

SmartStack
STS16-20D/STS16-20R
Token Ring Switches

Installation
and
User Guide

CABLETRON
SYSTEMS

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

© October 1999 by:

Cabletron Systems, Inc.
35 Industrial Way
Rochester, NH 03867

All Rights Reserved.

Order Number: 9032956-01
(OC-7054 v. 1.1, 710001812)

SmartStack is a trademark of Cabletron Systems, Inc.

CompuServe is a registered trademark of CompuServe, Inc.

i960 microprocessor is a registered trademark of Intel Corp.

Ethernet is a trademark of Xerox Corporation.

FCC Notice

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.

NOTE: 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 uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

WARNING: Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

VCCI Notice

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Industry Canada Notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration of Conformity Addendum

Application of Council Directive(s): **89/336/EEC**

73/23/EEC

Manufacturer's Name: **Cabletron Systems, Inc.**

Manufacturer's Address: **35 Industrial Way**

PO Box 5005

Rochester, NH 03867

European Representative Name: **Mr. J. Solari**

European Representative Address: **Cabletron Systems Limited**

Nexus House,

Newbury Business Park

London Road, Newbury

Berkshire RG13 2PZ, England

Conformance to Directive(s)/Product Standards: **EC Directive 89/336/EEC**

EC Directive 73/23/EEC

EN 55022

EN 50082-1

EN 60950

Equipment Type/Environment: **Networking Equipment, for use**

in a Commercial or Light

Industrial Environment.

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer

Legal Representative in Europe

Mr. Ronald Fotino

Full Name

Mr. J. Solari

Full Name

Principal Compliance Engineer

Title

Managing Director - E.M.E.A.

Title

Rochester, NH, USA

Location

Newbury, Berkshire, England

Location

Table of Contents

1. Introduction	1
Switching Technology	2
Switch of Switches	2
Switch of Servers	3
Switch of Hubs	3
Switch of Desktops	3
Switch of Floors and Buildings	4
Switch of Routers	4
Front Panel Details	5
The MANAGEMENT Port	5
Token Ring Ports	5
Reset Button	6
System Request Button	6
Labels	7
Status and Activity LEDs	7
Back Panel Details	9
Features and Specifications	10
Features	10
Specifications	13
2. Switch Overview	17
Multiple Simultaneous Conversations	18
Low Latency	19
Address Management	20
Multiple Bridging Modes	21
Source Route Switching (SRS)	22
Source Route Bridging (SRB)	22
Source Route Transparent (SRT)	23
SRT/SRB	23
Filtering	24
Congestion Control	24
Three Switching Modes	25
Cut-Through	25
Store and Forward	25
Auto (Adaptive Cut-Through)	25
Token Ring Port Operation Modes	26
RI/RO-Like Connection on SmartStack STS16-20R	27
Transmission Priority Queues	28
ClearSession Support	28
CrossLink Connections	29

Spanning Tree Protocol Support	30
VLAN Support	31
Dynamic Source Route Recovery	32
Management	35
SNMP	35
SmartStack Manager for Windows	36
Telnet Management and VT100 Management (Console)	36
IBM LAN Network Manager	36
RMON Support	37
Built-in Port Counters	39
Stackable Architecture	39
Back-to-Back	39
Internal Stacker	39
External Stacker	39
Optional Redundant Power Supply on SmartStack STS16-20R	40
3. Preparing for Installation	41
Safety Recommendations	41
Safety with Electricity	41
Preventing Electrostatic Discharge Damage	42
Site Requirements	43
Environment	43
Chassis Accessibility	43
Cooling and Airflow	43
Power	43
Configuration Guidelines	45
Frame Length Limit	45
IEEE 802.1D Spanning Tree	46
Ring Numbers	47
Sample Uses of the SmartStack STS16-20RM Family Switches Deployment Scenarios	48 51
4. Installation	55
Installation Summary	55
Package Contents	56
Materials needed for Installation	57
Mounting the Chassis	58
Rack or Cabinet Mounting	58
Table-Mounting	59
Cabling	60
Connecting Devices to the Token Ring Ports	60
Connecting Devices to the Token Ring Ports	

Using Building Wiring	61
Checking the Installation	62
Applying Power	63
Stacker Link Module	65
Installation	65
SmartStack STS-LM Connectors and LEDs	66
Connecting the Stacker Link Cable	66
Working with a Stack	67
Inter-box Parameters	67
Checking the Installation	68
5. Accessing Switch Management	69
Overview	69
Connecting the Console	70
Communication Problems	72
Diagnostic Screen	73
6. Switch Configuration	75
General Guidelines	76
Navigating within the Menus	77
Main Menu	78
Configuration Menu	79
Switch Configuration Screen	80
Stack Configuration Screen	83
Module Information Screen	84
VLAN Configuration	86
VLAN Configuration Menu	87
VLAN Configuration Screen	88
VLAN Parameter Configuration for CRF Screen	89
VLAN Parameter Configuration for BRFS Screen	91
VLAN Port Configuration	93
IP Configuration Screen	94
BootP Requests and Parameters	96
SNMP Configuration Menu	97
Spanning Tree Protocol	97
IEEE 802.1D Spanning Tree Protocol (STP)	98
Spanning Tree for BRFS Screen	99
Spanning Tree for CRF Screen	101
Port Spanning Tree Parameters Screen	104
Current Spanning Tree Information Screen	105
Port Configuration Screen	106
Switched Port Analyzer Menu from the Configuration Menu	110
CrossLink	110

CrossLink Menu	112
CrossLink Configuration Screen	113
Setting up a CrossLink	114
Current CrossLink Information Screen	115
Address Filtering	116
Filters and Port Security Menu	117
Configure Filters Screen	118
Configure Port Security Mode Screen	120
View Port Filters Screen	121
Protocol Filters Menu	122
Protocol Class Assignment Screen	123
Port Filtering Attributes Screen	124
Address Aging	126
Address Aging Menu	127
Port Address Table Aging Screen	127
Master Address Table Aging Screen	129
Password Menu	130
Console/Telnet Sessions	132
Console Configuration Menu	132
Serial Link Configuration Screen	133
Creating a Console Session Using a Modem	134
Stopping the Console Session	134
Telnet Configuration Screen	135
Telnet Sessions Screen	136
Starting the Telnet Session	137
Stopping the Telnet Session	137
Involuntary Termination of the Telnet Session	137
Syslog Daemon Screen	139
DSRR Configuration	141
DSRR Group Configuration Screen	143
DSRR Configuration Screen	144
Download/Upload Menu	147
Serial Link Download Screen	148
TFTP	149
TFTP Download/Upload Screen	150
Reset Screen	152

7. Monitoring the Network from the Console Statistics Menu 155

Statistics Menu	156
Switch Statistics Screen	157
Power Supply Information Screen	159
Port Status Screen	160

Port Statistics Menu	162
General Statistics Screen	163
802.5 Statistics Screen	167
802.5 State Information Screen	170
802.5 DTR MAC Information Menu	172
TXI Information Screen	173
Station-CPort Information Screen	175
Address Tables Menu	177
Master Address Table Screen	178
Master Route Descriptor Table Screen	180
VLAN Address Table Screen	182
VLAN Route Descriptor Table Screen	183
Locate MAC Address Screen	184
Current Spanning Tree Information Screen	185
Current Spanning Tree Information for a CRF Screen	188
VLAN Statistics	191
VLAN Statistics Screen for CRF	191
VLAN Statistics for BRF Screen	192
DSRR Status Screens	193
DSRR Status Tables Screen	193
DSRR Neighbor Table Screen	194
DSRR Acting as Backup Table Screen	195
Diagnostic Test Results Screen	196
Message Log Information Screen	197
Display Summary Screen	199
8. Monitoring the Network with SNMP	201
SNMP Setup	201
IP Configuration Screen	201
SNMP Configuration	202
SNMP Configuration Screen	202
Community Strings Screen	203
Trap Receivers Screen	205
List of Supported Traps from a STS16-20D/STS16-20R	206
9. Monitoring Port Traffic	211
Switched Port Analyzer Screen	213
10. Troubleshooting	215
Obtaining Service	215
Troubleshooting in a Network	215
Start of Troubleshooting Process	215
Choosing a Troubleshooting Procedure	216

11. Getting in Touch with Technical Support	221
Problem Report Form	222
Appendix A. Abbreviations	225
Appendix B. Cable and Pin Information	229
Connecting to the Out-of-Band Management Port	229
Out-of-Band Management Port and Cable Pin-Outs	229
Twisted-Pair Cable Pin Outs	232
Cabling Recommendations	233
Cable Length and Lobe Wiring Rules for Dedicated-Media LAN Segments	234
Cable Length and Lobe Wiring Rules for Shared-Media LAN Segments	235

List of Figures

Figure 1.	SmartStack STS16-20D Token Ring Switch	1
Figure 2.	Location of LEDs, Switches and Connectors	5
Figure 3.	The back panel of the SmartStack STS16-20D	9
Figure 4.	The back panel of the SmartStack STS16-20R	9
Figure 5.	Multiple Conversations Through a SmartStack STS16-20RM Switch	18
Figure 6.	Typical Configuration with SmartStack STS16-20R Switches Using Multiple Bridging Modes	21
Figure 7.	A SmartStack STS16-20R Switch Configured with Two VLANs	31
Figure 8.	Example of Dynamic Source Route Recovery, Base Configuration	32
Figure 9.	Example of Dynamic Source Route Recovery, Normal State	33
Figure 10.	Example of Dynamic Source Route Recovery, Switch 1 Failed	34
Figure 11.	Typical Network without the SmartStack STS16-20D/STS16-20R	49
Figure 12.	Relieving the Overstressed Backbone	49
Figure 13.	Replacing SRBs with a SmartStack STS16-20RM or SmartStack STS16-20R	50
Figure 14.	Delivering Dedicated Bandwidth to Individual Workstations	50
Figure 15.	Scenario using a Stacker Link and a Matrix Switch	52
Figure 16.	Setting Up CrossLinks	53
Figure 17.	Exposing the Rack Mounting Bracket	58
Figure 18.	Mounting the Switch in a Rack or Cabinet	59
Figure 19.	Connecting Devices to Token Ring Ports	61
Figure 20.	Connecting using Building Wiring	62
Figure 21.	The back panel of the STS16-20D	63
Figure 22.	The back panel of the STS16-20R	64
Figure 23.	SmartStack STS-LM Front Panel	65
Figure 24.	View of Console Connection	70
Figure 25.	SmartStack STS16-20D/STS16-20R with four VLANs	86
Figure 26.	Setting Up CrossLinks	110
Figure 27.	Primary and Traced DSRR Port	142
Figure 28.	TIA/EIA-232 Null-Modem Cable for 25-pin Connector	231
Figure 29.	EIA 232 Null-Modem Cable for 9-pin Connector	231
Figure 30.	Straight-Through Cable	232
Figure 31.	Data Connector-to-RJ-45 Straight-Through Cable	232

List of Tables

Table 1.	Status LEDs and their Meanings	7
Table 2.	Stack-link LEDs and Their Meanings	8
Table 3.	Port LEDs and Their Meanings	8
Table 4.	Back Panel Connectors	9
Table 5.	Capacity Specifications	13
Table 6.	Performance Specifications	14
Table 7.	Specifications of Physical Characteristics	16
Table 8.	Supported MIBs	35
Table 9.	Supported RMON Groups	37
Table 10.	SmartStack STS-LM Network Connector	66
Table 11.	SmartStack STS-LM LEDs	66
Table 12.	Inter-box Parameters	68
Table 13.	Console Configuration Settings	71
Table 14.	Modem Settings	134
Table 15.	Symptom, LED State and Recommended Procedure	216
Table 16.	Connecting to the Management Port	229
Table 17.	Pin-out of the Management Port	230
Table 18.	Copper Cable Types	233
Table 19.	Lobe Length for 150 Ohm Shielded Media	234
Table 20.	Lobe Lengths for 100 Ohm Shielded or Unshielded Cable	234
Table 21.	Lobe Lengths for 100 or 120 Ohm Shielded or Unshielded Cable	235

1. Introduction

This chapter discusses switching technology and how the SmartStack STS16-20D and/or SmartStack STS16-20R Token Ring Switch can be used to improve network performance. This chapter also includes a list of features and specifications for the SmartStack STS16-20D/STS16-20R.

The topics of this chapter are presented under the following titles:

- “Switching Technology”, starting on page 2.
- “Front Panel Details”, starting on page 5 and “Back Panel Details” starting on page 9.
- “Features and Specifications”, starting on page 10.

The front panels of the SmartStack STS16-20D Token Ring Switch and the SmartStack STS16-20R Token Ring Switch are exactly the same, only the product label differs. The following figure illustrates the front panel of a SmartStack STS16-20D Token Ring Switch.

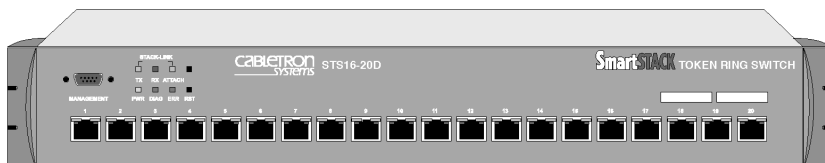


Figure 1. SmartStack STS16-20D Token Ring Switch

Switching Technology

Demand for network bandwidth continues to grow, driven by the increasing number of systems used in network-intensive applications. LAN segmentation has been the prevalent method for addressing these demands and has been further popularized by trends toward server centralization. However, the implementation costs of LAN segmentation, as well as the real performance characteristics of conventional network components, have served to limit growth of some Token Ring networks. Alternative technologies for addressing bandwidth demands present yet other inhibitors, usually relating to costs. Token Ring switching provides users with an easy, cost-effective technique for addressing these demands.

Token Ring switches, such as the SmartStack STS16-20D/STS16-20R, increase throughput between Token Ring segments by supporting simultaneous, parallel conversations. Switched connections between Token Ring segments last only for the duration of the packet—new connections can be made between different segments for the next packet.

Token Ring switches solve congestion problems caused by high-bandwidth devices and powerful applications as well as the number of users. Therefore, each of these devices—servers, for example—can be assigned its own 16 Mbps segment.

In Token Ring networks, the major bottleneck is typically the throughput to high-bandwidth devices such as servers, and between routers, bridges, and switches. An effective solution is full-duplex communication, an option for each segment connected to an SmartStack STS16-20D/STS16-20R port. Normally, Token Ring operates in half-duplex communication mode, which means stations can either receive or transmit. With full-duplex technology, two communicating stations can transmit and receive at the same time. When packets can flow in both directions simultaneously, effective Token Ring bandwidth doubles from 16 Mbps to 32 Mbps.

The SmartStack STS16-20D/STS16-20R can forward Token Ring frames among multiple, shared or dedicated Token Ring LAN segments. Using a frame forwarding technique similar to that of a multiport Token Ring transparent bridge, the switch uses Token Ring MAC addresses to forward Token Ring frames from any of its ports to any other.

Switch of Switches

The SmartStack STS16-20D/STS16-20R can be deployed in a variety of network configurations, all of which provide a significant increase in network performance. The family of Cabletron Systems Token Ring products allows users to build network systems that can transport data efficiently and scale upwards as throughput requirements increase. The SmartStack STS16-20D/STS16-20R delivers high-reliability and media flexibility. These features combine to allow the SmartStack

STS16-20D/STS16-20R to be used as a switch of switches which provides media flexibility in an Token Ring configuration.

The SmartStack STS16-20D/STS16-20R can easily connect with other SmartStack products to deliver a broad range of network carrying capacity. Bandwidth is easily scaled to meet all performance requirements.

Switch of Servers

With client/server applications, many client workstations may attempt to access a single server at the same time. This traffic pattern may create bottlenecks at the server. To further enhance performance, the SmartStack STS16-20D/STS16-20R can deliver dedicated bandwidth to high-speed file servers. All servers perform better with dedicated 16 Mbps bandwidth.

Even better performance can be achieved by installing multiple adapters in the server. By connecting these adapters to the switch, multiple 16 Mbps paths to the server are created, a solution that is only possible when using a switch.

The switch ties together all Token Ring devices lined to a local wiring center. In networks, where a significant portion of the traffic moves locally between client and server, the switch can be very effective.

Switch of Hubs

When network traffic increases beyond the capability of hubs, contention results. Applications suffer and may even fail. The net effect of such a network configuration is that all devices share a single 16 Mbps data path, thus reducing overall network efficiency. The SmartStack STS16-20D/STS16-20R can be very effective when used as a switch of hubs.

The SmartStack STS16-20D/STS16-20R can alleviate contention through microsegmentation, or reducing the number of devices in each shared segment. To provide microsegmentation, the SmartStack STS16-20D/STS16-20R divides a single 16 Mbps segment into multiple 16 Mbps segments. As an example, a workgroup has 16 Mbps of capacity. The 20 ports on the SmartStack STS16-20D/STS16-20R support 10 simultaneous conversations with 20 hubs, thus providing the workgroup with 160 Mbps bandwidth throughput, which results in a significant gain in bandwidth. Note that on the SmartStack STS16-20D, hubs can only be connected to the network ports 17–20.

Switch of Desktops

The SmartStack STS16-20D/STS16-20R is a cost-effective means of providing dedicated bandwidth to individual desktop workstations. In this application, the SmartStack STS16-20D/STS16-20R replaces a hub, providing excellent, hub-like

network management statistics. Total network capacity and throughput increase dramatically for attached desktop workstations.

Switch of Floors and Buildings

For network managers, multistorey buildings and campuses can represent a unique networking challenge. How can a network manager provide an efficient LAN interconnect for users that are located on several floors of a building or in different buildings?

Token Ring switching and the SmartStack product family can provide the best solution. The SmartStack STS16-20D/STS16-20R provides enhanced throughput to local wiring closets that can be connected to a switch located in the data center.

Many networks consist of users located in different buildings of a campus environment. The switches can be used as a collapsed backbone interconnecting multiple buildings of a campus. They can provide the connectivity solution and enhanced throughput that such campus environments require.

Switch of Routers

Router technology has had a significant impact on the design of today's internetworks. Routers have become the cornerstone of most production networks. Although well equipped to provide firewall, WAN connectivity, security, and connection between dissimilar LANs, routers are unable to provide high throughput between desktop devices and servers. Because of these limitations, routers and switches perform complimentary functions in the network.

The SmartStack STS16-20D/STS16-20R can be used as a front-end to routers to increase performance in each subnet. Communication between local clients and servers is enhanced at the workgroup level below the router.

The SmartStack STS16-20D/STS16-20R can also be used to back-end routers. In networks where many routers are interconnected over Token Ring and backbone performance is not acceptable, the SmartStack STS16-20D/STS16-20R provides nonblocking communication between the routers for enhanced network performance. This provides protocol transparency with enhanced throughput in each subnet between local servers and desktops, thus allowing network managers to build logical networks as large as network layer protocol and broadcast traffic allow.

The Switched Port Analyzer also gives a collapsed backbone network superior network management and the ability to perform protocol analysis from a single location. The Switch Port Analyzer provides the latest technology for monitoring switch-based networks and helps to reduce the cost of managing these networks.

Front Panel Details

The front panel details of the switches are illustrated in Figure 2. This section lists all the connectors, controls, and LEDs of the front panel.

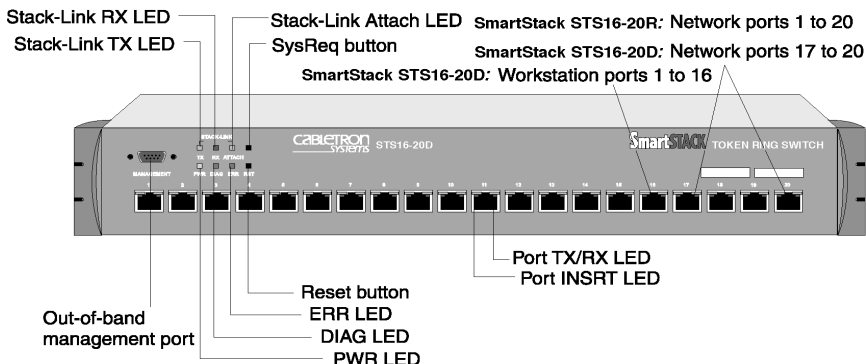


Figure 2. Location of LEDs, Switches and Connectors

The MANAGEMENT Port

The 9-pin, male, Out-of-Band Management (OBM) port labeled MANAGEMENT functions as a DTE port.

This port enables attachment of a terminal, either local or remote, through a modem connection. The terminal can be used to configure and monitor the switch.

The Out-of-Band Management port automatically detects the baud rate of the terminal to which it is attached.

Token Ring Ports

- Twenty shielded RJ-45 connectors for Token Ring connection.
 - Support for the IBM Cabling System via 150 ohm, shielded twisted-pair (150 ohm STP); or 100 or 120 ohm unshielded twisted-pair via Category 3, 4, or 5 cables.
 - These ports allow half-duplex (HDX) or full-duplex (FDX) connections to other switches, hubs, or end nodes.
- The SmartStack STS16-20D/STS16-20R will automatically sense what type of Token Ring connection is being employed on each of its ports, whether it is:

- a connection to a shared-media segment via a Token Ring concentrator, Station mode (on SmartStack STS16-20D only via the network ports 17– 20)
- a connection to another Token Ring switch (on SmartStack STS16-20D only via network ports 17–20)
- operating at 4 Mbps or at 16 Mbps
- a connection to a dedicated-media segment, directly to a Token Ring LAN station operating in half-duplex or full-duplex mode (Port mode).
- Ports 19 and 20 on SmartStack STS16-20R can attach to a MAU/CAU RI/RO port

The switch will automatically configure (requiring no operator action) each port to operate at the highest possible level of capability. No special crossover cables are required for Token Ring stations on dedicated-media segments or for switch-to-switch connections; the same straight-through cabling is used regardless of the type of connection. This auto-sense/auto-configure capability of the switch can be overridden by explicit console management.

