the spanning tree protocol, then *auto* is the default, and the protocol will be determined by the parent TrBRF. If the TrBRF is not participating in the spanning tree protocol, then forwarding is the *default*.

STP Priority

Priority associated with the TrCRF. The TrCRF with the lowest priority value has the highest priority and will forward the spanning tree frames. The default is *128*. The possible range is *0* through *255* (decimal).

STP Cost

Cost associated with the TrCRF. The spanning tree protocol uses path costs to determine which CRF to select as a forwarding CRF. Therefore, lower numbers should be assigned to CRFs that use faster media (such as FDX or CrossLink), and higher numbers should be assigned to CRFs that use slower media. The possible range is *1* to *65,535*. The default is *62*. The recommended path cost is 1000 /LAN speed in Mbps.

STP Participation (TrCRF to ports)

Whether this TrCRF participates in the spanning tree protocol and, if so, the protocol to be used. Possible values are *No*, *IEEE* and *Cisco*. The default is *No*.

The recommended protocol is IEEE, but if the TrCRF contains more than one port and the port(s) are connected to SRT bridges running the IEEE Spanning Tree Protocol (using the IEEE group address), then the Cisco protocol should be used.

- If **STP Participation** is set to *No*, then all ports belonging to this TrCRF will be set to forwarding mode. You can then override this by blocking a particular port.
- If **STP Participation** is set to *IEEE* or *Cisco*, then the selected protocol will be used to determine the *forwarding*/*blocked* mode of the ports that are configured with an STP mode of *auto*.

Switch Priority

Priority value for this switch (*0* through *65,535*). The lower the priority value, the higher the priority. The bridge or switch with the lowest priority value in a spanning tree becomes the root. The default is *32,768*. (To change individual port properties, select **Port Spanning Tree Parameters...**).

Switch Hello Time (in Seconds)

Time the switch waits before sending the next configuration message when this CRF is the root in STP. The default is *2*.

The minimum value is *1*. The maximum value is the lower of 10 or ((**Switch Maximum Message Age** / 2) – 1).

The valid range for this parameter is displayed when you select **Switch Hello Time**.

Switch Maximum Message Age (in Seconds)

Maximum message age used when this CRF is the root in STP. This parameter sets the time at which the configuration message used by the spanning tree algorithm should be discarded. The default is *20*. The minimum value is the higher of 6 or ((**Switch Hello Time** x 2) + 1).

The maximum cannot be more than the lower of 40 or ((**Switch Forward Delay** x 2) – 1).

The range limits that appear when you select this parameter are calculated using the values currently selected for **Switch Hello Time** and **Switch Forward Delay**.

Switch Forward Delay (in Seconds)

The time the switch waits between transitions from listening to learning and from learning to forwarding. The default is *15*. The minimum is the larger of 4 or ((**Switch Maximum Message Age** / 2) + 1). The maximum is *30*.

The lower range limit that appears when you select this parameter reflects the value currently selected for **Switch Maximum Age**.

Port Spanning Tree Parameters...

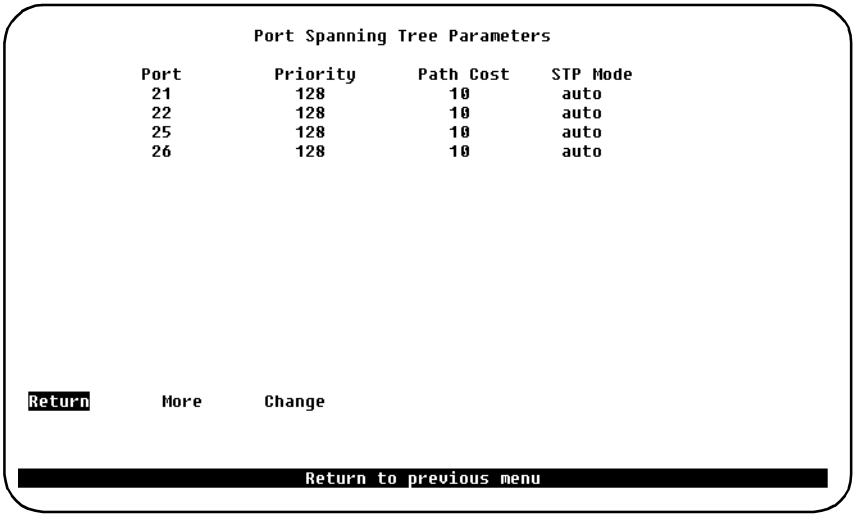
Selecting this item brings up the **Port Spanning Tree Parameters** screen.

Port Spanning Tree Parameters Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Spanning Tree.** A list containing available TrBRF VLANs appears.
2. Choose a TrBRF to open the **Spanning Tree for TrBRF** screen and then select the **TrCRF & Port Spanning Tree Parameters...** item.
3. A screen will appear displaying the TrCRFs that have the currently selected TrBRF as parent. When you select a TrCRF from this list, the **Spanning Tree for TrCRF screen** is displayed.
4. On the **Spanning Tree for TrCRF** screen, select **Port Spanning Tree Parameters...**

Use the **Port Spanning Tree Parameters** screen to set up STP priorities for each port.



Port

The number of the port.

Priority

Priority associated with the port. The port with the lowest priority value has the highest priority and will forward the spanning tree frames. The default is *128*. The possible range is *0* through *255* (decimal). If all ports have the same priority value, the lowest port number forwards the spanning tree frames.

Path Cost

Cost associated with the port. The spanning tree protocol uses port path costs to determine which port to select as a forwarding port. Therefore, lower numbers should be assigned to ports attached to faster media (such as FDX or CrossLink), and higher numbers should be assigned to ports attached to slower media. The possible range is *1* to *65,535*. The default is *62*. The recommended path cost is 1000 / LAN speed in Mbps.

STP Mode

The port's spanning tree mode. Possible values are *forwarding*, *blocked*, and *auto*. If the TrCRF to which the port belongs is participating in the spanning tree protocol, then *auto* is the default and the selected protocol will be used to determine whether the port is forwarding or blocked. If the TrCRF to which the port belongs is not participating in the spanning tree protocol, then *forwarding* is the default.

More

To view more ports in the table.

Change

To change or add values to specific ports.

Current Spanning Tree Information Screen

A summary of STP information for each port is available from the **Current Spanning Tree Information** screen. See page 173 in Chapter 4, "Monitoring the Network from the Statistics Menu" for more information.

Port Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.

Token-Ring Port Configuration

The Token-Ring ports are between 1 and 20. For these ports you will see the following screen:

```
                    Port 9 Port Configuration

Name                                  Enabled                  Yes
TrBRF trbrf-default                   Status                   Not Inserted
TrCRF trcrf-default                   Media Type               RJ-45

Cfg Loss Threshold          8         Forwarding Mode          A-store-fwd
Cfg Loss Sampling Interval  1         Error High Threshold     10
Priority Threshold          3         Error Low Threshold      1
Min Transmit Priority       4         Error Sampling Interval  10

Ring Parameter Server       Disabled  Duplex Mode              auto
Early Token Release         Yes       Operation Mode           auto
Force AC Bits on SR Frames  No        Media Speed              auto

BRF MTU                     4472      Max Explorer Rate        disabled
Port MTU                    Use BRF   Max Broadcast Rate       disabled


Return

                    Return to previous menu
```

Note: When *auto* is selected for fields that support the auto option, the current operational field value shown will be prefixed with *A-*.

Name

This field is for assigning a name to the Token-Ring port.

TrBRF

This field is for informational purposes only, and shows the parent TrBRF of the TrCRF that the port is assigned to.

TrCRF

This field is for informational purposes only, and shows the TrCRF that the port is assigned to.

Enabled

For the Token-Ring ports 1-20 this variable shows if the port is currently enabled via managing. Possible values are *Yes* (enabled) or *No* (disabled). The default value is *Yes*.

Status

This field is for informational purposes only, and shows if the port is currently inserted into the ring.

Address Demand Aging Level

Sets the threshold on the number of entries in the address table on which entries are aged faster. Possible values are *50, 60, 70, 80* and *90* percent and *Disabled*.

Default: *90 percent.*

Trace Mask

Sets a bit mask for which messages are logged in the message log. This is mainly for debugging purposes by Olicom support.

Media Type

This field is for informational purposes only, and shows the media type of the port. The value will always be *RJ-45*, since this is the type of all the ports on CrossFire 8730.

Media Speed

The Token-Ring media speed. Possibilities are *4* or *16 Mbps* or *Auto*. When a switch port configured with *Auto* discovers a connection to shared media, it will open and insert into the ring. If the open returns with an indication, that the port is the first station to enter the ring, it will close.

This algorithm is analogue to that of auto-sensing adapters, which dictates that an adapter, which is capable of speed adjustment, must have some other station on the ring (typically a server), from which it can sense the network speed.

If you want to have switch ports, which are attached to shared media, it is recommended that you change the default media speed configuration from *Auto* to either *16* or *4 Mbps.*

Max Explorer Rate on Input

The maximum Explorer frame forwarding rate per second. Possible values are *Disabled* (default) or *0 -5000.*

MTU

The **Maximum Transfer Unit** is the size of the information field of packets to be sent or received. Possible values are *1,500* and *4,472* (default), *8,144*, and *17,800*.

The actual value used depends also on the value configured for the TrBRF (the smaller value is used).

These values correspond to maximum frame size values of *1,548*, *4,546* (default), *9,236*, and *18,192* respectively.

Note: See the description on frame length limit in the *CrossFire 8730 Fast Ethernet Translation Switch Installation Guide*.

Force AC Bits on SR Frames

This field specifies if AC bits will be set unconditionally when a port forwards certain LLC frames. Possible values are *Yes* and *No* (default).

Early Token Release

Whether the port is enabled for Early Token Release (ETR). Possible values are *Yes* and *No*. The default is *Yes*. If **Early Token Release** is set to *Yes* and the media speed is 4 Mbps, the switch will force **Early Token Release** to *No*.

Operation Mode

The Token-Ring port operation mode. Possible values are as follows:

- *Auto* (default. Only HDX and FDX modes can be automatically detected.)
- *HDX port*
- *HDX station*
- *FDX port*
- *FDX station*
- *RI/RO*
  Only on ports 19 and 20.
- *Passive*
  (this value is not user-selectable, and will be displayed if the port has been selected as a passive monitoring port on the **Switched Port Analyzer** screen).

Forwarding Mode

Forwarding mode that will be used to transmit frames. Possible values are *auto*, *cut-through*, and *store & forward*. The default is *auto*. If the forwarding mode is set to *auto*, the actual mode will depend on the number of errors that occur during the sampling interval. If the error rate is below the error low threshold, then *cut-through* mode is used. If the error rate is above the error high threshold, then *store & forward* is used. The *store & forward* mode is always used for Token-Ring ports with a media speed of 4 Mbps and for teh Fast Ethernet ports.

Priority Threshold

The highest Token-Ring frame priority that will go to the low priority transmit queue. Possible values are *0–7*. The default value is *3*).

Min Transmit Priority

The minimum Token-Ring frame priority that will be used for transmits. Possible values are *0–6*. The default value is *4*.

Error High Threshold

This field is only valid when **Forwarding Mode** is set to *auto*, and is used to force a port to *store & forward* mode when the percentage of errors detected in the Sampling Interval is more than the error high threshold. Possible values are *0–100* percent. The default value is *10* percent.

Error Low Threshold

This field is only valid when **Forwarding Mode** is set to *auto*, and is used to return a port to *cut-through* mode when the percentage of errors detected in the Sampling Interval is less than the error low threshold. Possible values are *0–100* percent. The default value is *1* percent.

Error Sampling Interval

This field is only valid when **Forwarding Mode** is set to *auto*, and specifies a sampling period in minutes. The sampling period is used when counting errors to determine a ports forwarding mode. Possible values are *1–60* minutes. The default value is *10*.

Cfg Loss Threshold

Configuration loss occurs when a port completes a connection, allows data traffic to flow, and subsequently closes. This threshold is used to control the number of configuration losses that can occur within the **Cfg Loss Sampling Interval**. When the threshold is exceeded, the port is disabled and must be enabled via this screen or an SNMP manager. Possible values are *1–100*. The default value is *8*.

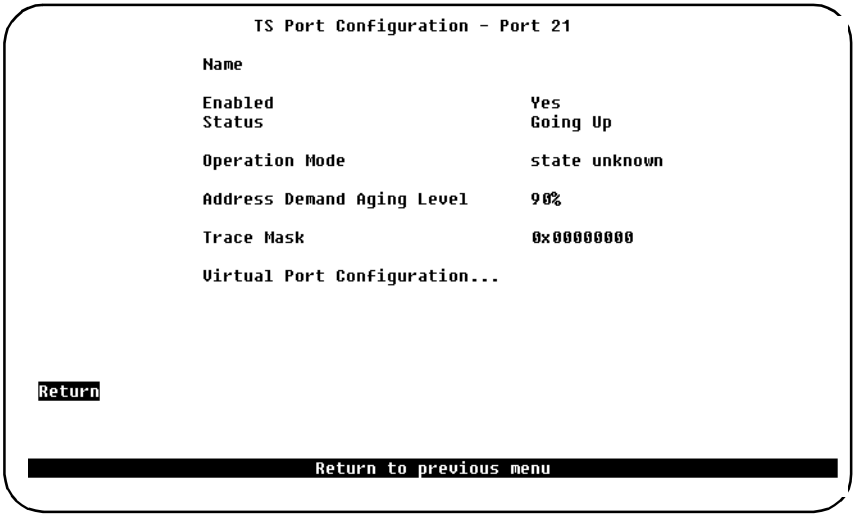
Cfg Loss Sampling Interval

Specifies a sampling period in minutes. The number of configuration losses occurring within this interval is compare to the **Cfg Loss Threshold** to determine if a port should be disabled. Possible values are *1–60* minutes. The default value is *10*.

Note: If you change any configuration parameters of a connected port, the port will close and reopen and you will lose all address information and statistics for that port.

Fast Ethernet Port Configuration

The Fast Ethernet ports are 21, 22, 25, and 26. For these ports you will see the following screen, **TS Port Configuration**:



Name

This field is for assigning a name to the port.

Enabled

For the Fast Ethernet ports 21, 22, 25, and 26, this variable sets the administrative state of the port, possible values are *Yes* and *No*. When the port is disabled, the LINK LED will blink.

Default: *Yes*.

Status

This field is for informational purposes only, and shows if the port is currently inserted into the ring. The value displayed can be one of the following:

- *Down* The port is down.
- *Going Up* The port is enabled and the auto-negotiation is trying to establish a protocol connection.
- *Up* The port is up.

Operation Mode

This parameter displays the mode of the Fast Ethernet port. The value can be one of the following:

- *Auto FDX 10* The port is running in full duplex 10Mbps
- *Auto FDX 100* The port is running in full duplex 100Mbps
- *Auto HDX 10* The port is running in half duplex 10Mbps
- *Auto HDX 100* The port is running in half duplex 100Mbps
- *state-unknown* The port is disabled or the link is off

Address Demand Aging Level

Sets the threshold on the number of entries in the address table on which entries are aged faster. Possible values are *50, 60, 70, 80* and *90* percent and *Disabled*.

Default: *90 percent.*

Trace Mask

Sets a bit mask for which messages are logged in the message log. This is mainly for debugging purposes by Olicom support.

Virtual Port Configuration

Opens the **Virtual Port Configuration** screen, see page 78.

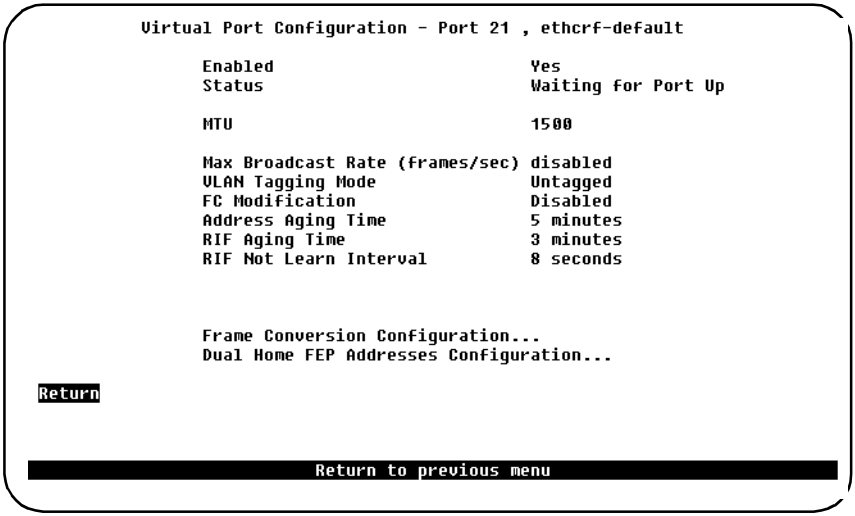
Virtual Port Configuration

This section describes virtual port configuration for the Fast Ethernet ports.

Virtual Port Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Select a Fast Ethernet port, that is, 21, 22, 25, or 26. If the Fast Ethernet port has more than one virtual port, a list of the corresponding CRFs appears, from which the virtual port must be selected. The **Port Configuration** screen appears.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...



The following menu options are available:

Enabled

Sets the administrative state of the virtual port, possible values are *Yes* and *No.* Default: *Yes.*

Status

Display only. Shows the current status of the virtual port.

- *Admin down* The port or virtual port is disabled.

- *Waiting for port up* The virtual port is waiting for the port to come up.
- *Up* The virtual port is up but not forwarding.
- *Forwarding* The virtual port is up and forwarding.
- *Temporary down* The virtual port is currently down because the port is temporarily down.

MTU

You can only use the value *1500* as MTU.

MTU configured:	*1500*
Actual Fast Ethernet frame size:	*1558*
LF bits:	*001*

Max Broadcast Rate (frames/sec)

Sets the maximum broadcast frame rate; possible values are *0* to *5000* frames/sec or *Disabled*. If enabled, this will limit the amount of broadcast frames being forwarded from the Fast Ethernet side of the virtual port to the switch.

Default: *Disabled*

VLAN Tagging Mode

Sets the VLAN tagging mode of the virtual port; possible values are *Tagged* and *Untagged*. As explained previously at most one virtual port on each Fast Ethernet port can be untagged. All other virtual ports must be tagged and the 802.1Q VLAN ID must be the same in both ends.

Preferably, the VLAN which is expected to have the largest amount of traffic should be untagged, since VLAN tagging does impose a small overhead.

Default: *Untagged* for the first virtual port and *Tagged* for the subsequent ports.

FC Modification

Enabled FC modification preserves frame priority during translation between Ethernet and Token-Ring (both directions). Possible values are Enabled and Disabled. As discussed earlier a VLAN frame tag also contains a 3-bit priority field. If FC modification is enabled, the Token-Ring frame priority in the FC byte is set to the frame tag priority. If FC modification is disabled, the FC priority is set to 0, and the frame tag priority is discarded.

When a Fast Ethernet port inserts a frame tag in a frame, and FC modification is enabled the Fast Ethernet port uses the FC priority from Token-Ring frame. Otherwise the frame tag priority is set to 0 and the FC priority is discarded.

Default: *Disabled*

Address Aging Time

Sets the aging time for addresses learned on an Fast Ethernet port. Possible value are *1* to *9999* minutes or *0* to *disable aging*. When there has been no activity on an address using the RIF entry for the specified period of time it is deleted from the RIF tables.

Default: *5 minutes*

RIF Aging Time

Sets the aging time for RIF entries learned on a Fast Ethernet port. Possible values are *1* to *9999* minutes or *0* to *disable aging*. When no frames with the RIF have been received for the specified period of time the RIF entry is deleted from the RIF table and the status is changed to *RIF unknown*.

This is also true for addresses learnt from transparent frames. Such addresses have the *no RIF* status set. In such case the status is aged to “RIF unknown” status.

Default: *3 minutes*

RIF Not Learn Interval

Sets the learning blocked interval for RIF entries. Possible value are 0 to 900 seconds. A new RIF cannot be learned unless a specified period of time has passed since the current RIF entry was learned.

Default: *8 seconds*

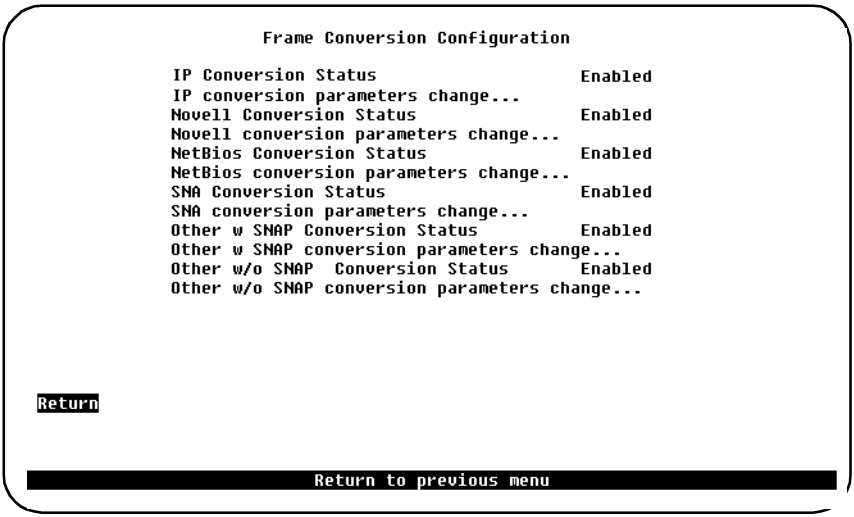
Frame Conversion Configuration

This section describes how to configure frame conversion on a Fast Ethernet port.

Frame Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...**. The **Frame Conversion Configuration** screen appears.



IP Conversion Status

Information only. Shows the current status of the IP Conversion.
Possible values are *Enabled* and *Disabled*.

IP Conversion Parameters Change...

This item opens a screen on which you can change IP conversion parameters. See page 83 for information.

Novell Conversion Status

Information only. Shows the current status of the Novell Conversion. Possible values are *Enabled* and *Disabled*.

Novell Conversion Parameters Change

This item opens a screen on which you can change Novell conversion parameters. See page 85.

NetBios Conversion Status

Information only. Shows the current status of the NetBios Conversion. Possible values are *Enabled* and *Disabled*.

NetBios Conversion Parameters Change

This item opens a screen on which you can change NetBios conversion parameters. See page 87.

SNA Conversion Status

Display only. Shows the current status of the SNA Conversion. Possible values are *Enabled* and *Disabled*.

SNA Conversion Parameters Change

This item opens a screen on which you can change SNA conversion parameters. See page 89.

Other Frames w/SNAP Conversion Status

Display only. Shows the current status of the Other Frames With SNAP Conversion. Possible values are *Enabled* and *Disabled*.

Other Frames w/SNAP Conversion Parameters Change

This item opens a screen on which you can change **Other Frames w/SNAP Conversion** parameters.

Other Frames w/o SNAP Conversion Status

Display only. Shows the current status of the Other Frames Without SNAP Conversion. Possible values are *Enabled* and *Disabled*.

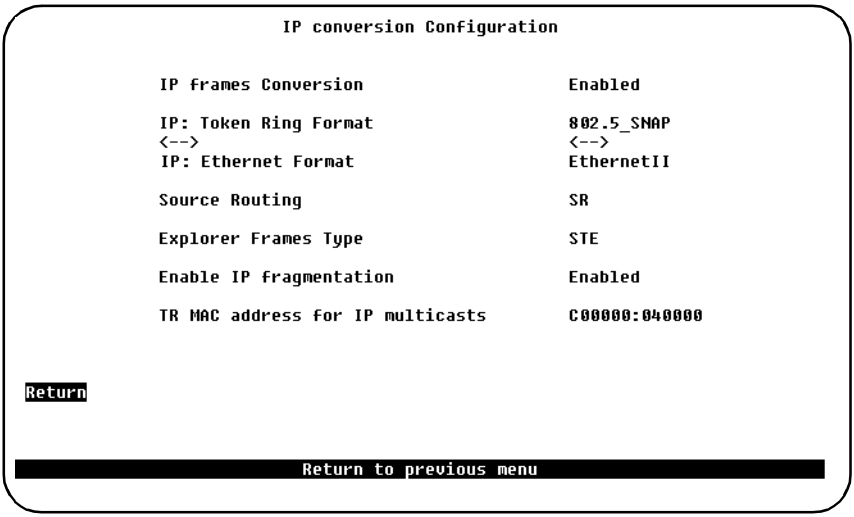
Other Frames w/o SNAP Conversion Parameters Change

This item open a screen on which you can change **Other Frames w/o SNAP Conversion** parameters.

IP Frames Conversion Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...** The **Frame Conversion Configuration** screen appears. Select **IP Conversion Parameters Change**...



IP Frames Conversion

Sets the state of the IP frames Conversion. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled,* IP traffic will be dropped.

Default: *Enabled*.

IP: Token-Ring Format

Sets the format of IP frames on Token-Ring. Available formats:

- *802.5 SNAP* Frame in the IEEE 802.5 format with SNAP

IP: Ethernet Format

Sets the format of IP frames on Ethernet. Available formats:

- *802.3 SNAP* Frame in the IEEE 802.3 format with SNAP
- *Ethernet II* Frame in Ethernet II format

Default: *Ethernet II.*

Source Routing

Enables or disables Source Routing in IP frames transmitted to Token-Ring. The possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *SR.*

Explorer Frames Type

Sets the types of explorer that should be used for IP traffic. Possible values:

ARE The All Routes Explorer should be used.

STE The Spanning Tree Explorer should be used.

Default: *STE.* (change to ARE for typical Token-Ring behaviour for ARP frames)

Enable IP Fragmentation

Enables or disables fragmentation of IP frames received from Token-Ring and transmitted to Ethernet. The possible values are *Enabled* and *Disabled*.