Switched Port Analyzer

Any of the Token Ring ports can be configured as an analyzer port. An analyzer port is used to monitor any of the other ports in the same physical switch. The activity can then be traced by a Token-Ring network analyzer attached to the analyzer port.

Reset Button

The SmartStack STS16-20D/STS16-20R has a recessed reset button labeled RST that is located on the front panel. Pressing the reset button resets the hardware and software and clears all tables and memory, including the address tables. Pressing the reset button does not clear the values stored in nonvolatile random access memory (NVRAM).

System Request Button

This unlabeled recessed button is located on the front panel above the Reset button. Pressing the button causes the **System Request** Menu to appear on the console device attached to the MANAGEMENT port. Pressing the button for more than five seconds will initiate a modem download of the main image.

- ▶ **Note:** The system request button should be used only at the direction of service personnel. The button is recessed to prevent accidental activation.

Labels

The two labels in the right side of the front panel are:

- The MAC Address Label: The unique globally assigned base Base MAC-Address of the switch.
- The Switch Number Label: Blank label for an individual user identification of the switch.

Status and Activity LEDs

The SmartStack STS16-20D/STS16-20R features three status LEDs at the left on the front panel that show the current status of the switch. There are also three *activity* LEDs at the left that indicate the activity of the optional stacker link module. Moreover, each Token Ring port has two LEDs.

Refer to Figure 2 on page 5 for the locations of all the LEDs.

Table 1 lists the status LEDs and their meanings.

LED	State	Meaning
PWR	Off	The switch is not connected to a power outlet, or the power supply is faulty.
	On	The switch is receiving power.
DIAG	On	The DIAG diagnostics LED is on during the power-on self-test. During download of a new software image, the DIAG LED blinks to indicate the clearing (slow blink) and loading (faster blink) of FLASH memory.
ERR	On	The ERR LED is off during normal operation. If the LED turns on, an error has occurred. Power the switch down and up again. The ERR LED should not turn on again. If it does, the switch is faulty. Note that on SmartStack STS16-20R, the ERR LED might turn on if the switch is powered only by an external power supply.

Table 1. Status LEDs and their Meanings

The stack-link LEDs and port LEDs are described in the tables on the next page.

Back Panel Details

The back panel of the switches are illustrated in

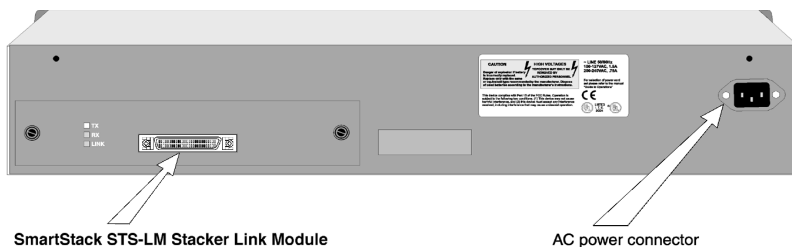


Figure 3. The back panel of the SmartStack STS16-20D

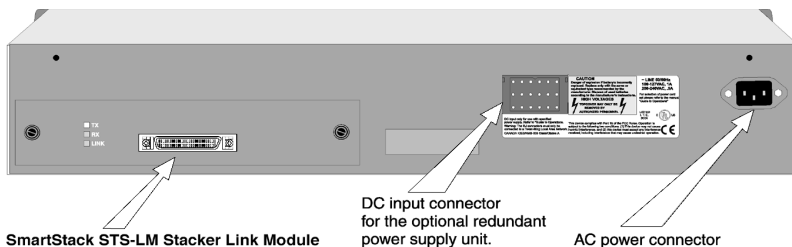


Figure 4. The back panel of the SmartStack STS16-20R

Table 4 lists the back panel connectors on the switch.

Name	Description
AC connection	Standard AC power connection.
Redundant power supply (SmartStack STS16-20R only)	Connector for the optional redundant power supply unit.

Table 4. Back Panel Connectors

Features and Specifications

This section lists important switch features as well as technical specifications.

Features

Performance and Advanced Features

- Three switching modes:
 - Low latency cut through
 - Store and forward
 - Auto (Adaptive cut-through)
- Enhanced bridging modes:
 - Transparent bridging
 - Source route switching
 - Source route bridging (SRB)
 - Source route transparent bridging (SRT)
- Support for duplicate MAC address schemes
- Automatic port sensing of operating mode and media speed
- Multiple Token Ring port operation modes:
 - Half-duplex concentrator and station
 - Full-duplex concentrator and station (Dedicated Token Ring)
 - RI/RO-like connection (SmartStack STS16-20R only)
- Spanning tree protocol support on SmartStack STS16-20D for the designated network ports 17–20 and on SmartStack STS16-20R for all the ports 1–20:
 - IEEE 802.1D
 - IBM Spanning Tree Protocol

On SmartStack STS16-20D the workstation ports 1–16 will always be in forwarding state. They are not affected by the spanning tree protocol.
- CrossLink high-speed inter-switch connection
 - On SmartStack STS16-20D up to 128 Mbps using the network ports 17–20. On SmartStack STS16-20R the workstation ports 1–16 do not support CrossLinks.

- On SmartStack STS16-20R up to 256 Mbps for all the ports 1–20, when using 8 ports.
- Advanced filtering (MAC address / Protocol)
- VLAN (Virtual LAN) support
- Support for transmission priorities
- Congestion control
- SRB Redundancy
- Support for ClearSession high availability features

Management

- Extensive and sophisticated network management:
 - SNMP management
 - Out-of-band management via Telnet and VT100 consoles
 - Graphical management application for Windows 95 and Windows NT (for information on additional management applications for Unix, please contact your local Cabletron Systems sales representative)
- Support for RMON and standard MIBs
- Network statistics
- LAN probe port mirroring
- Fault isolation and detection
- Download via TFTP or X-modem of new switch microcode
- Up- and download of switch configuration via TFTP

Scalability and High Availability

- SmartStack STS16-20D:
One active LAN station can be attached to each of the workstation port 1–16. Up to 5,500 active LAN stations for the four network ports 17–20 combined with a maximum of 10,000 active LAN stations per SmartStack STS16-20D..
- SmartStack STS16-20R:
Up to 5,500 active LAN stations per group of four ports with a maximum of 10,000 active LAN stations per SmartStack STS16-20R.
- Stackable architecture

- SmartStack STS16-20R: Optional Redundant Power Supply
Six switches can receive backup power from one SmartStack STS-RPC Redundant Power Center equipped with six SmartStack STS-PSU Redundant Power Supply Units.

Installation

- No special crossover cable required
- Rack or surface mounting
- Plug and Play for transparent forwarding:
 - Automatic learning of network configuration
 - Transparent to high-level protocol
 - Automatic sensing and configuration of ports
- A factory-assigned MAC address (the switch can also be configured with a locally administered MAC address)

Specifications

The tables on the following pages list the product specifications for the SmartStack STS16-20D/STS16-20R.

Capacity

Specification	Value
Number of Token Ring ports	SmartStack STS16-20D: 16 workstation ports (1 to 16) 4 network/workstation ports (17 to 20) SmartStack STS16-20R: 20 network/workstation ports
Number of Token Ring switches in stack	8 using the SmartStack STS-8SU Stacker Unit 5 using the SmartStack STS-5SU Stacker Unit 2 using the SmartStack STS-LM Link Module
Global lookup table size (stations and bridges)	10,000
Local lookup table size, total for four network ports (on SmartStack STS16-20D ports 17 to 20) (stations and bridges)	5,500
Maximum number of logical rings	63
Maximum number of VLANs	63

Table 5. Capacity Specifications

Physical Characteristics

Specification	Value
Rack mount	19" rack mount (hardware included) 1.5 U
Dimensions	Width: 19" (48.3 cm) Depth: 15.74" (40.0 cm) Height 2.59" (6.6 cm)
Weight	15.9 lbs. (7.2 Kg)
Power	100 to 240 VAC autosensing
Frequency	50/60 Hz
AC current rating	1.5 A @ 100 V; 0.75 A @ 220 V
Thermal dissipation	75 W, 256 BTU/h
MTBF	SmartStack STS16-20D: 72,100 hours SmartStack STS16-20R: 70,200 hours Calculated using Bellcore TR-332, issue 6
Operating Temperature: Non-operating Temperature:	10 to 40°C (50 to 104°F) -10 to 70°C (13 to 158°F)
Humidity: Operating Non-operating	8 to 80% (non-condensing) 90% @ 45°C (113°F)
Electromagnetic compability immunity	EN 50082-1 EN 61000-3-2 EN 61000-3-3
Electromagnetic emissions certification	FCC Part 15, subpart b, Class A EN 55022 Class A CISPR 22 Class A
Safety	IEC 950 UL1950 CSA C22.2 No. 950 EN 60950
MANAGEMENT port	TIA/EIA-232-F, DB9 male connector
Software updates	Flash PROM, TFTP, X-modem

2. Switch Overview

The SmartStack STS16-20D/STS16-20R is an IEEE 802.5-compliant device designed to boost throughput on Token Ring networks. It operates as a Media Access Control (MAC)-layer device that is protocol independent.

This chapter describes how the SmartStack STS16-20D/STS16-20R operates as a single stand-alone unit. The switch contains the following main elements, as listed below:

- **Switching Bus**—the architecture of the SmartStack STS16-20D/STS16-20R 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 (on SmartStack STS16-20D, ports 1–16 are workstation ports). 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.
- **Stack Link Module**—the SmartStack STS16-20D/STS16-20R switch family includes a stack link module that can be used to connect two SmartStack STS16-20D/STS16-20R family switches in a back-to-back configuration. Alternatively, up to five switches can be connected together using an 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 Token Ring is that it supports only one packet at a time. The SmartStack STS16-20D/STS16-20R improves data throughput by supporting multiple, simultaneous, full-duplex conversations. By using High-Speed bus switching technology, the SmartStack STS16-20D/STS16-20R creates multiple data paths. These switched connections between Token Ring 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.

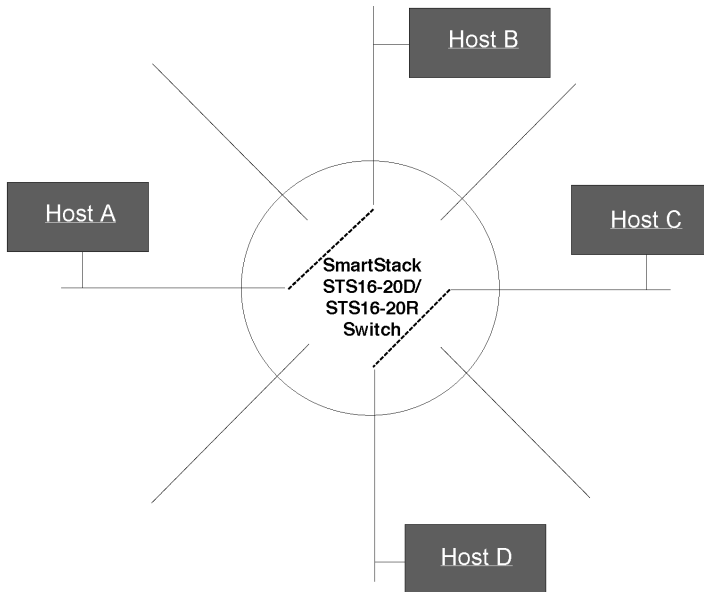


Figure 5. Multiple Conversations Through a SmartStack STS16-20RM Switch

For example, as shown in Figure 5, while host A is transmitting a byte to host B, the SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R transmits broadcast and multicast packets on several SmartStack STS16-20D/STS16-20R ports simultaneously.

The increase in throughput is directly proportional to the number of physical token-rings that are interconnected through the switch. A SmartStack STS16-20D/STS16-20R with 20 ports interconnected provides up to ten concurrent paths. With ten simultaneous conversations, the SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R ports.

By transporting multiple Token Ring packets simultaneously, it boosts overall network throughput.

Low Latency

When operating in cut-through mode, the SmartStack STS16-20D/STS16-20R minimizes latency—the time it takes to forward a packet from one Token Ring segment to another—by beginning switching immediately after looking at the first six bytes of the destination address in the packet. If the packet needs to be switched to another LAN segment, its data begins flowing through the destination port before the entire packet has been received. The result: packets can appear at the output port 35 microseconds after entering the input port. Network devices that use store-and-forward technology introduce much longer delays because they wait to receive the entire packet before forwarding it.

By minimizing delay, the SmartStack STS16-20D/STS16-20R can move more packets freely throughout the LAN without degrading performance.

Address Management

At power up, the system address tables do not contain any information. Whenever a SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R will learn the responder's location and adds it to the address table. Once the address table entries are created, the SmartStack STS16-20D/STS16-20R uses these learned address to switch all subsequent packets to the port where the destination address is located.

SmartStack STS16-20D Token Ring Switch

The system address table maintains up to 10,000 entries known across the networks and stations attached to the switch.

On SmartStack STS16-20D, the local port address table for the designated network ports 17 to 20 maintains up to 5,500 active Token Ring addresses. If more than this maximum number of addresses appear as a source MAC address, these additional addresses will not be learned, resulting in frames from these additional addresses being sent to all switch ports.

The workstation ports 1 to 16 maintain one active Token Ring address per port. If more than one address appears as a source MAC address, these additional addresses will not be learned, and frames from these additional addresses will be not be forwarded.

Addresses on both workstation and network ports are monitored for activity. If an address has not been active for a configurable aging time, the address is removed from the address tables. This ensures that the port's address table is populated only by the most recently used addresses.

This capability allows users to transparently connect to high-volume backbone networks.

SmartStack STS16-20R Token Ring Switch

The system address table maintains up to 10,000 entries. On SmartStack STS16-20R each port address table maintains 5,500 active Token Ring addresses (each port address table is shared by four ports, using the following: 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 tables. This ensures that the port's address table is populated only by the most recently used address.

Just as on SmartStack STS16-20D, this capability allows users to transparently connect to high-volume backbone networks.

Multiple Bridging Modes

The SmartStack STS16-20D/STS16-20R 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 in the following:

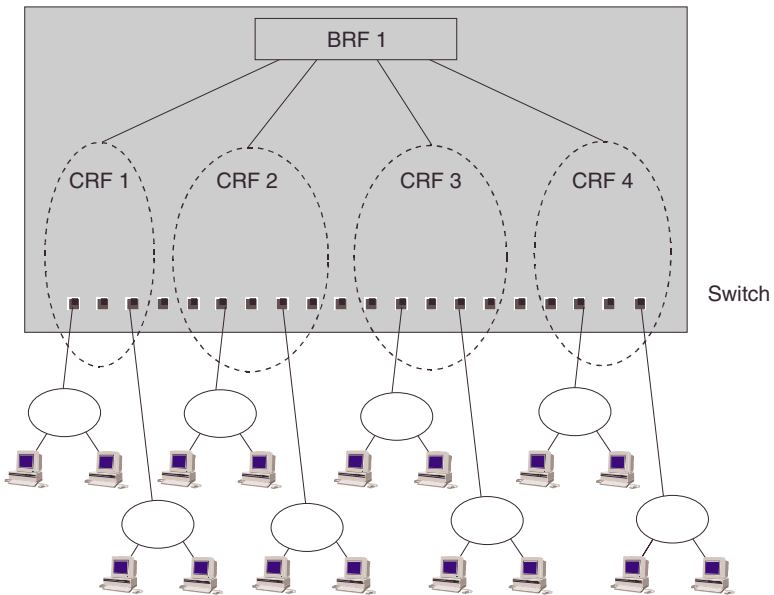


Figure 6. Typical Configuration with SmartStack STS16-20R Switches Using Multiple Bridging Modes

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 a 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 SmartStack STS16-20D/STS16-20R can support up to 63 logical rings.

There are two levels of relay functions supported by the SmartStack STS16-20D/STS16-20R. The first level is the CRF to which the ports are assigned. The second level is the BRF. This is the parent relay function to which CRFs are assigned. The SmartStack STS16-20D/STS16-20R maintains certain configuration information and management statistics on a per BRF/CRF basis. Therefore, when you access VLAN-specific SmartStack STS16-20D/STS16-20R configuration or management screens (such as the Current Spanning Tree Information screen), you will be prompted to specify the desired BRF or CRF.

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. Note that on SmartStack STS16-20D the spanning tree protocol is only available on the network ports 17 to 20.

- **Note:** On SmartStack STS16-20D only the designated network ports 17 to 20 will allow multiple MAC addresses to be learned. On SmartStack STS16-20R all ports allow multiple MAC addresses.

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-routed 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 the 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 SmartStack STS16-20D/STS16-20R 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 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

This section describes the three switching modes available on the switch.

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 μ s. 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.

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 μ s depending on the packet size. Though slower than cut-through mode, this is still much faster than conventional bridges.

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.

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. Compatible with older adapters.
- **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**
Allows connection of the RI/RO port from a MAU or CAU directly to the switch (only on SmartStack STS16-20R, ports 19 and 20).

The mode of operation can be configured manually or sensed automatically. Note that for SmartStack STS16-20R this is 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.

Transmission Priority Queues

To address the needs of delay-sensitive data, such as multimedia, the Token Ring ports of the SmartStack STS16-20D/STS16-20R 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.

ClearSession Support

The SmartStack STS16-20RM switch family support the ClearSession high availability and network redundancy features.

ClearSession is a framework for mission critical networks. It prevents session loss by providing a network failure recovery time of, typically, less than three seconds. ClearSession consists of a several product features. Some of these, ClearServer, CrossLinks and Dynamic Source Route Recovery, are supported by the CSmartStack STS16-20RM switch family. These features provide the following functionality:

ClearServer. Token-Ring ClearServer for LAN, allow multiple adapters to be treated as one virtual adapter in the server, thus allowing multiple connections between a server and the backbone switch or switches. During normal operation the traffic is distributed on the links. The SmartStack STS16-20RM switch family support ClearServer for LAN to be used on servers connected to the switch.

CrossLinks. Any Token-Ring link or dedicated Token-Ring link between SmartStack STS16-20RM family switches may be expanded to a CrossLink. A CrossLink is an aggregation of two to eight identical parallel links, working as one link of the aggregate capacity, providing protection from physical link failure. Should one of the links fail, the traffic is redistributed among the remaining operational links.

Dynamic Source Route Recovery. DSRR is a feature that enables two or more SmartStack STS16-20RM family switches performing source route bridging between a shared-media access ring and a common backbone ring to function as backup for each other. Should one of the switches fail or lose connectivity to one of the access rings, the other switch immediately takes over and bridges source-routed traffic marked with the failed path. DSRR protects source-routed traffic to and from shared access segments, such as user rings, with redundant connections to two Token-Ring switches. Traffic to and from such rings that is non-source-routed relies on the spanning tree.

CrossLink Connections

Two or more Token-Ring ports can be configured to comprise a CrossLink.

A CrossLink is a collection of identical parallel links between two switches or between a switch and an end node, aggregated to appear as one single link of the aggregate capacity. The traffic distribution mechanism attempts to balance the load on the individual links. If one of the links in a CrossLink fails, the traffic is automatically moved from this link and distributed among the other links, thus providing active resilience.

The CrossLink ports on a STS16-20x switch can be used to connect to another STS16-20x switch, or a server with multiple RapidFire adapters using ClearServer for Token-Ring. (Please note that ClearServer for Token-Ring is supported on selected models of RapidFire adapters only. For details, refer to the ClearServer for LAN product information.)

The CrossLinks provide load distribution as well as resilience. In normal operation, the traffic is distributed on the physical ports of the CrossLink according to the frame MAC addresses. This ensures the sequence of a flow. Should a link fail or otherwise become inoperative, the switch dynamically redistributes the traffic to the remaining links. The CrossLink remains in operation as long as there is at least one link in operation. If a failed link is restored, traffic is once more redistributed to make use of the restored link.

A CrossLink is in many ways operating as one single link. For example, the spanning tree protocol will only have one port entity covering all ports in the CrossLink. The ports will all have the same operating state. As for VLAN and CRF configuration, the CrossLink is also seen as one link. Configuration changes apply to all links in the CrossLink.

On the STS16-20/RM/STS16-20FRM switch, CrossLinks can also be configured on the High-Speed Token-Ring ports of the SSIM-R2-02/SSIM-R8-02 High Speed Token Ring SmartStack modules or on the Fast Ethernet ports of the SSIM-H2-02 Fast Ethernet -Translational Switch SmartStack module. CrossLinks on Fast Ethernet ports can only consist of two ports available on the same SSIM-H2-02 Fast Ethernet -Translational Switch SmartStack module.

The CrossLink concept is designed to be compatible with the coming Link Aggregation standard, IEEE 802.3ad.

On SmartStack STS16-20D only the network ports 17–20 will allow CrossLinks. On this switch you can achieve up to 128 Mbps using four ports. On the SmartStack STS16-20R up to 256 Mbps can be achieved, using eight ports.

The STS16-20/RM/STS16-20FRM switch allows up to eight CrossLinks, each consisting of up to eight Token-Ring links.

For details about CrossLink configuration, please refer to the section “CrossLink” on page 110 in Chapter 6, “Switch Configuration”.

Spanning Tree Protocol Support

IBM initially supported only source route bridging (SRB) in its bridges, so most 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 source route transparent bridges. The IEEE Spanning Tree Protocol is not compatible with the IBM Spanning Tree Protocol.

The SmartStack STS16-20D/STS16-20R supports both the IEEE 802.1D Spanning Tree Protocol and IBM Spanning Tree Protocols.

- ▶ **Note:** On SmartStack STS16-20D only the network ports 17–20 support the spanning tree protocol at the port level.

VLAN Support

The virtual LAN (VLAN) concept creates a virtual switch within a physical switch or stack of switches. A VLAN consists of CRFs and has its own bridge relay function attached. Frames are not forwarded across VLANs and ring numbers must be unique within a VLAN.

- A VLAN consists of a number of ports of a switch or stack of switches
- No frames are forwarded between ports belonging to different VLANs
- Port groups on different VLANs may be assigned the same ring number, but ring numbers must be unique within the same VLAN
- For each VLAN, the stack can be assigned a separate IP address
- The spanning tree protocol is executed independently within each VLAN. However, since all BRFs use the same Bridge ID for the spanning tree algorithm, the spanning tree protocol will not function if ports from different BRFs within one switch are connected.

A sample VLAN with SmartStack STS16-20R is shown below.

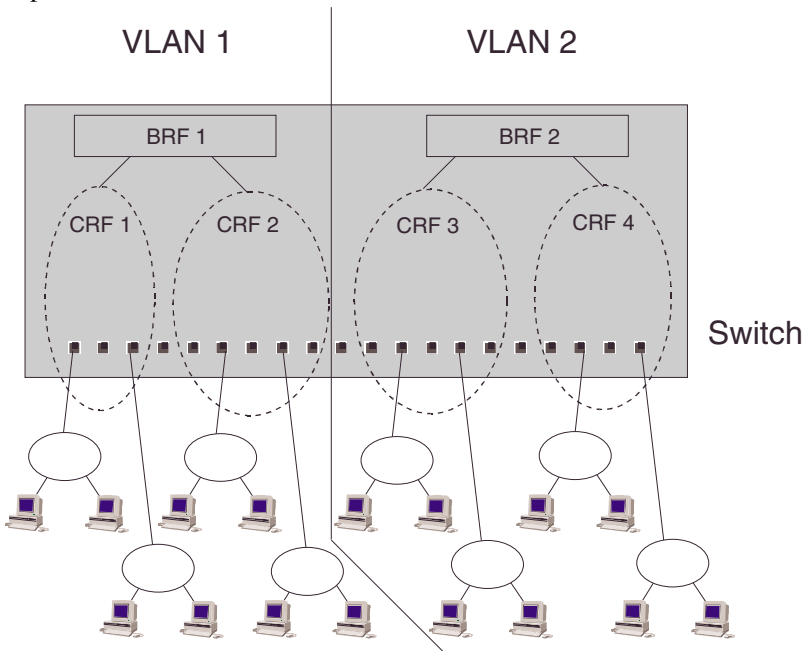


Figure 7. A SmartStack STS16-20R Switch Configured with Two VLANs

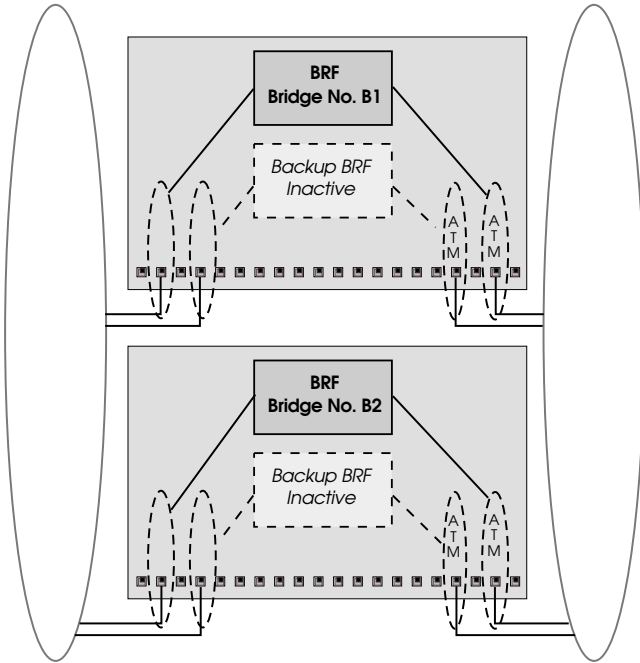


Figure 9. Example of Dynamic Source Route Recovery, Normal State

If one of the switches (Figure 9) or its link to any of the Token-Rings fail, (one of the remaining active switch(es) will after a short interval activate its backup path to take over the traffic of the failed switch (see Figure 10) When the failing switch has been repaired/replaced, the traffic will automatically revert to it.

Management

This section describes the management options for the switch.

SNMP

The SmartStack STS16-20D/STS16-20R can be managed via a SNMP manager. The SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R. SNMP management is supported via IP and MAC.

The following MIBs are supported:

Specification	MIB
RFC1213	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
STS16 MIB	1.3.6.1.4.1.52.285
STS16 MIB	1.3.6.1.4.1.9 (crosslinks)

Table 8. 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.

SmartStack Manager for Windows

The SmartSwitch Manager is an application that runs under Windows. It provides an intuitive graphical user interface (GUI) that displays a view of the switch front panel and supports configuration, performance monitoring, and troubleshooting.

This application is included with the SmartStack STS16-20D/STS16-20R.

Telnet Management and VT100 Management (Console)

The Console Management function may be accessed out-of-band via the TIA/EIA-232-F (that is, RS-232) port labeled MANAGEMENT or in-band via Telnet.

IBM LAN Network Manager

The SmartStack STS16-20D/STS16-20R 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. The switch also implements a mini Ring Parameter Server to supply attached NICs (such as CAUs) with the configured ring number.

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 SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R will send a trap to the client. This monitoring method reduces traffic between the SNMP client and the SmartStack STS16-20D/STS16-20R.

The switch implements a mini RMON probe for the physical ports by supporting some of the RMON groups RFC 1757 and RFC 1513.

For full RMON an external probe must be used.

For information on supported groups, see the following table:

Name	Support Info
1. Statistics:	<i>Supported:</i> — The Token-Ring MAC-Layer Statistics Group. The Token-Ring Promiscuous Statistics Group.
2. History	<i>Supported:</i> — The Token-Ring MAC-Layer History Group. — The Token-Ring Promiscuous History Group.
3. Alarm	— <i>Supported</i> for all RMON variables. — <i>Not supported</i> for other MIB variables.
4. Hosts	<i>Not supported.</i>
5. HostTopN	<i>Not supported.</i>
6. Matrix	<i>Not supported.</i>
7. Filter	<i>Not supported.</i>
8. Capture	<i>Not supported.</i>

Table 9. Supported RMON Groups

Name	Support Info
9. Event	<i>Supported.</i>
10. Token-Ring	<p><i>Supported:</i></p> <ul style="list-style-type: none"> — The Token-Ring Ring Station Group. Only <i>supported as read</i>. That is, only the entries created as default can be read. The ring station table is not supported. — The Token-Ring Ring Station Order Group. — The Ring Station Config Table. <p><i>Not supported:</i></p> <ul style="list-style-type: none"> — The Token-Ring Ring Station Config Group. — The Token-Ring Source Routing Group.

Table 9. Supported RMON Groups

Built-in Port Counters

The SmartStack STS16-20D/STS16-20R 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

All SmartStack STS16-20x switches are stackable.

SmartStack STS16-20D/STS16-20R switches can be stacked using the included SmartStack STS-LM Link Module, the optional SmartStack STS-5SU Stacker Unit or the optional SmartStack STS-8SU Stacker Unit for connecting up to eight switches in a stack.

The STS-LM Stacker Link Module is a built-in feature of the SmartStack STS16-20D and SmartStack STS16-20R Switches, the other two stacker units are optional. The following sections describe how to stack the STS16-20x switches.

Back-to-Back

Two STS16-20x units can be connected together by fitting each switch with the SmartStack STS-LM Link Module and connecting the switches together using an appropriate stacker link cable. This simple connection doubles the number of ports available.

Internal Stacker

The STS-5SU Internal Stacker Unit can be inserted into the stacker port of a switch. It allows up to five switches from the SmartStack STS16-20RM switch family to be stacked together. One of the switches in the stack must contain the STS-5SU Internal Stacker Unit. The other switches in the stack must be equipped with a STS-LM Stacker Link Module and an appropriate stacker link cable. This can result in a stack of as many as five STS16-20x switches. The STS-5SU Internal Stacker Unit works as a common backplane switching fabric, which provides 1.4 Gbps of aggregate bandwidth.

External Stacker

The SmartStack STS-8SU External Stacker Unit is an external stack unit that allows up to eight STS16-20x switches to be stacked together. Each switch in the

stack must be equipped with a STS-LM Stacker Link Module and an appropriate stacker link cable. The SmartStack STS-8SU External Stacker Unit works as a common backplane switching fabric, which provides 2.2 Gbps of aggregate bandwidth.

- ▶ **Note:** The SmartStack STS16-20D and the SmartStack STS16-20R can be stacked together with other switches from the STS16-20x family in any desired combination. All switches in a stack must, however, run the same software version.

Optional Redundant Power Supply on SmartStack STS16-20R

The SmartStack STS16-20R Token Ring Switch has an input for a backup power supply (see Figure 22. in Chapter 4, “Installation”). It is compatible with the SmartStack STS-RPC Redundant Power Center, which can supply back-up power for up to six switches, when up to six SmartStack STS-PSU Redundant Power Supply Unit are installed in the chassis. This gives a high degree of resilience to power supply failures. The SmartStack STS16-20R will switch to 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 SmartStack STS-8SU Stacker Unit also accommodates an optional switch matrix STS-SM, which includes a redundant power supply, ensuring the highest degree of resilience in the stack of switches.

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



3. Preparing for Installation

Before installing the SmartStack STS16-20D/STS16-20R, read this chapter carefully.

Safety Recommendations

Follow these guidelines to ensure general safety during and after the installation:

- Keep the chassis area clear and dust-free during and after installation.
- Keep tools away from walk areas where you and others could trip over them.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

Safety with Electricity

Follow these guidelines when working on equipment powered by electricity.

- ▶ **Danger:** Do not open the switch. Dangerous voltage inside.
- ▶ **Danger:** To avoid shock hazard, the power cord must be connected to a properly wired and earthed receptacle. Any equipment to which the switch will be attached must also be connected to properly wired and earthed receptacles.
- ▶ **Warning:** Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, bracelets and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.
- ▶ **Warning:** Do not work on the system or connect or disconnect cables during periods of lightning activity. Read the installation instructions before you connect the system to its power source.

To turn **off** the switch, you must disconnect the power cord; there is no on/off switch. ON/OFF switch. Note that if the switch is connected to an external Redundant Power Supply Unit (RPSU), the power cord must be removed from both units.

- Locate the emergency power-off switch for the room in which you are working. Then, if an electrical accident occurs, you can act quickly to turn off the power.

Site Requirements

Following are the site requirements for installation.

Environment

Choose a clean, dust-free, preferably air-conditioned location. Avoid direct sunlight, heat sources, or areas with high levels of EMI (Electromagnetic Interference).

Chassis Accessibility

Make sure the front and back panel of the equipment is accessible so that you can monitor the LED indicators and access the control switches. Leaving enough clearance at the front and back will also allow easier cabling and service.

Cooling and Airflow

Two fans, which are located at the left side of the switch, cool the interior by drawing air through vents on the left side and forcing heated air out through holes in the right side. If the internal temperature exceeds 50°C (112°F), a temperature error is reported to the console.

- **Caution:** To protect the equipment from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 40°C (104°F). To prevent airflow restriction, you must allow at least 7.6 cm (3") of clearance around chassis openings for proper airflow.

Power

The source electrical outlet should be installed near the switch, be easily accessible, and be properly grounded.

Also, observe the following power cable considerations before you start the installation of the SmartStack STS16-20D Token Ring Switch and/or the SmartStack STS16-20R Token Ring Switch.

11. The socket outlet shall be installed near the equipment and shall be easily accessible.
12. To prevent electrical shock, the power cord set used must comply with national regulations.
 - a. The female receptacle of the cord must meet CEE-22 requirements.

- b. 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.
- c. 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 SmartStack STS16-20D Token Ring Switch and/or the SmartStack STS16-20R Token Ring Switch while you are installing the unit to avoid dropping it on the floor or any equipment beneath it in the rack. The SmartStack STS16-20D Token Ring Switch and the SmartStack STS16-20R Token Ring Switch unit each weighs approximately 7.2 kg (15.9 lbs).
- ▶ **Caution:** To separate the switch from the power, pull the power cord completely out from the socket. The power socket must be easily accessible and located near the unit.
- ▶ **Warning:** All RJ-45 connectors must only be connected to safety extra low voltage (SELV) circuits like local area networking (LAN).
- ▶ **Warning:** This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).
- ▶ **Warning:** A voltage mismatch can cause equipment damage and may pose a fire hazard. If the voltage indicated on the label is different from the power outlet voltage, *do not connect the chassis to that receptacle.*
- ▶ **Caution:** If you are using the redundant power supply unit SmartStack STS-PSU (only available for SmartStack STS16-20R), note that this unit is **not** hot-swappable. You must *turn off* the SmartStack STS-PSU Unit and the switch before connecting or disconnecting the DC power cable.

Configuration Guidelines

This section will help you understand the physical configuration restrictions for the SmartStack STS16-20D/STS16-20R. Read the guidelines in the following sections before you start installing the switch. In brief, remember the following rules when planning to install the switch:

- 18,192 byte maximum physical frame length.
- For shared-media LAN segments, acceptable distances are defined by the hub or concentrator attached to the switch port.
- Straight-through cables for all ports.
- If you create parallel paths directly between switches, be sure that you have enabled the spanning tree (see “Spanning Tree for BR/Screen” on page 99). The default setting for the spanning tree protocol is disabled.
- The spanning tree protocol will not function between different BRFs within one switch.

The following sections contain more detailed information.

Frame Length Limit

The SmartStack STS16-20D/STS16-20R supports a maximum physical frame length of 18,192 bytes (from the Frame Control, FC, to the Frame Check Sequence, FCS, characters). This corresponds to a Maximum Transfer Unit (MTU) of 17,800 bytes.

The *default* maximum physical frame length of the switch is 4,546 bytes which corresponds to an MTU of 4,472 bytes. The *actual* MTU size of a VLAN is configured in the **VLAN Parameter Configuration for BR/Screen** screen, see page 91.

The switch truncates frames larger than the configured maximum physical frame length and adds an abort sequence at the end. Characteristically, if frames are sent longer than the frame length limit, the abort sequences will be reported as frame errors by other ring stations.

In a stack of switches, all stacker link modules in the stack must support 18 KB frames for any switch in the stack to support frames sizes longer than 4,546 bytes. Additionally, if you are using ATM uplinks in any SmartStack STS16-20RM/STS16-20FRM, all ATM uplinks in the stack must support 18 KB frames for any switch in the stack to support MTU sizes greater than 4,472 bytes.

To verify that your hardware supports 18 KB frames, view the **Module Information** screen, described on page 84. Stacker link modules and ATM uplinks that do not support 18 KB frames will have the text (4K) displayed immediately after the hardware revision level.

Ring Numbers

Forwarding 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, auto-configuration of ring numbers is not possible. In this case, you have to configure the ring numbers manually.

Sample Uses of the SmartStack STS16-20RM Family Switches

The Cabletron Systems SmartStack STS16-20D/STS16-20R switches allow you to increase the performance of the network by providing dedicated bandwidth to individual workstations. You will typically deploy SmartStack STS16-20D/STS16-20R as a second step of migration from a hierarchical Token Ring network consisting of a backbone segment and workgroup segments towards a fully switched network:

- Step 1 of the migration involves redesign of the backbone by replacing a shared 16 Mbps Token-ring backbone with a switched backbone utilizing SmartStack STS16-20RM or SmartStack STS16-20R. The backbone usually serves as interconnection of the workgroup segments and the server farm segment.
- Step 2 of the migration increases the performance of the network by providing dedicated full-duplex 16 Mbps bandwidth to individual workstations utilizing SmartStack STS16-20D/STS16-20R switches.

Figures 11, 12, 13 and 14 illustrate the migration steps. Figure 11 shows a typical 3-layer network design built with source-routing bridges. Figure 12 shows how the backbone is optimized using SmartStack STS16-20RM or SmartStack STS16-20R. Figure 13 shows the deployment of SmartStack STS16-20RM or SmartStack STS16-20R as segment switches while Figure 14 shows the next step where a dedicated bandwidth is delivered to individual workstations. For such network design SmartStack STS16-20RM provides all the flexibility needed to use fiber to extend distances, or increase the number of ports, while SmartStack STS16-20D/STS16-20R provides the low-cost needed for dedicated bandwidth to individual workstations.

The SmartStack STS16-20D/STS16-20R switch is intended to increase the network bandwidth. Replacing a shared Token Ring segment with a SmartStack STS16-20D/STS16-20R delivers N times 16 Mbps bandwidth. For example, replacing a shared ring with 10 users with a SmartStack STS16-20D/STS16-20R delivers 10 times 16 Mbps—a 10-fold bandwidth increase.

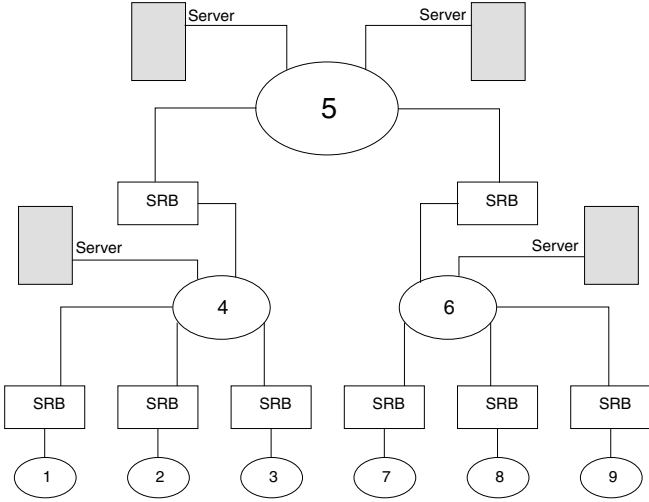


Figure 11. Typical Network without the SmartStack STS16-20D/STS16-20R

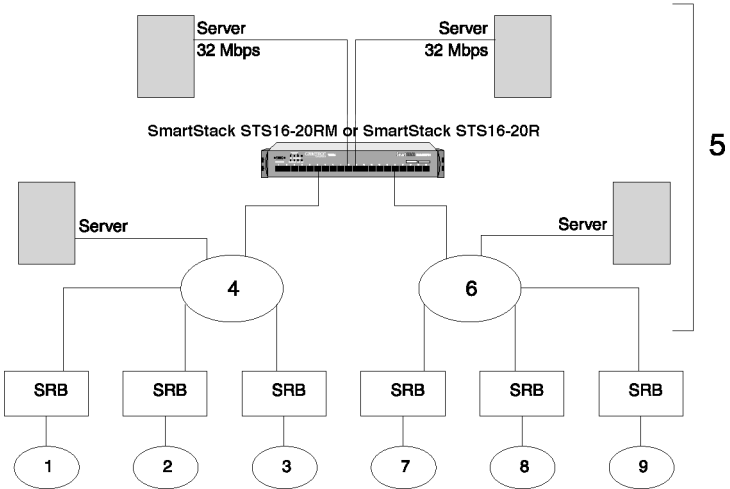


Figure 12. Relieving the Overstressed Backbone

Deployment Scenarios

SmartStack STS16-20D/STS16-20R includes a built-in stacker link. To create a stack of SmartStack STS16-20x switches you can use any switch in this series as an interface point for the stack. To do this, you use either a SmartStack STS-8SU Stacker Unit or a SmartStack STS-5SU Stacker Unit. Using the stacker link and an appropriate stacker unit it is possible to build a large switch stack combining several ports on one switch with ports on one or more other several SmartStack STS16-20x switches. You can use the expansion module slots of the SmartStack STS16-20RM/STS16-20FRM to get ATM, High-Speed Token-Ring as well as Fast Ethernet Translational Switching connectivity for the whole stack including the SmartStack STS16-20D/STS16-20R.

You can use all the ports in the stack as one switched ring (a single CRF), or should your network design call for it, allocate ports on to different rings. The SmartStack STS16-20D/STS16-20R provides all the flexibility of the SmartStack STS16-20RM/STS16-20FRM with respect to defining switched rings (CRFs) and bridges (BRFs).

Figure 15 shows a scenario using a stacker links and a switch stacker unit.

- Several ports on SmartStack STS16-20RM are combined with ports on the SmartStack STS16-20D/STS16-20R to create a switched ring.
- Ports on SmartStack STS16-20D/STS16-20R are intended for users who need the dedicated bandwidth and for file servers while SmartStack STS16-20RM/STS16-20FRM supports shared media Token Rings in a transition period and extends the backbone Token Ring using fiber.

An alternative way of migrating shared rings to switched rings is to use existing cables as connections between SmartStack STS16-20RM and SmartStack STS16-20D/STS16-20R. In this way, the distance limitations of the stack solution are bypassed and the ring is geographically extended to cover more than one wiring closet. A network port (ports 1 to 20 on SmartStack STS16-20R and ports 17 to 20 on SmartStack STS16-20D) can be used to connect two switches from the SmartStack STS16-20RM family together using existing cables. In order to increase the resilience of the network you can connect the SmartStack STS16-20D/STS16-20R to two different switches from the SmartStack STS16-20x family that use multiple network ports.