Default: *Enabled.*

TR MAC Address for IP Multicasts

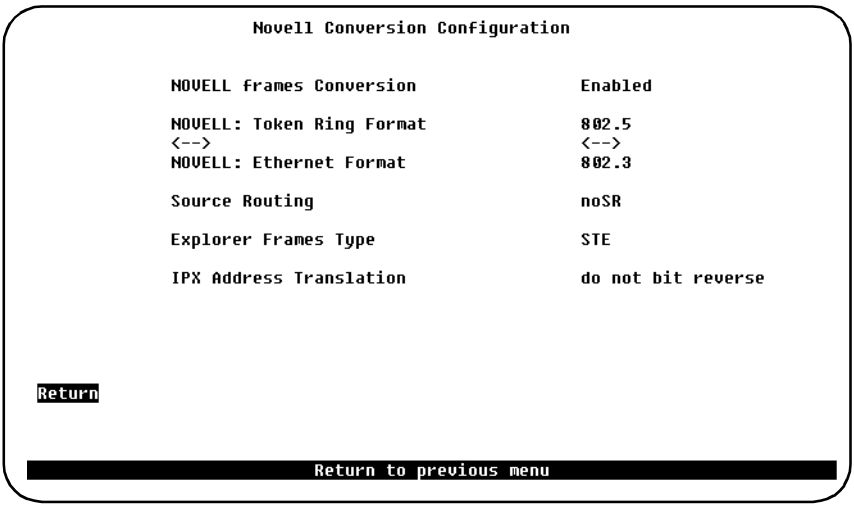
Allows entering the IP multicast address. The address is entered in the MAC address format.

Default: *C00000:040000.*

Novell Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...**. The **Frame Conversion Configuration** screen appears. Select **Novell Conversion Parameters Change**...



NOVELL Frames Conversion

Determines how Novell frames are converted. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled* Novell traffic will be dropped.

Default: *Enabled*

NOVELL: Token-Ring Format

Sets the format of Novell frames on Token-Ring. Available formats:

- *802.5 SNAP* Frame in the IEEE 802.5 format with SNAP
  Novell naming convention: Token-Ring SNAP
- *802.5* Frame in the IEEE 802.5 format without SNAP
  Novell naming convention: Token-Ring

Default: *802.5*

NOVELL: Ethernet Format

Sets the format of Novell frames on Ethernet. Available formats:

- *802.3* Frame in the IEEE 802.2 format
  Novell naming convention: 802.2
- *Novell 802.3* Frame in the IEEE 802.3 format
  Novell naming convention: Normal 802.3
- *802.3 SNAP* Frame in the IEEE 802.3 format with SNAP
  Novell naming convention: Ethernet SNAP
- *Ethernet II* Frame in Ethernet II format
  Novell naming convention: Ethernet II

Default: *802.3*

Source Routing

Enables or disables Source Routing in Novell frames transmitted to Token-Ring.
Possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *noSR*

Explorer Frames Type

Sets the type of explorer that should be used for IPX traffic.
Possible values:

- *ARE* The All Routes Explorer should be used.
- *STE* Spanning Tree Explorer should be used.

Default: *STE*

IPX Address Translation

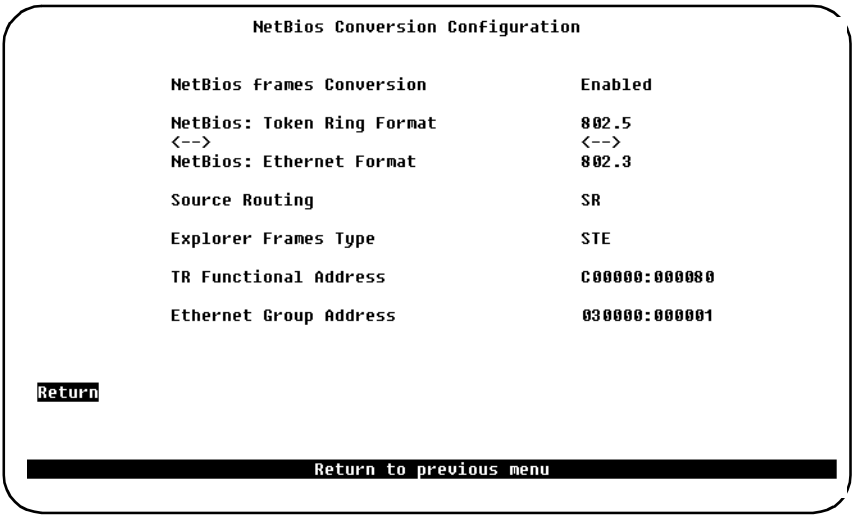
Enables and disables reversing MAC address bits in Novell frames.
The possible values are *do not bit reverse* and *bit reversed*.

Default: *do not bit reverse*

NetBios Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...** The **Frame Conversion Configuration** screen appears. Select **NetBios Conversion Parameters Change...**



NetBios Frames Conversion

Determines how NetBios frames are converted. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled*, NetBios traffic will be dropped.

Default: *Enabled*

NetBios: Token-Ring Format

Sets the format of NetBios frames on Token-Ring. Available formats:

- *802.5* Frame in the IEEE 802.5 format

NetBios: Ethernet Format

Sets the format of NetBios frames on Ethernet. Available formats:

- *802.3* Frame in the IEEE 802.3 format.
- *Ethernet II* Frame in Ethernet II format

Default: *802.3*

Source Routing

Enables or disables Source Routing in NetBios frames transmitted to Token-Ring. Possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *SR*

Explorer Frames Type

Sets the type of explorer that should be used for NetBios traffic. Possible values:

- *ARE* The All Routes Explorer should be used.
- *STE* Spanning Tree Explorer should be used.

Default: *STE*

TR Functional Address

Allows entering the TR Functional Address. The address is entered in the MAC address format.

Default: *C00000:000080*

Ethernet Group Address

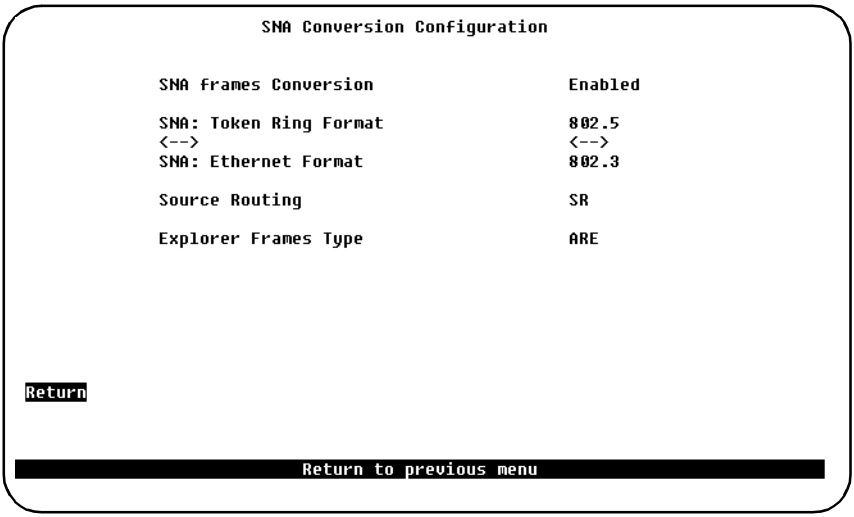
Allows entering the Ethernet Group Address. The address is entered in the MAC address format.

Default: *030000:000001*

SNA Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...**. The **Frame Conversion Configuration** screen appears. Select **SNA Conversion Parameters Change**...



SNA Frames Conversion

Sets the state of the SNA frames Conversion. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled*, SNA traffic will be dropped.

Default: *Enabled*.

SNA: Token-Ring Format

Sets the format of SNA frames on Token-Ring. Available formats:

- *802.5* Frame in the IEEE 802.5 format.

SNA: Ethernet Format

Sets the format of SNA frames on Ethernet. Available formats:

- *802.3* Frame in the IEEE 802.3 format.
- *Ethernet II* Frame in Ethernet II format

Default: *802.3*

Source Routing

Enables or disables Source Routing in SNA frames transmitted to Token-Ring. Possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *SR*.

Explorer Frames Type

Sets the type of explorer that should be used for SNA traffic. Possible values:

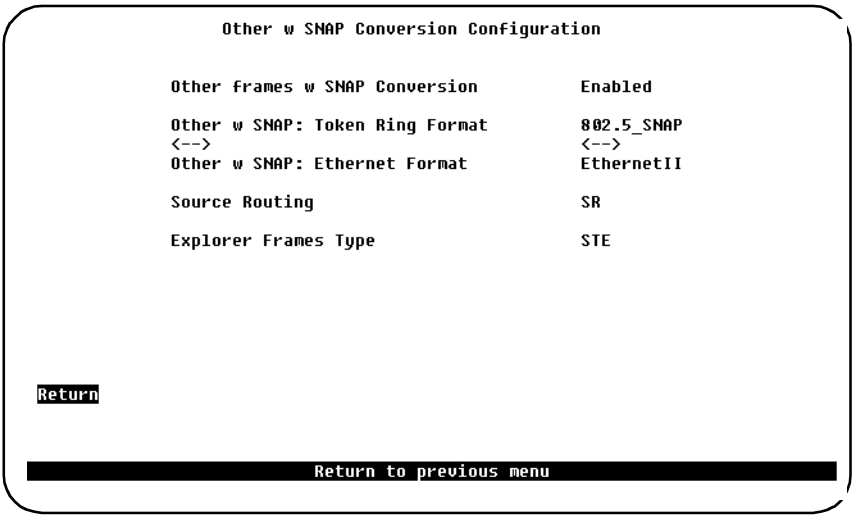
- *ARE* The All Routes Explorer should be used.
- *STE* Spanning Tree Explorer should be used.

Default: *ARE*.

Other w SNAP Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...**. The **Frame Conversion Configuration** screen appears. Select **Other Frames w/SNAP Conversion Parameters Change**...



Other Frames w/SNAP Frames Conversion

Sets the state of the Other Frames w/SNAP frames Conversion. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled*, Other Frames w/SNAP traffic will be dropped.

Default: *Enabled*.

Other Frames w/SNAP: Token-Ring Format

Sets the format of Other Frames w/SNAP frames on Token-Ring.
Formats available:

- *802.5 SNAP* Frame in the IEEE 802.5 format with SNAP

Other Frames w/SNAP: Ethernet Format

Sets the format of Other Frames w/SNAP frames on Ethernet.
Formats available:

- *802.3 SNAP* Frame in the IEEE 802.3 format with SNAP
- *Ethernet II* Frame in Ethernet II format

Default: *Ethernet II*

Source Routing

Enables or disables Source Routing in Other Frames w/SNAP frames transmitted to Token-Ring. Possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *SR*

Explorer Frames Type

Sets the type of explorer that should be used for Other Frames w/SNAP traffic.
Possible values:

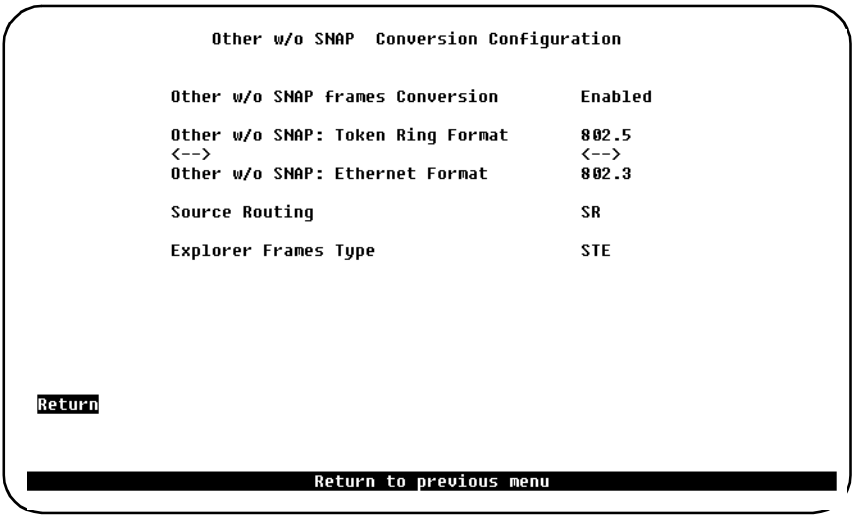
- *ARE* The All Routes Explorer should be used.
- *STE* Spanning Tree Explorer should be used.

Default: *STE*

Other w/o SNAP Conversion Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. Token-Ring ports are 1-20, Fast Ethernet ports are 21, 22, 25, or 26. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Frame Conversion Configuration...**. The **Frame Conversion Configuration** screen appears. Select **Other Frames w/o SNAP Conversion Parameters Change**...



Other Frames w/o SNAP Frames Conversion

Sets the state of the Other Frames w/o SNAP frames Conversion. Possible values are *Enabled* and *Disabled*. If the state is set to *Disabled*, Other Frames w/o SNAP traffic will be dropped.

Default: *Enabled*.

Other Frames w/o SNAP: Token-Ring Format

Sets the format of Other Frames w/o SNAP frames on Token-Ring. Formats available

- *802.5* Frame in the IEEE 802.5 format.

Other Frames w/o SNAP: Ethernet Format

Sets the format of Other Frames w/o SNAP frames on Ethernet.
Formats available:

- *802.3* Frame in the IEEE 802.3 format.

Source Routing

Enables or disables Source Routing in Other Frames w/o SNAP frames transmitted to Token-Ring. Possible values:

- *SR* Source Routing information will be added to frames converted from Ethernet to Token-Ring format.
- *noSR* Frame will be transmitted to Token-Ring as a transparent frame.

Default: *SR*.

Explorer Frames Type

Sets the type of explorer that should be used for Other Frames w/o Snap traffic. Possible values:

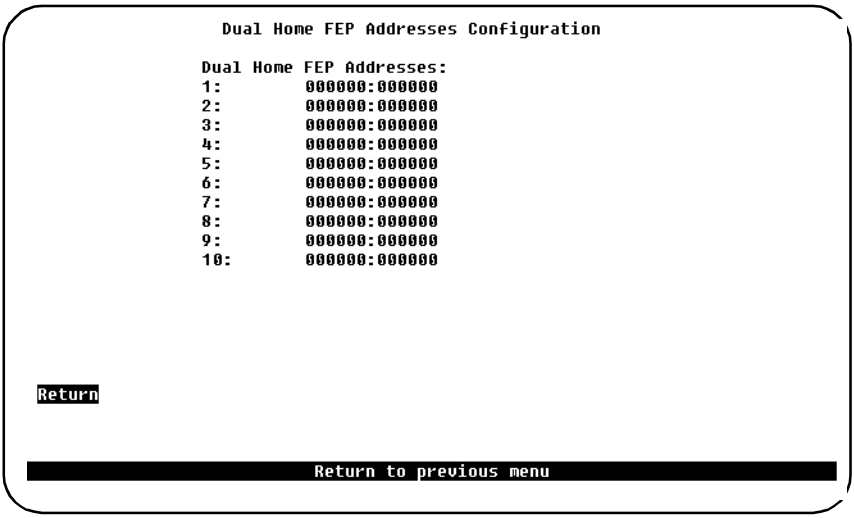
- ARE The All Routes Explorer should be used.
- STE Spanning Tree Explorer should be used.

Default: *STE*

Dual Home FEP Addresses Configuration Screen

To open this screen do the following:

1. Starting from the main menu, select **Configuration → Port Configuration.**
2. You will be prompted for a port number. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.
3. On the **Port Configuration** screen, select **Virtual Port Configuration**...
4. On the **Virtual Port Configuration** screen, select **Dual Home FEP Addresses Configuration.**



The CrossFire 8730 supports “dual home FEP”, which allows duplicate MAC addresses in a source-route bridging Token-Ring network. This is often used by IBM mainframes connected to a Token-Ring network, and is therefore important to the migrating customer who uses such a solution.

For each Virtual Port on each Fast Ethernet port, 10 addresses can be configured as Dual Home FEP addresses. A constant list of 10 MAC addresses numbered 1-10 is shown when this menu is opened. Addresses which consist entirely of zeros represent empty entries.

To add or change an address, highlight the address, press ENTER, and then either enter the new MAC address or simply press ENTER once more to enter a NULL address (empty entry).

Switched Port Analyzer Menu

The S**witched Port Analyzer** screen is accessed from the **Configuration** menu. This screen and its submenus are presented in Chapter 6, “Monitoring Port Traffic”.

CrossLink

A CrossLink Token-Ring connection is used to improve interswitch bandwidth. A CrossLink is used to connect two switches with two to eight Token-Ring links. A CrossLink provides bandwidth of from 32 to 128 Mbps in half-duplex mode, or from 64 to 256 Mbps in full-duplex mode.

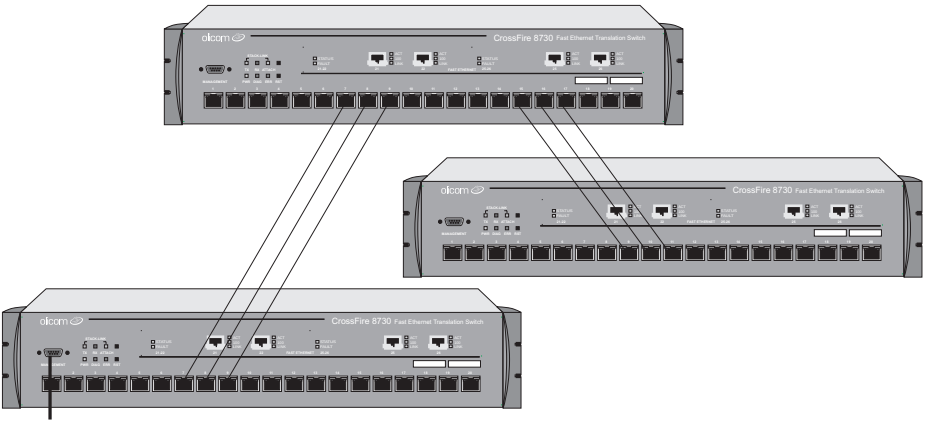


Figure 16. Setting up CrossLinks for Token-Ring Ports

The CrossLink feature affects other switch features in the following ways:

- *Half-duplex and full-duplex.* A single CrossLink can include a combination of half-duplex and full-duplex connections—for example, a CrossLink containing three Token-Ring ports can have two full-duplex and one half-duplex connections. However, each pair of interconnected Token-Ring ports must both be either half-duplex or full-duplex.
- *Statistics reporting.* Statistics for the CrossLink are displayed for individual Token-Ring ports, not for the CrossLink as a whole. Station addresses are distributed among the Token-Ring ports in the CrossLink. See Chapter 4, “Monitoring the Network from the Statistics Menu”.
- *Address filtering.* Address filters are automatically added to every Token-Ring port in a CrossLink.

The lowest numbered Token-Ring port of the CrossLink is called the primary port. CrossLink software learns addresses differently than regular ports, as follows:

- *New source address.* When a packet arrives at a CrossLink port with an unknown source address, the system module creates an entry in the master table and the port table for the CrossLink. The system module assigns the primary port in the CrossLink as the location of the address.

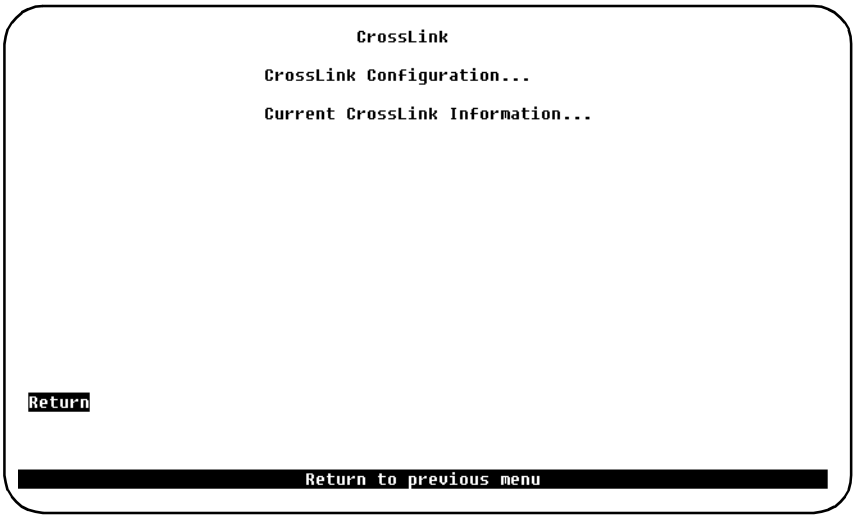
For additional source addresses, the system module assigns locations alternately to other Token-Ring ports in the CrossLink. When all the Token-Ring ports in the CrossLink have at least one address assigned, the system module starts assigning from the primary port again.

- *New destination address.* An unknown destination address packet is sent out on the primary Token-Ring ports of the CrossLink, but entries are not made in ports tables until a reply packet comes back. Entries in port tables depend upon the destination. See the description of primary ports on page 100.
- *Broadcast and multicast packets.* Broadcast and multicast packets go to the primary port of each CrossLink.
- *Link failure.* If one link in a CrossLink fails, a trap is sent and the entire CrossLink connection is disabled.

CrossLink Menu

To open this menu from the main menu, select **Configuration → CrossLink.**

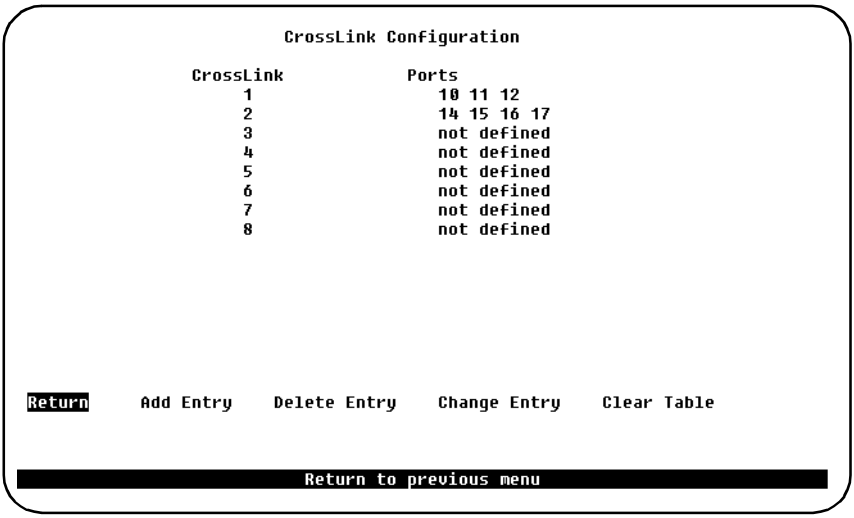
This menu gives access to the **CrossLink Configuration** and **Information** screens.



CrossLink Configuration Screen

To open this screen from the main menu, select **Configuration → CrossLink → CrossLink Configuration.**

Use this screen to add, delete, and change CrossLinks for Token-Ring ports. A description of creating a CrossLink connection follows.



CrossLink

List of different CrossLink setups (*1* to *8*).

Ports

The Token-Ring ports within that specific CrossLink.

Add Entry

Prompts you to enter Token-Ring port numbers for each CrossLink. Enter at least two ports, but no more than eight ports, from lowest number to highest, separated by spaces. All ports must belong to the same TrCRF.

Delete Entry

Asks whether you want to remove the entry; then deletes the selected CrossLink.

Change Entry

Prompts you to reenter the Token-Ring port numbers in the selected CrossLink, from lowest to highest, separated by spaces.

Clear Table

Deletes all CrossLinks.

Setting up a CrossLink

To add a CrossLink between two switches, determine which Token-Ring ports to use for the CrossLink. Use at least 2 Token-Ring ports.

The switch treats the port with the lowest number as the primary port. For example, if a CrossLink consists of ports 8, 11, and 13, the primary port is 8. Broadcast, multicast, and unknown destination packets are forwarded to the primary port in a CrossLink. The primary ports of both CrossLinks must be connected to each other. For example, if a CrossLink links ports 8, 11, and 13 of one device and ports 3, 6, and 9 of another device, ports 8 and 3 must be connected to each other.

Observe the following precautions and use the following steps to set up a CrossLink:

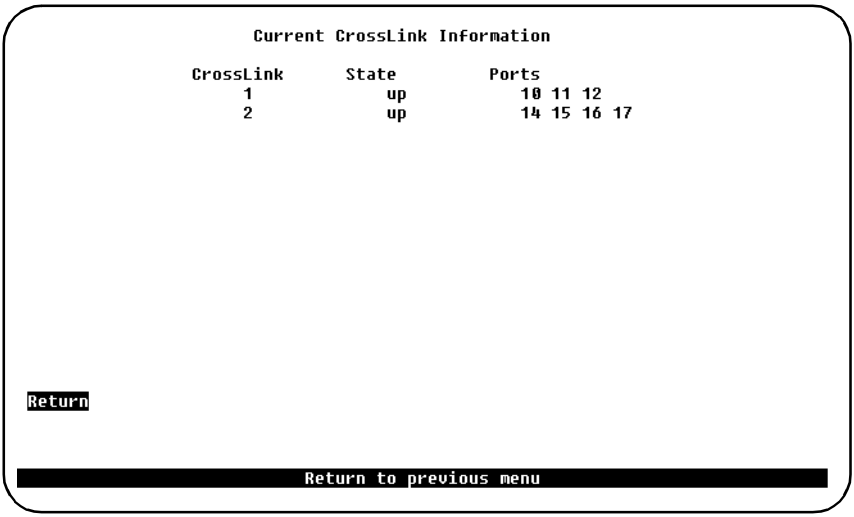
- Disable or disconnect the Token-Ring ports before creating or changing a CrossLink.
- You must define the CrossLink for both connected switches before physically connecting their linked ports. Do not connect the cables before configuring the switches; if you do, you may create loops.
- Cable only the Token-Ring ports you have added to the **CrossLink** menu. If you connect additional ports between two switches, a loop results.

1. Disconnect the Token-Ring ports you want to add to the CrossLink, or disable them using the **Port Configuration** menu.
2. For each switch, select the **CrossLink Configuration** menu, then choose **Add Entry** from the menu bar at the bottom of the screen.
3. Enter the Token-Ring ports for the first CrossLink, separated by spaces.
4. Choose **Return.** (A reset is not required).
5. Repeat steps 1 through 4 for the other switches.
6. Set the **Address Aging Time** to the same value for the switch devices.
7. If you disconnected the Token-Ring ports in the CrossLink, reconnect them. If you disabled them using the **Port Configuration** menu, use the menu to re-enable them.

Current CrossLink Information Screen

To open this screen from the main menu, select **Configuration → CrossLink → Current CrossLink Information.**

Use this screen from the CrossLink menu to display the status of the CrossLink.



CrossLink

The number of the CrossLink referring to the information displayed on the present screen.

State

Whether the specified CrossLink is active or not.

Ports

What Token-Ring ports are in that CrossLink.

Address Filtering

The Address Filtering feature enables you to restrict certain users from communicating with other users. To do this, you can specify source and destination MAC-layer Token-Ring addresses to be filtered at the source port. Token-Ring addresses can be unicast, multicast, or broadcast.

The advantage of address filtering is increased access control and network segmentation. For example, suppose one port is connected to a server containing confidential information from the engineering workgroup. You can prevent access to the server by setting up filters for the addresses of connections from workgroups other than engineering. This is an example of two “types” of filters, “allowing a source address” (engineering) or “blocking a source address(es)” (other workgroups). Examples of different types of filters are allowing, forcing, or blocking packets from a source address, or allowing, forcing, or blocking packets to a destination address. For a detailed explanation of filter types, see the “Configure Filters Screen” section within this chapter.

Observe the following guidelines when setting up address filters:

- Use the **Filters & Port Security** menu to create port filters.
- Filters are port specific and applied to a switch’s incoming traffic only.
- Up to 250 “filters” can be created for each switch (the filters must be applied to specific ports at a specified switch). A “filter” is a combination of a MAC address *and* the “type” of filter it is. For example, if the MAC address 0000A3 C00021 is configured as source type at a port and also configured as a destination type, that would count as two different filters (towards the maximum of 250 filters).
- You can apply these filters to any combination of ports as long as there is a maximum of 250 *filters* (not 250 ports, because more than one port can be part of a filter). For example:
  - Filter “A” (MAC address 0000A3 C00021, source type) can be applied to ports 1, 5, 7, 14 (or to all the ports)
  - Filter “B” (MAC address 0000A3 C00021, destination type) can be applied to the same ports, or different ports, or once again, to all the ports
  - Filter “C” (MAC address 0340B7 A02026, source type) can be applied to any combination of ports; until a maximum of 250 *filters* are created.

Note: If you set up a filter for broadcast packets, hosts on the other side of the switch may not see ARP broadcast packets. To prevent this, let the switch learn the host addresses before implementing the filter. Most hosts time out their local address entries and attempt to relearn with a broadcast ARP.

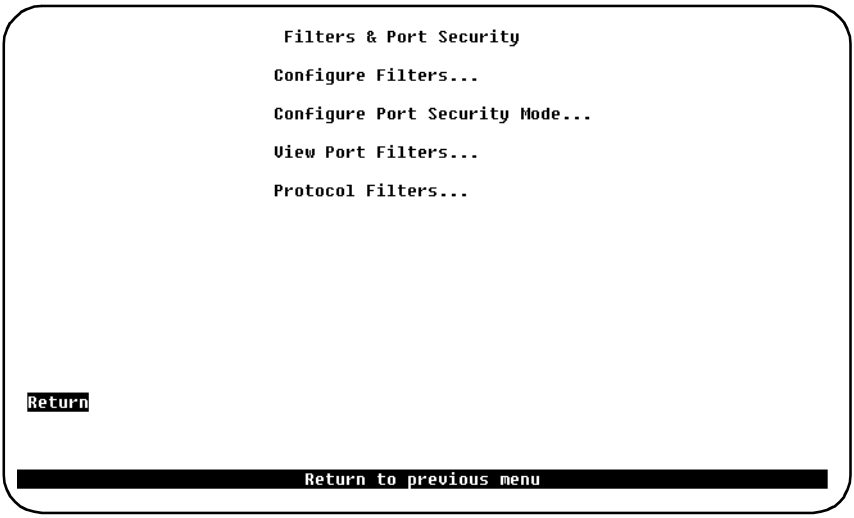
Note: To restrict access from one segment to an entire segment—not just an address—see the “VLAN Configuration” section in this chapter.

The following address filtering menus are used to set up address filtering. Additional information on address filtering is provided as the following filtering menus are presented.

Filters and Port Security Menu

To open this screen from the main menu, select **Configuration → Filters & Port Security.**

Use this menu to access the filtering menus.



Configure Filters...

Displays the **Configure Filters** screen, where you can establish specific filtering based on MAC addresses.

Configure Port Security Mode...

Displays the **Configure Port Security** mode screen, where you can establish address security at specific ports.

View Port Filters...

Displays the **View Port Filters** screen, where you can view port filters for a specific port.

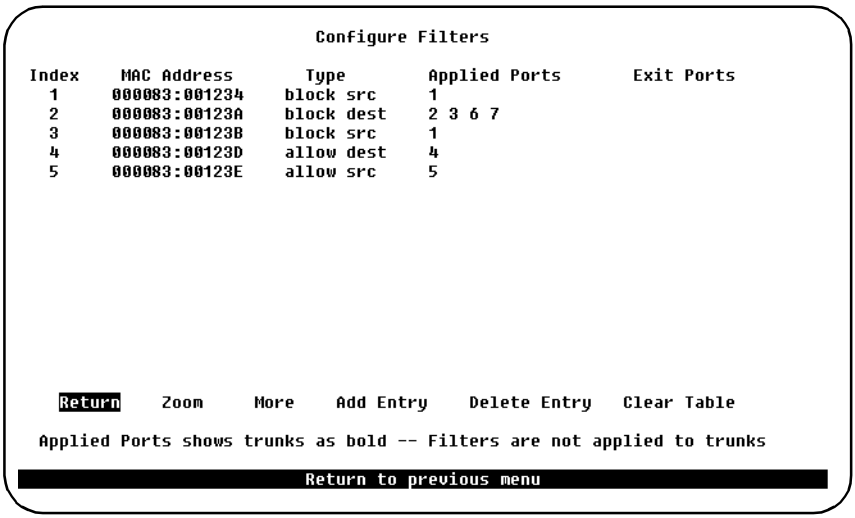
Protocol Filters...

Displays the **Protocol Filters** menu.

Configure Filters Screen

To open this screen from the main menu, select **Configuration → Filters & Port Security.** Then select **Configure Filters....**

When you select **Add Entry** on this screen, a list is displayed of the available filter functions with a selectable highlight. After a choice is made, the console prompts you for the necessary parameters.



Index

The number index.

MAC Address

MAC address contained in packets to be filtered. See a detailed description of MAC addresses on page 46.

Type

Possible types are listed below:

- Block any packet with Source Address—Block Src
  - — That is, any packet from that specific address is blocked from entering the specified port(s).
- Block any packet with Destination Address—Block Dest

- Any packet with the specified destination address is blocked at the specified port(s).

- Allow any packet with Source Address—Allow Src
  - If a packet is received from a specific address it is allowed to go to the specified port(s). This feature is used in conjunction with port security.
- Allow any packet with Destination Address—Allow Dest
  - If a packet is sent to a specific address, it is allowed to go to the specified port(s). This feature is used in conjunction with port security.
- Allow any packet with Limited Multicast Address to ports(s)—Allow Lma
  - If a packet is sent to the specific multicast address, it is allowed to go to the specified port(s) only.
- Force a packet with the Destination Address to certain port—Force Dest
  - When a packet with a specific address must go to a specified port.

Note: Force a packet is for test in network or troubleshooting only. Must not be combined with Port Security Filter.

Applied Ports

The input port(s) that this filter entry is applied to (for that specified MAC address).

Exit Ports

The specified port(s) where a packet is allowed to go, or forced to go (for that specific MAC address). This applies only to the Allow lma and Force Dest filters.

Configure Port Security Mode Screen

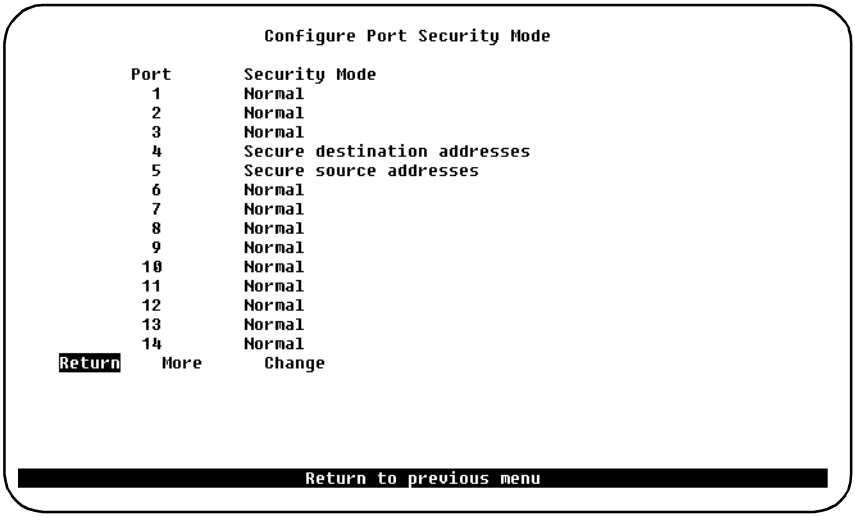
This function disables address learning of source and/or destination addresses at specified ports on a switch. Port security totally blocks (secures) these addresses. *Port security mode is used in conjunction with port filtering.* Configure a port security mode on a port and then use "allow" filters to selectively control traffic through that port.

For instance, if you only want one or some small number of addresses to be able to send to a specific port, you can block all source addresses at that port and then use port filtering (as explained in the previous sections of port filtering) to selectively allow specific addresses to send to that port.

There are four address security choices:

- *Normal*—No security mode is defined for a port. This is the default.
- *Secure source addresses*—Block all source addresses, except those allowed by a configured filter.
- *Secure destination addresses*—Block all destination addresses, except those allowed by a configured filter.
- *Secure both source and destination addresses*—Block all source and destination addresses, except those allowed or forced by a configured filter.

To open this screen from the main menu, select **Configuration → Filters & Port Security.** Then select **Configure Port Security Mode...**

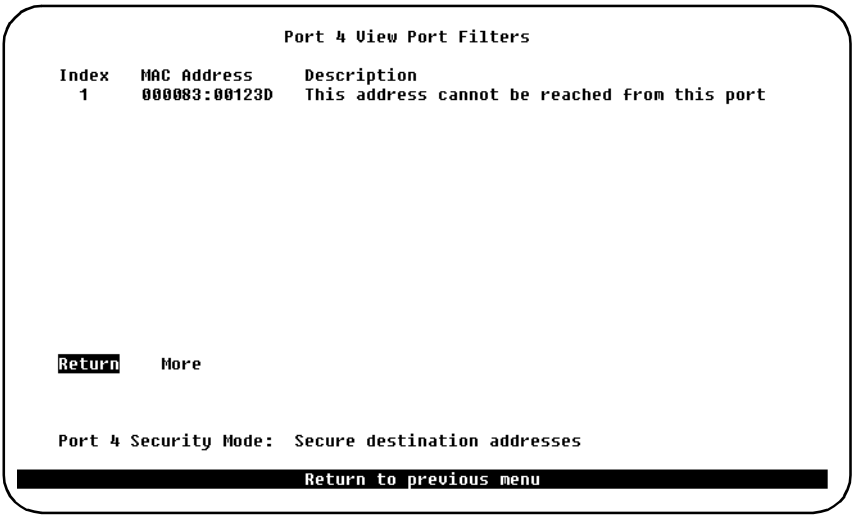


View Port Filters Screen

To open this screen, do the following:

1. From the main menu, select **Configuration → Filters & Port Security.**
2. Select **View Port Filters...**
3. You will be prompted for a port number. Enter a Token-Ring port number, that is, 1-20.

The following screen displays an example of a Token-Ring port using the MAC address filters and port security.



Index

Numerical order of entries.

MAC Address

The specific MAC address the filter is applied to. See a detailed description of MAC Addresses on page 46.

Description

List of descriptions of security modes as assigned at **Configure Port Security Mode** menu:

- This address is blocked
- This address is allowed to talk to ports (as specified)
- This address cannot be reached from this port

- Traffic to this address will be forced to the ports (as specified)

Return
Return to the main menu.

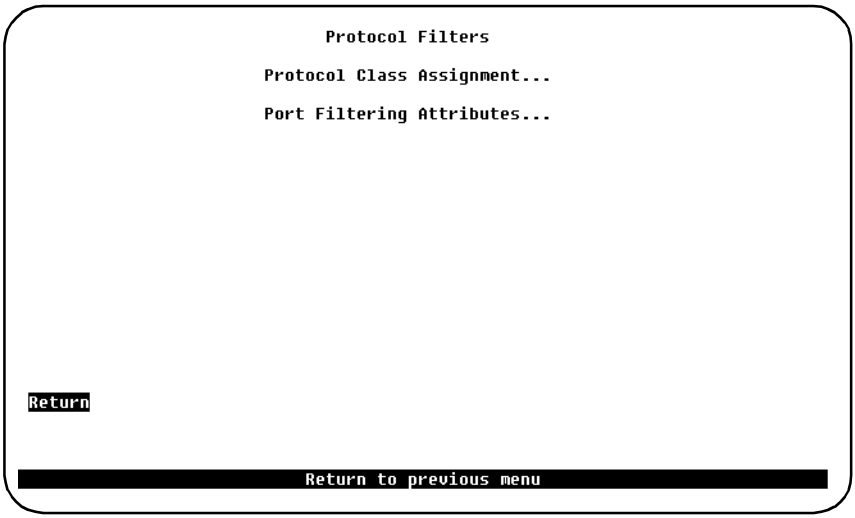
More
Displays additional entries in the filter table if the table contains multiple pages.

Port (number) Security Mode
The type of security mode applied to this Token-Ring port.

Protocol Filters Menu
This menu is accessed from the **Filters and Port Security** menu.

To filter data based on protocol, you can define protocol classes and then assign filtering attributes to these classes on a per port basis. The classes in protocol filtering are based on destination service access point (DSAP) information. In protocol filtering, each incoming frame is assigned to one of the protocol classes based on the DSAP or Ethertype of the frame. If the DSAP is 0xAA (which indicates the Subnetwork Access Protocol [SNAP]), the assignment is based on the Ethertype of the SNAP header. The mapping from DSAP or Ethertype to protocol class is common for all switch ports in a stack.

To open this menu from the main menu, select **Configuration → Filters & Port Security.** Then select **Protocol Filters...**



Protocol Class Assignment...

Selecting this item will open the **Protocol Class Assignment** screen.

Port Filtering Attributes...

Selecting this item will open the **Port Filtering Attributes** screen.

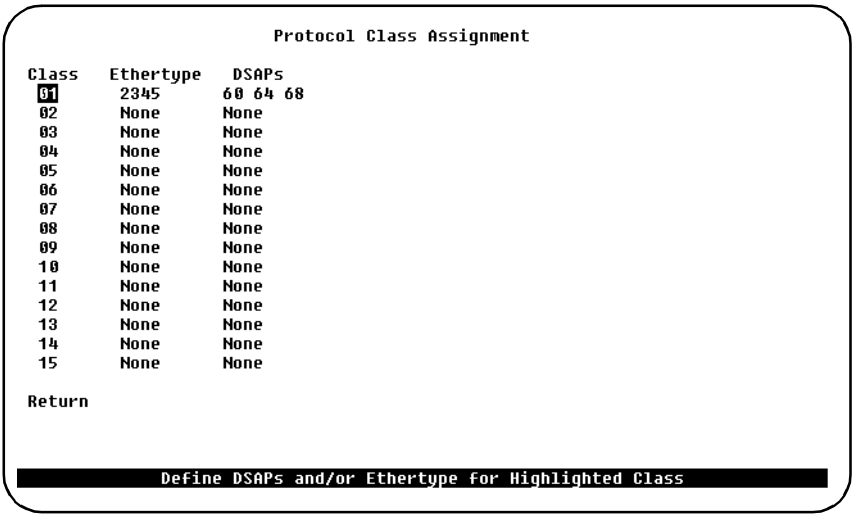
Protocol Class Assignment Screen

The **Protocol Class Assignment** screen shows the 15 protocol classes that may be defined by the user. Note that Class 0 is the default class and will contain all DSAPs and Ethertypes not assigned to any other class.

You modify a class by highlighting the class and pressing ENTER. You will then be prompted for the field to modify: **Name**, **Ethertype** or **DSAPs**. When all classes have been defined as desired, select **Return** to save the values and exit the screen.

To open this screen, do the following:

1. From the main menu, select **Configuration → Filters & Port Security.** Then select **Protocol Filters...**
2. On the **Protocols Filters** screen, select **Protocol Class Assignment...**



Class

For the selected port, use the **Class** field to select a class to modify.

Ethertype

The Ethernet protocol type that you want to filter. You can specify one **Ethertype**

(in its 4-digit hexadecimal format) for each of the classes 1 through 8. You cannot specify an **Ethertype** for protocol classes 9 through 15.

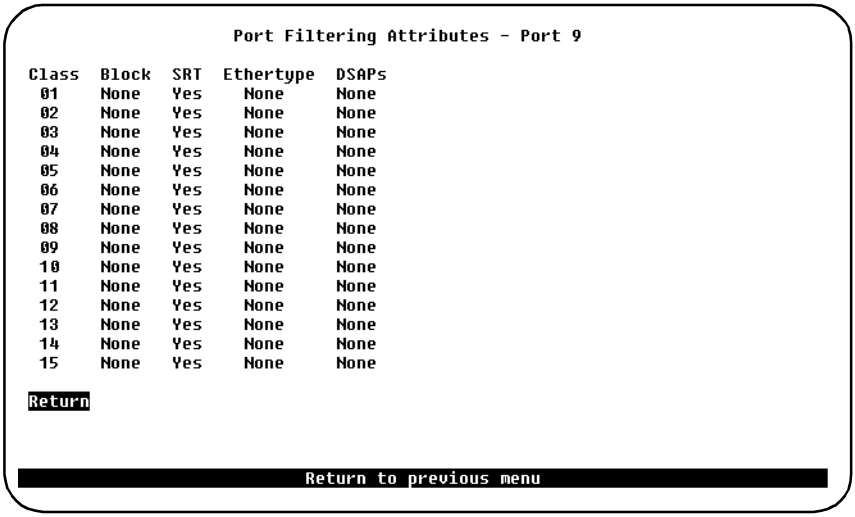
DSAPs

List of the **DSAPs** that you want to filter. You can specify up to 16 **DSAPs** (in their hexadecimal format) separated by spaces.

Port Filtering Attributes Screen

To open this screen, do the following:

1. From the main menu, select **Configuration → Filters & Port Security.** Then select **Protocol Filters...**
2. On the **Protocols Filters** screen, select **Port Filtering Attributes...** Before the **Port Filtering Attributes** screen appears, you will be prompted for a port to modify.



Class

For the selected port, use the **Class** column to select a class to modify.

Block

The **Block** column may have the following values:

- *All*—Block all frames in this protocol class.
- *SR*— Block all source-routed frames in this protocol class.
- *NSR*— Block all non-source-routed frames in this protocol class.

- *None*— Allow all frames in this protocol class (default value).

SRT

The **SRT** column may have the following values:

- *Yes*— Allow transparent bridging for frames in this protocol class (default value).
- *No*— Disallow transparent bridging for frames in this protocol class. If *No* is selected, only source-routed frames can be bridged between CRFs for this protocol class.

Ethertype

Information column showing the **Ethertype** defined for this class.

DSAPs

Informational column showing the **DSAPs** currently in this class.

Address Aging

You can set the per-port aging value using the **Address Aging** menu. The following describes the types of address aging.

There are two types of aging:

- Port aging
  - Any address in a port's address table that has not been active for a port's configured aging time will be removed from the port's table
  - Set at the **Port Address Table Aging** menu
- System aging
  - Addresses that are local to a port but did not fit in its address table will be removed from the master and all port address tables after the system aging time
  - Set at the **Master Address Table Aging** menu

There are two levels to set for the port and master aging tables:

Time Interval Aging is a time limit, in minutes, which will drop older addresses after the selected time.

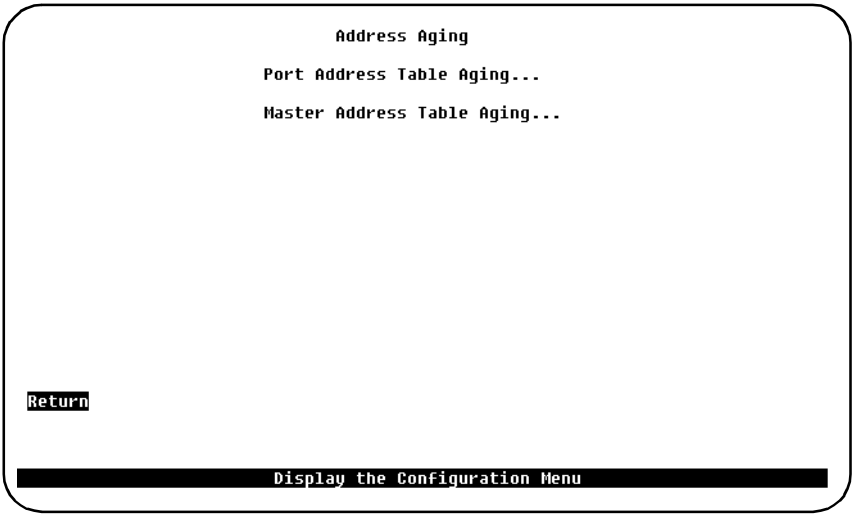
Automatic On-Demand Aging stores addresses until reaching maximum capacity of the table, then deletes addresses, (in the following specific order) down to a selected percentage level and continues to cycle in the same manner.

- Random remote addresses
- Sequential remote addresses
  - sequentially aged from the top of the **Address Aging** table to the bottom of the table
- Random local addresses
- Sequential local addresses

More information on address aging and the address aging screens is presented in the following sections.

Address Aging Menu

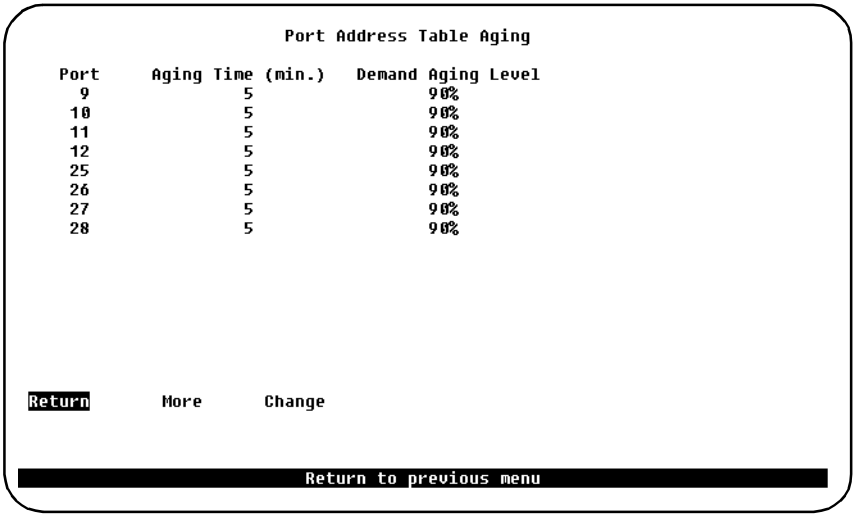
To open this menu from the main menu, select **Configuration → Address Aging**.



The following subsections describe the submenus for the **Address Aging** menu.

Port Address Table Aging Screen

To open this menu from the main menu, select **Configuration → Address Aging**. Then select **Port Address Table Aging**...



The following is an explanation of the information in the **Port Address Table Aging** screen.

Port

The port to which you want to assign an aging time.

Aging Time (min.)

A valid port aging time associated with the port. Addresses will be discarded after reaching the set time limit. The default setting for this parameter is *5* minutes. The maximum time for this value is *9999* minutes. *0* indicates that address aging is disabled.

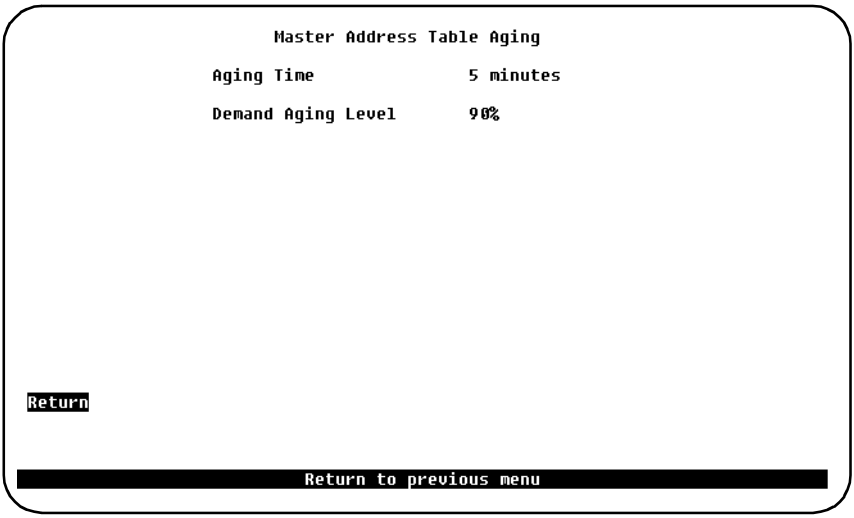
Demand Aging Level

Sets a percentage threshold of address table capacity to ensure that the port's address table is populated only by the most frequently used addresses. Addresses are stored until reaching the maximum capacity of the table, then discarded in a specific order until the set percentage of table capacity is reached. If the table fills again, the aging process continues to cycle in the same manner. The default value is *90%*.

Master Address Table Aging Screen

Master Address Table Aging is the aging value of a set time, in minutes, and a set percentage level after which unused addresses are removed from its table.

Note: If a port address table does not hold enough space for all the needed addresses, some addresses may be present in the master address table but not in any port tables. Such addresses will be removed from the master address table after the master aging time. The addresses will be removed, regardless of whether they have been seen within that time period. This situation is not very likely, but the function is a security against remaining unused addresses in the memory for an indefinite time.To open this menu from the main menu, select **Configuration → Address Aging**. Then select **Master Address Table Aging**...



The **Master Address Table Aging** screen contains two main items:

Aging Time

Master table addresses will be discarded after reaching the set time limit. The default setting for this parameter is *5* minutes. The maximum time for this value is *9999* minutes. A value of *0* will disable the removal of addresses based on age.