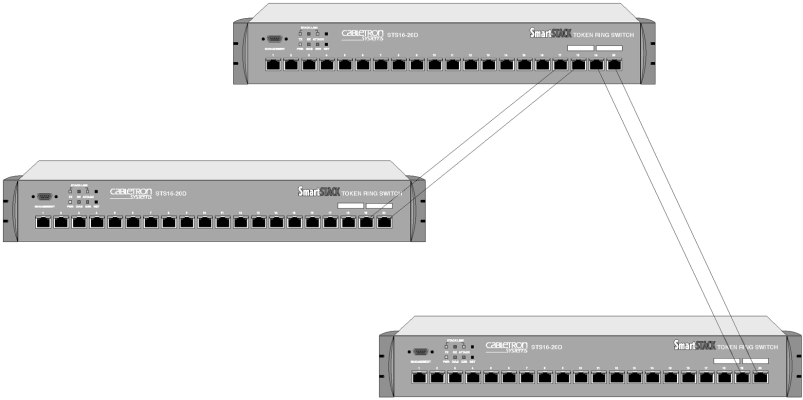


Figure 16. Setting Up CrossLinks



4. Installation

This chapter contains step-by-step instructions for installing, connecting and verifying that the SmartStack STS16-20D Token Ring Switch and/or the SmartStack STS16-20R Token Ring Switch is operating properly.

Installation Summary

The installation sequence is listed in the following steps.

1. Plan for installation. Read Chapter 3, “Preparing for Installation”.
2. Unpack the switch.
3. Gather the materials.
4. Mount the switch.
5. Connect the switch to the network.
6. Verify the operation of the switch.

► **Note:** Complete the following step only if you will be customizing the configuration of the switch or monitoring its activity.

7. Configure the switch.

► **Note:** For information on front panel and back panel connectors, buttons, slots, and LEDs, please see “Front Panel Details” on page 5 and “Back Panel Details” on page 9 in Chapter 1.

Package Contents

Immediately after receiving the equipment, examine all shipping containers and contents for damage. If any damage has occurred, notify the shipping carrier. Unpack the unit by removing the packing material and lifting it from its protective enclosures. Visually examine the equipment and check the container for related parts and accessories. You should have the following items:

- One SmartStack STS16-20D Token Ring Switch
OR
One SmartStack STS16-20R Token Ring Switch
- One CD-ROM containing the Token-Ring switch software and the SmartStack Manager for Windows, as well as user documentation in PDF format
- One printed *SmartStack Manager for Windows Installation and User Guide*
- One printed *SmartStack STS16-20D/STS16-20R Token-Ring Switches Installation and User guide*
- One serial cable for the management port
- One plastic bag containing four adhesive rubber feet and rack mounting screws, an Allen key, nuts and washers

Report any missing parts and any damage, not related, to shipping to your customer service representative.

► **Note:** Keep the packing materials for future use. *All components returned under warranty should be shipped in their original packing materials.*

If you have received your equipment before your site is fully prepared, after inspection, you should keep all of the components in the original shipping containers and store them in a physically and environmentally safe place.

Materials needed for Installation

To install the switch, you need the following items:

- If the unit will be installed in a rack, you need:
 - A rack inventory chart and a cabling chart from your network administrator.
 - The supplied set of screws, nuts and washers along with the Allen key tool.
 - A properly earthed power cord.
- If the unit will be installed on a surface (such as a tabletop), you will need:
 - A cabling chart from your network administrator.
 - The four supplied adhesive rubber feet.
 - A properly earthed power cord.

Mounting the Chassis

The SmartStack STS16-20D/STS16-20R can be mounted in a standard 19-inch rack or cabinet, or can be mounted on any flat surface such as a tabletop. The installation area should be near a power source and should have enough room around the front and back panels for cabling and access to controls. Use the following procedures for the installation of the SmartStack STS16-20D/STS16-20R.

- ▶ **Warning:** Only trained and qualified personnel should be allowed to install or replace this equipment.

Rack or Cabinet Mounting

If you install the equipment in a closed or multi-unit rack, observe the environmental guidelines from the previous chapter, Chapter 3, “Preparing for Installation”.

- ▶ **Caution:** The following rack mounting instructions need to be observed to ensure that the SmartStack STS16-20D/STS16-20R and any other equipment are mechanically stable.

The following steps describe how to mount the SmartStack STS16-20D/STS16-20R in a rack or cabinet:

1. Remove the bracket covers on each side of the SmartStack STS16-20D/STS16-20R to expose the rack mounting brackets. Access to the retaining screws is obtained by opening the cap on the front of each bracket cover. Use the Allen key supplied with the switch to remove the two 6 mm Allen screws. When you have removed the screws, push the bracket cover towards the back of the switch and lift the cover off. Keep the screws for later use.

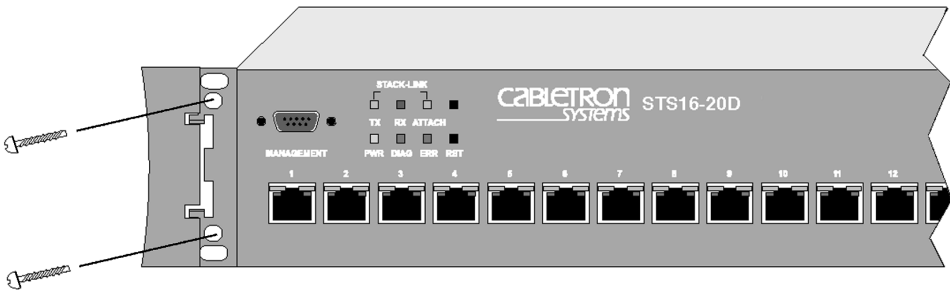


Figure 17. Exposing the Rack Mounting Bracket

Before going on to the next step, be sure you have the proper hardware for mounting the chassis with the exposed brackets to your cabinet or rack.

- Position the SmartStack STS16-20D/STS16-20R, with the exposed mounting brackets, in the rack or cabinet and slide it up or down until the bracket holes line up with the rack holes. Attach the chassis brackets to the rack using the Allen screws you removed in the previous step and the nuts supplied with the switch. Close the cap again to conceal the screws.

► **Note:** Only fixed brackets are supplied with these units. If you want to install a sliding pullout mount, you will need to provide the extra mounting hardware.

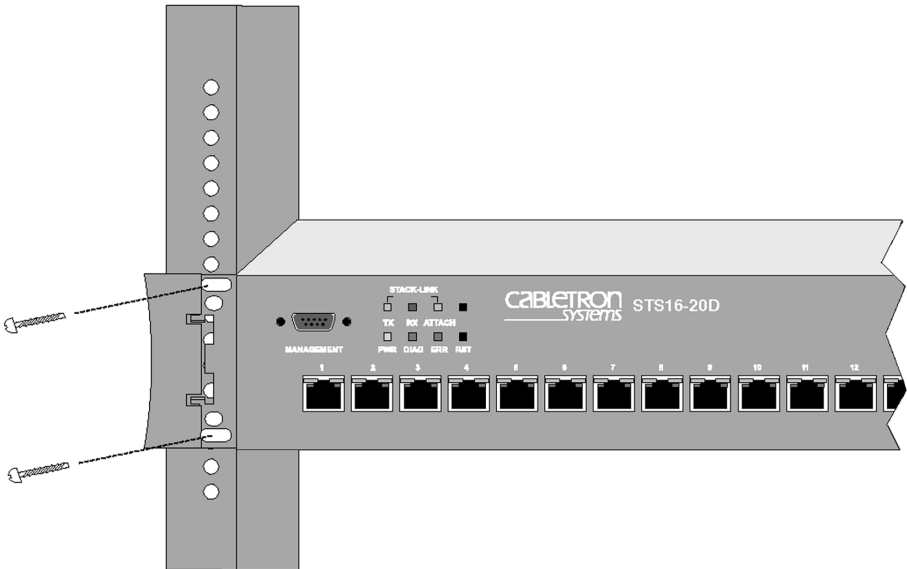


Figure 18. Mounting the Switch in a Rack or Cabinet

Table-Mounting

The SmartStack STS16-20D/STS16-20R operates at a low noise level, which makes it suitable for a large enough flat surface such as a table.

Four self-adhesive pads are supplied with the switch. The pads must be mounted in the four recesses on the bottom of the switch. When the pads are mounted, simply place the switch on a clear, level location. Leave enough room around the switch for ventilation and access to the controls and cable connectors.

► **Caution:** Due to weight constraints, place no more than three units (or the equivalent weight of other equipment) directly on top of another chassis. More than three units on top of another unit may cause damage to the lower unit.

Cabling

- **Note:** For information on connectors, buttons, slots, and LEDs, please see “Front Panel Details” on page 5 and “Back Panel Details” on page 9 in Chapter 1.

This section provides instructions for connecting devices (such as hubs, servers, personal computers, and workstations) to the SmartStack STS16-20D/STS16-20R. Remember these tips when connecting cables:

- Avoid stretching or bending the cables excessively.
- Avoid routing the cables near potential sources of electromagnetic interference, such as motorized devices and fluorescent lights.
- Avoid trip hazards by routing the cables away from aisles and other areas where people walk. If such routes cannot be avoided, use floor cable covers or similar material to secure and protect the cables.
- Be sure that the cables connected to the switch are supported so that the cable connectors are not excessively strained.
- Use a Category 3 or better UTP cable or a 150 ohm, STP or STP-A cable with an impedance-matching balun at each end.

See Appendix B, “Cable and Pin Information” for specific information on supported cable types, cable lengths and connector pinouts.

Connecting Devices to the Token Ring Ports

If you will not be using building wiring (in-the-wall cables) to connect the device to the SmartStack STS16-20D/STS16-20R, perform the following steps. If you will be using building wiring, follow the steps beginning with step 1 on page 61.

Follow these steps to connect one or more devices to the Token Ring ports on the switch:

1. Using the SmartStack STS16-20D/STS16-20R Cabling Chart provided by your network administrator as a guide, connect the cables between the switch and other devices as illustrated in Figure 19. Note that the figure illustrates an RJ-45 connector on each end. Depending on the cable type you use, the device end of the cable may also have a 9-pin D-shell or 150 ohm Data Connector.
2. If the switch is rack-mounted, dress the switch end of the cables through a cable management bracket, if one is present on your rack.
3. Label each end of the cables so that it will be easy to find the device if you have to troubleshoot a network problem.

Suggested information to place on the label includes the room location of the

device at the other end, a unique cable identification number, the MAC address of the connected device, and the number of the port to which the cable is attached.

4. To continue installing the switch, go to “Applying Power” on page 63.

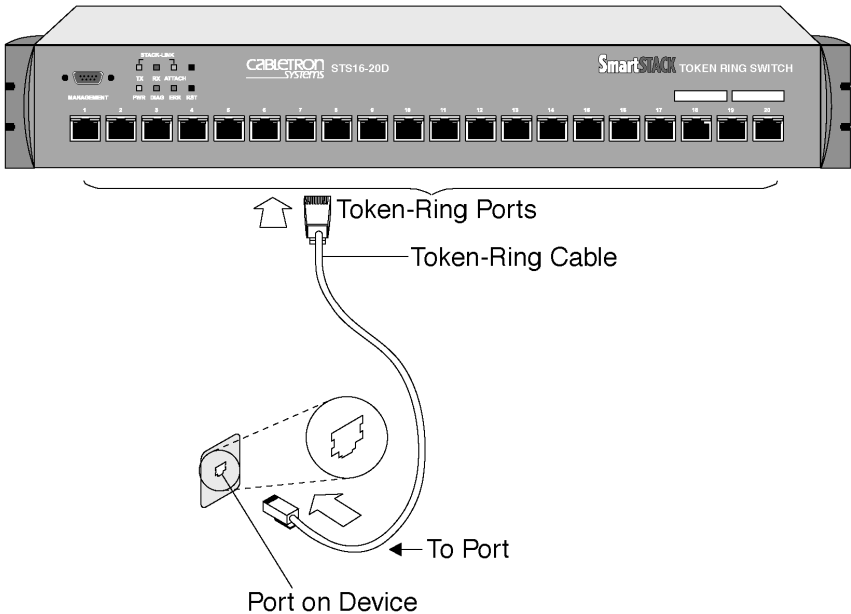


Figure 19. Connecting Devices to Token Ring Ports

Connecting Devices to the Token Ring Ports Using Building Wiring

If you will use building wiring (in-the-wall cables) to connect the device to the switch, perform the following steps:

1. Using the Switch Cabling Chart provided by your administrator as a guide, connect the cables between the devices and the faceplates as illustrated in Figure 20.
2. Label the faceplate, so that it will be easier to find the device if you have to troubleshoot a network problem.
3. In the wiring closet, connect a cable to the Token Ring connector on the patch panel or other equipment where the building wiring terminates.

Applying Power

The SmartStack STS16-20D/STS16-20R chassis does not have an on/off switch. *Power is on when the unit is plugged into a power source.*

There are no user serviceable parts inside an SmartStack STS16-20D/STS16-20R. Any internal upgrades or service should be performed by qualified personnel **only**.

- ▶ **Caution:** If you are using the STS-PSU Redundant Power Supply Unit on STS16-20R, note that this unit is *not* hot-swappable. You must *turn off* the STS-PSU Redundant Power Supply Unit and the switch before connecting or disconnecting the DC power cable.
- ▶ **Warning:** Unplug the power cord before you work on a system that does not have an on/off switch.
- ▶ **Warning:** When installing the unit, the ground connection must always be made first and disconnected last.
- ▶ **Warning:** This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Use the following steps to power on your equipment.

1. Ensure that you are using the correct power source.
2. Using a power cable that complies with national regulations, plug the female end of the cable into the AC power connector on the back panel of the switch (see Figure 21 or Figure 22).
3. Plug the male end of the power cord(s) into a properly grounded electrical outlet.

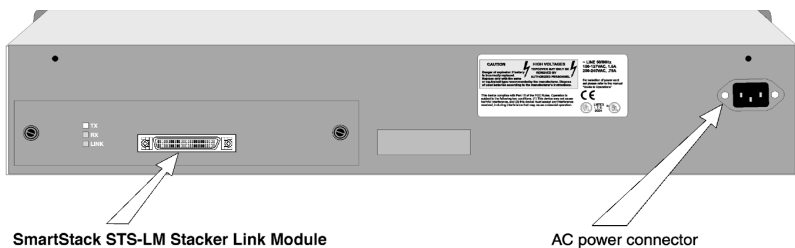


Figure 21. The back panel of the STS16-20D

Stacker Link Module

The SmartStack STS-LM Internal Stacker Unit which is factory installed in the SmartStack STS16-20D/STS16-20R switch is a single port interface module that is installed into the back slot of the Switch. When SmartStack STS16-20RM family Switches are connected through SmartStack STS-LM Modules, the switches can be combined to form one logical switch. The SmartStack STS-LM front panel is shown in Figure 23.

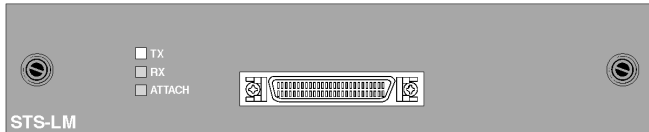


Figure 23. SmartStack STS-LM Front Panel

Installation

Use the following steps if you need to reinstall the SmartStack STS-LM module in the SmartStack STS16-20D/STS16-20R Token Ring Switch.

► **Note:** Stacker Link modules are **not** hot-swappable. Always be sure that the power is off before installing or removing a module. If the power is on, damage to the equipment may result. Once the module is installed in the SmartStack STS16-20D/STS16-20R, external cables may be connected or removed without having to remove power from the switch.

1. Disconnect power to the SmartStack STS16-20D/STS16-20R switch.
2. If a blank cover is over the stacker slot on the back panel, remove it by unscrewing the two attachment screws.
3. To prevent possible static damage to the module, hold it by its edges only. Be careful not to touch the top or bottom.
4. Slide the module into the slot evenly, taking care to line up the edges with the guides.
5. Seat the module by pressing the front of the module with your thumbs.
6. Secure the module to the chassis by tightening the thumb (panel) screws at the left and right edges of the module's front panel. Do not overtighten the screws.
7. Return power to the switch.

SmartStack STS-LM Connectors and LEDs

The following tables describe the connectors and LEDs on the STS-LM front panel.

Connector	Description
Stacker Port	50-pin SCSI-2 connector for proprietary Stacker Link cable.

Table 10. SmartStack STS-LM Network Connector

LED	State	Description
TX	On	Data is being transmitted from the attached switch.
RX	On	Data is being received by the attached switch.
ATTACH	Off	No connection has been established.
	On	A connection has been established.

Table 11. SmartStack STS-LM LEDs

Connecting the Stacker Link Cable

When connecting two or more stacker link modules together to form a stack, you must use the proprietary 50-pin cable supplied with the module.

The SmartStack STS16-20D/STS16-20R switch can be configured in three different ways to form a stack of switches:

- Two of the SmartStack STS16-20RM family switches back-to-back via two SmartStack STS-LM modules
- Up to five SmartStack STS16-20RM family Switches via one SmartStack STS-5SU Stack Link Module and up to four SmartStack STS-LM Modules.
- Up to eight SmartStack STS16-20RM family Switches via one SmartStack STS-8SU Stacker Unit and up to eight SmartStack STS-LM Modules.

When inserting the cable connector, keep the connector straight to minimize the risk of bent or damaged pins.

Note: Stacked SmartStack STS16-20RM family switches must all have the same software version.

Working with a Stack

When the SmartStack STS16-20D/STS16-20R switch powers up, it runs through a series of diagnostics. Immediately after the diagnostics are complete, the SmartStack STS16-20D/STS16-20R enters the stack discovery mode. The discovery mode is used to sense if the unit is cabled to other SmartStack STS16-20D/STS16-20R units. If the SmartStack STS16-20D/STS16-20R is connected to other units during the discovery mode, the switches automatically combine to form a stack.

Each unit is assigned a box number, and the box with the lowest number becomes the stackmaster. When accessing switch-specific settings from a management console, you will be prompted for the box number. In a back-to-back configuration, the box number is determined by software. In configurations using the SmartStack STS-8SU or STS-5SU units, the box number is determined by the port number.

The switches in the stack combine certain configuration parameters so that the stack as a unit uses one set of parameters. These parameters are discussed below in “Inter-box Parameters”.

The stack can now be managed as a single entity from a management console or management application.

Inter-box Parameters

The SmartStack STS16-20D/STS16-20R switches participating in the stack must combine configuration information so that the stack as a whole uses common parameters. One of the participating switches becomes the provider of inter-box parameters.

If the switches have the same configuration information, the switch that becomes Box 1 becomes the provider. If the configuration information is different, a split-stack will be formed and a warning message will be displayed on the console screen. You will be requested to briefly press the SysReq button on the switch that is to be the provider of inter-box parameters. When you have selected the provider, the other switch will replace its stack related configuration parameters with those of the provider.

5. Accessing Switch Management

The switches can be configured in two ways:

1. Using the switch console.

You can access the switch console interface

- directly, by connecting a VT100 terminal emulator to the RS-232 port labelled MANAGEMENT.

OR

- remotely, via Telnet.

2. Using SNMP based graphical management applications:

- The SmartStack Manager for Windows
- Other Simple Network Management Protocol (SNMP) based applications

Overview

This chapter only describes how to access the switch console via the MANAGEMENT port. Refer to the section “Console/Telnet Sessions” on page 132 for information on configuring serial console and/or telnet console sessions.

Network management applications (in-band management) are beyond the scope of this guide. However, note that to be able to manage the switch by the network management application via SNMP, you will have to configure a few settings first in the switch console. These are typically the IP Address, SNMP Community, and Trap Receiver.

3. Use the values listed in the following table to set the configuration parameters on your console for interfacing to the SmartStack STS16-20D/STS16-20R.

Specification	Value
Baud Rate	2400, 4800, 9600, 19200, 38400, 57600
Parity	None
Data bits	8
Stop bits	1
Handshaking	None
Terminal emulation	VT100
Duplex	Full
Software flow control (XON/XOFF)	Off (input and output)
Hardware flow control (RTS/CTS)	Off
Autobaud upon break	On
Line wrap	On
Screen scroll	On
CR translation	CR
Backspace (BS) translation	Destructive
Break length (milliseconds)	350
Enquiry (ENQ)	Off
EGA/VGA true underline	Off
Terminal width	80
ANSI 7 or 8 bit commands	7

Table 13. Console Configuration Settings

Specification	Value
Microsoft Windows terminal emulation	Disable the “Use Function, Arrow, and Ctrl Keys for Windows” option located in the Terminal Preference menu

Table 13. Console Configuration Settings

- At power on (cold boot), the SmartStack STS16-20D/STS16-20R performs a series of self-test diagnostics verifying that hardware components are functioning. An example of the self-test diagnostic screen is shown later in this chapter.

Communication Problems

If the diagnostic list does not appear, or is garbled, try adjusting the baud rates between the console and the SmartStack STS16-20D/STS16-20R by using the Autobaud routine within the switch. To do this, press the reset button on the front of the switch and wait for the internal diagnostics to finish (the DIAG LED turns off). The reason for the reset is that in case the switch’s Autobaud routine is disabled, resetting it will set it to its default mode *Autobaud enabled*.

Depending on the type of the console, there are several console command keys that will potentially initiate the Autobaud routine in the SmartStack STS16-20D/STS16-20R. Four of these keys are RETURN, the combination keys ALT-B, the BREAK key, and ESC.

After the DIAG LED turns off, try one of the command keys at the console, and press it repeatedly. If there is no response, wait several seconds and again, press it repeatedly. If necessary, perform the same routine using the other command keys.