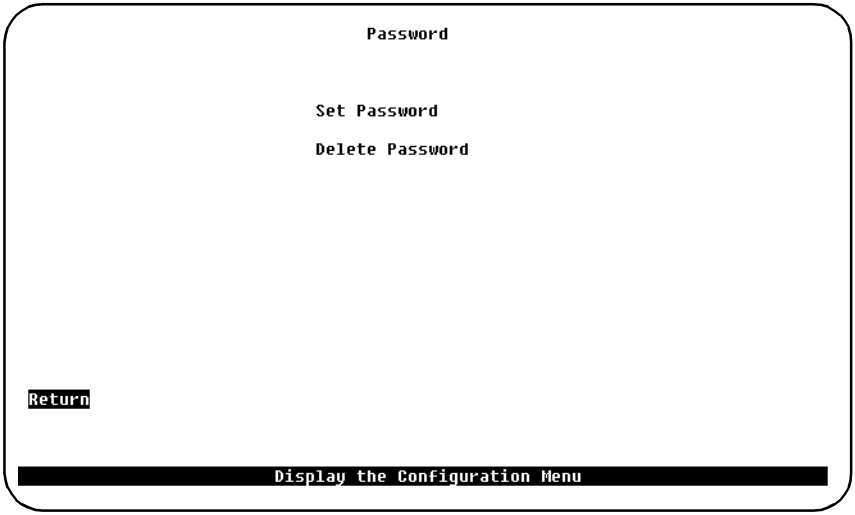
Demand Aging Level

This parameter works in the same way as port demand aging level, only using the system address table. The default value is *90*%.

Password Menu

To open this menu from the main menu, select **Configuration → Password**.

Use the **Password** menu to add, change, or delete a password. If you establish a password, users must enter it to access the console menus. If there is no password, just press ENTER at the password prompt.



Set Password

Establishes or changes the password.

Delete Password

Deletes the password.

The system prompts you to enter the present password before it allows you to change or delete the password. If you are establishing a new password, press ENTER at the **Set Password** prompt.

The password is saved across warm boots and power cycles.

Note: If you have forgotten the password, you can delete it by depressing the unlabeled SysReq button on the front panel of the switch for one second, releasing it, then selecting **Point 4. Clear the system password**.

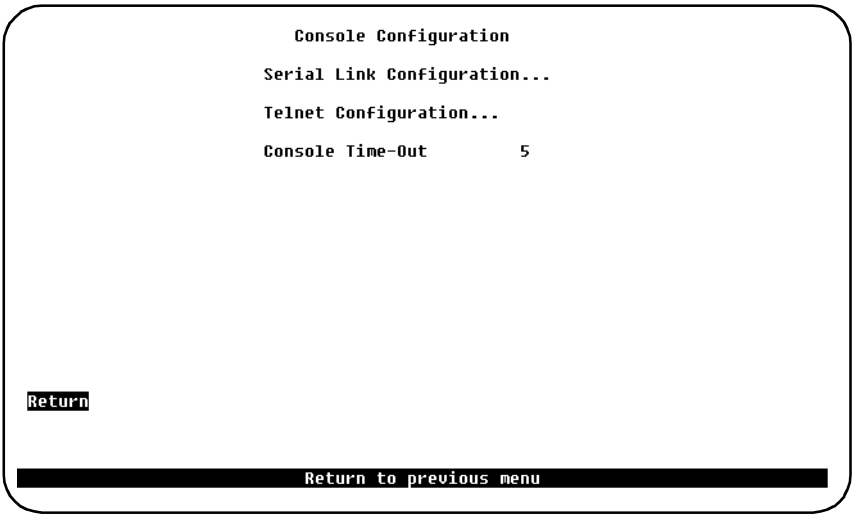
Console/Telnet Sessions

The following section describes how to establish a console or Telnet session.

Console Configuration Menu

This menu lists items for configuring console and Telnet sessions. The **Serial Link Configuration** (console) and **Telnet Configuration** items are selected by highlighting and pressing ENTER.

To open this menu from the main menu, select **Configuration → Console Configuration**.



Serial Link Configuration...

An example of this screen and an explanation of its contents follows below.

Telnet Configuration...

An example of this screen and an explanation of its contents follows below.

Console Timeout

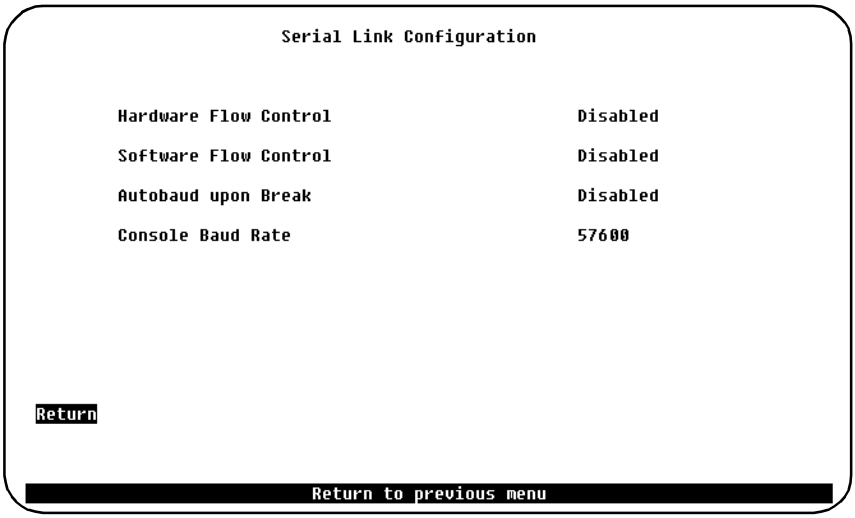
A value that can be set to determine when the console session will timeout and return to the greeting menu. If the value is set to zero, the console will never time out. Default is *5* minutes.

Note: You cannot select **Serial Link Configuration...** if you are accessing the configuration program via Telnet.

Serial Link Configuration Screen

Use the **Serial Link Configuration** screen to configure a switch when using a modem to create a console session.

To open this screen from the main menu, select **Configuration → Console Configuration**. Then select **Serial Link Configuration**.



Hardware Flow Control

Enables or disables RTS/CTS handshaking.

Default: *Disabled*

Software Flow Control

Enables the XON and XOFF characters, which are 11 and 13 hexadecimal, respectively.

Default: *Disabled*

Autobaud Upon Break

Indicates whether the baud rate is reset when a Break key sequence (pressing ENTER rapidly for five seconds) is sent or received. The default is *Disabled*. When set to enabled, a baud rate change can be accomplished by changing the baud rate of the terminal emulator, disconnecting and reconnecting the TIA/EIA-232 cable, and then pressing ENTER until a screen appears.

Console Baud Rate

The baud rate of the TIA/EIA-232 port. Acceptable baud rates for the console are *1200, 2400, 4800, 9600, 19200, 38400, 57600,* or *Autobaud*. The default value for

this parameter is *9600*. Make sure that your terminal emulator baud rate matches the console baud rate you set.

Creating a Console Session Using a Modem

Use the **Serial Link Configuration** menu to configure the switch in order to communicate with a console via a modem.

Set your modem according to the table below.

Setting	Value
Echo	*Off*
Result codes	*Off*
Wait for connection	*45* seconds
Pause between calls	*6* seconds
Drop DTR between calls	*Yes*
Send CR between calls	*Yes*
Auto baud detect	*On*
Send init if CD high	*Yes*
Maximum dial attempts	*999*

Table 12. Modem Settings

Caution: Some modems use slightly different names for the options. It is important that your modem be configured correctly. The settings shown in italics are particularly important. If your modem is not configured correctly, the connection may cause the switch to reset.

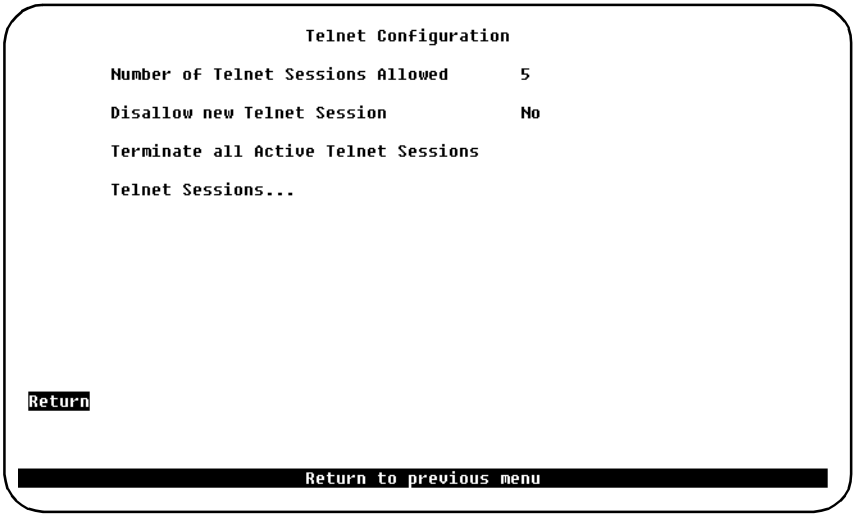
Start the console by pressing ENTER. If a Telnet session is active, press ENTER at the console to terminate the Telnet session and press ENTER again to start the console session.

Stopping the Console Session

Pressing CTRL-P returns the console session to the main menu, and pressing CTRL-B returns to the greeting menu.

Telnet Configuration Screen

To open this screen from the main menu, select **Configuration → Console Configuration**. Then select **Telnet Configuration**...



Return to Previous Menu

Returns to the **Console Configuration** menu.

Number of Telnet Sessions Allowed

Limits the number of Telnet sessions. Numbers allowed are from *1* to *5*. Highlight this selection, press ENTER, and enter the number. Default is *5*.

Disallow New Telnet Session

Choose *Yes* or *No* to allow or disallow a new Telnet session. Press ENTER at this selection, use arrow keys to highlight *Yes* or *No*, and then press ENTER again.

Terminate All Active Telnet Sessions

If you highlight this selection and press ENTER, all Telnet sessions are terminated.

Telnet Sessions...

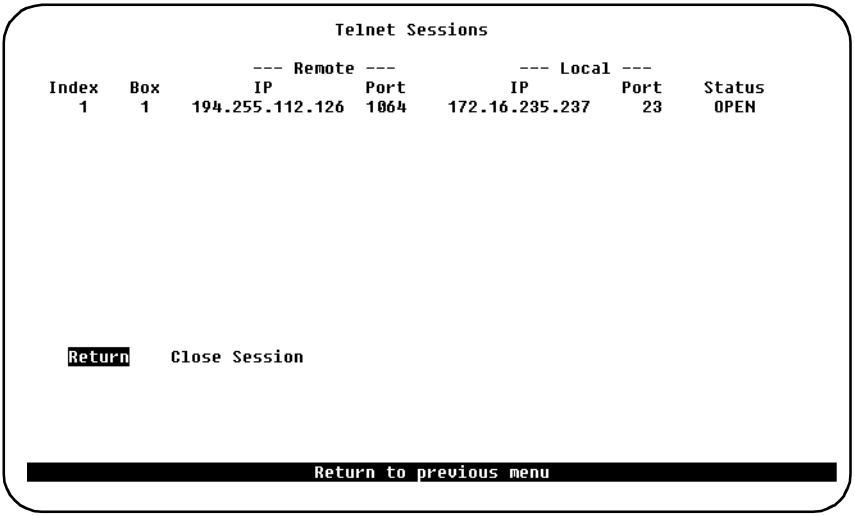
This item opens the **Telnet Sessions** screen that displays the status of Remote and Local Telnet sessions.

Note: You cannot select **Number of Telnet Sessions Allowed**, **Disallow New Telnet Sessions**, or **Terminate All Active Telnet Sessions** if you are accessing the configuration program via Telnet.

Telnet Sessions Screen

To open this screen, do the following:

1. From the main menu, select **Configuration → Console Configuration**. Then select **Telnet Configuration**...
2. On the **Telnet Configuration Screen**, select **Telnet Sessions...**



Index

Numerical order of entries.

Box

The box number ID of the switch in a stack.

Remote

Lists the IP address and the port number of the Remote Telnet session.

Local

Lists the IP address and the port number of the Local Telnet session.

Status

The status of the telnet session. Possible values are *Open* (the connection is active), *Closing* (the connection is going down) and *Exit* (the connection is closed).

Starting the Telnet Session

Observe the following when starting a Telnet session to the switch:

- In the **IP Information** screen, the **IP State** must be set to *BootP When Needed* or *BootP Always* for the IP stack and Telnet to work.
- The Telnet must be pre-configured to have a VT100/VT220 compatible setup.
- Only one type of session is supported at any time, either the console or Telnet session. Starting a Telnet session before ending the console session causes the screen to display a `Console is currently in use` message.
- There may be conflicts between Telnet sessions. If one Telnet session is disrupted by the user at the console, the Telnet session's configuration may not have been completed. In some menus, changes take effect immediately, as in adding filters, and in other menus, such as STP, the changes are not saved until the menu is exited.

Stopping the Telnet Session

Telnet sessions can be terminated by pressing CTRL-B or any other means available through the user's Telnet application.

Involuntary Termination of the Telnet Session

The following can terminate a Telnet session:

- A Telnet session can be terminated involuntarily by the console or by itself. When the console is idle and Telnet is active, a user at the console can terminate the Telnet session without warning. When the Telnet sessions ends, the Telnet session screen displays the message: `Your session has been terminated due to system maintenance work.`
- If any changes are made in the STP configuration.
- The Telnet session also ends if a user makes changes in any of the following IP parameters:
  - — IP address
  - — Default gateway

- Subnet mask
- IP state

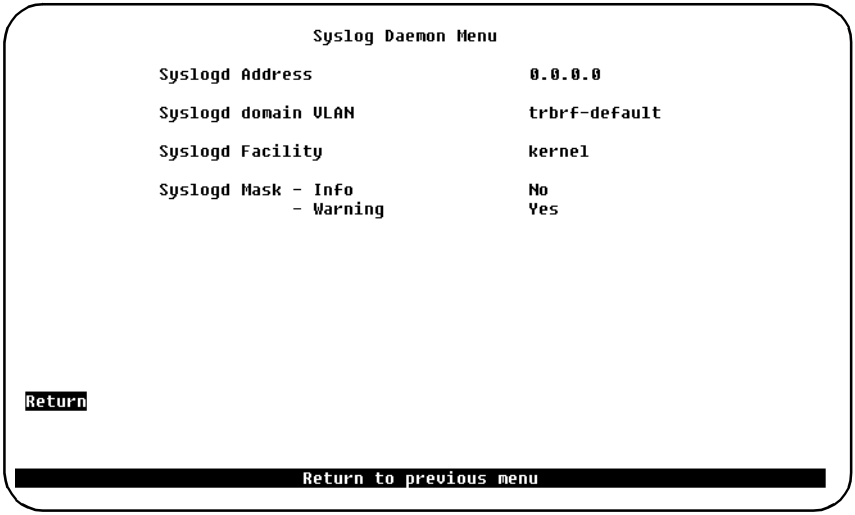
- The Telnet session also times out if there has been no activity for 5 minutes.

Note: If you are in a Telnet session and change the IP parameters either in the **IP Information Session** screen or **Virtual LAN IP Configuration** screen, and save the changes using the **Exit** command from the screen, you will lose the connection to your Telnet session, even if the IP parameters you change are in another VLAN.

Syslog Daemon Screen

To open this menu from the main menu, select **Configuration → Syslog.**

This menu displays the parameters for the Syslog Daemon facility. The Syslog Daemon sends log messages to the IP address specified on this screen. This means that the messages can be accessed from the computer at this address.



Syslogd Address

This parameter displays the IP address of the computer to which the log messages are sent.

Syslogd Domain VLAN

This parameter displays the VLAN in which the messages are sent.

Syslogd Facility

The facility code sent.

Possible values are *daemon, kernel, user, local0, local1, local2, local3, local4, local5, local6, local7*

Syslogd Mask

- **Info** determines whether *informative messages* are sent to the specified IP address for logging or not. Possible valuees are *Yes* and *No*.
- **Warning** determines whether *messages containing warnings* are sent to the specified IP address for logging or not. Possible values are *Yes* and *No*.

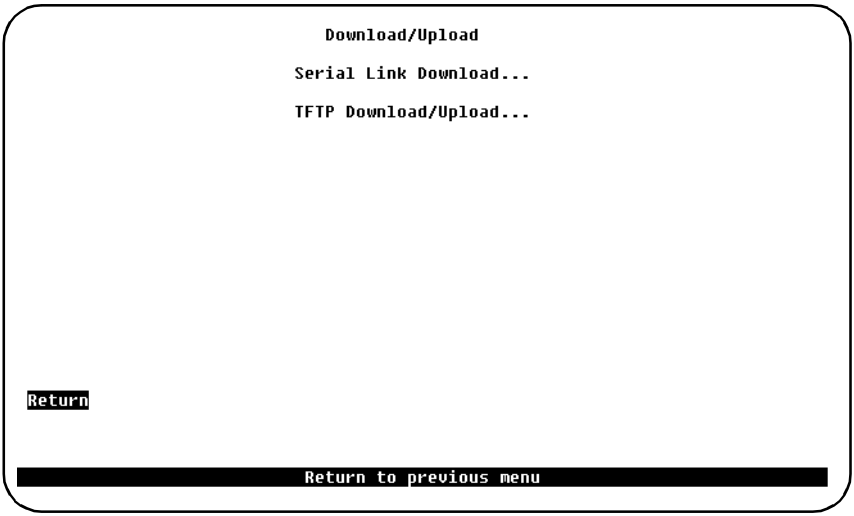
Download/Upload Menu

As enhancements are made to the switch, you may need to update the software, or microcode, that is contained in the switch. This chapter describes how to upgrade the switch flash memory.

Caution: After downloading the new software, you must reset the switch. The switch is not operational while it is resetting. Before starting this procedure, make sure the network will not be effected.

Downloading is used to load the flash memory within the switch. The **Download/Upload** menu displays two download choices. The two choices are **TFTP** (Trivial File Transfer Protocol) **Download/Upload** and the **Serial Link Download** (console). You can also use TFTP transfers to store or retrieve the complete set of switch configuration parameters.

To open this menu, select **Download/Upload** in the main menu.



Serial Link Download...

Displays the **Serial Link Download** screen.

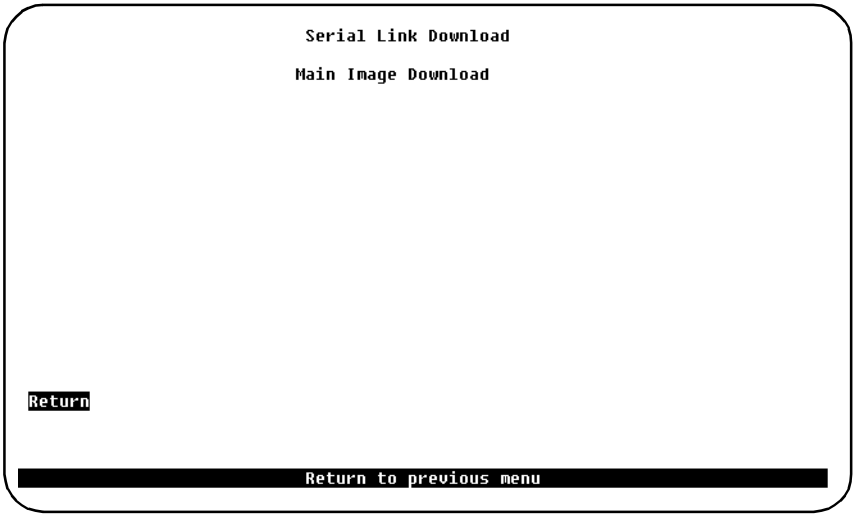
TFTP Download/Upload...

Displays the **TFTP Download/Upload** screen.

Serial Link Download Screen

Open this screen from the main menu by selectiong **Download/Upload → Serial Link Download...**

Serial Link download is for downloading via the Out-of-Band management port.



Proceed as described below to update the switch software:

1. Use a terminal emulation program, which supports the X-modem protocol.
2. Insert the upgrade disk in your terminal emulator drive.
3. If you have not already done so, start a console session.
4. Select **Download/Upload** on the main menu.
5. Select **Serial Link Download**.
6. Select **Main Image Download**.
7. Confirm the download. The download takes approximately 12 minutes at 9600 baud. Note, there is no validation of the image, before the flash is updated.
8. Start the X-modem download on the terminal.

Note: Do not interrupt the download, or the image will be corrupted and needs to be reloaded. During the download, the DIAG LED on the switch will be blinking.

9. When the download is complete, you will be prompted to reset the switch. Press `Y` to confirm the reset. The procedure is now complete. If the download was interrupted or the image was invalid, the switch will discover this during startup, and a new serial download must be performed prior to normal operation.

TFTP

TFTP is not invoked automatically on the switch as it is on certain other network devices, such as a diskless workstation. This is because there should normally be a functional software image in flash memory and, therefore, TFTP is not a standard part of the switch bootup procedure (under normal circumstances). TFTP is intended for use during software upgrades and, once a new image is installed, there should be no need for TFTP until the next software upgrade is installed.

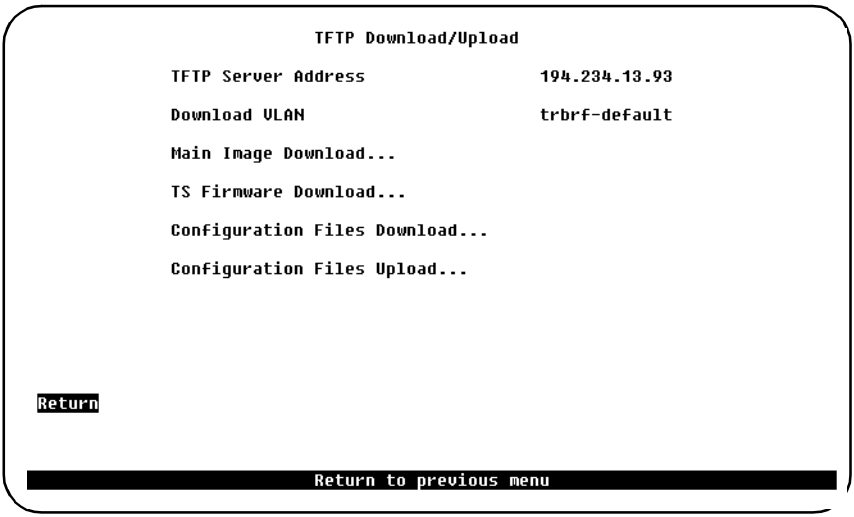
In view of this, the TFTP function in the switch is designed as an explicitly requested operation with operator settable parameters. Note that changes to these parameters may be altered and will be used when starting a download in the display, however, they are not recorded until the display is exited normally.

The **TFTP Download/Uploa**d menu is accessed through the main menu. From the main menu select **Download/Upload** and then select **TFTP Download/Upload**.

TFTP Download/Upload Screen

Open this screen from the main menu by selecting **Download/Upload → TFTP Download/Upload...**

The following is an example of the **TFTP Download/Upload** screen.



TFTP Server Address

The address of the host serving as the TFTP server.

Download VLAN

The VLAN name through which the download is attempted.

Main Image Download..., Configuration Files Download..., Configuration Files Upload..., TS Firmware Download

Select the required function and input the path and filename of the file the switch attempts to download or upload, as it is to be received and interpreted by the TFTP server. (The security mode in use on the TFTP server may affect this function.)

Note: By using **Download VLAN**'s default gateway, if it has one, the file can be downloaded from another network anywhere on the Internet from which the VLAN can get packets routed (even another directly connected VLAN). In the latter case, the switch will actually load, or attempt to load, through the gateway and not ignore its **Download Domain** parameter. If the switch is unable to reach a TFTP server to which it should have a direct or indirect route, an incorrectly set **Download VLAN** may be the reason.

Execute <name> Download/Upload

This command is displayed on the sub-screens that are opened from the **TFTP Download/Upload** screen.

The command **Execute <name> Download/Upload** initiates the download or upload for a single switch only. The screen displays the block it last received from the server (block 0 if no reply has been received) until the last packet arrives. The switch does not attempt to load any of the image into flash memory until it receives the final packet. Therefore, if interrupted or cancelled for any reason before the last packet, the previous system image remains intact in flash memory.

Once the last packet has arrived, the switch immediately begins clearing flash memory and loads it with the new image.

The switch will continue to use its previously loaded software until its next reset by whatever means. The newly stored image is not functional until a reset is performed.

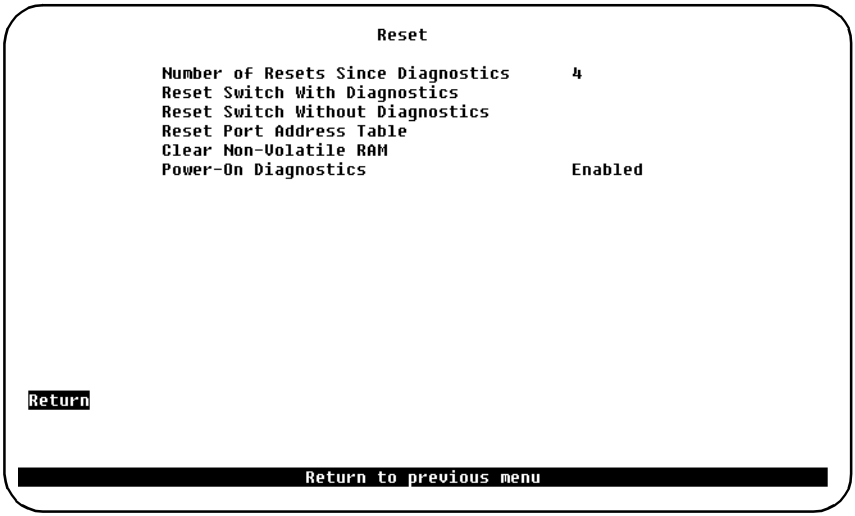
Note: Be careful - if the process is interrupted during this time, the stored image may be corrupted and the switch will not be able to boot normally! If this happens, it is necessary to download the switch via its Out-of-Band Management port since the system boot image does not contain software capable of operating the network hardware of the switch or understanding IP and TFTP protocols. During this fairly short vulnerable period of time, the diagnostic LED on the switch blinks to indicate the clearing (slow blink) and reloading (faster blink) of flash memory. The screen also displays messages indicating these events.

Remember:

- Do not configure multiple TFTP servers to download code updates using TFTP to a single switch (or to multiple domains).
- If the network broadcast traffic is 200 packets per second or more, the TFTP request might not be initiated by the switch. You must reset the switch and download a new image using the serial port download (refer to the section "Serial Link Download Screen" on page 126).

Reset Screen

To open this screen, select **Reset...** in the main menu. The **Reset** screen displays the reset options available with the switch.



Number of Resets Since Diagnostics

Number of times the switch has been reset since the switch was powered on or ran power-on diagnostics. This is an informational heading; the data cannot be changed.

This number is not reset to 0 when nonvolatile RAM is cleared.

The following four items within the **Reset** screen are command functions that you can select and initiate by moving the highlight over the item and pressing ENTER.

Reset Switch With Diagnostics

A reset function is initiated with this command. It resets the switch hardware; runs diagnostic tests; clears all counters, including address tables; and restarts the switch. When the switch reboots, administrative parameters from non-volatile memory are used to initialize the operational parameters. This takes approximately 4 to 5 minutes.

Reset Switch Without Diagnostics

This command resets the switch hardware; clears all counters, including address tables; and starts the switch. When the switch reboots, administrative parameters from non-volatile memory are used to initialize the operational parameters. This procedure takes approximately 40 seconds.

Reset Port Address Table

Selecting this command clears all address table entries for a specified port (user is queried for which port to reset), sets port traffic counters to zero, and sets **Time Since Last Reset** for this port to zero.

Clear Non-Volatile RAM

Selecting this command will erase all user-configured parameters (rate, IP address information, CrossLink, Virtual Token-Ring Switch, STP) and reset the switch.

Note: Clearing NVRAM (non-volatile RAM) erases all configuration parameters.

Follow these guidelines if you must clear NVRAM:

- If you are using the CrossLink feature, be sure to disconnect the affected Token-Ring ports—or disable them on the **Port Configuration** screen and reset the switch—*before* clearing NVRAM.
- If you are using the STP option, be aware that port costs and priorities will be lost, which may result in loops. Use the menus to reestablish port costs and priorities, then reset the switch to make the new parameters take effect.
- If you are using an SNMP manager, you will need to reconfigure all IP and SNMP parameters.

Power-On Diagnostics

This is a selectable option that determines whether diagnostics are, or are not, initiated during a switch power-on sequence. To change the selection, highlight the item and press ENTER; then select *Enabled* or *Disabled*, and press ENTER.

Default: *Enabled*

4. Monitoring the Network from the Statistics Menu

This chapter explains how to monitor the CrossFire 8730 Fast Ethernet Translation Switch through a directly connected VT100 console or through a VT100 telnet session. For information how to connect directly, see the *CrossFire 8730 Fast Ethernet Translation Switch Installation Guide*.

To use SNMP (in-band, through the network management), see Chapter 5, “Monitoring the Network with SNMP”.

The information presented on the statistics screens in this chapter is typically used for monitoring purposes only. This information is usually the result of input data from the configuration menus (see Chapter 3, “Switch Configuration”). The specifications presented on the statistic screens normally can not be modified.

Information within the statistics menus are updated (screens are refreshed) every 5 seconds.

The next section explains how to access the statistics menus, and the following sections describe the information and submenus of the statistics menu.

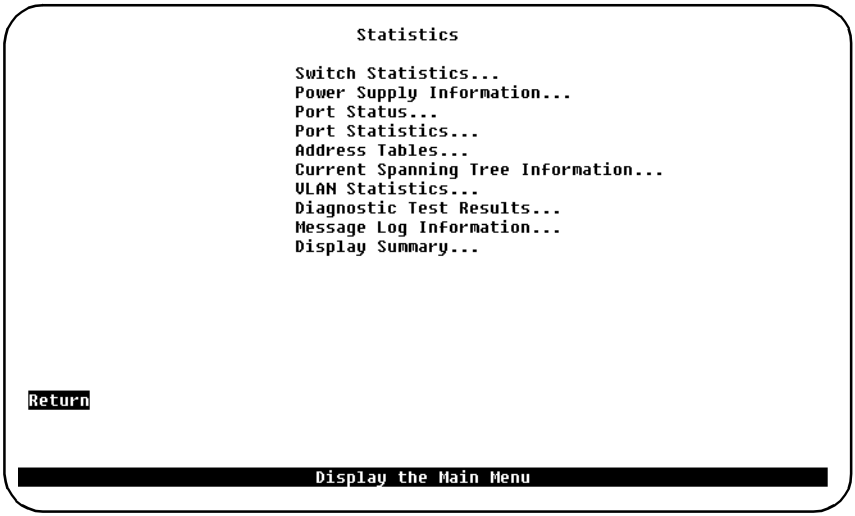
Note: The switch allows LAN Network Manager LLC frames to flow through the switch. Therefore, communication between LAN Network Manager and existing source-route bridges and controlled access units is maintained. However, some error reporting functions and ring map functions might be lost for the rings attached to the switch.

For information on how to navigate in the menus, see See “Navigating within the Menus” on page 43.

Statistics Menu

To open the **Statistcis** menu, select **Statistics...** in the main menu.

The following sections describes the **Statistics** submenus and screens.

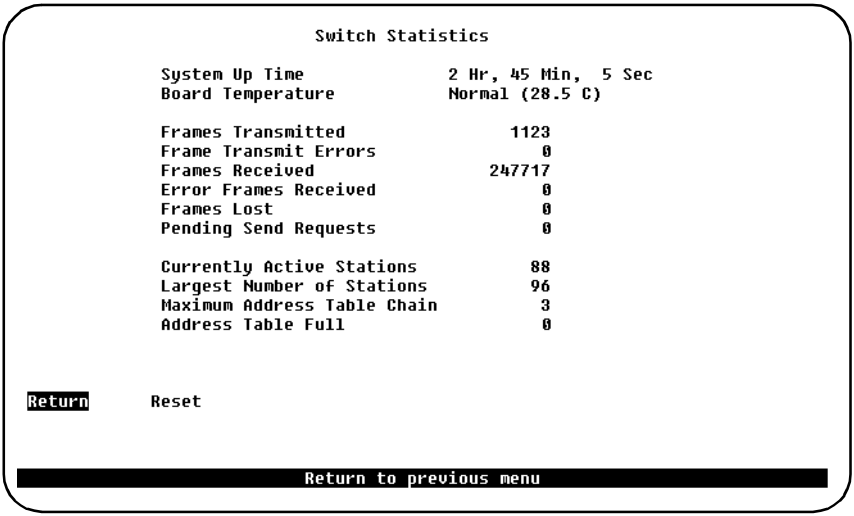


Switch Statistics Screen

To open this screen from the main menu, select **Statistics → Switch Statistics**.

The **Switch Statistics** screen shows statistics and information about stations connected to the switch.

Note: References to “frames” in this menu refer to the frames that are handled by the CPU within the switch, for example SNMP requests. The **Port Statistics** screen (described in a later section) refers to frames handled by the ports on the switch.



System Up Time

Length of time since the last reset or power cycle.

Board Temperature

Indicates whether the switch is operating at normal or unacceptably high (over 50°C (122°F)) temperatures. The actual board temperature is also shown.

Frames Transmitted

Number of frames transmitted by the CPU of the switch.

Frame Transmit Errors

Number of errors recorded (by the CPU) when attempting to transmit frames.

Frames Received

Number of frames received (by the CPU).

Error Frames Received

Number of frames received (by the CPU) that were corrupted or have CRC errors.

Frames Lost

Number of frames dropped (by the CPU) due to exceeding the capacity of the software buffers.

Pending Send Requests

Number of software transmitted packets that are waiting for queues to hardware.

Currently Active Stations

Number of entries in the address table, representing the number of currently active stations (MAC addresses), or nodes, on all ports of the switch.

Largest Number of Stations

The most stations (MAC addresses) ever active on all ports at one time since the last reset or power cycle.

Maximum Address Table Chain

Largest number of MAC addresses that have hashed to the same location in the lookup tables. Used for technical system evaluation and troubleshooting.

Address Table Full

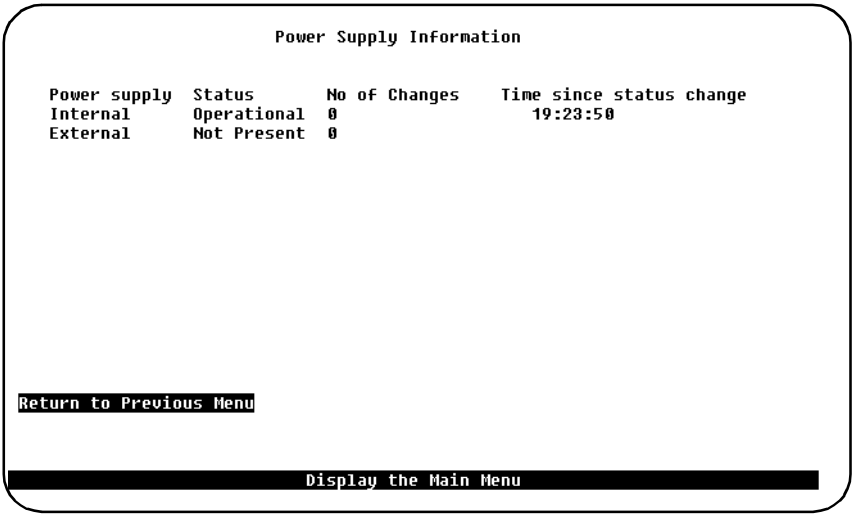
Number of times the hash table reached capacity. Used for technical system evaluation and troubleshooting.

Reset

Resets the switch statistics on this screen.

Power Supply Information Screen

To open this screen from the main menu, select **Statistics → Power Supply Information**.

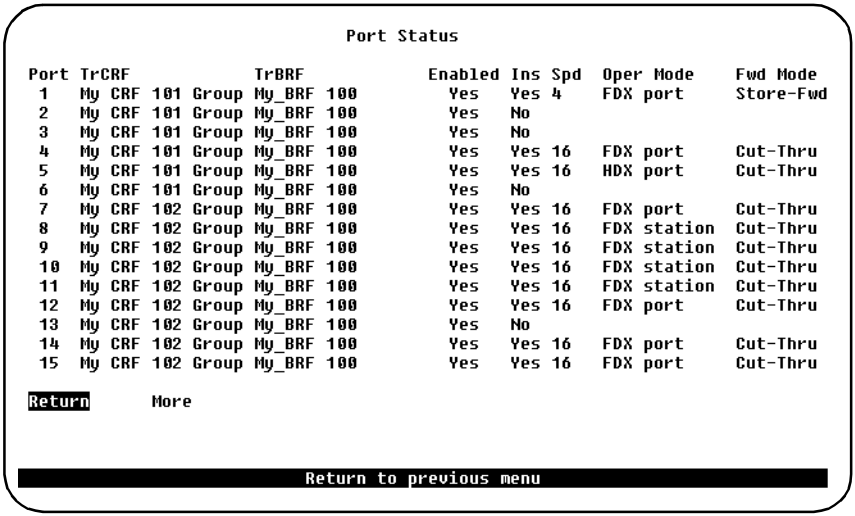


This screen displays information about any installed internal or external power supplies.

Port Status Screen

To open this screen from the main menu, select **Statistics → Port Status.**

The **Port Status** screen provides a summary of the status of all ports.



Port

The port number.

TrCRF

For the Token-Ring ports, the name of the TrCRF to which the port is assigned.

For the Fast Ethernet ports, the name of the CRF in which the virtual port is defined.

TrBRF

For the Token-Ring ports, the name of the TrBRF to which the port is assigned.

For the Fast Ethernet ports, the name of the BRF in which the virtual port is defined.

Enabled/Ins

For the Token-Ring ports 1-20, this parameter displays the current enabled status of the port. Possible values are *Yes* and *No*.

For the Fast Ethernet ports, this parameter displays the current state of the virtual port. Please refer to the description of virtual port configuration for details

Ins

Indicates if the port is currently inserted into the ring. Possible values are *Yes* and *No*.

Spd

For the Token-Ring ports, the Token-Ring media speed. Possible values are *4* and *16*.

For the Fast Ethernet ports, the connect speed in Mbps, which is always displayed as 100 for Fast Ethernet virtual ports. Note that 100 Mbps full-duplex is the total bandwidth available on a Fast Ethernet port and is shared by all the virtual ports on that port. The actual bandwidth on a particular virtual port thus depends on the amount of traffic on other virtual ports.

Oper Mode

The port operation mode. Possible values for Token-Ring ports are:

- *HDX port*—Half-duplex mode in which only a dedicated connection to a station is supported. The Tx/Rx pinouts are the same as a concentrator's.
- *HDX station*—Half-duplex mode in which the port operates like a station. The connection may be dedicated or shared. The Tx/Rx pinouts are the same as an adapter's.
- *FDX port*—Full-duplex mode in which only a dedicated connection to a station is supported. The Tx/Rx pinouts are the same as a concentrator's.
- *FDX station*—Full-duplex mode in which the port operates like a station. The connection may be dedicated or shared. The Tx/Rx pinouts are the same as an adapter's.
- *RI*—Ring In. Only displayed for ports 19 and 20.
- *RO*—Ring Out. Only displayed for ports 19 and 20.
- *RI/RO*—Ring-in/ring-out mode. Only displayed for ports 19 and 20.
- *Passive* - this value will be displayed if the port is selected as a passive monitoring port on the **Switched Port Analyzer** configuration screen.

The operation mode for Fast Ethernet virtual ports is *HX* (Half dupleX) or *FX* (Full dupleX).

Fwd Mode

The forwarding mode that will be used for transmit. Possible values for Token-Ring ports are:

- *Cut-Thru*—cut-through

- *Store-Fwd*—store-and-forward

For ports operating at a speed of 4 Mbps, the only possible mode is *Store-Fwd*.

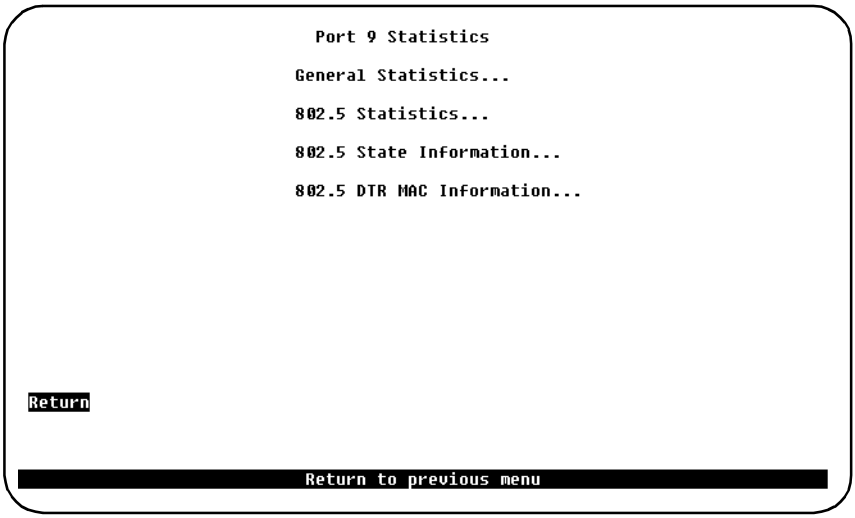
For the Fast Ethernet ports, the only possible mode is *Store-Fwd*.

Port Statistics Menu for Token-Ring Ports

To open this screen from the main menu, select **Statistics → Port Statistics**.

The **Port Statistics** menu provides access to statistical information for any particular port. To enter the menu, you must first enter a port number.

The following screen is displayed when you select a Token-Ring port, that is, port numbers 1 - 20.



General Statistics...

Displays general statistics for the selected port (page 142).

802.5 Statistics...

Displays 802.5 statistics for the selected port (page 149).

802.5 State Information...

Displays 802.5 state information for the selected port (page 152).

802.5 DTR MAC Information...

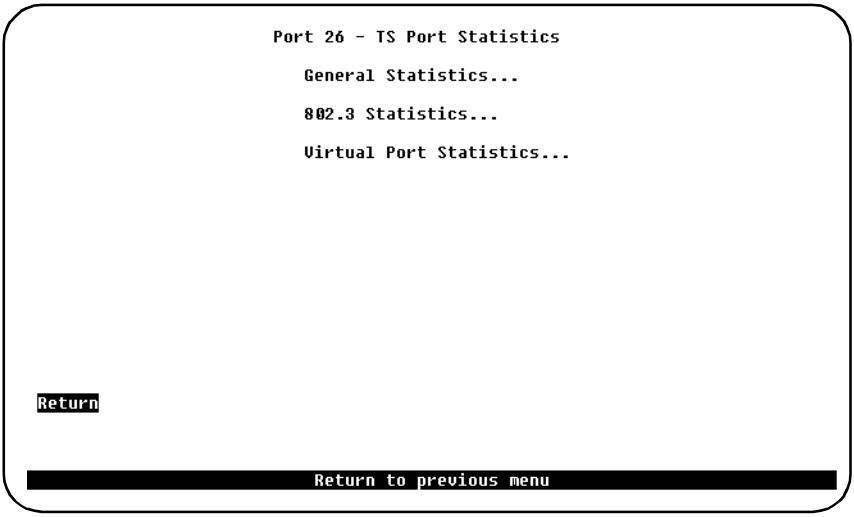
Displays 802.5 DTR MAC information for the selected port (page 154).

Port Statistics Menu for Fast Ethernet Ports

To open this screen from the main menu, select **Statistics → Port Statistics**.

The **Port Statistics** menu provides access to statistical information for any particular port. To enter the menu, you must first enter a port number.

The following screen is displayed when you select a Fast Ethernet port, that is, port numbers 21, 22, 25, or 26.



General Statistics...

Displays general statistics for the selected port See page 142.

802.3 Statistics...

Displays 802.3 statistics for the selected port. See page 158.

Virtual Port Statistics...

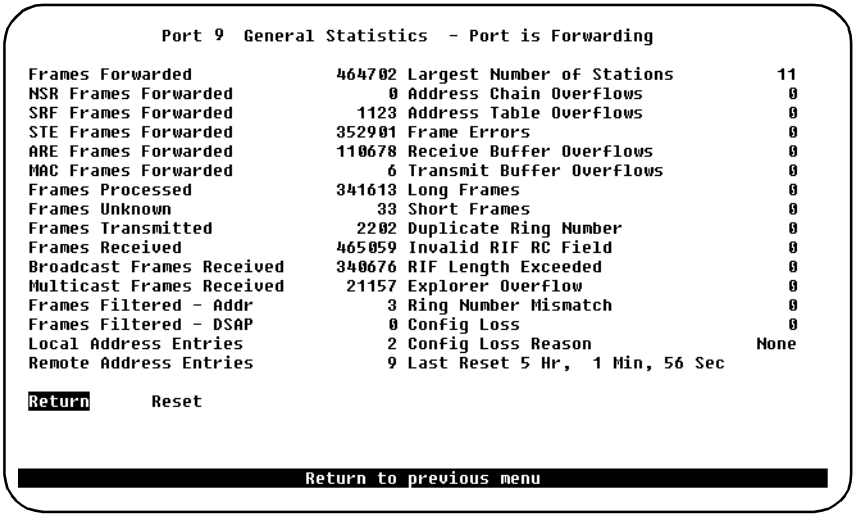
Opens the **Virtual Port Statistics** screen. See page 161.

General Statistics Screen for Token-Ring Ports

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **General Statistics**...

Use the **General Statistics** screen to view detailed information about a particular port.



Frames Forwarded

Number of frames forwarded by the port, excluding those delivered to the host CPU system software for processing, or to a monitoring port.

NSR Frames Forwarded

Number of non source-routed frames forwarded by the port.

SRF Frames Forwarded

Number of source-routed frames forwarded by the port.

STE Frames Forwarded

Number of Spanning Tree Explorer frames forwarded by the port.

ARE Frames Forwarded

Number of All Route Explorer frames forwarded by the port.

MAC Frames Forwarded
Number of MAC layer frames forwarded by the port.

Frames Processed
Number of frames received on this port and delivered to the host CPU system software for processing.

Frames Unknown
Frames processed by the host CPU system software that contained an unknown source or destination address.

Frames Transmitted
Total number of frames transmitted by this port.

Frames Received
Total number of frames received on this port .

Broadcast Frames Received
Number of broadcast frames received on this port without errors.

Multicast Frames Received
Number of multicast frames received on this port without errors.

Frames Filtered - Addr
Number of frames filtered by the MAC address filters.

Frames Filtered - DSAP
Number of frames filtered by the protocol filters.

Local Address Entries
Number of local stations in the address table of the port.

Remote Address Entries
Number of remote stations in the address table of the port.

Largest Number of Stations
Highest number of stations active on this port at any time.

Address Chain Overflows
Number of address table chain overflows.

Address Table Overflows
Number of address tables overflows.

Frame Errors

Total number of frames received or transmitted by/from this port with an error.

Receive Buffer Overflows

Total number of frames received on this port which caused a buffer overflow.

Transmit Buffer Overflows

Total number of frames which could not be transmitted from this port because of transmit buffer overflow.

Long Frames

Total number of frames received on this port which exceeded the maximum frame length.

Short Frames

Total number of frames received on this port which were less that 18 bytes.

Duplicate Ring Number

Indicates the number of times a frame which contains a duplicate ring number in the RIF field has been seen by the port.

Invalid RIF RC Field

Indicates the number of times a frame which contains an illegal Routing Control field has been seen by the port.

RIF Length Exceeded

Indicates the number of times a frame which contains a RIF field which is too long has been seen by the port.

Explorer Overflow

Indicates the number of times that an explorer frame has been dropped because of explorer rate throttling.

Ring Number Mismatch

Indicates the number of times that an incoming frame did not correctly include the port's ring number.

Config Loss

Number of configuration loss events after the port has completed the join process and then lost communication.

Config Loss Reason

Latest Config Loss error code. Possible values are:

- *None*
- *Wire Fault* - Wire fault.
- *Lobe Test* - Lobe test failure.
- *HDX in FDX* - HDX MAC frame received in FDX mode.
- *Heart Beat* - Heart beat failure.
- *FDX New Sta* - FDX new station.
- *Auto* - Disable reason.

Last Reset

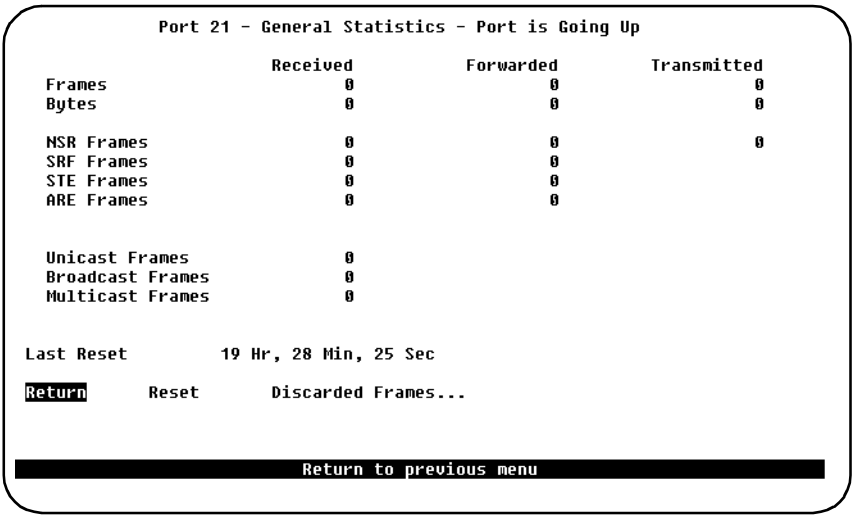
Time since last reset of port statistics.

General Statistics Screen for Fast Ethernet Ports

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Fast Ethernet port number, 21, 22, 25, or 26.
3. Select **General Statistics**...

For a Fast Ethernet port, the screen shows the number of frames and bytes received, forwarded and transmitted on the port. These numbers include traffic for all virtual ports. The screen will automatically update itself every 5 seconds.



Frames Forwarded
Frames received from Fast Ethernet and forwarded to other ports in the switch.

Frames Transmitted
Frames transmitted to Fast Ethernet.

Frames Received
Frames received from Fast Ethernet, but not necessarily forwarded.

NSR Frames Forwarded
Number of non source-routed frames forwarded by the port.

SRF Frames Forwarded
Number of source-routed frames forwarded by the port.

STE Frames Forwarded
Number of Spanning Tree Explorer frames forwarded by the port.

ARE Frames Forwarded
Number of All Route Explorer frames forwarded by the port.

Unicast Frames
Number of Unicast frames forwarded.

Broadcast Frames Received
Number of broadcast frames received on this port without errors.

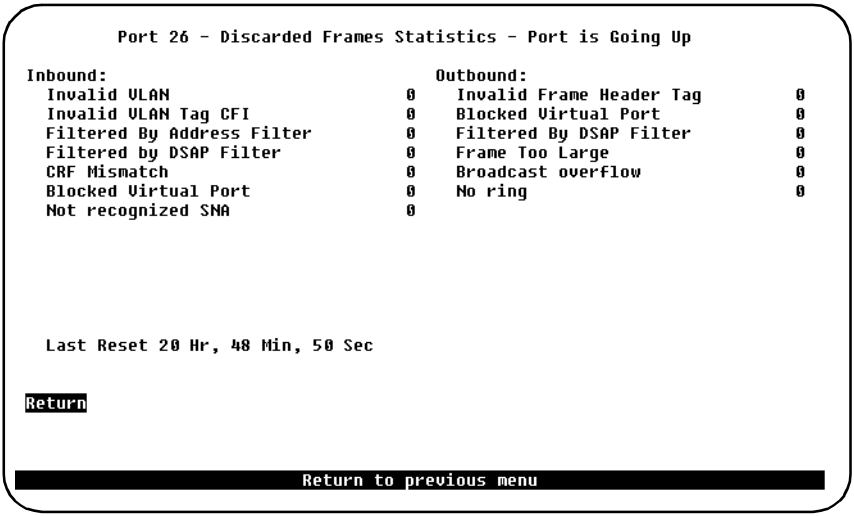
Multicast Frames Received
Number of multicast frames received on this port without errors.