If this does not work, and there is garbled output on the screen, try pushing the unlabeled system request button on the SmartStack STS16-20D/STS16-20R. As soon as garbled characters appear, press the console’s ENTER (or RETURN) key twice in rapid succession. (Again, try the other command keys as necessary).

If the problem remains, try the following steps:

- Check all of the cable connections.
- Check the baud rate at the console’s set up screen; if it is not set to 9600, try this setting.
- Try setting the console baud rate to different values up or down, and pressing RETURN for each selection.
- If you are using a terminal emulation program, try exiting the program and restarting.

5. If you still can not get the connection to work, contact a support person.

Diagnostic Screen

The diagnostic self-test displays two different screens, depending on whether you perform a cold boot (power-on cycle with full diagnostics), or a warm boot (a reset without full diagnostics). The warm boot contains portions of the complete cold boot list.

The following is an *example* of a diagnostic screen during a boot process. The actual screen may vary depending on, for example, hardware, options, and software version levels:

BootStrap Firmware v2.3, Copyright 1996-1998

- Initiating bootstrapping sequence.
- Boot image integrity check...Passed.
- Control transferred to boot process.

Boot Firmware (Phase II) v2.3

- Program memory test.....Passed.
- Relocating main image to
DRAM.....Done.
- Main image integrity check...succeeded.
- Control transferred to main process.
- Starting Power On Self Test Diagnostics.
 - Network memory test 32-bits.....Passed.
 - Network memory test 16-bits.....Passed.
 - Network memory test 8-bits.....Passed.
 - Port register and memory test.....Passed.
 - Single port loopback test.....Passed.
 - All ports linked loopback test.....Passed.
 - Port MAC test.....Passed.
- Completed Power On Self Test Diagnostics.

System Software Version 4.0.0, Copyright 1994-1999.

System started on Mon. June 21, 1999 14:30:03

8 Megabytes System memory

2 Megabytes Network memory

- Initialization started
- File system initialized
- System temperature is within safe operating levels
- Checking file system integrity
- Warmboot initialization started
- LAN ports detected:
 - RJ-45 Token Ring: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
 - StkPort : 29
 - Initializing Ports: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

```

20 29
- Initializing system address table
- System entering stand-alone mode
- Enabling port: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 22 22
23 24
Press RETURN key to activate console...

```

Depending upon which tests have run, verify that all diagnostics have passed and that the ERR LED is off. If the ERR LED is on, read the screen to determine which test failed. Also see Chapter 10, “Troubleshooting”, to help find the cause.

At the end of the boot messages, you should be prompted to press RETURN (ENTER). The following greeting screen of the switch console manager should appear:

```

                                Cabletron Systems SmartStack Manager
                                (c) Copyright CABLETRON Systems, Inc. 1999
                                    P.O. Box 5005
                                Rochester, NH 03866-5005 USA
                                    (603) 332-9400

MAC Address:                000083:E34DC0

System Description: Cabletron SmartStack STS16-20; SW Rev 4.0.0

System Name:

System Contact:

System ID:                   1.3.6.1.4.1.52.3.9.1.13.1

                                Type Password, then press <RETURN>:
                                -- No password has been set, press <RETURN> to continue. --
                                -- To terminate TELNET connection now, press <CTRL><B> --

```

At the top level screen, press ENTER (RETURN) to enter the main menu. The contents of the main menu, the submenus and screens, are described in subsequent chapters. The information in these chapters includes configuring, monitoring, and viewing statistics on the SmartStack STS16-20D/STS16-20R.

► **Note:** If you have forgotten the password, you can delete it by pressing the unlabeled system request button on the front panel of the switch for one second. Then release it and select **Point 4. Clear the system password**. This will clear both the *Read-Only* and the *Read/Write* password.



6. Switch Configuration

This chapter explains how to set up the SmartStack STS16-20D/STS16-20R and to modify the configuration using a VT100 console 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 the console, see Chapter 5, “Accessing Switch Management”.

Subjects covered in this chapter:

- General guidelines (page 76)
- Main menu screen (page 78)
- Configuration menu (page 79)
- Switch and stack configuration (page 80)
- Module information (page 84)
- Virtual LANs (page 86)
- IP configuration (page 94)
- Spanning tree protocol (STP) (page 97)
- Port configuration (page 106)
- CrossLink channels (page 110)
- Address filtering (page 116)
- Address aging (page 126)
- Console password (page 130)
- Console/Telnet sessions (page 132)
- Syslog facility (page 139)
- DSRR configuration page 141()
- Download/Upload menu (page 147)
- Reset menu (page 152)

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 an 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 31.
- 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. In release 4.0 (and later) two types of users can be defined:

Read-only users:

These users cannot modify any of the configuration parameters. They can read everything (except the SNMP communities).

Read-write users:

These users have full access to all configuration parameters.

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 130 later in this chapter. To open the **Password** menu, select **Configuration → Password**.

For more explanation on the greeting screen, see Chapter 5, "Accessing Switch Management".

Navigating within the Menus

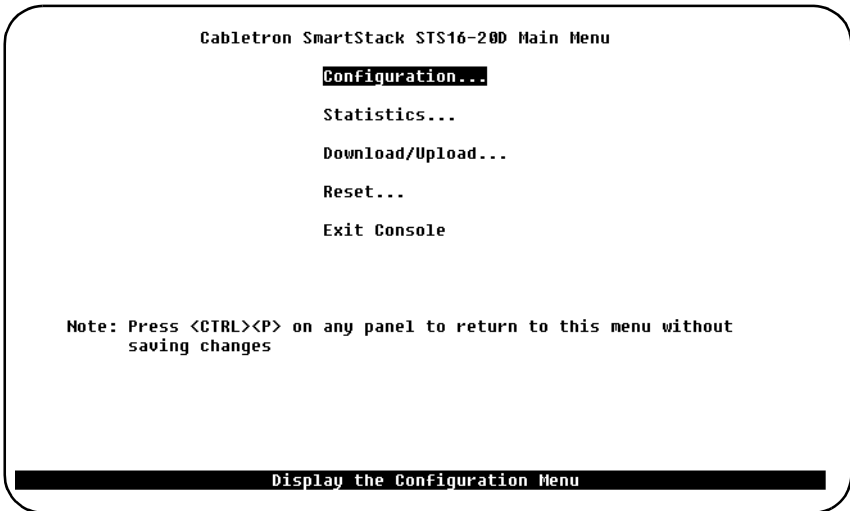
Use the arrow keys (cursor keys) to highlight an item on the screen or menu.

- 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



The main menu contains the following items, that give access to console screens and submenus:

Configuration...

Displays the **Configuration** menu, which enables you to view and set the SmartStack STS16-20D/STS16-20R configuration parameters. A detailed explanation of the configuration submenus is given on page 79.

Statistics...

Displays the **Statistics** menu for the SmartStack STS16-20D/STS16-20R. Explanations of screens in the **Statistics** menu are in Chapter 7, “Monitoring the Network from the Console Statistics Menu” on page 155.

Download/Upload...

Displays the **Download/Upload** menu that is explained in this chapter starting from page 147.

Reset...

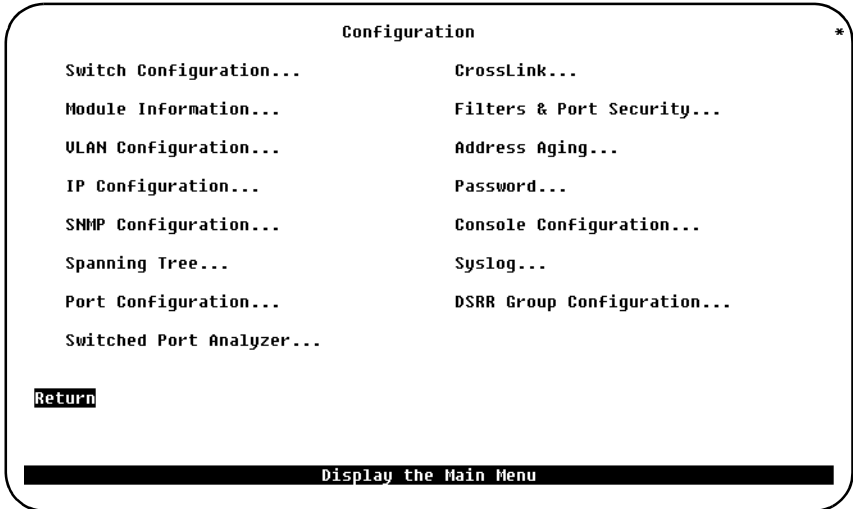
Displays the **Reset** menu that is explained starting from page 152.

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 selecting **Configuration** in the main menu. From the **Configuration** menu you can view and set the switch configuration parameters.



This chapter describes all submenus and screens.

Switch Configuration Screen

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

Use the **Switch Configuration** 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.

Switch Configuration	
System Description	Cabletron SmartStack STS16-20; SW Rev 4.0.0
Build Description	Release Software created Fri 24-Sep-99 10:28
DRAM/FLASH Installed	8 MB / 2048 KB
Burned-in MAC Address	000083:E34DC0
Configured MAC Address	000000:000000
Address Format	Non-canonical
System Name	
System Location	
System Contact	
Time of Day...	Thu. October 21, 1999 09:27:31
Return	Stack Configuration...
Display the Configuration Menu	

The following explains the fields in the **Switch Configuration** screen.

System Description

Name and model of the switch, or, in the case of a stack, the generic stack name. In addition to this, the firmware release is displayed. Information in this field cannot be changed.

Build Description

Describes when the firmware running in the switch was built. Information in this field cannot be changed.

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.

Burned-in MAC Address

The factory-assigned base MAC address of the SmartStack STS16-20D/STS16-20R. 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 SmartStack STS16-20D/STS16-20R, 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 address, the base MAC address, and possibly the next 96 addresses.

To configure a LAA address, use the **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 SmartStack STS16-20D/STS16-20R reserves 31 addresses for ports.

The Token Ring ports on a SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R reserves 63 addresses for BRF (VLAN).

Each VLAN has an attached bridge relay function (BRF) and a Management entity (IP-protocol stack), and consequently it needs a MAC Address. In the SmartStack STS16-20D/STS16-20R, 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 BRF's from the Switch Base Address + 32 (0x20) and upwards. The SmartStack STS16-20D/STS16-20R 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 BRF.

Summarizing each SmartStack STS16-20D/STS16-20R reserve: Switch Base Address + 31 Addresses for Token Ring ports + 63 MAC Addresses for BRFs = 95, which is rounded up to 96 or hexadecimal 0x60.

The MAC address of the default BRF (trnet-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 BRF will be based on the address of the stackmaster. The stackmaster is determined by software, when the stack consists of two switches back to back and by the port numbers in STS-8SU/STS-5SU stack configurations.

There is no simple rule to find the default MAC address of other BRF, but it is always in the range described in the following:

Stack Master Base Address + 32 < BRF MAC Address < Stack Master Base Address + 95. And a BRF (VLAN) MAC address is assigned, when the VLAN becomes preferred (that is, 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 (because, for example, ports are moved from one BRF 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 (BRF).

In version 3.10.0 (and later) it is possible to assign an individual, locally administrated MAC address to each VLAN.

► **Note!** A reboot of the switch is necessary after assigning the VLAN LAA. See "VLAN Configuration" on page 86.

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

Any text string of max. 64 characters that you have assigned for the switch.

System Contact

Any text string of max. 64 characters that you have assigned for the switch.

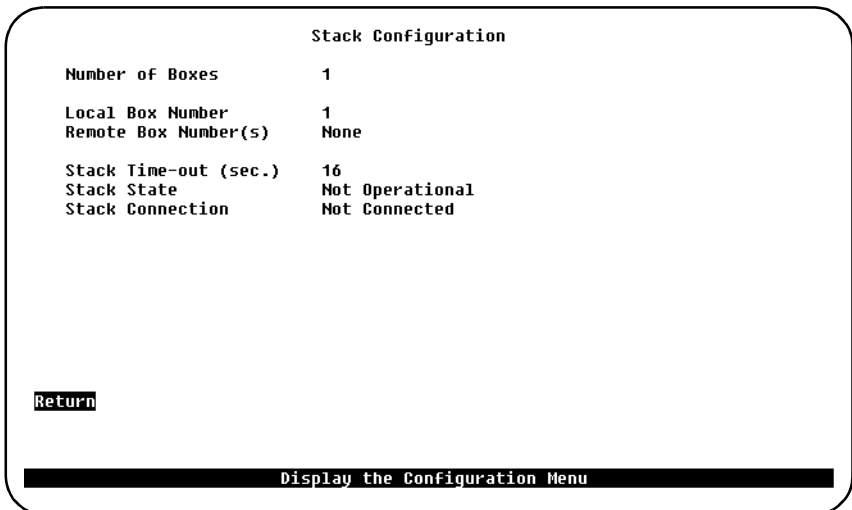
Time of Day

An internal clock is used to calculate total time of operation and time of day. To adjust the time, select this item, press RETURN, 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. Display only.

Local Box Number

Number assigned to the currently selected switch. The local box is also the source of the information displayed on this screen. Display only.

is listed as module 2.

Status

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

Model

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

Board ID

Decimal identifier of the module.

HW Rev

Hardware revision level. If (*4K*) is displayed after the number, this module will prevent the switch (or stack of switches) from operating with an MTU size above 4,472 bytes. If **HW Rev** is set to *NA*, the module does not support reading of the hardware revision.

FW Rev

Firmware revision level.

Ports

Number of ports on the module.

Up Time

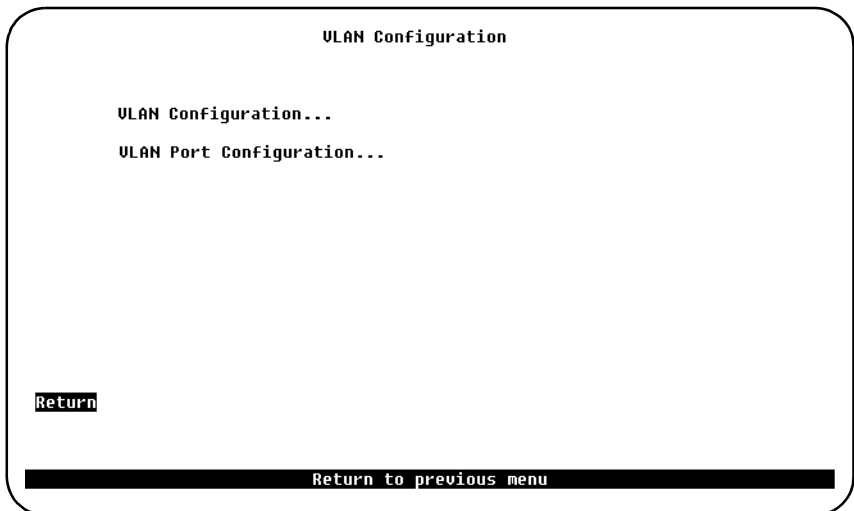
Amount of time that the module has been up (since the last reset).

You cannot change the information that appears on this screen.

- *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 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 ports in an existing CrossLink to different CRFs. On SmartStack STS16-20D only ports 17 to 20 allow CrossLink configuration.

VLAN Configuration Menu

To open this screen from the main menu, select **Configuration** → **VLAN Configuration**. See the section “VLAN Support” on page 31 for a discussion of VLANs.



More information on the various submenus follows.

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 BRV or CRF to change and brings up the VLAN Parameter Configuration screen.

Delete

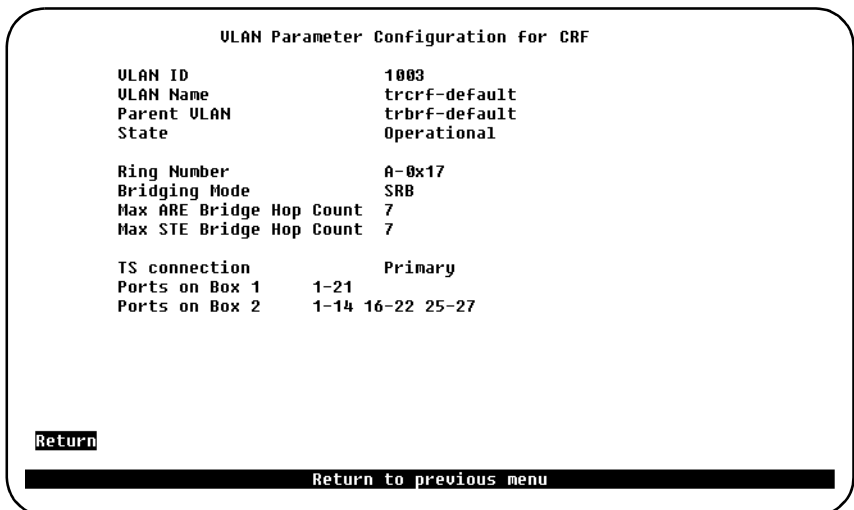
Lets you delete a BRV or CRF. You cannot delete a BRV if there are CRFs assigned to it, or a CRF if there are ports assigned to it.

VLAN Parameter Configuration for CRF 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 CRF.

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 BRVs.



The following information is displayed on this screen:

For each CRF of translational links connected to the same logical Ethernet segment, a connection attribute must be assigned:

- *Primary* connection—for a main connection to the Ethernet Cloud (default value for each CRF). This connection is always forwarding if active.
- *Secondary1*—for a backup connection to the logical Ethernet segment. This connection is always blocking if the primary is active.
- *Secondary2*—for a second backup connection to the logical Ethernet segment. This connection is always blocking if Primary or Secondary1 are active.

Each CRF of the translational links connected to the same logical Ethernet segment must have a different connection attribute.

VLAN Parameter Configuration for BRF 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 BRF.

Use this screen to add or change a BRF. Note that the trbrf-default cannot be deleted.

VLAN Parameter Configuration for BRF

VLAN ID	1005
VLAN Name	trbrf-default
State	Operational
MTU	4472
Bridge Number	0x0F
802.1Q VLAN ID	1005
LAA VLAN MAC address	000000:000000

Return

Return to previous menu

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. These values cannot be changed.

VLAN Name

ASCII name associated with the BRF. Up to 32 characters are allowed. The name must be unique. Neither BRFs nor CRFs can have identical names.

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 also depends on the hardware and 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 hardware and 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

This parameter configures the QTAG to be used for High-Speed Token-Ring and Translational Switching. If Q-tagging is used for this BRF, the default is set to the VLAN ID of the BRF. Refer to the guide shipped with the relevant module (only relevant for the SmartStack STS16-20RM/STS16-20FRM switches).

LAA VLAN MAC Address

Used to configure a LAA MAC address used for in-band management of the switch.

► **Note!** The switch must be rebooted before this configuration takes effect.

VLAN Port Configuration

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

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

VLAN Port Configuration			
Port	Type	CRF	BRF
1	TR	Logical-ring 3	BRIDGE-1
2	TR	Logical-ring 500	BRIDGE-1
3	TR	trcrf-default	trbrf-default
4	TR	trcrf-default	trbrf-default
5	TR	trcrf-default	trbrf-default
6	TR	trcrf-default	trbrf-default
7	TR	trcrf-default	trbrf-default
8	TR	trcrf-default	trbrf-default
9	TR	trcrf-default	trbrf-default
10	TR	trcrf-default	trbrf-default
11	TR	trcrf-default	trbrf-default
12	TR	trcrf-default	trbrf-default
13	TR	trcrf-default	trbrf-default
14	TR	trcrf-default	trbrf-default
15	TR	trcrf-default	trbrf-default

Return to previous menu

Port

The port number.

Type

Port type. Possible values are:

- *TR* For Token-Ring ports.
- *HSTR* For High-Speed Token-Ring ports.
- *ATM* For ATM ports.
- *TS* For translational switching ports.

CRF

CRF to which the port is currently assigned.

BRF

Parent BRF of the CRF to which the port is currently assigned.

IP Configuration Screen

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

Note! Ports must be assigned to a CRF that is a sibling of the selected BRF before IP assignment.

IP Configuration - trbrf-default

Interface MAC Address	000083:E261A0
IP Address	172.16.216.222
Default Gateway	172.16.160.6
Subnet Mask	255.255.0.0
IP State	BootP When Needed
Send PING	

Return

Display the Configuration Menu

Interface MAC Address

Displays the MAC address assigned to this BRF.

IP Address

Used to configure the IP address of the switch in the selected VLAN (BRF). To change it, highlight the field and press ENTER.

Default: 192.0.2.1

Default Gateway

Used to configure the default gateway. When sending IP packets from this VLAN to other IP networks, the packets are sent to the default gateway. This is why it must be on the same IP net as the IP address.

Default: 0.0.0.0

Subnet Mask

Changes the current subnet mask. If none is specified, the net mask used is the

default for the class of the IP address. If a subnet mask is specified, it will be used as a net 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 in the following:

- *IP Disabled*—When a VLAN is IP-disabled, it will not process any IP or ARP packets it receives. This means that no Ping, Telnet, or ARP Packets will be responded to when received. SNMP management is only possible over MAC.
- *BootP When Needed*—In this state, the switch will send out BootP requests at regular intervals on all ports in the VLAN until the VLAN is assigned an IP address different from *0.0.0.0* or *192.0.2.1*.

The assignment can come from NVRAM during a boot, from the console management or via BootP.

- *BootP Always*—In this state, the switch will at boot time clear the IP address assigned to this VLAN and send out BootP requests at regular intervals until it receives a BootP answer. Then normal IP communication will resume.

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

Send PING

Prompts you to enter an IP address to which the switch will attempt ping.

► **Note!** The configuration of the IP-address, default gateway etc. takes effect when you close the **IP Configuration** screen. This means that if any parameter has been changed you have to return to the **Configuration** menu and enter the **IP Configuration** screen before attempting to ping. Otherwise the old values will be used.