Discarded Frames
Opens the **Discarded Frames** screen. See below.

Discarded Frames Screen

To open this screen , do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Fast Ethernet port number, 21, 22, 25, or 26.
3. Select **General Statistics**...
4. Select **Discarded Frames...**



This screen shows the number of frames discarded on the Fast Ethernet port in both inbound (from Fast Ethernet) and outbound (to Fast Ethernet) directions. The discard reasons are described in the following sections.

Discarded Inbound Frames

The following discard reasons are defined for inbound frames:

Invalid VLAN

A frame was received on an unknown VLAN. This is either a VLAN tagged frame containing an unknown VLAN ID, or an untagged frame when no untagged virtual ports are defined. Make sure that the 802.1Q VLAN ID and virtual port tagging mode is set to the same value on both sides of the connection.

Invalid VLAN Tag CFI

A VLAN tagged frame with an invalid Canonical Format Indicator (CFI) was received. The CFI is a bit in the Tag Control Information field of a VLAN tag. This

bit indicates the bit order of any MAC addresses in the information field. It is 0 for Ethernet format and 1 for Token-Ring format. It should always be 1 in received frames.

Filtered by Address Filter

The frame by discarded because of a MAC address filter.

Filtered by DSAP Filter

The frame by discarded because of a protocol (DSAP or protocol type) filter.

CRF Mismatch

The frame is discarded because the destination MAC address or destination source route hop is registered as local for the virtual port. That is, the frame would have to be forwarded back to same port. This might be due to an error in the configured 802.1Q VLAN ID for one or more VLANs.

Blocked Virtual Port

The frame is discarded because the virtual port is currently not in forwarding state.

Unrecognized SNA

Number of unrecognized SNA frames.

Discarded Outbound Frames

The following discard reasons are defined for outbound frames:

Invalid Frame Header Tag

A frame could not be transmitted because it has an invalid internal frame header tag (note that this internal frame header tag is not the same thing as the VLAN tag).

Blocked Virtual Port

The frame is not transmitted because the virtual port is currently not in forwarding state.

Filtered by DSAP Filter

The frame is not transmitted because of a protocol (DSAP or protocol type) filter.

Frame Too Large

The frame is larger than the maximum frame size, which has been configured for the virtual port. Please refer to the “Virtual Port Configuration” section on page 78.

Broadcast Overflow

Number of broadcast frames dropped because the ring number was exceeded.

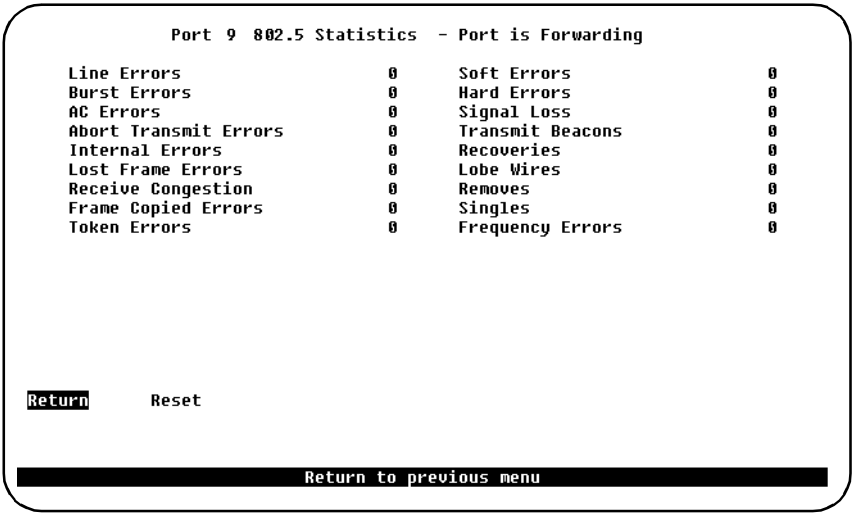
No Ring

Number of frames dropped because the ring number was unknown.s.

802.5 Statistics Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **802.5 Statistics**...



Line Errors

This counter is incremented when a frame or token is copied or repeated by a station, the E bit is zero in the frame or token, and one of the following conditions exists: 1) there is a non-data bit (J or K bit) between the SD and the ED of the frame or token, or 2) there is an FCS error in the frame.

Burst Errors

This counter is incremented when a station detects the absence of transitions for five half-bit timers (burst-five error).

AC Errors

Number of times a station received an Active Monitor Present (AMP) frame or a Standby Monitor Present (SMP) frame in which both the address recognized (A) bit and the frame copied (C) bit are set to 0, indicating that no station has recognized

the destination address and copied the frame, and then receives another SMP frame in which both the address recognized bit and the frame copied bit are set to 0 without first receiving an AMP frame. This condition indicates a station that cannot set the address recognized and the frame copied bits properly.

Abort Transmit Errors

This counter is incremented when a station transmits an abort delimiter while transmitting.

Internal Errors

This counter is incremented when a station recognizes an internal error.

Lost Frame Errors

This counter is incremented when a station is transmitting and its TRR timer expires. This condition denotes a condition where a transmitting station in strip mode does not receive the trailer of the frame before the TRR timer goes off.

Receive Congestion

This counter is incremented when a station recognizes a frame addressed to its specific address, but has no available buffer space indicating that the station is congested.

Frame Copied Errors

This counter is incremented when a station recognizes a frame addressed to its specific address and detects that the FS field A bits are set to 1 indicating a possible line hit or duplicate address.

Token Errors

This counter is incremented when a station acting as the active monitor recognizes an error condition that needs a token transmitted.

Soft Errors

The number of Soft Errors the port has detected. It directly corresponds to the number of Report Error MAC frames that this port has transmitted. Soft Errors are those which are recoverable by the MAC layer protocols.

Hard Errors

The number of times this port has detected an immediately recoverable fatal error. It denotes the number of times this port is either transmitting or receiving beacon MAC frames.

Signal Loss

The number of times this port has detected the loss of signal condition from the ring.

Transmit Beacons

The number of times this port has transmitted a beacon frame.

Recoveries

The number of Claim Token MAC frames received or transmitted after the port has received a Ring Purge MAC frame. This counter signifies the number of times the ring has been purged and is being recovered back into a normal operating state.

Lobe Wires

The number of times the port has detected an open or short circuit in the lobe data path. The adapter will be closed and **Ring State** will signify this condition.

Removes

The number of times the port has received a Remove Ring Station MAC frame request. When this frame is received the port will enter the closed state.

Singles

The number of times the port has sensed that it is the only station on the ring. This will happen if the port is the first one up on a ring, or if there is a hardware problem.

Frequency Errors

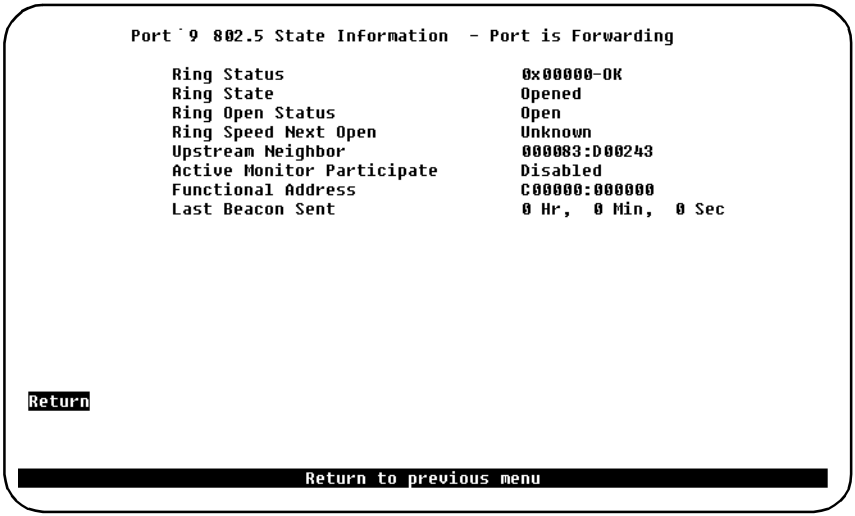
The number of times the port has detected that the frequency of the incoming signal differs from the expected frequency by more than that specified by the IEEE 802.5 standard.

802.5 State Information Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **802.5 State Information**...

This screen provides IEEE 802.5 state information.



Ring Status

The current port status on the ring. This could be used to diagnose fluctuating problems that can occur on token rings, after a station has successfully been added to the ring. This field has the general format "0x##### - text string" where ##### is a hexadecimal error code value, and 'textstring' can be *No Status, OK*, or a short text string indicating an error. Before an open is completed, the field has the value: *0x20000 - No Status*. If no problems are detected, this field will display *0x00000 - OK*.

Error conditions are indicated by 0x##### and a text string identifying the error. The text 'see below' may also be displayed. In this case the error text is displayed further down on the screen.

Ring State

The current port state with respect to entering or leaving the ring. Possible values are: *Opened, Closed, Opening, Closing.*

Ring Open Status

This field indicates the success, or the reason for failure, of the station's most recent attempt to enter the ring. Possible values are: *No Open, Lobe Failed, Signal Loss, Insertion Timeout, Ring Failed, Beaconing, Duplicate MAC Address, Request Failed, Remove Received, Open*.

Ring Speed Next Open

Indicates the ring speed that will be attempted at the next open. Possible values are: *Unknown, 4 Mbps, 16 Mbps*. Unknown can indicate that the port will attempt to auto insert into the ring.

Upstream Neighbor

The MAC address of the upstream neighbor station in the ring.

Active Monitor Participate

If this field has a value of *Enabled*, then this port will participate in the active monitor selection process. If the value is *Disabled* then it will not.

Functional Address

The bit mask of all Token-Ring functional addresses for which this port will accept frames.

Last Beacon Sent

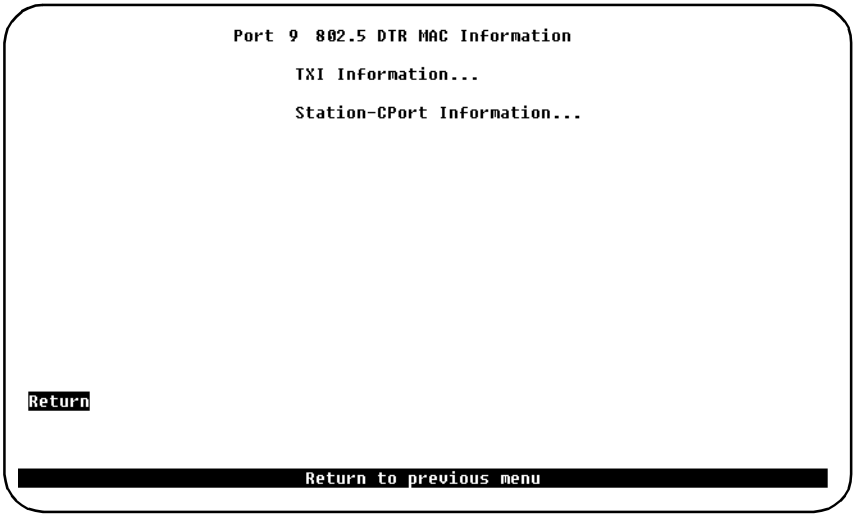
The elapsed time since a beacon frame was last sent on this port.

802.5 DTR MAC Information Menu

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **802.5 DTR MAC Information**...

The **802.5 DTR MAC Information** menu provides access to the appropriate DTR information screen.



TXI Information...

Displays the **TXI Information** screen.

Station-CPort Information...

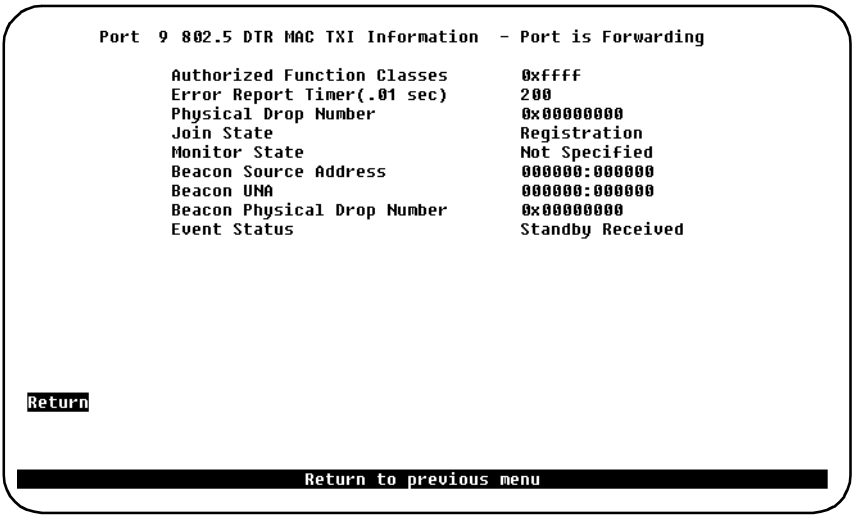
Displays the **Station-CPort Information** screen.

TXI Information Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **802.5 DTR MAC Information**...
4. Select **TXI Information...**

The **TXI Information** screen provides information about IEEE 802.5 DTR MAC TXI.



Authorized Function Classes

Functional classes that a node is enabled to transmit. This field displays the value set by the Authorized Function Classes subvector X'06' of the Change Parameters MAC frame. Valid range is from *0x0000* to *0xFFFF*. Each bit that is enabled('1') corresponds to a function class that is enabled.

Error Report Timer

Timeout value of the ring station's soft error report timer. This field displays the value of the timer TSER as set by the Error Timer Value subvector X'05' from the Change Parameters or the Initialize Station MAC frame. This object indicates the value in .01 second increments.

Physical Drop Number

Physical location of the sending ring station. This field displays the value set by the

Assign Physical Drop Number subvector X'04' of the Change Parameters or the Initialize Station MAC frame. Valid range is from *0x00000000* to *0xFFFFFFFF*.

Join State

This field displays the present state of the Join FSM. Possible values are *Not Specified, Bypass, Registration, Lobe Test, Dup Addr Check, Dup Addr Det, Join Complete* and *Await Notify*.

Monitor State

This field displays the present state of the Monitor FSM. Possible values are *Not Specified, Operational, Transmit Beacon, Wire Fault Delay,* and *Int Test Wait*.

Beacon Source Address

This field displays the source address used in the last Beacon MAC frame transmitted or received.

Beacon UNA

This field displays the value of the UNA subvector X'02' used in the last Beacon MAC frame transmitted or received. It will indicate the individual MAC address of the sending ring station's nearest active upstream neighbor (NAUN). The value could be a valid individual MAC address or *Unknown*.

Beacon Physical Drop Number

Physical location of the sending ring station. This field displays the value of the Physical Drop Number subvector X'0B' used in the last Beacon MAC frame transmitted or received. Valid range is from *0x00000000* to *0xFFFFFFFF*.

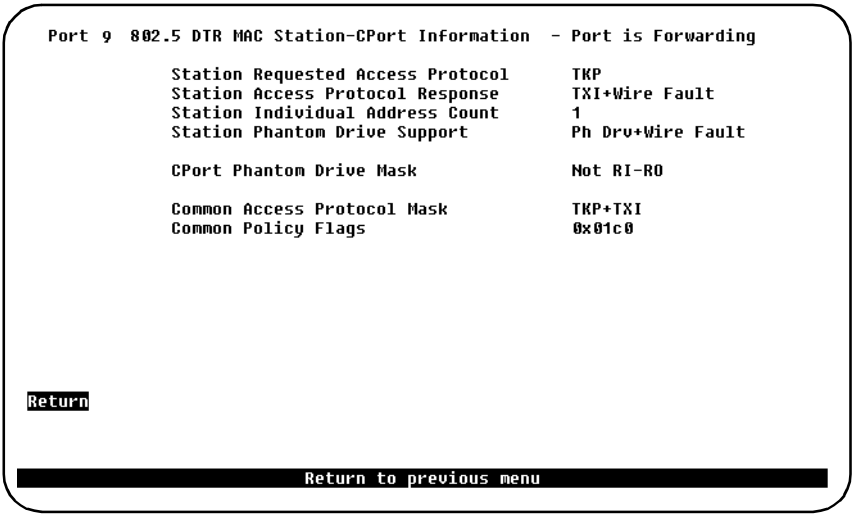
Event Status

This field displays the latest event status of the TXI interface. Possible values are *Insert REQ Rec, Insert RPS Rec, Report Error, Heart Beat Lost, Signal Loss, Beacon Received, Remove, Internal Error, Station/CPort Err, Wire Fault, Claim Received, Purge Received, Standby Received, Invalid SA, Act Mon Recvd, Phantom Loss,* and *Dup Addr Det*.

Station-CPort Information Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Token-Ring port number, 1 - 20.
3. Select **802.5 DTR MAC Information**...
4. Select **Station-CPort Information...**



Station Requested Access Protocol

Protocol requested for station access. This field displays the value of the Access Protocol Request subvector X'0E' transmitted in the Registration Request MAC frame. Possible values are *TXI* and *TKP*.

Station Access Protocol Response

Response to protocol request. This field displays the value of the Access Protocol Response subvector X'0F' received from the Registration Response MAC frame. Possible values are *Access Denied* and *FDX+Wire Fault.*

Station Individual Address Count

This field displays the number of individual addresses supported by the MAC and used in the Individual Address Count subvector X'21'. This field will always display the value *1*.

Station Phantom Drive Support

This field displays the MAC's support of Phantom Drive and Wire Fault detection.

It indicates the value of the SPV(PD) variable and the value of the Phantom subvector X'0C' used in the Registration Request MAC frame. This field will always display *Ph Drv+Wire Fault* for Phantom Drive and Wire Fault support.

CPort Phantom Drive Mask

This field displays the value of the C-Port policy variable PPV(PD_MASK). It represents the Phantom Drive and Wire Fault detection methods supported by the C-Port. Possible values are *RI-RO* and *Not RI-RO*.

Common Access Protocol Mask

This field displays which access protocols can be supported by the PMAC. It displays the value of the PPV(AP_MASK). Possible values for this field are *TKP*, *TXI* and *TKP+TXI*.

Common Policy Flags

This field displays the station policy flags as a hexadecimal value of the form 0x####.

802.3 Statistics Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Fast Ethernet port number, 21, 22, 25, or 26.
3. Select **802.3 Statistics**...

```
            Port 21 - 802.3 Statistics - Port is Up

  Bytes Received              2252821  Carrier Check Failures          0
  Bytes Transmitted             33083  Short Circuits                  0
  Frames Received               15556  Open Circuits                   0
  Frames Transmitted              180  Remote Failures                 0
  Multicast Bytes Received     380442  CRC Errors                      0
  Multicast Frames Received      5076  Framing Errors                  0
  Frms Transmitted, Deferred        0  Frames Too Long                 0
  Single Collisions                 0  Data Overrun                    0
  Multiple Collisions               0  System Buffers Unavailable      0
  Excessive Collisions              0  User Buffer Unavailable         0
                                       Frames Congested                0

Return      Reset

                        Return to previous menu
```

Bytes Received

Number of bytes received on this port.

Bytes Transmitted
Number of bytes transmitted by this port.

Frames Received
Number of frames received on this port.

Frames Transmitted
Number of frames transmitted by this port.

Multicast Bytes Received
Number of bytes in multicast frames received on this port.

Multicast Frames Received
Number of multicast frames received on this port without errors.

Frms Transmitted, Deferred
Number of frames transmitted by this port, but initially deferred.

(The 21143 Fast Ethernet transceiver had to defer while ready to transmit a frame because the carrier was asserted.)

Single Collisions
Number of frames transmitted by this port after single collision.

Multiple Collisions
Number of frames transmitted by this port after multiple collision.

Excessive Collisions
Number of frames dropped because of excessive collisions.

Carrier Check Failures
Number of frames dropped because of late collision and loss of carrier.

Short Circuits
Number of frames dropped because of short circuits.

Open Circuits
Number of frames dropped because of open circuits.

Remote Failures
Number of frames dropped because of remote failures.

CRC Errors
Number of frames received on this port with a CRC error.

Framing Errors
Number of frames dropped because of framing errors.

Frames Too Long
Number of frames received with a length greater than the maximum lenght receivable.

Data Overrun
Number of frames dropped because of data overrun.

System Buffers Unavailable
Number of frames dropped because of lack of system received buffers.

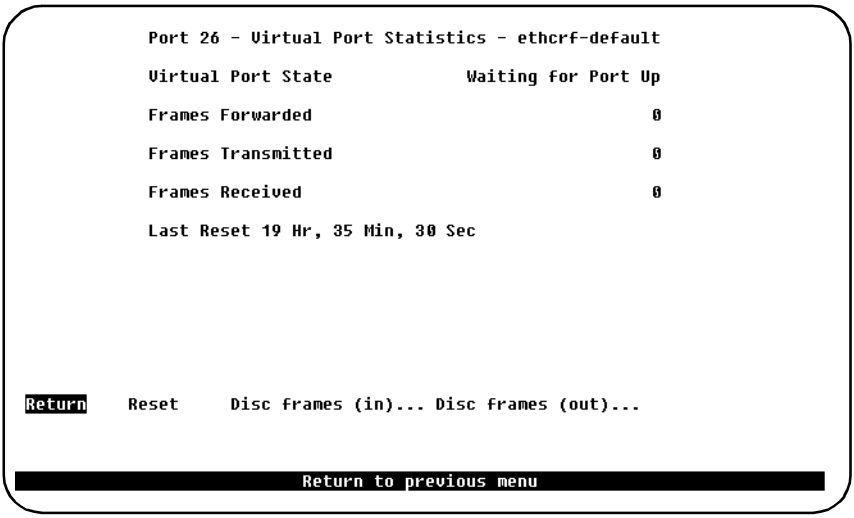
User Buffer Unavailable
Number of tries of buffer allocation.

Frames Congested
Number of frames congested, due to lack of space in Tx queue.

Virtual Port Statistics Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics → Port Statistics.**
2. Enter a Fast Ethernet port number, 21, 22, 25, or 26.
3. Select **Virtual Port Statistics...**



This screen dispays some counters for the virtual ports. If more than one virtual port is defined for the Fast Ethernet port the requested virtual port must first be selected by choosing from a list of CRFs.

Virtual Port State

This is the current state of the virtual port. Refer to section “Virtual Port Configuration” in Chapter 3, “Switch Configuration” for details.

Frames Forwarded

The number of LLC frames received and forwarded on this virtual port.

Frames Transmitted

The number of LLC frame transmitted on this virtual port.

Frames Received

The number of LLC frames received, but not necessarily forwarded on this virtual port.

Reset

Also shown is the time since the last reset of these counters. Select **Reset** to reset the counters on this screen.

Discarded Frames Statistics

When **Disc Frames (in)** or **Disc Frames (out)** is selected from the Virtual Port Statistics menu, counters of discarded frames are displayed. Depending on which option was chosen (in or out), inbound or outbound statistics are displayed.

Inbound Discarded Frames Statistics - No Translation

IP

Number of frames dropped because IP translation is disabled or inbound frames are received from Ethernet in a format different than that specified in the Fast Ethernet configuration dialog.

IPX

Number of frames dropped because IPX translation is disabled or inbound frames are received from Ethernet in a format different than that specified in the Fast Ethernet configuration dialog.

NetBios

Number of frames dropped because NetBios translation is disabled or inbound frames are received from Ethernet in a format different than that specified in the Fast Ethernet configuration dialog.

SNA

Number of frames dropped because SNA translation is disabled or inbound frames are received from Ethernet in a format different than that specified in the Fast Ethernet configuration dialog.

Generic w/SNAP

Number of frames dropped because this translation is disabled or inbound frames are received from Ethernet in a format different than that specified in the Fast Ethernet configuration dialog.

Generic w/o SNAP

Number of frames dropped because this translation is disabled.

Inbound Discarded Frame Statistics - Translation Errors

IP

Number of frames dropped because of IP translation errors.

IPX

Number of frames dropped because of IPX translation errors.

NetBios

Number of frames dropped because of NetBios translation errors.

SNA

Number of frames dropped because of SNA translation errors.

Generic w/SNAP

Number of frames dropped because of translation errors for generic frames with SNAP.

Generic w/o SNAP

Number of frames dropped because of translation errors for generic frames without SNAP.

Outbound Discarded Frame Statistics - No Translation

IP

Number of frames dropped because IP translation is disabled.

IPX

Number of frames dropped because IPX translation is disabled or outbound frames received from Token-Ring in different format than specified in Fast Ethernet configuration dialog.

NetBios

Number of frames dropped because NetBios translation is disabled.

SNA

Number of frames dropped because SNA translation is disabled.

Generic w/SNAP

Number of frames dropped because translation is disabled for generic frames with SNAP.

Generic w/o SNAP

Number of frames dropped because translation is disabled for generic frames without SNAP.

Outbound Discarded Frame Statistics - Translation Errors

IP

Number of frames dropped because of IP translation errors.

IPX

Number of frames dropped because of IPX translation errors.

NetBios

Number of frames dropped because of NetBios translation errors.

SNA

Number of frames dropped because of SNA translation errors.

Generic w/SNAP

Number of frames dropped because of translation errors for generic frames with SNAP.

Generic w/o SNAP

Number of frames dropped because of translation errors for generic frames without SNAP.

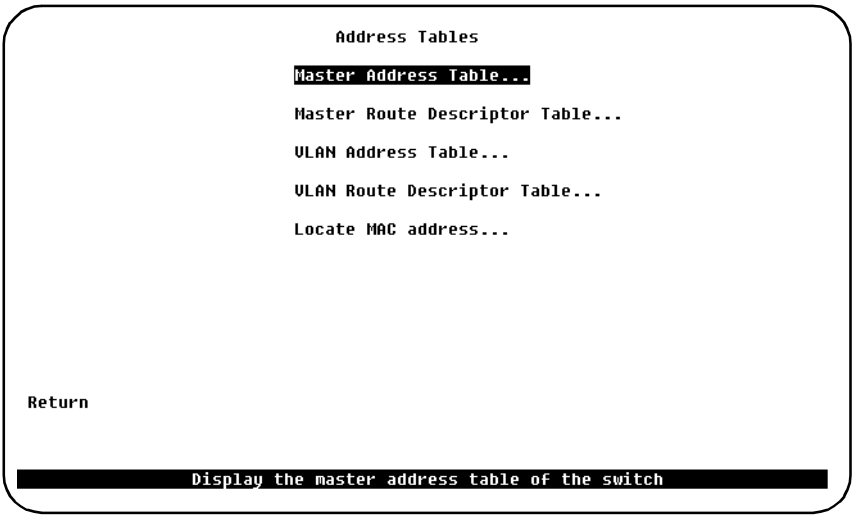
Fragmentation error

IP only. Number of frames dropped because IP fragmentation finished with an error or an IP frame was received with the Don't Fragment bit set.

Address Tables Menu

To open this menu from the main menu, select **Statistics → Address Tables.**

Use the **Address Tables** menu to select which address table statistics you want to view.



Information on each of the submenus and screens is given in the next sections.

Master Address Table Screen

To open this menu from the main menu, select **Statistics → Address Tables → Master Address Table.**

The **Master Address Table** screen contains MAC addresses of all the ports known to the switch. The table can contain up to 10,000 entries memory. See a detailed description of MAC Adresses onpage 46.

```
                          Master Address Table

Address       Type                  Ports (Filtered:high-lighted, Trunks:Bold)
000083:687DB9 Known-TR Port 17      17
000083:8DF740 Switch Base Address   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
000083:8DF760 trbrf-default         1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
000083:E346B4 Known-TR Port 17      17
000083:E346C0 Known-TR Port 17      17
000083:E34B40 Known-TR Port 17      17
800143:000000 STP Multicast         1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
800778:020200 STP Multicast-Cisco   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
C00000:000100 STP Multicast-IBM     1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
C000FF:FFFFFF Broadcast             1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
                                     17 18 19 20
Return      More      Search

                          Return to previous menu
```

Address

MAC address of a node.

Type

The **Type** column of the **Master Address Table** screen can contain the following types:

- *Switch Base Address*
  - — The burned-in or configured MAC Address of the switch box.
  - — Present on all ports.
- <VLAN Name>
  - — The MAC Address used by the IP Protocol Stack for the specified VLAN.
  - — Present on all ports of that VLAN.

- *Known-*<port type> *Port* <nn>
  - A known address on Port nn
  - Port type = TR: The address is known at the specified token-ring port.
  - The address will be present at port nn
  - Port type = STK: The address is known at a port of another switch in the stack.

    If the address has occurred as a destination address in incoming frames at other ports, it will be present in these ports too.
- *Unknown*
  - The address is a unicast address and has occurred as a destination address in incoming frames at one or more ports. The switch has however not yet learned the location of the address because the station has not sent any response frames.
- *Multicast*
  - The address is a group address or a functional address and has occurred as a destination address in incoming frames at one or more ports.
- *STP Multicast*
  - The group address used as a destination address in IEEE Spanning Tree Protocol frames.
  - Present on all ports.
- *STP Multicast-Cisco*
  - The group address used as a destination address in Cisco Spanning Tree Protocol frames.
  - Present on all ports.
- *STP Multicast-IBM*
  - The functional address used as a destination address in IBM Spanning Tree Protocol frames.
  - Present on all ports.
- *Broadcast*
  - One of the token-ring broadcast addresses.
  - Present on all ports.
- *STP Port* <nn>
  - The MAC Address of port nn

Ports

The ports whose address tables include this MAC address; filtered ports are highlighted.

More

Refreshes a one-page table or displays subsequent entries on a larger table.

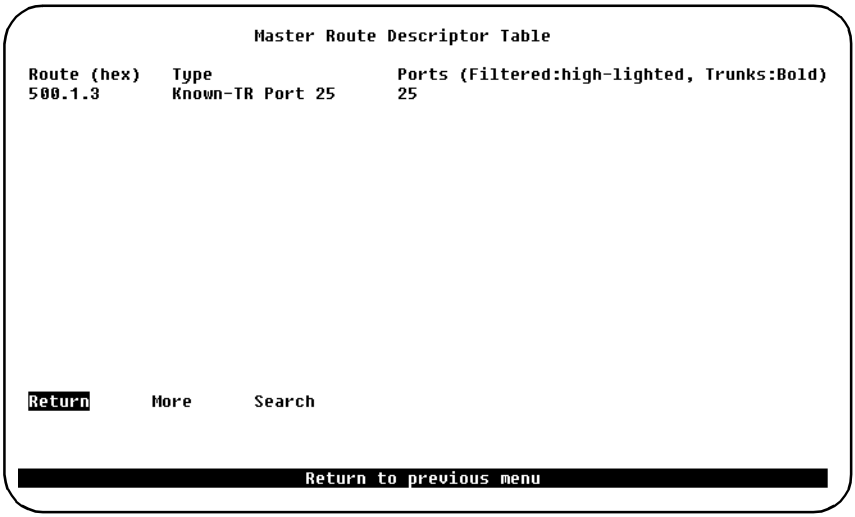
Search

Prompts you to enter the MAC address of a node and the ports whose address tables you want to search, then displays the ports whose address tables contain the MAC address.

Master Route Descriptor Table Screen

To open this menu from the main menu, select **Statistics → Address Tables → Master Route Descriptor Table.**

The **Master Route Descriptor Table** lists the learned route descriptors in the switch master table. These descriptors are contained within the 10,000 entries allowed for the master address table.



Route (hex)

The route descriptor triplet: Ring In.Bridge Number.Ring Out. This field will always have the format ###.#.### (displayed in hexadecimal). Ring numbers are in the range *001–FFF*, bridge numbers are in the range *0–F*.

Type

The **Type** column of the **Master Route Descriptor Table** can contain the following types:

- *Known*-<port type> *Port* <nn>:
  - — A known route descriptor (bridge) on Port nn.
  - — Port type = TR: The route descriptor is known at the specified token-ring port.
  - — The route descriptor will be present at port nn.
  - — Port type = STK: The route descriptor is known at a port of another switch in the stack.

    If the route descriptor has occurred as next hop in the RIF of incoming frames at other ports, it will be present in these ports too.
- *Unknown*:
  - — The route descriptor has occurred as next hop in the Route Information Field of incoming frames at one or more ports. The switch has however not yet learned the location of the route descriptor (bridge) because the target station has not sent any response frames.

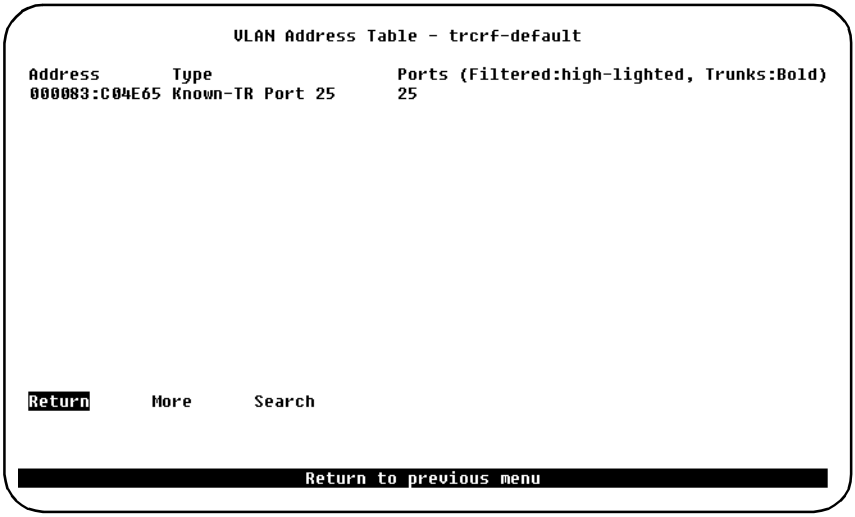
Ports

Ports of the switch whose address table includes this route descriptor.

VLAN Address Table screen

To open this menu, do the following:

1. From the main menu, select **Statistics → Address Tables.**
2. Select VLAN Address Table.
3. Select a CRF, when prompted. The **VLAN Address Table** screen appears.

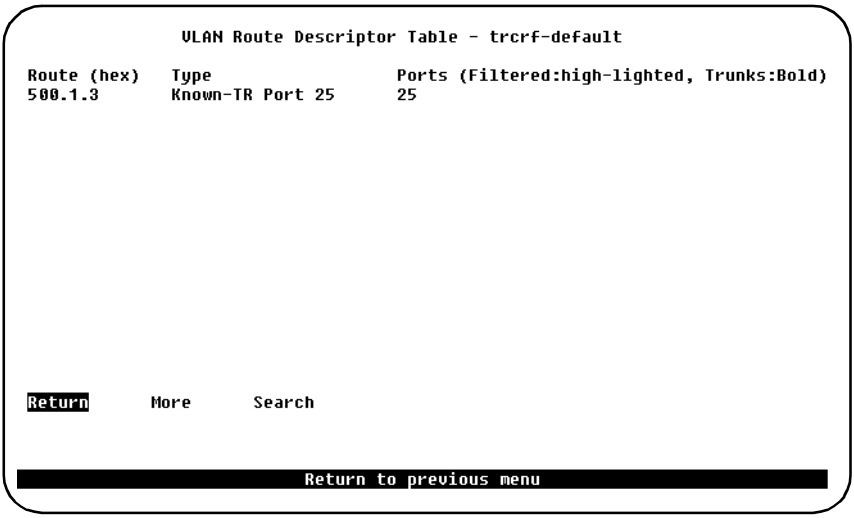


For a description of the fields and their meanings, see the section “Master Address Table Screen” above.

VLAN Route Descriptor Table Screen

To open this menu, do the following:

1. From the main menu, select **Statistics → Address Tables.**
2. Select **VLAN Route Descriptor Table**.
3. Select a CRF, when prompted. The **VLAN Route Descriptor Table** appears.



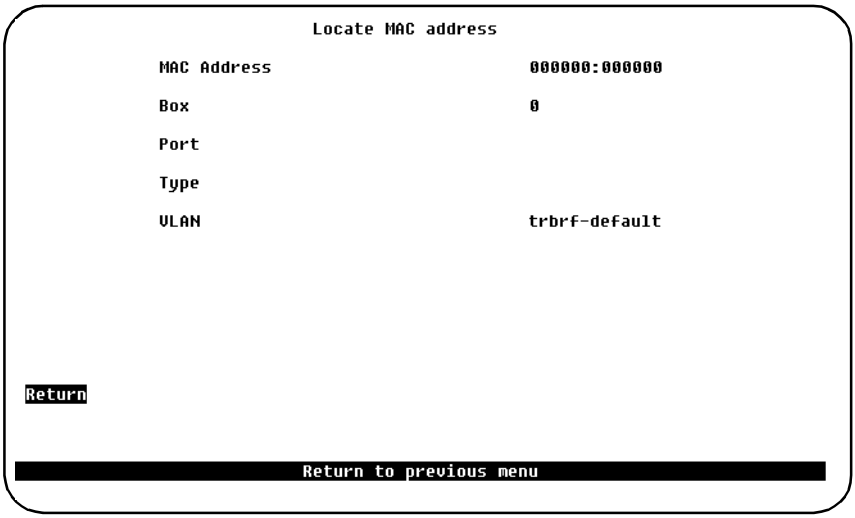
For a description of the fields and their meaning, see the section “Master Route Descriptor Table Screen” above.

Locate MAC Address Screen

To open this menu, do the following:

1. From the main menu, select **Statistics → Address Tables.**
2. Select **Locate MAC Address**.

Use this screen to locate a computer in the network.



MAC Address

The MAC address of the a computer on the network. Type in the address you want to locate.

Box

The stack number of the switch on which the MAC address is recognized.

The value can be *1 - 8*.

Port

The number of the switch port on which the MAC address is recognized.

The value can be *1 - 28*.

Type

The port type, as described in the **Master Addre ss Table** screen, see page 166.

VLAN

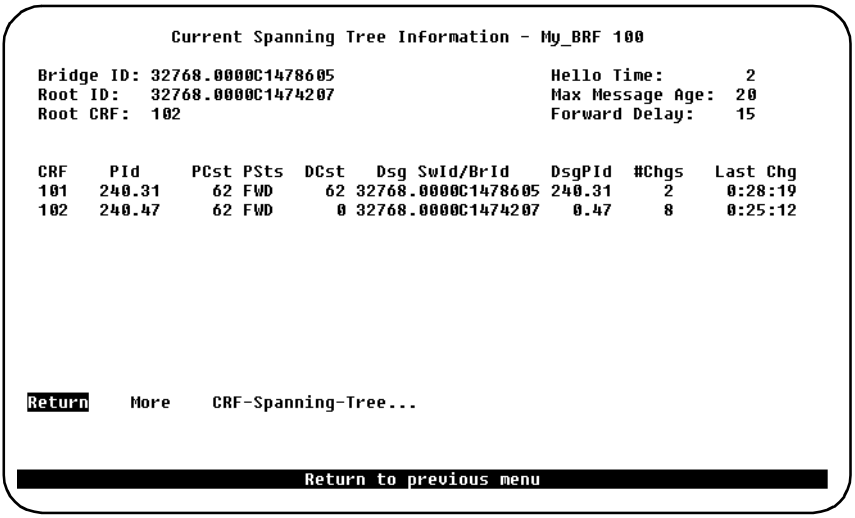
The first VLAN to which the MAC address is known.

Current Spanning Tree Information Screen

To open this screen from the main menu, select **Statistics → Current Spanning Tree Information.**

Use the **Current Spanning Tree Information** screens to view a summary of all STP information for each port. Information on this screen cannot be changed. When the STP is turned off—that is, you have selected *No* for the **Participate in Spanning Tree** prompt (at the **Configuration** menus)—this menu will only display the headers with no information below them.

When the switch is configured with CrossLink channels, STP packets use the primary Token-Ring port of the CrossLink.



Bridge ID

Priority and MAC address of this bridge.

Root ID

Priority and MAC address of the root bridge.

Root CRF

The VLAN ID of the TrCRF that is closest to the root. This switch communicates with the root through this TrCRF.

Hello Time

Time (in seconds) that the root waits between sending configuration messages. This time is advertised by the root and used by all devices and switches in the active topology of the spanning-tree network.

Max Message Age

Time at which the configuration message used by the spanning-tree algorithm should be discarded. This time is advertised by the root and used by all devices and switches in the active topology of the spanning-tree network.

Forward Delay

Time the root waits between transitions from listening to learning, and from learning to forwarding. This time is advertised by the root and used by all devices and switches in the active topology of the spanning-tree network.

CRF

VLAN ID of a TrCRF belonging to this TrBRF.

PId

Port ID that is used to determine the role of the port in the spanning tree. The port ID is expressed in the form *port priority.port number*.

PCst

Cost associated with each port. Lower numbers are generally assigned to ports attached to faster media (such as FDX or CrossLinks), and higher numbers are generally assigned to ports attached to slower media.

PSts

Current status of this CRF within the spanning tree. Possible values are:

- *DIS* (Disabled)
- *BLK* (Blocked)
- *LSN* (Listening)
- *LRN* (Learning)
- *FWD* (Forwarding)

The rules that define the state of the port are as follows:

- A CRF that does not connect to other switches or bridges is always forwarding.
- When the switch is booted, all CRFs are blocked initially, and then some of them change to a different state: listening, learning, and forwarding, in that order. All CRFs that are going to change states from blocking to forwarding will have done so after two to three times the value of:
  Switch Maximum Message Age + (2 x **Switch Forward Delay**)

DCst

Cost for a packet to travel from this CRF to the root in the current spanning-tree configuration. The slower the media, the higher the cost.

Dsg SwId/BrId

Priority and MAC address of the device through which this port has determined it must communicate with the root of the spanning tree.

Dsg PId

Port on the designated bridge through which this switch will communicate with the root of the spanning tree. This information is useful if the switch is the designated bridge on one or more network segments.

Chgs

Number of topology changes, that is, the number of times the CRF has entered the forwarding state plus the number of times the CRF has made the transition from forwarding to blocking. The counter is reset when the switch is reset or the spanning tree is turned on.

Last Chg

Time since the CRF last entered the forwarding state or made the transition from forwarding to blocking.

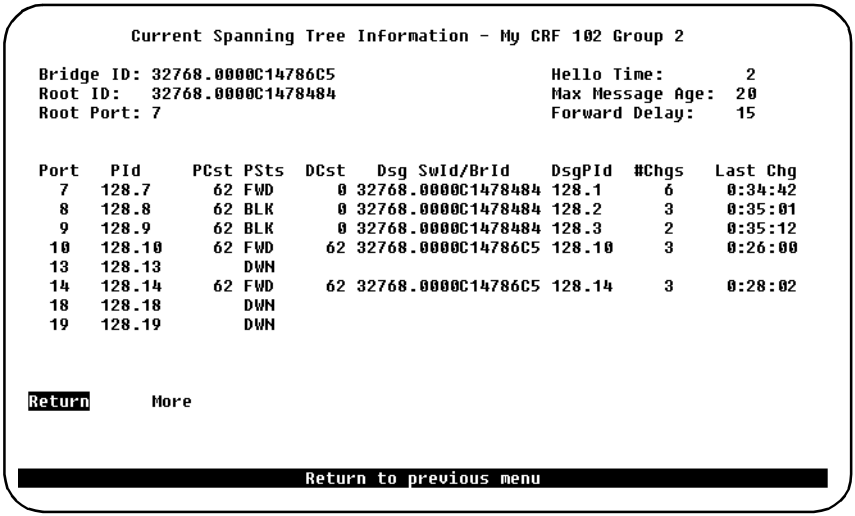
You cannot change any information on this screen. To change the spanning tree parameters, refer to the section “Spanning Tree for TrBRF Screen” on page 65.

Current Spanning Tree Information for a TrCRF Screen

To open this screen, do the following:

1. From the main menu, select **Statistics → Current Spanning Tree Information.**
2. Selec**t CRF-Spanning-Tree**. Select a CRF, when prompted.

This screen displays the spanning tree parameters for a TrCRF that belongs to the currently selected TrBRF**.**



The following information is displayed on this screen:

Bridge ID

Priority and MAC address of this bridge.

Root ID

Priority and MAC address of the root bridge.

Root Port

Number of the port on this switch that is closest to the root. This switch communicates with the root through this port. If this switch has been accepted as the root of the spanning tree network, this field displays *This Bridge*.

Hello Time

Time (in seconds) that the root waits between sending configuration messages. This time is advertised by the root and used by all devices and switches in the active topology of the spanning-tree network.

Max Message Age

Time at which the configuration message used by the spanning tree algorithm should be discarded. This time is advertised by the root and used by all devices and switches in the active topology of the spanning tree network.

Forward Delay

Time the root waits between transitions from listening to learning, and from learning to forwarding. This time is advertised by the root and used by all devices and switches in the active topology of the spanning tree network.

Port

Port number.

PId

Port ID that is used to determine the role of the port in the spanning tree. The port ID is expressed in the form *port priority.port number*.

PCst

Cost associated with each port. Lower numbers are generally assigned to ports attached to faster media (such as FDX or CrossLink), and higher numbers are generally assigned to ports attached to slower media (such as 2400-baud modem links).

PSts

Current status of this port within the spanning tree. Possible values are:

- *DIS* (Disabled)
- *BLK* (Blocked)
- *LSN* (Listening)
- *LRN* (Learning)
- *FWD* (Forwarding)
- *DWN* (Down)

The rules that define the state of the port are as follows:

- A port on a network segment that contains no other switch or bridge is always forwarding.
- If two ports of the switch are connected to the same network segment and there is no other bridge or switch, the port with the lower ID is forwarding and the other is blocked.

- When the switch is booted, all ports are blocked initially, and then some of them change to a different state: listening, learning, and forwarding, in that order. To see the change in states you must repeatedly exit from this menu, and then select it again. All ports that are going to change states from blocking to forwarding will have done so after two to three times the value of:

  Switch Maximum Message Age + (2 x **Switch Forward Delay**)

DCst

Cost for a packet to travel from this port to the root in the current spanning-tree configuration. The slower the media, the higher the cost.

Dsg SwId/BrId

Priority and MAC address of the device through which this port has determined it must communicate with the root of the spanning tree.

Dsg PId

Port on the designated bridge through which this switch will communicate with the root of the spanning tree. This information is useful if the switch is the designated bridge on one or more network segments.

Chgs

Number of topology changes, that is, the number of times the port has entered the forwarding state plus the number of times the port has made the transition from forwarding to blocking. The counter is reset when the switch is reset or the spanning tree is turned on.

Last Chg

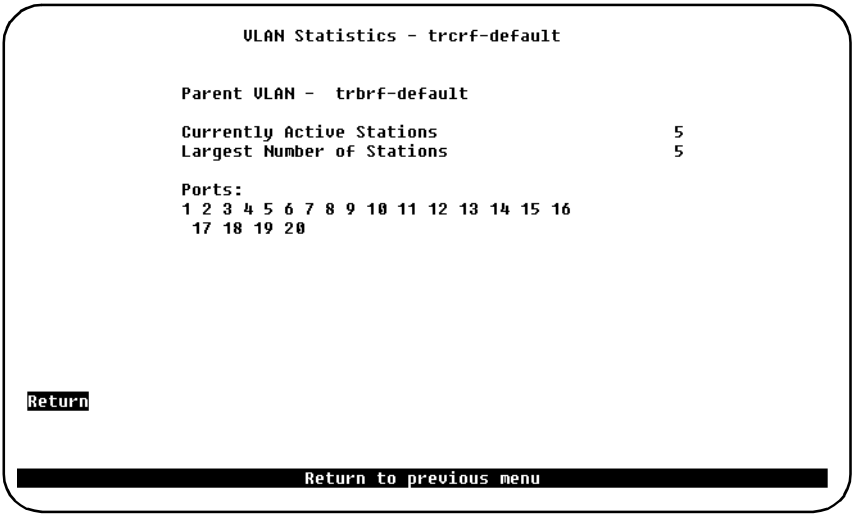
Time since the port last entered the forwarding state or made the transition from forwarding to blocking.

You cannot change any information on this screen. To change the spanning tree parameters, refer to the section “Spanning Tree for TrBRF Screen” on page 65.

VLAN Statistics Screen for TrCRF

To open the VLAN Statistics screen for TrCRF, do the following:

1. From the main menu, select **Statistics → VLAN Statistics.**
2. You will be prompted for a VLAN type. Select TrCRF.
3. You will be prompted to select a TrCRF. Select one. The **VLAN Statistics Screen for TrCRF** appears.



Parent VLAN

The parent TrBRF.

Currently Active Stations

Number of MAC addresses currently in the master address table that are recognized as ports belonging to this domain.

Largest Number of Stations

Largest number of MAC addresses in the master address table—since the last reset or power cycle—that are recognized by ports belonging to this domain.

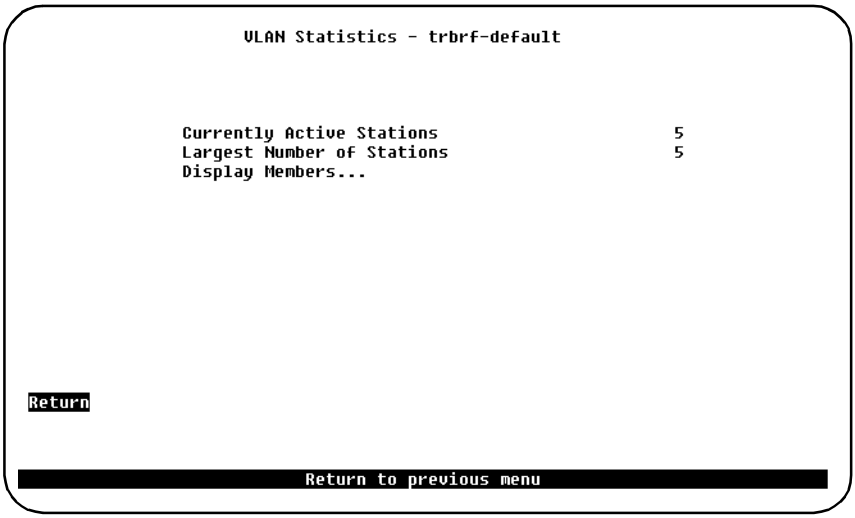
Ports

List of ports that belong to this TrCRF.

VLAN Statistics Screen for TrBRF

To open the VLAN Statistics screen for TrCRF, do the following:

1. From the main menu, select **Statistics → VLAN Statistics.**
2. You will be prompted for a VLAN type. Select TrBRF.
3. The **VLAN Statistics Screen for TrBRF** appears.



Currently Active Stations

Number of MAC addresses currently in the master address table that are recognized as ports belonging to this domain.

Largest Number of Stations

Largest number of MAC addresses in the master address table—since the last reset or power cycle—that are recognized by ports belonging to this domain.

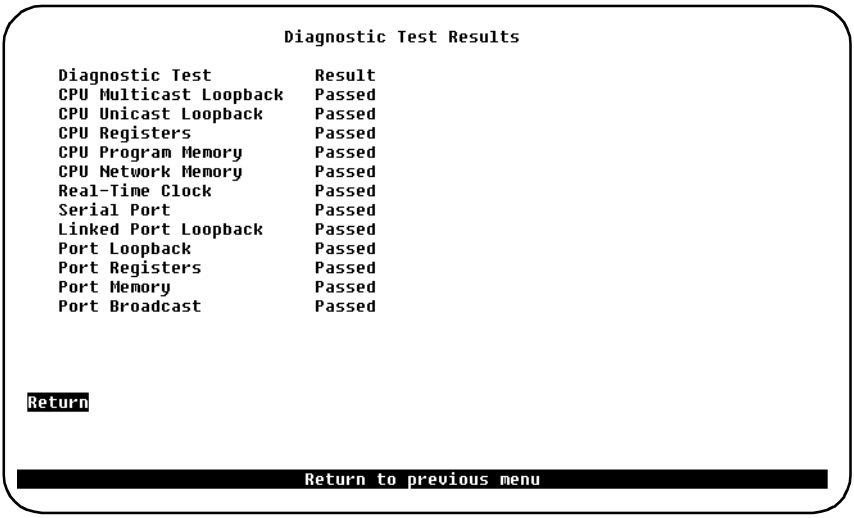
Display Members...

Selecting this item will open a new screen that lists all TrCRFs that are members of the TrBRF.