BootP Requests and Parameters

When using BootP to determine its IP address, the SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R may cease using BootP if the parameters are set (on menu 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 SmartStack STS16-20D/STS16-20R 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 VLAN enters a state where it would be necessary again.

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 the note on this page)
- Subnet Mask
- TFTP Main Code File 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 SmartStack STS16-20D/STS16-20R receives a BootP response that specifies a TFTP Bootfile name, the SmartStack STS16-20D/STS16-20R 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 149 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 8, “Monitoring the Network with SNMP”.

The next section describes the spanning tree protocol and the STP menus that you 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, the 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 this tree to reestablish the links. To prevent loops, STP selects just one SmartStack STS16-20D/STS16-20R 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.

The IBM Spanning Tree Protocols will only block for spanning tree explorer frames and will work on the BRF level in the switch.

The IEEE spanning tree can operate on two levels—BRF and CRF. It is possible to have a spanning tree entity running on the bridge entity and a spanning tree entity running in every CRF at the same time. Logically, there is an internal port between the BRF and the CRFs. All BRFs in the switch uses the same bridge id, which prevents running the spanning tree protocol between two BRFs on the same switch. All CRFs use a unique bridge id. This means that the ports in a CRF can be connected.

- ▶ **Note:** On SmartStack STS16-20D, only ports 17 to 20 support the spanning tree protocol. Ports 1 to 16 are always in a forwarding state. (On SmartStack STS16-20R all ports support the spanning tree protocol.)
- ▶ **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.

- **Note!** All bridge relay functions in the switch use the same bridge identifier. As a consequence, you must not divide one switch into two or more VLANs by connecting them together and using the spanning tree protocol. The tree will collapse since the same bridge will be seen in several places in the network.

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 (for example, 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 start forwarding frames, when default STP parameters are used. The client and server stations may have given up before then and the first many packets are 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.

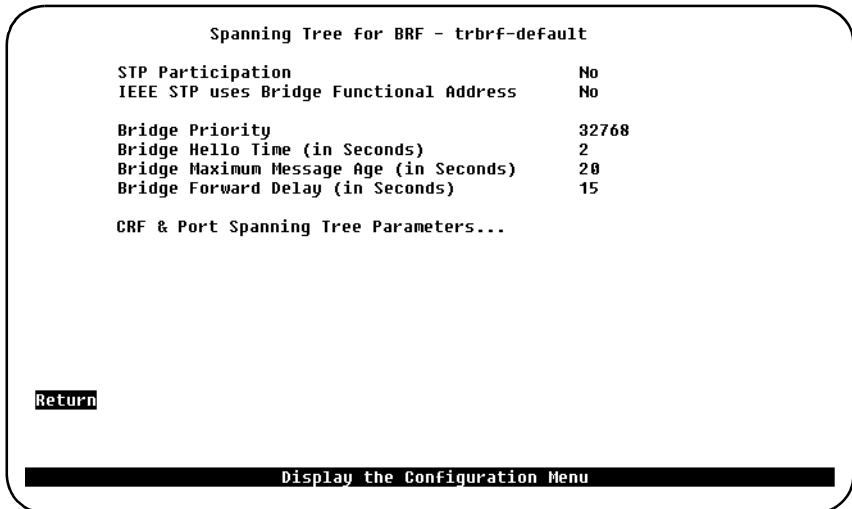
Another reason for not enabling STP on dedicated ports is that the whole spanning tree domain will go into Topology Change state each time a station opens or closes. This will cause the whole spanning tree domain to use short aging timers, which means that all address tables will be trashed. The result 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 105.

Spanning Tree for BRF Screen

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

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



STP Participation

Whether this BRF 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*, the internal links between this bridge entity and the concentrator entities having this BRF as a parent will be set to forwarding mode. You can then override this by blocking the link at a particular CRF.
- If **STP Participation** is set to *IEEE*, the bridge relay function will participate in an 802.1D Spanning Tree domain and block or forward frames over the internal link between the bridge relay function and the CRF.
- If **STP Participation** is set to *IBM*, the bridge relay function will participate in the IBM Source Route Spanning Tree Protocol and block or forward Spanning Tree Explorer frames. Other frames are forwarded by the bridge relay function.

Default: 20

Bridge Forward Delay (in Seconds)

Enter the time the BRF spanning tree entity waits between transitions from listening to learning, and from learning to forwarding. The minimum may not be less than the larger of 4 or $((\text{Switch Maximum Message Age} / 2) + 1)$. 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

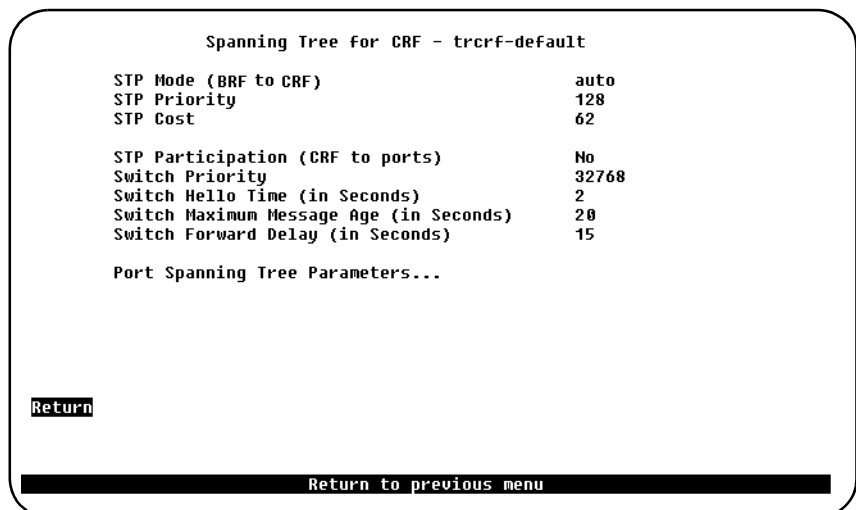
CRF & Port Spanning Tree Parameters...

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

Spanning Tree for CRF Screen

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

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



Switch Hello Time (in Seconds)

The time this CRF spanning tree instance waits before sending the next Hello BPDU message when this entity is the root in STP. The default is 2.

The minimum value is 1. The maximum value is the lower of 10 or $((\text{Switch Maximum Message Age} / 2) - 1)$.

Switch Maximum Message Age (in Seconds)

Maximum message age used when this CRF instance is the root in a spanning tree domain. 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 $((\text{Switch Hello Time} \times 2) + 1)$.

The maximum cannot be more than the lower of 40 or $((\text{Switch Forward Delay} \times 2) - 1)$.

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 SmartStack STS16-20D/STS16-20R waits between transitions from listening to learning and from learning to forwarding. The default is 15. The minimum is the larger of 4 or $((\text{Switch Maximum Message Age} / 2) + 1)$. 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.

- ▶ **Note:** For **SmartStack STS16-20D n/a** will be displayed for ports 1 to 16 as they do not support spanning tree protocol.

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.

- ▶ **Note:** For SmartStack STS16-20D, the text **n/a** will be displayed for ports 1 to 16 as they do not support spanning tree protocol.

STP Mode

The port's spanning tree mode. Possible values are *forwarding*, *blocked*, and *auto*.

When *auto* is selected, the spanning tree protocol will be used to determine the forwarding/blocking state.

When set to *blocked*, the port will not forward any frames.

When set to *forwarding*, the port will always forward frames.

On SmartStack STS16-20D ports 1 to 16 will always be in *forwarding* state.

If the port is used to connect to a single station, forwarding might be the preferred mode since it might take 30 seconds or more before a port is opened until it starts forwarding frames. If connected to a shared media or a bridge, be careful not to create loops.

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 Chapter 7, “Monitoring the Network from the Console Statistics Menu” on page 185 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. When you have entered the port number, the **Port Configuration** screen for that port will be displayed.

For the base switch ports, the screen will look as in the following example screen. For the interface module ports, refer to the interface module guide.

```

Box 1 Port 9 Port Configuration

Name                               Enabled                               Yes
BRF trbrf-default                   Status                               Not Inserted
CRF 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 (actual)                     4472                                  Max Explorer Rate                     disabled
Port MTU                              Use BRF

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. The name can be 0–31 characters long.

BRF

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

CRF

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

Enabled

Shows the administrative state of this port. 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.

Media Type

This field is for informational purposes only, and shows the media type of the port. Possible value is RJ-45.

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 a 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 compared to the **Cfg Loss Threshold** to determine if a port should be disabled. Possible values are *1–60* minutes. The default value is *1*.

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*.

Ring Parameter Server

Configures whether this port should respond to the MAC Frame Request Initialization (*Enabled*) or not (*Disabled* = default). When the ring parameter server is enabled, other network interfaces on the ring will be informed about the CRF ring number. Only one device on the ring should act as a ring parameter server.

Early Token Release

Determines 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*.

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*.

Duplex Mode

The port operation mode. Possible values are, as follows:

- *Auto (A-HDX, A-FDX)*, the port determines the full-duplex or half-duplex mode automatically.
- *HDX*, half-duplex mode
- *FDX*, full-duplex mode

Operation Mode

The port operation mode. Possible values are as follows:

- *Auto*
The port is automatically detected, station mode.
- *Port*
The port will simulate a MAU/LAM and allow NICs to connect directly.
- *Station*
The port will simulate a NIC and connect to an existing MAU/LAM.
- *RI/RO*
For SmartStack STS16-20R only, ports 19 and 20. Allows the switch to connect to the RI/RO connector of a MAU or CAU.

► **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.

Switched Port Analyzer Menu from the Configuration Menu

The Switched Port Analyzer screen is accessed from the Configuration menu. This screen and its submenus are presented in Chapter 9, “Monitoring Port Traffic”.

CrossLink

A CrossLink connection is used to improve interswitch bandwidth. A CrossLink is used to connect two switches from the SmartStack STS16-20RM family with two to eight links (on SmartStack STS16-20D the maximum is 4 ports). A CrossLink provides bandwidth of from 32 to 128 Mbps in half-duplex mode, or from 64 to 256 Mbps in full-duplex mode.

- **Note:** On SmartStack STS16-20D only ports 17 to 20 allow CrossLinks to be configured.

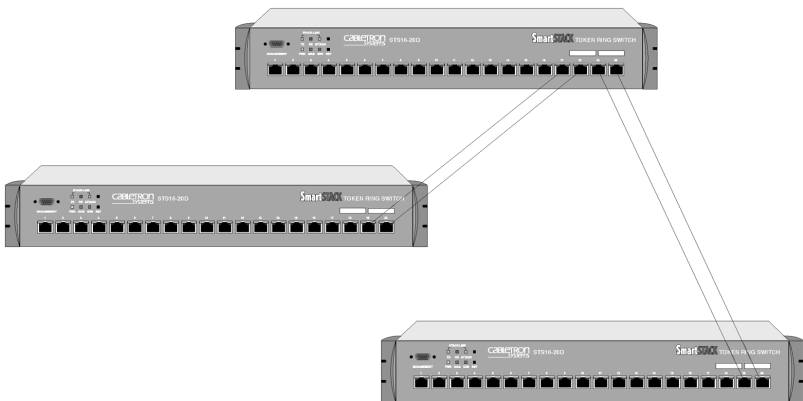


Figure 26. Setting Up CrossLinks

The CrossLink feature affects other SmartStack STS16-20D/STS16-20R 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 ports can have two full-duplex and one half-duplex connections. However, each pair of interconnected ports must both be either half-duplex or full-duplex.

- *Statistics reporting.* Statistics for the CrossLink are displayed for individual ports, not for the CrossLink as a whole. Station addresses are distributed among the ports in the CrossLink. See Chapter 7, “Monitoring the Network from the Console Statistics Menu”.
- *Address filtering.* Address filters are automatically added to every port in a CrossLink.

The port with the lowest number *configured in the CrossLink* is called the base port. The *active port* with the lowest number is selected as the primary port. The 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 ports in the CrossLink. When all 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 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 114.
- *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 CrossLink connection continues with the rest of the links. If the link that is going down is the primary port, a new primary port will be selected instead.

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. A description of creating a CrossLink connection follows.

Box 1 CrossLink Configuration

CrossLink	Ports
1	17 18
2	not defined

Return
Add Entry
Delete Entry
Change Entry
Clear Table

Return to previous menu

CrossLink

List of different CrossLink setups.

Ports

The ports within that specific CrossLink.

Add Entry

Prompts you for port numbers for a CrossLink. Enter at least 2-8 ports, no more than four ports on SmartStack STS16-20D. Start with the lowest number and go to the highest, separating the numbers by spaces. All ports must belong to the same CRF.

Delete Entry

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

Change Entry

Prompts you to reenter the 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 SmartStack STS16-20RM family switches, determine which ports to use for the CrossLink. Use at least 2 ports, on SmartStack STS16-20D no more than four and on SmartStack STS16-20R no more than eight.

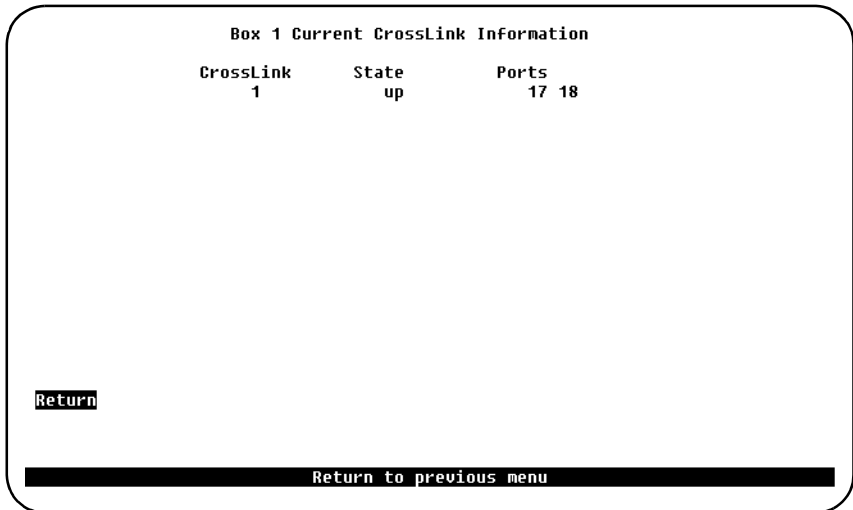
Observe the following precautions and use the following steps to set up a CrossLink:

- Disable or disconnect the 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 ports you have added to the CrossLink menu. If you connect additional ports between two switches, a loop results.
1. Disconnect the 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 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 all of the switches.
 7. If you disconnected the 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 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 ports are in that CrossLink.

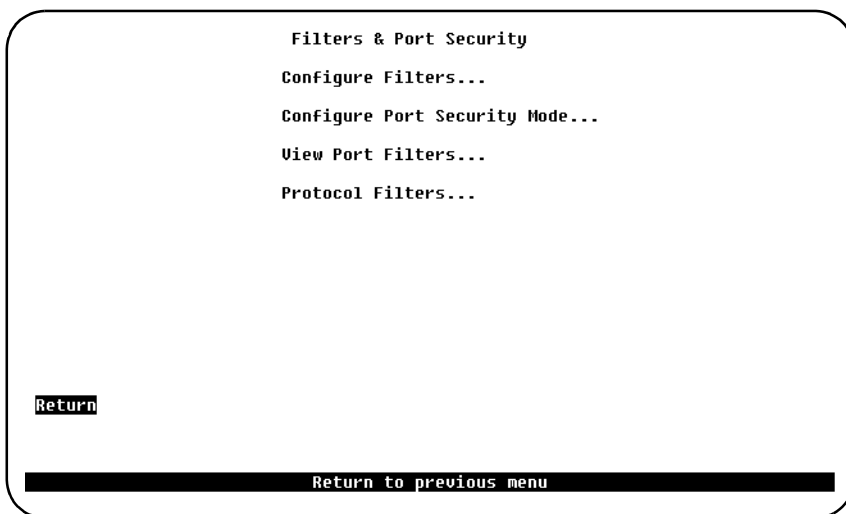
- ▶ **Note:** To restrict access from one segment to an entire segment—not just an address—see the “VLAN Configuration” section in this chapter.

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.

- Any packet with the specified destination address is prevented from entering the switch through the specified port(s).
 - Allow any packet with source address—Allow Src
 - If a packet is received with a specified source address, it is allowed to enter through 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 specified address, it is allowed to enter the switch through the specified port(s). This feature is used in conjunction with port security.
 - Force a packet with the destination address to certain port—Force Dest
 - Packets with a specified address must go to the 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

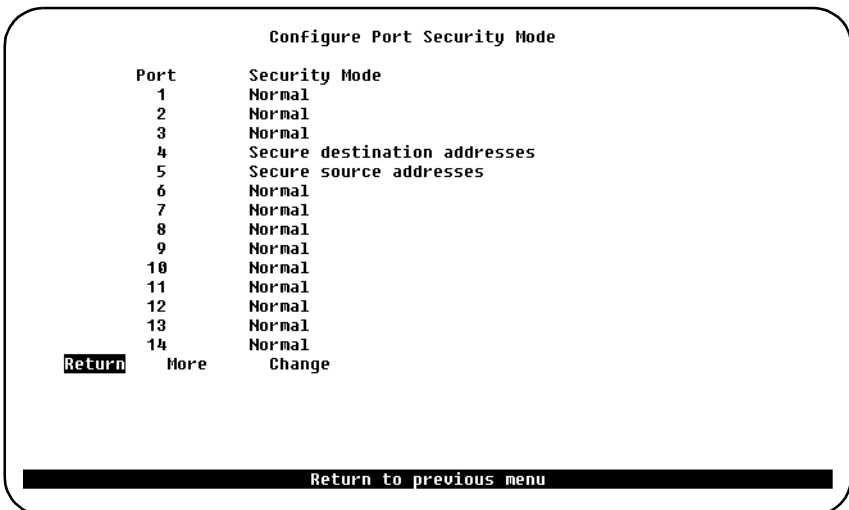
This function disables address learning of source and/or destination addresses at specified ports on an SmartStack STS16-20D/STS16-20R. Port security totally blocks (secures) these ports. *Port security mode is used in conjunction with port filtering.* Configure a port security mode on a port and then 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 from a specific port, you can block all source addresses by secure source at that port and then use port filtering (as explained in the previous sections) to selectively allow specific addresses to send from 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...**

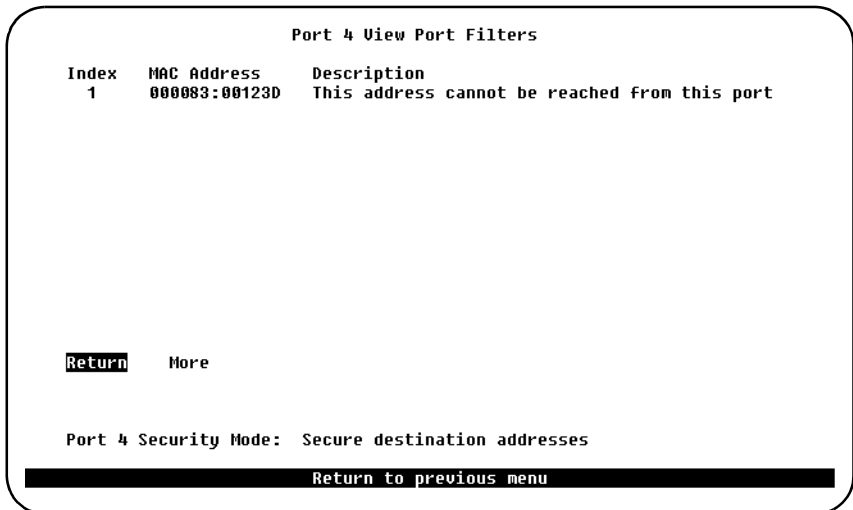


View Port Filters Screen

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 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 81.

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

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

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...**

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 Etherypes 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.

Protocol Class Assignment

Class	Ethertype	DSAPs
01	2345	60 64 68
02	None	None
03	None	None
04	None	None
05	None	None
06	None	None
07	None	None
08	None	None
09	None	None
10	None	None
11	None	None
12	None	None
13	None	None
14	None	None
15	None	None

Return

Define DSAPs and/or Ethertype for Highlighted Class

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 Etheretype

(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.

Port Filtering Attributes - Port 9				
Class	Block	SRT	Ethertype	DSAPs
01	None	Yes	None	None
02	None	Yes	None	None
03	None	Yes	None	None
04	None	Yes	None	None
05	None	Yes	None	None
06	None	Yes	None	None
07	None	Yes	None	None
08	None	Yes	None	None
09	None	Yes	None	None
10	None	Yes	None	None
11	None	Yes	None	None
12	None	Yes	None	None
13	None	Yes	None	None
14	None	Yes	None	None
15	None	Yes	None	None

Return

Return to previous menu

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** field 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

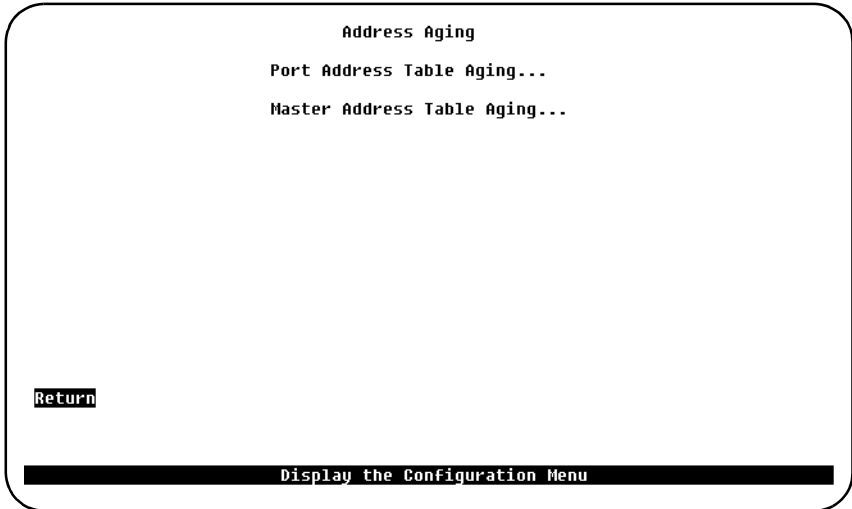
Information column showing the Ethertype defined for this class.

DSAPs

Informational column showing the DSAPs currently in this class.

Address Aging Menu

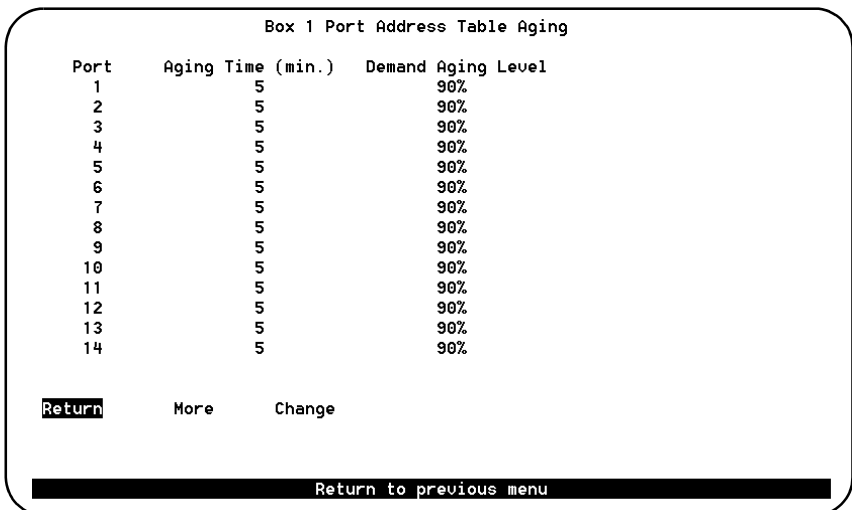
To open this menu from the main menu, select **Configuration → Address Aging**.



The screens opened from this menu are described in the following sections.

Port Address Table Aging Screen

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



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

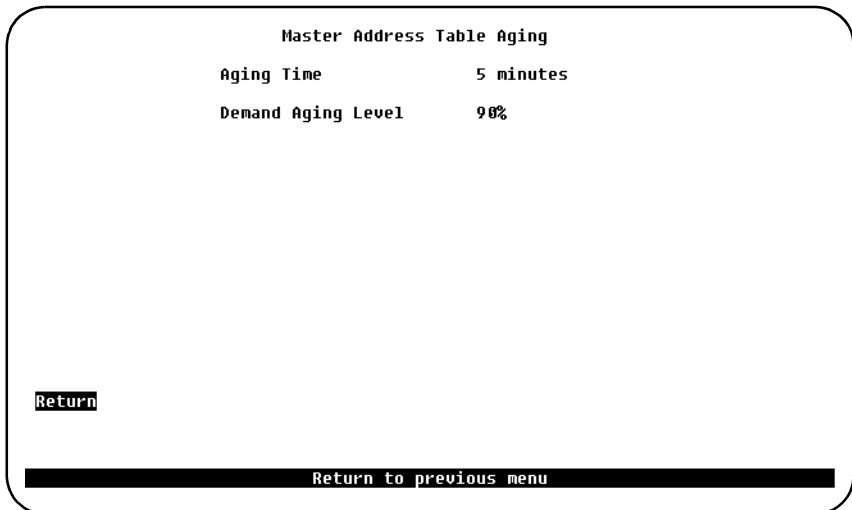
Sets a percentage threshold of address table capacity to ensure that the port's address table is populated only by the most frequently used addresses. Addresses are stored until reaching the maximum capacity of the table, then discarded in a specific order until the set percentage of table capacity is 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%.

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 system request button on the front panel of the switch for one second, releasing it, then selecting **Point 4. Clear the system password**. This will clear both the *Read-Only* and the *Read/Write* password.

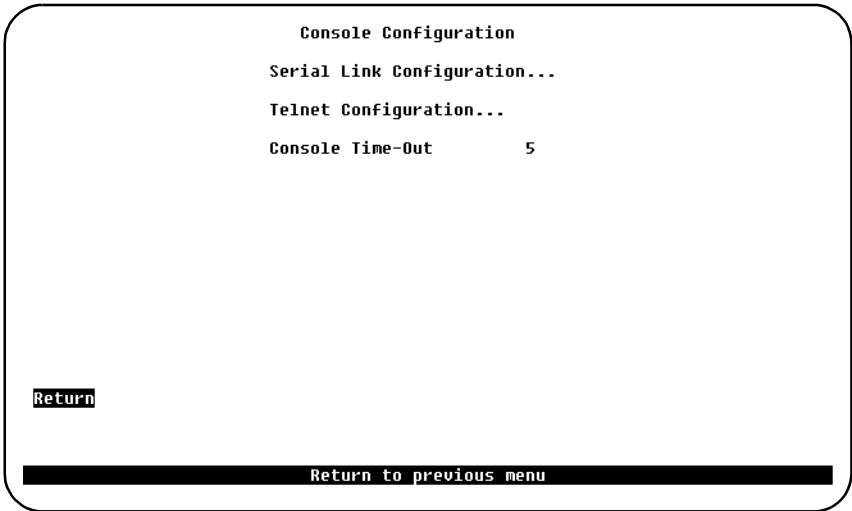
Console/Telnet Sessions

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...

See page 133 for an example of this screen and an explanation of its contents.

Telnet Configuration...

See page 135 for an example of this screen and an explanation of its contents.

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 SmartStack STS16-20D/ STS16-20R 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**.

Serial Link Configuration

Hardware Flow Control	Disabled
Software Flow Control	Disabled
Autobaud upon Break	Disabled
Console Baud Rate	57600

Return

Return to previous menu

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

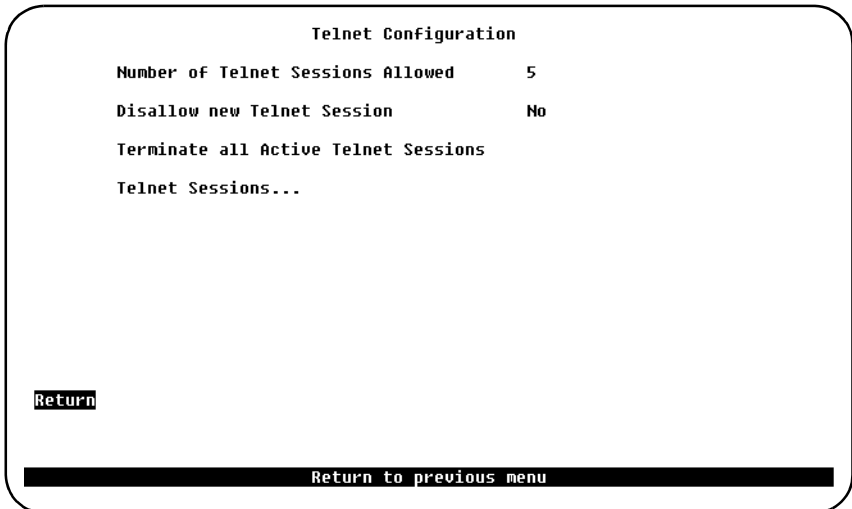
Indicates whether the baud rate is reset when a Break key sequence (pressing ENTER rapidly for five seconds) is sent or received. The default is Disabled. When set to Enabled, a baud rate change can be accomplished by changing the baud rate of the terminal emulator, disconnecting and reconnecting the 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

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...**

Telnet Sessions							
Index	Box	--- Remote ---		--- Local ---		Status	
		IP	Port	IP	Port		
1	1	194.255.112.126	1064	172.16.235.237	23	OPEN	

Return Close Session

Return to previous menu

Index

Numerical order of entries.

Box

The box number ID of the SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R:

- In the **IP Information** screen, the **IP State** must not be set to *IP-Disabled*. Any other value will do 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.

Syslog Daemon Screen

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

The syslog facility is used to send messages to a central place in your network where messages can be logged. Any message that is entered into the message log of the switch is also sent to up to 20 syslog receivers using IP UDP communication. There are two types of messages in the switch, Warnings and Info messages. A syslog facility code can be assigned to each of them.

Syslog Daemon Menu				
Index	IP Address	Info-facility	Warning-facility	BRF
1	172.16.160.1	daemon	user	trbrf-default

Return to previous menu

On this screen you can configure up to 20 receivers.

More

Displays more information.

Add Entry

Adds a new entry to the list. To add an entry, select **Add Entry** and type in the Receiver's IP address. A menu of available VLANs are then displayed. Select the VLAN to be used for transport (note that more than one VLAN can be selected). After this, select the syslog facility code to be used, first, for *Info* messages and, second, for *Warnings*. After this, messages entering the message log will be sent to the chosen IP-host provided the IP stack is running in the box.

Delete Entry

Deletes an entry.

DSRR Configuration

Dynamic Source Route Recovery enables a set of switches performing source route bridging between the same legacy Token-Ring and emulated Token-Ring (or the same pair of legacy Token-Rings) to handle link or switch failures without session loss. During normal operation, each switch forwards frames containing a Specific Route Descriptor. If a switch or its link to the legacy or emulated Token-Ring fails, another switch will after, typically, less than 3 seconds start forwarding frames containing the Route Descriptor associated with the failing switch.

The configuration of DSRR redundancy for source routing between two Token-Rings is performed in two steps:

- Configuration of a VLAN per switch, defining the normal source route bridging function between the two rings in question. Note that the CRFs are not allowed to have more than one port each, and that the ring number must be specified.
- Configuration of timer values and port pairs used for back-up. The timer values configured on each participating switch must be identical.

For an overview on DSRR, see “Dynamic Source Route Recovery” on page 32 in Chapter 2, “Switch Overview”.

► **Note!** Making the LANE Clients that correspond to the backup Virtual ATM Ports (VAPs) join the same Emulated LAN (ELAN) as those that correspond to the active VAPs, may depend on properly configuring a possible LAN Emulation Client Server (LECS) and/or the SSIM-A2-01/SSIM-A8-01 ATM 155 SmartStack Interface Modules. The primary policy used for assigning LANE Clients to ELANs is by ELAN name. The backup LANE Clients will attempt to join an ELAN with the same name as the active LANE Clients. Consequently, the backup LANE Clients will join the correct ELAN if the active LANE Clients were successfully assigned to an ELAN based on the default “by-name” policy. In other situations (for example, when the LECS is not employed), the following information may be of use for LECS configuration:

- A standby LANE Client will join with an ATM address, which only differs from that of the corresponding active LANE Client in the selector byte.
- A standby LANE Client will join with a source MAC address, which is constructed as follows:
0x02<random byte><4 last bytes of switch MAC address>.

Restrictions

When configuring a DSRR group, please note the following restrictions:

- The primary port and the backup for the primary port (see Figure 27) must be connected to same legacy Token-Ring.

DSRR Group Configuration Screen

► **Note!** Before entering the **DSRR Group Configuration** menu, the VLAN configuration must be defined.

Open the menu from the main menu by selecting **Configuration → DSRR Group Configuration**.

DSRR Group Configuration					
Ix	Box	Port	Group	Enabled	State
1	1	2	1	yes	active
2	1	8	3	yes	tracedPortDown
3	1	12	4	no	inactive

Return More View... Add... Change... Delete

Return to previous menu

The information displayed for each group on this screen is, as follows.

IX

Index for selecting a group to be viewed, changed, or deleted.

Box, Port

Primary DSRR port. This column displays the port that is connected to the legacy Token-Ring (on which DSRR protocol frames will be transmitted). See Figure 27 on page 142.

Group

This is a global group identification. Active DSRR groups (on different switches) with the same Group ID and with primary ports connected to the same ring will provide backup for each other.

Enabled

This column shows if the switch participates actively in the group.

<i>inactive</i>	Disabled
<i>stop</i>	Transient state during enable/disable
<i>idle</i>	Both primary and traced port down
<i>groupPortDown</i>	Primary port down
<i>tracedPortDown</i>	Traced port down
<i>active</i>	Operational
<i>stopOnError</i>	Error condition. Check the Message Log. Then disable the group, correct the error and enable the group again.

Group Priority

Whenever more than one switch is able to take over from a failed switch, the one with the highest priority will be chosen. Possible values are 0–255, the default is 100.

Hello Time

Interval between hello packets sent by DSRR for this group. Possible values are 100–600,000 milliseconds, the default is 500.

Hold Time

If no hello packets are received from a switch for this group within the interval specified here, the switch will be declared failed. Possible values are 100–600,000 milliseconds, the default is 1,700.

Traced Port

Identification of the (virtual ATM) port connected to the emulated (or other legacy) Token-Ring. When you select this item, you will be prompted for a box (stack only) and port number. If the value(s) entered identifies an ATM Trunk Port, a list of CRFs configured on this port are displayed. Select one. See Figure 27 on page 142.

Backup for Primary Port

Identifies a port for forwarding traffic that has been taken over from a failed switch. This port must be connected to the same legacy Token Ring as the port that identifies (together with Group Id) the DSRR group that is being configured. See Figure 27. on page 142.

Backup for Traced Port

Identifies a backup port for forwarding traffic that has been taken over from a failed switch. If the **Traced Port** is a Virtual ATM Port, the backup port must be able to join the same emulated Token-Ring as the **Traced Port**. Otherwise it must be connected to the same ring as the **Traced Port**. See Figure 27. on page 142.

ATM Address

This is the ATM address that identifies the Lan Emulation Client implementing the Virtual ATM Traced Port (when applicable). You cannot change the value of this parameter.

Return

Saves the changes made on the screen and returns to the previous menu.

Download/Upload Menu

As enhancements are made to the switch, you may need to update the software that is contained in the switch. Or you may wish to save the configuration, that is, upload the configuration files. The files may be needed if the switch is replaced.

The flash memory in the base switch contains three distinct different parts:

1. **Bootstrap**

During the startup it will display

```
BootStrap Firmware v2.3, Copyright 1996-1998
```

on an attached terminal. The image will never need to be changed.

2. **Boot**

During startup it will display

```
Boot Firmware (Phase II) v2.3, Copyright 1996-1998
```

on an attached terminal. The image is included on the diskette in a file called STS_230.bt

The boot code is upgraded from the **TFTP** or the **System Request** menu.

3. **Main code**

During startup it will display