Diagnostic Test Results Screen

To open this screen from the main menu, select **Statistics → Diagnostic Test Results. (**If a prompt appears**,** enter the box number you want to view).

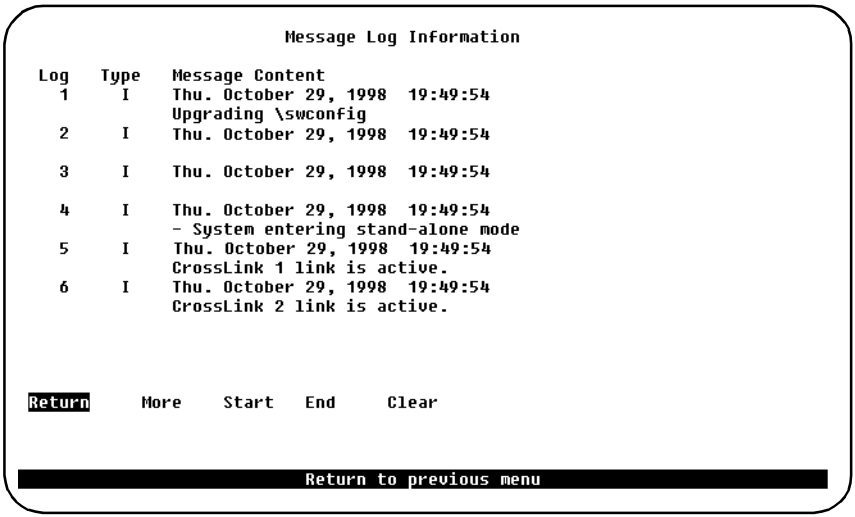
The **Diagnostic Test Results** screen is a list showing whether errors or a specific diagnostic test has failed at the switch. The data that is shown on this screen is for monitoring information only, and is meant for network personnel experienced with this type of information. The explanation of this information is extensive and outside the scope of this guide. However, the instructions on how to access this information is provided so that the user can view the data to provide information for problem solving. If this menu is reporting errors and you can not find a cause, contact your local place of purchase.



Message Log Information Screen

To open this screen from the main menu, select **Statistics → Message Log Information.**

The data on this screen is useful to technical experts in solving complex problems.



Log

Index number identifying the log file.

Type

Message type. Possible values are:

- *W*—Warning
- *I*—Informational

Message Content

The full text of the message.

More

Shows the next screen.

Back

Shows the previous screen (if any).

Start/End

Move to the first or last page.

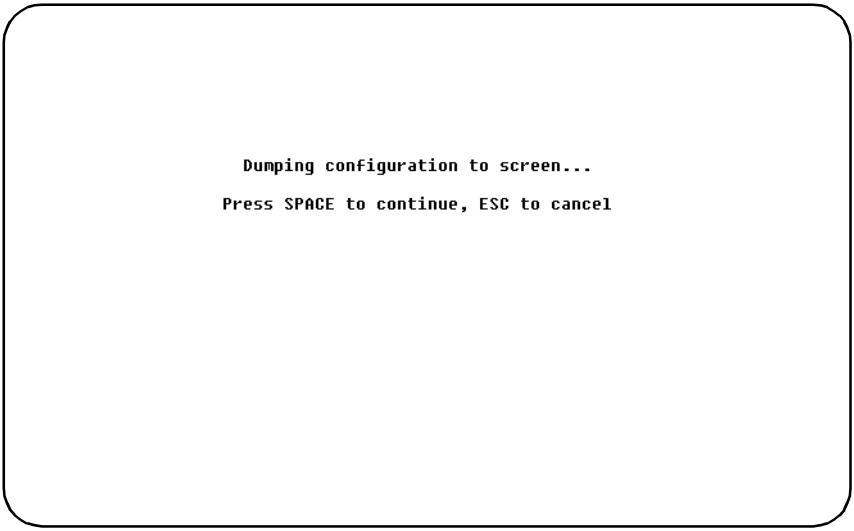
Clear

Clear all messages.

Display Summary Screen

To open this screen from the main menu, select **Statistics → Display Summary.**

This screen gives access to the most important switch configuration parameters to the console in a summary form. The information is suitable for capturing into an ASCII file by means of a capture function in the terminal emulation program used. This file will often be requested by the Olicom technical support personnel in case of troubleshooting:



SPACE

Pressing the SPACE key, you will start a screen report of all entered parameters, which runs through the display, until you stop it, or the bottom is reached. Press any key to return to the menu.

ESC

Pressing ESC, you cancel and return to previous menu.

❑

5. Monitoring the Network with SNMP

This chapter explains how to monitor the CrossFire 8730 Fast Ethernet Translation Switch from a network management system using an application that supports Simple Network Management Protocol (SNMP).

The following topics are described in this chapter:

- SNMP setup
- IP configuration
- SNMP configuration

SNMP Setup

Follow these steps to use in-band management:

1. Attach the switch to the console and start a console session as described in "Connecting a Network Management Console" in the *CrossFire 8730 Fast Ethernet Translation Switch User Guide.*
2. Make the necessary configurations in the **IP Configuration** screen.
3. Make the necessary configurations in the **SNMP Configuration** menu and the following subscreens:

- **Community String** screen
- **Trap Receiver** screen

The following sections describe the SNMP setup screens.

IP Configuration Screen

The **IP Configuration** screen sets the IP address, gateway address, subnet mask, and IP state.

The **IP Address** and **Default Gateway** must be in the same subnet address class—that is, Class A, Class B, or Class C. The system prevents you from entering values from different classes. If you do inadvertently enter an incorrect value, enter *0.0.0.0* in every field, then reenter the correct values.

Refer to **Chapter 3, "Switch Configuration"** for a complete description on how to configure the **IP Configuration** menu.

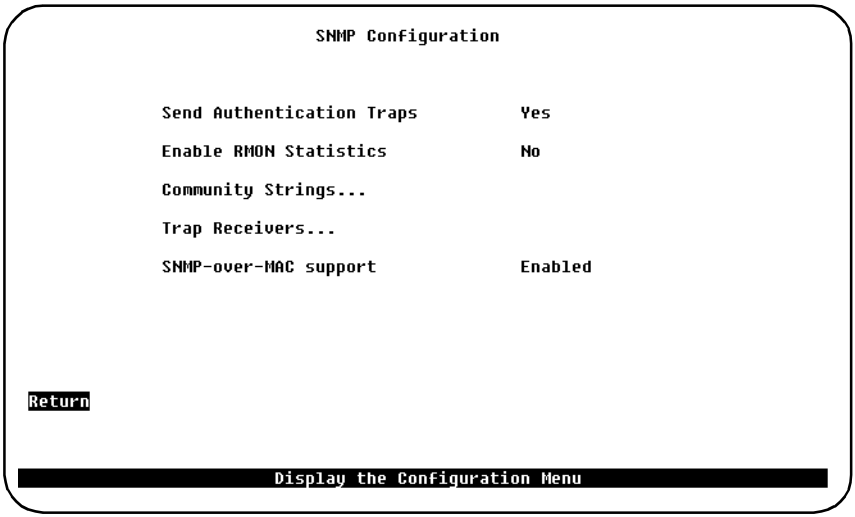
SNMP Configuration

Use the **SNMP Configuration** screen and all of its submenus to configure specific attributes related to SNMP.

SNMP Configuration Screen

To open this screen from the main menu, select **Configuration → SNMP Configuration.**

The **SNMP Configuration** screen is shown below.



Send Authentication Traps

Indicates whether SNMP should issue an authentication trap to trap receivers whenever an unauthorized request is detected.

Default: *Yes*

Enable RMON Statistics

Enables the gathering of a subset of the RMON statistics from the RMON MIB. The default setting is *No.* The statistics collected are:

- Token-Ring Statistics
- History

See detailed description of RMON Support on page 39.

Community Strings...

Changes the community string table. The community string is the name associated with the switch and a set of SNMP managers. Entries in the table are saved across resets and power cycles.

Trap Receivers...

Displays table of managers to which traps are sent. Entries in the table are saved across resets and power cycles.

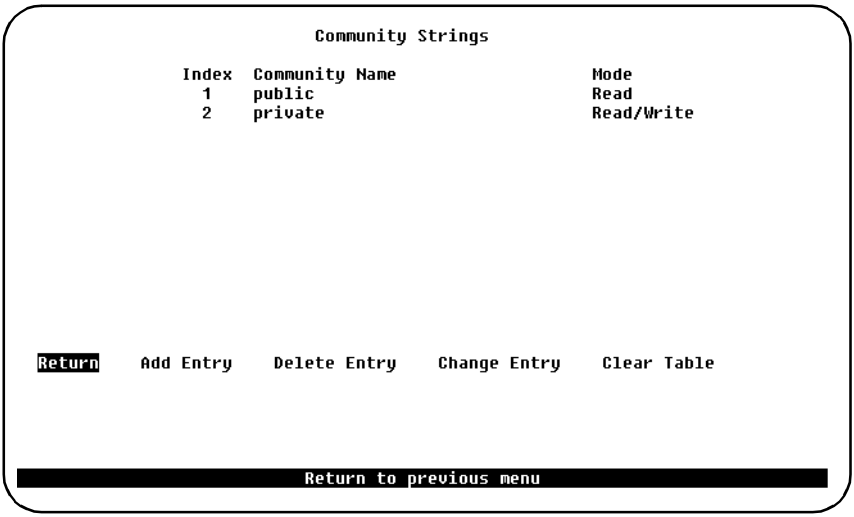
SNMP over MAC Support

The default value is *Enabled*. SNMP over MAC is a way of sending SNMP traffic to manage the switch without IP.

Community Strings Screen

To open this screen from the main menu, select **Configuration → SNMP Configuration → Community Strings.**

Use the **Community Strings** screen to configure the community string for the switch. The community string is the name associated with the switch and a set of SNMP managers allowed to manage it with the specified privilege level.



Note: Text within the community string is upper/lower case sensitive.

Entries are displayed in the order in which they are encountered. There is a limit of 5 community strings.

Community string table entries are saved when you select **Return**. Entries are preserved across resets and power cycles.

Index

Sequential number of entries in the table.

Community Name

Name, or password, used to identify the SNMP managers.

Note: Community names are case sensitive.

Mode

The privilege level assigned to this name. *Read* specifies that SNMP managers can only view SNMP information. *Read/Write* specifies that SNMP managers can both view and change SNMP information.

Add Entry

Adds community string.

Delete Entry

Deletes community string.

Change Entry

Modifies community string and/or access mode.

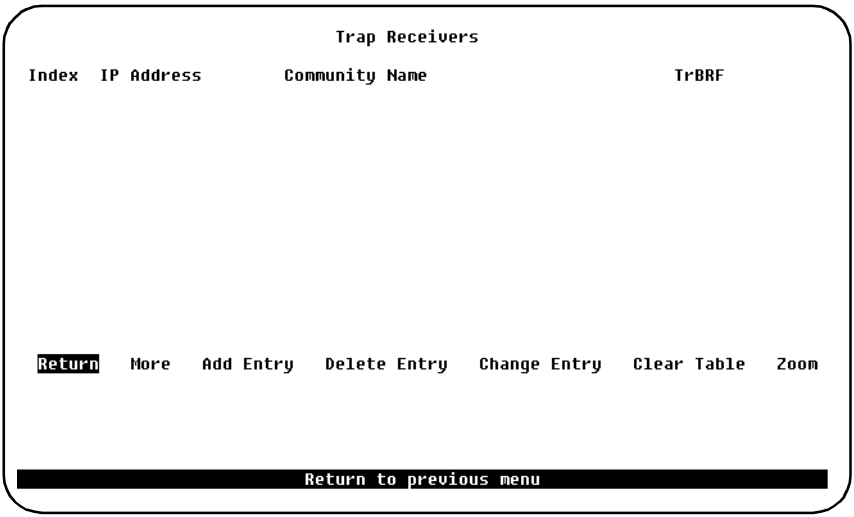
Clear Table

Deletes all community strings.

Trap Receivers Screen

To open this screen from the main menu, select **Configuration → SNMP Configuration → Trap Receivers.**

Trap receiver tables tell the switch where to send traps. The table contains the IP address associated with an SNMP manager.



The Trap receiver table contains a maximum of 20 entries. It is redisplayed each time the table changes.

Trap receiver table entries are saved when you select **Return**. Entries are preserved across resets and power cycles.

Index

Sequential number of entries in the table.

IP Address

The IP address associated with an SNMP manager.

Community Name

The name used to identify SNMP managers.

TrBRF

TrBRF VLAN name for which traps are sent to the specified SNMP manager.

More

Used to view next page of table.

Add Entry
Adds a new entry to the trap receiver table.

Delete Entry
Deletes an entry from the trap receiver table.

Change Entry
Modifies an entry in the trap receiver table.

Clear Table
Deletes all table entries.

Zoom
Displays the complete list of TrBRFs assigned to an IP address.

List of Supported Traps from a Switch

General traps
The coldStart Trap

A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

The warmStart Trap

A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

The linkDown Trap

A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.

The Trap-PDU of type linkDown contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.

The linkUp Trap

A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.

The Trap-PDU of type linkUp contains as the first element of its variable-bindings, the name and value of the ifIndex instance for the affected interface.

The authenticationFailure Trap

An authenticationFailure trap signifies that the sending protocol entity is the

addressee of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation-specific mechanism.

Enterprise specific traps - from OC8600.MIB

oc8600TsStackCfgChange

This trap is generated when there is a change in the stack configuration i.e. when either a new switch is added to the stack or a switch leaves a stack.

oc8600TsNumSwitches indicates the current number of switches which are part of the stack. The management station should update its stack information according to the stack table.

oc8600TsStackStackMatrixChange

This trap is generated when the stack switches over from primary to secondary Matrix or from secondary back to primary Matrix.

oc8600TsStackTempChange

This trap is generated when the temperature in a switch exceeds normal or returns to normal.

oc8600sPowerSupply

This trap is generated when the status of the power supply units changes.

Per Port Traps

oc8600TsPortStrNFwdEntry

This trap is generated when a port automatically enters store and forward mode when the error rate exceeds the threshold.

oc8600TsPortCfgLossTrap

This trap occurs when a port is disabled because it has exceeded its Configuration Loss Threshold within the configured Sampling Period.

oc8600TsBeaconStart

This trap is generated when a port or a station local to a port begins to beacon. It is sent out only when a ring status change indicates that a station is beaconing.

oc8600TsBeaconEnd

This trap is generated when the ring status change indicates that a ring is no longer beaconing. This trap only occurs once when the status actually changes.

oc8600TsDuplicateMACAddr

This trap is generated when a duplicate MAC address is detected on a port in a TrCRF which already has learned that MAC address.

oc8600TsDuplicateBridge

This trap is generated when a duplicated bridge number is detected on a port in a TrCRF.

oc8600TsRingNumberMismatch

This trap is generated when a mismatch in ring numbers is detected on a port in TrCRF.

Traps for the Spanning Tree Protocol

oc8600TsTrCRFNewRoot

This trap is a TrCRF specific version of the newRoot trap as described in RFC1493.

The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.

oc8600TsTrCRFTopologyChange

This trap is a TrCRF specific version of the topologyChange trap as described in RFC1493.

A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition.

oc8600TsTrBRFNewRoot

This trap is a TrBRF specific version of the newRoot trap as described in RFC1493.

The newRoot trap indicates that the sending agent has become the new root of the spanning tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.

oc8600TsTrBRFTopologyChange

This trap is a TrBRF specific version of the topologyChange trap as described in RFC1493.

A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition.

Traps for CrossLinks

oc8600TsCrossLinkFailed

This trap is sent when one of the Token-Ring links in an CrossLink fail. The variable oc8600TsCLPorts contains the Token-Ring ports which are operational in the CrossLink.

❑

6. Monitoring Port Traffic

The CrossFire 8730 Fast Ethernet Translation Switch allows you to configure a Switched Port Analyzer function for monitoring traffic on a port by defining a monitor port where an external probe can observe traffic from a selected monitored port. The monitoring function does not interfere in any way with the normal traffic flow in the switch.

The external probe (e.g. a protocol analyzer) is not supplied with the switch.

You can monitor traffic going through a monitored port in two different ways:

Active Monitoring

Data-only monitoring - you can select the monitored port and monitor port, all data traffic received and transmitted on the monitored port is copied to the monitor port such that it can be received by an external probe. The MAC frames are **not** copied to the monitor port.

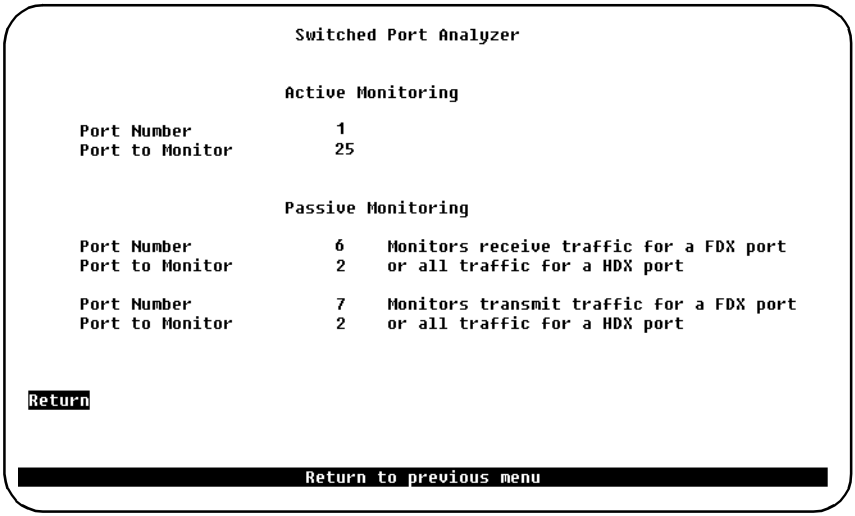
Passive Monitoring for Token-Ring Ports

All traffic monitoring (data and MAC protocol) - makes a copy of all data and MAC frames received and transmitted on the monitored Token-Ring port to up to two monitor Token-Ring ports; you can specify a dedicated monitor Token-Ring port for traffic received on the monitored port and a different monitor port for traffic transmitted on the monitored port. You must use two monitor ports if the monitored port operates in FDX mode.

Note that passive monitoring only is available for Token-Ring ports.

Switched Port Analyzer Screen

To open this screen from the main menu, select **Configuration → Switched Port Analyzer.**



On this screen you can configure a Switched Port Analyzer port. The following information is displayed:

Port Number

Port to which the network analyzer or RMON probe will be attached.

Note: This port should be assigned to its own TrCRF. For information about assigning ports to a TrCRF, see “VLAN Configuration” on page 52.

Port To Monitor

The port that will be monitored.

To change the current settings, select the appropriate parameter and specify a new value. To disable the Switched Port Analyzer port, select **Port to Monitor** and specify 0 as its value. Save the changes by selecting **Return**.

Note: It is only possible to monitor ports within a physical switch, and not in a stack.

7. Getting in Touch with Technical Support

If support is not provided by your organization or the local vendor, you can at any time relay information to or contact Olicom Technical Support via one of the listed services. In addition, BBS, e-mail, FTP or WWW provide up-to-date software updates, application notes, quick fixes and various utilities which may solve your problem.

Before You Contact Olicom Technical Support

- Boot the switch to run the power-on diagnostics. Capture and print the diagnostics (note that any traffic through the switch will be disrupted). . ☐
- Dump the switch configuration to a file using Display Summary and print the file . . . . . ☐
- Print any messages in the Message Log Information Screen . . . . . ☐
- If possible, attach a display summary screen captured from the console or telnet . . . . . ☐
- If possible, simplify the environment by removing other devices. . . . . ☐
- Fill in as much as possible in the included Problem Report Form . . . . ☐
- Contact your place of purchase . . . . . ☐

Hotline Support

Call the following numbers for help with *any* problem you may encounter when installing Olicom software and hardware products:

USA: (+1) 1-800-OLICOM-1(24 hours a day, 7 days a week)
(+1) 972 907-4200 (24 hours a day, 7 days a week)

Europe: (+45) 45 27 01 02 (Denmark, Monday to Friday, 7 am to 6 pm GMT + 1)

(+48) 58 348 15 20 (Poland, Monday to Friday, 8 am to 6 pm GMT + 1)

Fax Support

For assistance with any problem you may encounter when installing Olicom software and hardware products, Olicom's Support department will reply either by fax or by telephone within 24 hours, Monday to Friday. Use one of the following fax numbers:

USA: (+1) 972 671-7524

Europe: (+45) 45 27 02 40 (Denmark)

(+48) 58 348 15 01 (Poland)

Internet E-Mail

Olicom customer support is available on e-mail through Internet. You will receive a reply within 24 hours. Use one of the following e-mail addresses:

USA: support@olicom.com (the Americas)

Europe: support@olicom.dk (ROW, the rest of the world)

Anonymous Internet FTP Server

All Olicom's software updates, application notes, quick fixes, etc. can be obtained from our anonymous FTP server. To connect, open an FTP session to:

USA: ftp.olicom.com

Europe: ftp.olicom.dk

Internet World Wide Web Server (WWW)

The Olicom WWW server contains up-to-date information about Olicom products, newsletters and press releases. It also contains addresses of all Olicom offices and support centers worldwide. Our software library contains the latest driver and software revisions. The WWW server can be accessed using the following web addresses:

USA: http://www.olicom.com

Europe: http://www.olicom.dk

Olicom Support WEB

The Olicom Support WEB contains, for example, technical support hints, driver and software updates, a problem report form, support news as well as updated versions of guides and manuals.

USA: http://www.olicom.com

Europe: http://www.olicom.dk

On the home page, select **Services & Support**.

Problem Report Form

Fill in both sides of this Problem Report Form, print out the relevant system configuration files and fax or mail to Olicom Technical Support. You can also fill in and send a Problem Report Form from Olicom's web site on the Internet.

Switch Information	
Switch type:	
Hardware revision:	
Software version:	
Switch Configuration	
Port configuration:	
Stack Configuration:	
UEM Configuration:	
Adapter Information	
Adapter type:	
Operating system:	
Network OS:	
Driver name:	
Driver version:	

Company: _____ Name: _____

Address: _____

Country: _____ Phone/Fax: _____

E-mail: _____

Problem Description

Network Installation Sketch

Appendix A. Abbreviations

AMP	Active Monitor Present
ARE	All-Routes Explorer
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BLK	Blocked
BPDU	Bridge Protocol Data Unit
BRF	Bridge Relay Function
CAU	Controlled Access Unit
CRF	Concentrator Relay Function
DSAP	Destination Service Access Point
DIS	Disabled
DTR	Dedicated Token-Ring
EIA	Electronic Industry Association
FDX	Full-duplex
FSM	Finite State Machine
FTP	File Transfer Protocol
FWD	Forwarding
HDX	Half-duplex
IEEE	Institute of Electrical and Electronics Engineers
LAA	Local Administrated Address
LAN	Local Area Network
LAM	Lobe Attachement Module

LED	Light Emitting Diode
LLC	Logical Link Control
LRN	Learning
LSN	Listening
MAC	Media Access Control
MAU	Media Access Unit
Mbps	Megabits per second
MIB	Management Information Base
MTU	Maximum Transfer Unit
NNM	Network Node Manager
NSR	Non Source-Routed
OBM	Out-of-Band Management
RMON	Remote Monitoring
RS	Recommended Standard
SMP	Standby Monitor Present
SNA	Systems Network Architecture
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SRB	Source Route Bridging
SRS	Source Route Switching
SRT	Source Route Transparent Bridging
STE	Spanning Tree Explorer
STP	Spanning Tree Protocol *or* Shielded Twisted Pair (see the installation guide)

TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
TFTP	Trivial File Transfer Protocol
TKP	Token Passing
TrBRF	Token-Ring Bridge Relay Function
TrCRF	Token-Ring Concentrator Relay Function
TXI	Transmit Immediate
UAA	Universal Administrated Address
UNA	Upstream Neighbour Address
UTP	Unshielded Twisted Pair
VLAN	Virtual LAN

❑

Index

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Olicom A/S
Nybrovej 114
2800 Lyngby
Denmark
Tel: (+45) 45 27 00 00
Fax: (+45) 45 27 01 01

Olicom, Inc.
1680 North Prospect Drive
Richardson, TX 75081
USA
Tel: (+1) 972 907 4600
Fax: (+1) 972 671 7525

Olicom Australia
Level 14
213 Miller Street
North Sydney, NSW 2060
Tel: (+61) (0)2 9955 1755
Fax: (+61) (0)2 9955 8488

Olicom Benelux
Bolduc Office Centre
Utopialaan 35-N
5232 CD's-Hertogenbosch
Tel: (+31) 73 6 49 15 46
Fax: (+31) 73 6 49 15 45

Olicom France
Immeuble Plein Ouest
177, Avenue G. Clemenceau
92024 Nanterre cedex
Tel: (+33) (0)1 41 91 17 17
Fax: (+33) (0)1 41 91 17 00

Olicom Germany
Hessengring 13a
64546 Mörfelden
Tel: (+49) (0)6 105 2892-0
Fax: (+49) (0)6 105 2892-10

Olicom Ibérica
C/Basauri, 17 - 2° Drcha.A
Edificio Valrealty A
La FLorida
28023 Madrid
Tel: (+34) 1 372 9814
Fax: (+34) 1 372 9645

Olicom Japan K.K.
4 Floor Omori Center Building
1-17-2, Omori-kita, Ohta-ku
Tokyo 143-0016
Tel: (+81) 3 5753 0221
Fax: (+81) 3 5753 0222

Olicom Poland Sp. z o.o.
ul. Slowackiego 173
80-298 Gdansk
Tel: (+48) 58 348 15 00
Fax: (+48) 58 348 15 01

Olicom Sweden
Orrvägen 26-28
191 55 Sollentuna
Tel: (+46) (0)8 594 704 94
Fax: (+46) (0)8 594 704 96

Olicom UK Ltd.
Swan House
Peregrine Business Park
Gomm Road
High Wycombe
Bucks HP13 7DL
Tel: (+44) 1494 556 600
Fax: (+44) 1494 556 616

World Wide Web URLs
http://www.olicom.com
http://www.olicom.dk

DOC-7047/1.1