```
System Software Version 4.0.0, Copyright 1994-1999
```

on an attached terminal. The image is include on the diskette as Cabletron version #.

► **Note!** Some of the switches in the SmartStack STS16-20RM family currently support three types of uplinks that requires embedded software:

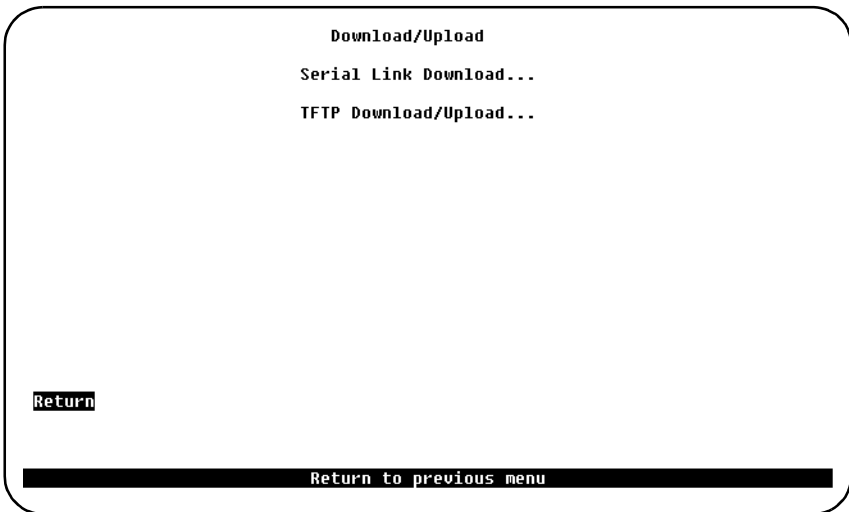
- ATM Uplink
- HSTR Uplink
- FE Uplink code

If you are using any of these modules, their software should be upgraded together with the switch to make sure that they are running at the same level.

Also note that as long as the versions are upgraded, that is, going to a *later* version, for example from 3.10.0 to 3.11.0, the configuration in the switch will be maintained. If, however, you decide to go back to a previous version, for example

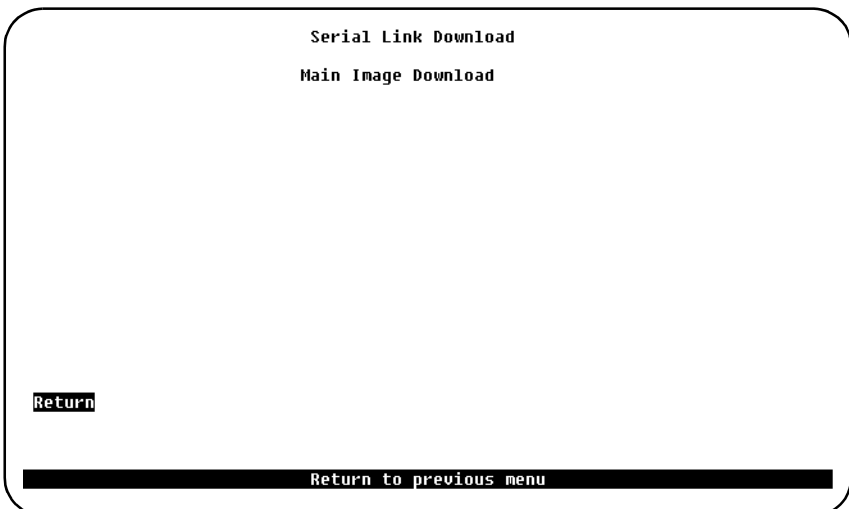
from 4.0.0 to 3.11.0, the configuration will be deleted. It is recommended that you save the configuration before upgrading the software.

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



Serial Link Download Screen

Open this screen from the main menu by selecting **Download/Upload → Serial Link Download**. This screen is for downloading via the Out-of-Band management port.



Use the following steps 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 upload on the terminal. (Note that you are uploading at the terminal and downloading at the switch.).

► **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 SmartStack STS16-20D/STS16-20R will discover this during startup, and a new serial download must be performed prior to normal operation.

If it is necessary to upgrade the boot code, press the unlabeled system request button above the reset button on the front panel. Select menu point 1 in the menu and download the image as described earlier in this chapter. Note that while you do this, the normal operation of the switch is interrupted.

TFTP

TFTP is intended for use during software upgrades and during saving/restoring configurations.

The TFTP function in the SmartStack STS16-20D/STS16-20R 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/Upload** menu is accessed through the main menu. From the main menu, select **Download/Upload → 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. Note that this screen may contain additional items, depending on the modules installed.

TFTP Download/Upload

TFTP Server Address	0.0.0.0
Download VLAN	trbrf-default
Main Image Download...	
Configuration Files Download...	
Configuration Files Upload...	

Return

Return to previous menu

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...

Select the required function and input the path and filename of the file the SmartStack STS16-20D/STS16-20R 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!** When uploading configuration files, many TFTP servers require that the file exists on the server.

- **Note!** When upgrading the boot code, append the string **boot* to the filename when entering the filename. For example, to download the 2.3 bootcode to the switch, type the following:

main image download filename: STS_230.bt*boot

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. On a locally attached console, 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.

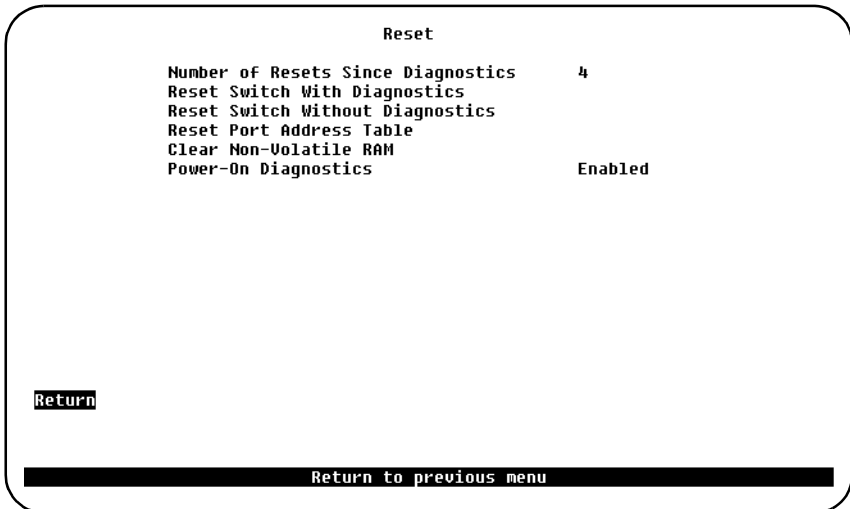
When downloading configuration, all configurable parameters will be replaced with this new configuration, the message log will be cleared and the switch must be reset immediately after.

While uploading configuration files, the switch can continue normal operation. Note that some TFTP servers requires that the file exist before it will allow uploading. The switch will append the box number (.#) to the filename, that is, stand-alone boxes will append “.1”.

- **Note:** Be careful - if the process is interrupted during this time, the stored image may be corrupted and the SmartStack STS16-20D/STS16-20R 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 interpreting 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.

Reset Screen

To open this screen, select **Reset...** in the main menu. This 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 SmartStack STS16-20D/STS16-20R. When the SmartStack STS16-20D/STS16-20R reboots, administrative parameters from nonvolatile 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 SmartStack STS16-20D/STS16-20R. When the SmartStack STS16-20D/STS16-20R reboots, administrative parameters from nonvolatile 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 Nonvolatile RAM

Selecting this command will erase all user-configured parameters 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 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 SmartStack STS16-20D/STS16-20R power-on sequence. To change the selection, highlight the item and press ENTER; then select *Enabled* or *Disabled*, and press ENTER.

Default: *Enabled*



7. Monitoring the Network from the Console Statistics Menu

This chapter explains how to monitor the SmartStack STS16-20D/STS16-20R through a directly connected VT100 console or through a VT100 telnet session. To use SNMP (in-band, through the network management), see Chapter 8, “Monitoring the Network with SNMP”.

The information presented on the Statistic 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 6, “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 five seconds.

For information on how to use the console interface, see “General Guidelines” on page 76 and “Navigating within the Menus” on page 77 in Chapter 6, “Switch Configuration”.

- ▶ **Note:** The SmartStack STS16-20D/STS16-20R 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 SmartStack STS16-20D/STS16-20R.

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 SmartStack STS16-20D/STS16-20R.

- **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.

Switch Statistics	
System Up Time	2 Hr, 45 Min, 5 Sec
Board Temperature	Normal (28.5 C)
Frames Transmitted	1123
Frame Transmit Errors	0
Frames Received	247717
Error Frames Received	0
Frames Lost	0
Pending Send Requests	0
Currently Active Stations	88
Largest Number of Stations	96
Maximum Address Table Chain	3
Address Table Full	0
Return	Reset
Return to previous menu	

System Up Time

Time passed 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 SmartStack STS16-20D/ STS16-20R.

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

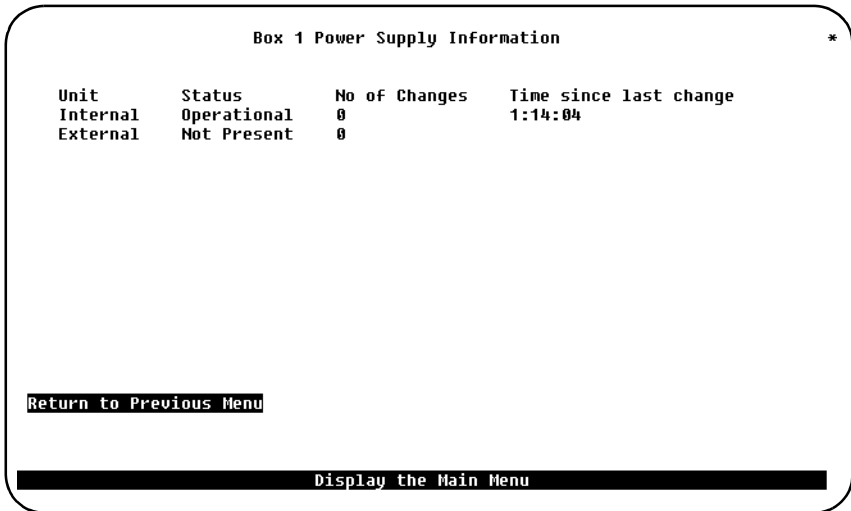
Number of times the hash table reached capacity. Used for technical system evaluation and troubleshooting.

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.

Oper Mode

The port operation mode. Possible values 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 only a dedicated connection to a port is possible. The Tx/Rx pinouts are the same as an adapter's.
- *RI—Ring In*. Only for SmartStack 16-20R, ports 19 and 20.
- *RO—Ring Out*. Only for SmartStack 16-20R, ports 19 and 20.
- *RI/RO—Ring-in/ring-out mode*. Only for SmartStack 16-20R, 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.

Fwd Mode

The forwarding mode that will be used for transmit. Possible values 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.

General Statistics Screen

To open this screen, do the following:

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

Use this screen to view detailed information about a particular port.

Box 1 Port 2 General Statistics - Link is Down		
Frames Forwarded	0	Largest Number of Stations 8
NSR Frames Forwarded	0	Address Chain Overflows 0
SRF Frames Forwarded	0	Address Table Overflows 0
STE Frames Forwarded	0	Frame Errors 0
ARE Frames Forwarded	0	Receive Buffer Overflows 0
MAC Frames Forwarded	0	Transmit Buffer Overflows 0
Frames Processed	0	Long Frames 0
Frames Unknown	0	Short Frames 0
Frames Transmitted	0	Duplicate Ring Number 0
Frames Received	0	Invalid RIF RC Field 0
Broadcast Frames Received	0	RIF Length Exceeded 0
Multicast Frames Received	0	Explorer Overflow 0
Frames Filtered - Addr	0	Ring Number Mismatch 0
Frames Filtered - DSAP	0	Config Loss 0
Local Address Entries	0	Config Loss Reason None
Remote Address Entries	8	Last Reset 2 Hr, 12 Min, 37 Sec
Return	Reset	
Return to previous menu		

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. Note that MAC frames are not forwarded to other ports, only to the CPU.

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. That is, the number of addresses (or route descriptors) seen as source addresses on this port.

Remote Address Entries

Number of remote stations in the address table of the port. That is, the number of addresses that is used as destination address on this port.

Largest Number of Stations

The maximum value of the number of local stations on this port at any time since reset of statistics.

Address Chain Overflows

Number of address table chain overflows. An overflow will result in an address being deleted from the address table, which means a decrease in performance.

Address Table Overflows

Number of address tables overflows. An overflow will result in an address being deleted from the address table, which means a decrease in performance.

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 than 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. That is, a routing control with an odd length or a length of zero.

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. That is, the ring number of the port must be the last, if it is an explorer frame. Note that the switch performs a ring number test when the topology of the network changes. At that time the port might be disabled.

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

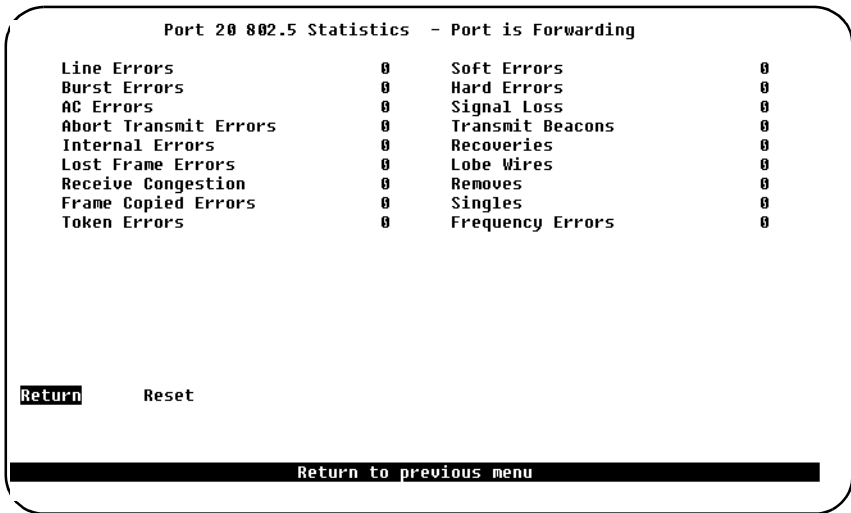
Time since last reset of port statistics.

802.5 Statistics Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics** → **Port Statistics**.
2. Enter a port number.

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

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.

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.

Uptime When Beacon

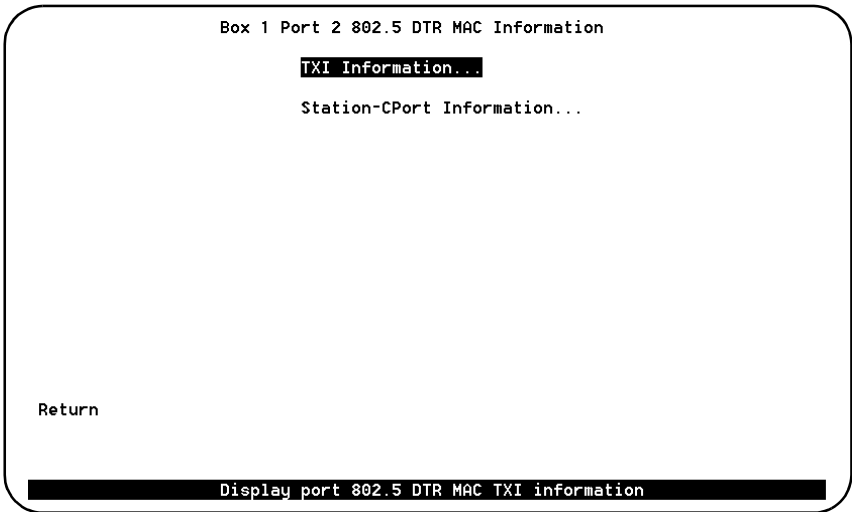
The time the switch had been running when the last beacon was sent on this port.

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 port number.
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...

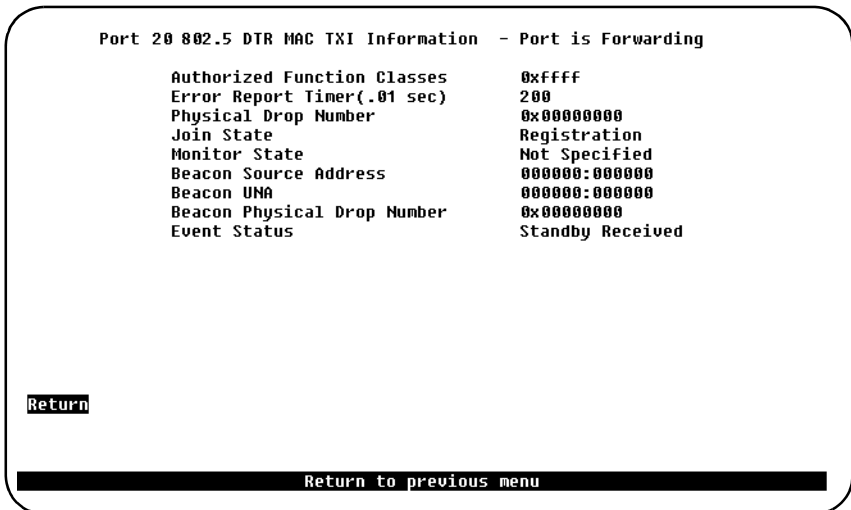
Displays the **Station-CPort Information** screen.

TXI Information Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics** → **Port Statistics**.
2. Enter a port number.
3. Select **802.5 DTR MAC Information...**
4. Select **TXI Information...**

This 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

Time-out 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.

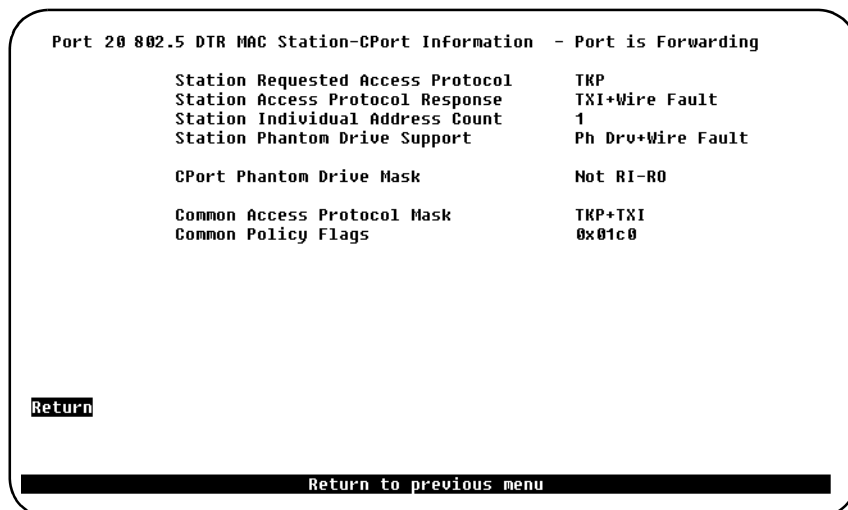
Physical Drop Number

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

Station-CPort Information Screen

To open this screen, do the following:

1. Starting from the main menu, select **Statistics** → **Port Statistics**.
2. Enter a port number.
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.

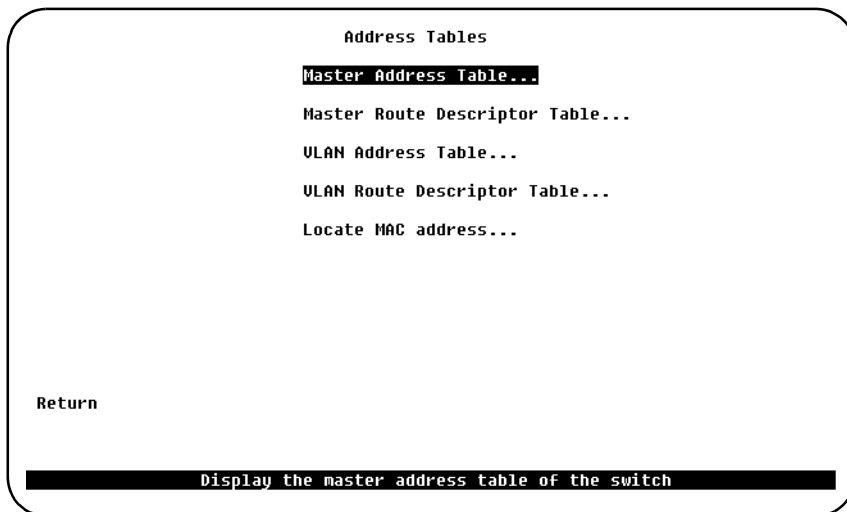
Station Phantom Drive Support

This field displays the MAC's support of Phantom Drive and Wire Fault detection.

Address Tables Menu

To open this menu from the main menu, select **Statistics** → **Address Tables**.

Use this menu to select which address table statistics you want to view.



The following pages describes the screens you access from this menu.

Master Address Table Screen

To open this menu from the main menu, select **Statistics** → **Address Tables** → **Master Address Table**.

This screen contains MAC addresses of all the ports known to the SmartStack STS16-20D/STS16-20R. The table can contain up to 10,000 entries memory. See a detailed description of MAC addresses on page 81.

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:E34840	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. The port number “nn” can be followed by *SRT* which means that the address is known as source of frames that shall be switched using the SRT switching mode. If a BRF is configured for SRT/SRB mode, a MAC address can be known both as an SRT address and as an SRB address.
 - <port type> can be:
 - TR*—The address is known at the specified Token-Ring port.
 - ATM*—The address is known at the specified ATM port
 - HSTR*—The address is known at the specified High-Speed Token-Ring port
 - TS*—The address is known at the specified Translational Switch.
 - Port*—In this case “nn” will appear as <box number>/<port number>. 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.

Route (hex)

The route descriptor triplet: My ring number.Bridge Number.Distant ring. 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> can be:
 - TR*— The route descriptor is known at the specified Token-Ring port.
 - ATM*—The route is known at the specified ATM port
 - HSTR*—The route is known at the specified High-Speed Token-Ring port.
 - The route descriptor will be present at port nn.
 - *Port*— The route descriptor is known at a box or port.
 - 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.

```

                                VLAN Address Table - trcrf-default
Address      Type                Ports (Filtered:high-lighted, Trunks:Bold)
000083:4192BF Known-TR Port    10    10
000083:687DB9 Known-TR Port    10    10

Return      More      Search

Return to previous menu
  
```

For a description of the fields and their meanings, see the section “Master Address Table Screen” on page 178.

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.

VLAN Route Descriptor Table - trcrf-default			
Route (hex)	Type		Ports (Filtered:high-lighted, Trunks:Bold)
17.1.3	Known-TR Port	10	10

Return to previous menu

For a description of the fields and their meaning, see the section “Master Route Descriptor Table Screen” on page 180 above.

Locate MAC Address Screen

To open this menu, do the following:

1. From the main menu, select **Statistics** → **Address Tables**.

Select **Locate MAC Address**. Enter a MAC address. The switch software will then try to locate the box and port that have seen it as a source address.

Use this screen to locate a computer in the network.

Locate MAC address *

MAC Address		000000:000000
Box		0
Port		
Type		
VLAN		trbrf-default

Return

Return to previous menu

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 Address Table** screen, see page 178.

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 SmartStack STS16-20D/STS16-20R is configured with CrossLink channels, STP packets use the primary port of the CrossLink.

```

Current Spanning Tree Information - My_BRF 100

Bridge ID: 32768.0000C1478605          Hello Time:      2
Root ID:  32768.0000C1474207          Max Message Age: 20
Root CRF: 102                          Forward Delay:  15

CRF   Pid   PCst PSts  DCst  Dsg SwId/BrId  DsgPid  #Chgs  Last Chg
101   240.31  62  FWD   62  32768.0000C1478605  240.31  2      0:28:19
102   240.47  62  FWD   0   32768.0000C1474207   0.47    8      0:25:12

Return   More   CRF-Spanning-Tree...

Return to previous menu

```

► **Note:** On SmartStack STS16-20D only ports 17 to 20 can support the spanning tree protocol.

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 CRF that is closest to the root. This SmartStack STS16-20D/STS16-20R communicates with the root through this CRF.

- 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 (Designated Cost)

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 Swld/Brid (Designated Switch Id/Bridge Id)

Priority and ID of the device through which this port has determined it must communicate with the root of the spanning tree. A BRF will use the base MAC address + 0x20 for the ID. The first defined CRF will use the base MAC address + 0x21 for the ID, etc.

Dsg Pld (Designated Port Id)

Port on the designated bridge through which this SmartStack STS16-20D/STS16-20R will communicate with the root of the spanning tree. This information is useful if the SmartStack STS16-20D/STS16-20R 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 BRF Screen” on page 99.

Current Spanning Tree Information for a CRF Screen

To open this screen, do the following:

1. From the main menu, select **Statistics** → **Current Spanning Tree Information**.
2. Select **CRF-Spanning-Tree**. Select a CRF, when prompted.

This screen displays the spanning tree parameters for a CRF that belongs to the currently selected BRF.

Current Spanning Tree Information - My CRF 102 Group 2									
Bridge ID: 32768.0000C14786C5					Hello Time: 2				
Root ID: 32768.0000C1478484					Max Message Age: 20				
Root Port: 7					Forward Delay: 15				
Port	PIId	PCst	PSts	DCst	Dsg SwId/BrId	DsgPIId	#Chgs	Last Chg	
17	128.17	62	FWD	0	32768.0000C1478484	128.1	6	0:34:42	
18	128.18	62	BLK	0	32768.0000C1478484	128.2	3	0:35:01	
Return		More							
Return to previous menu									

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. This field might show *Internal* if the root port is between the CRF and the BRF.

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)

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 (Port Cost)

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 (Port Status)

Current status of this port within the spanning tree. Possible values are:

- DIS (Disabled)
- BLK (Blocked)
- LSN (Listening)
- LRN (Learning)
- FWD (Forwarding)
- DWN (Down)

DCst (Designated Cost)

Cost for a packet to travel from this port to the root in the current spanning tree configuration. Found by adding all path cost to the root when using the designated port.

Dsg Swld/Brd (Designated Bridge ID)

A unique bridge identifier of the bridge that is assumed to be the device through which this port has determined it must communicate with the root of the spanning tree.

Dsg Pld (Designated Port Identifier)

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 BRF Screen” on page 99.

VLAN Statistics

If you select VLAN Statistics, you will be prompted for a VLAN type. On selection of the VLAN type, a screen will be displayed listing available VLANs and prompting for a selection. Following your selection, the **CRF** or **BRF VLAN Statistics** screen will be displayed.

VLAN Statistics Screen for CRF

To open the **VLAN Statistics** screen for CRF, do the following:

1. From the main menu, select **Statistics** → **VLAN Statistics**.
2. You will be prompted for a VLAN type. Select CRF.
3. Select a CRF. The **VLAN Statistics** screen for CRF appears.

```

Box 1 VLAN Statistics - trcrf-default

Parent VLAN - trbrf-default

Currently Active Stations           4
Largest Number of Stations         6

Ports:
 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
 17 18 19 20

Return

Return to previous menu

```

Parent VLAN

The parent BRF.

Currently Active Stations

Number of MAC addresses currently in the master address table that are recognized as belonging to this CRF.

Largest Number of Stations

Largest number of MAC addresses in the master address table—since the last reset or power cycle—that are recognized as belonging to this CRF.

DSRR Status Screens

You access the DSRR related status screens by selecting by selecting **Statistics** → **DSRR Status**. This section contains information on the specific screens.

DSRR Status Tables Screen

Open this menu from the main menu by selecting **Statistics** → **DSRR Status**:

DSRR Status Tables					
Ix	Box	Port	Group	Enabled	State
1	1	2	1	yes	active
2	1	8	3	yes	tracedPortDown
3	1	12	4	no	inactive

Return More View Neighbour... View Backup...

Return to previous menu

Select **View Neighbor** or **View Backup** to view status tables for a group. You will be prompted for the Index (Ix) value of the DSRR group. The table screen will then appear.

DSRR Neighbor Table Screen

Open this screen from the main menu by selecting **Statistics** → **DSRR Status**. Then select **View Neighbor**. You will be prompted for the Index (Ix) value of the group, then the screen will appear.

This screen contains a one-page entry for each switch currently participating in the Redundancy Group, including the one on the console of which the values are displayed.

DSRR Neighbour Table for Port 2, Group 1	
Neighbour MAC Address	000083:E22100
Neighbour Bridge Number	5
Neighbour Hello Time	500
Neighbour Hold Time	1700
Neighbour Priority	100
Neighbour Last seen	0
Neighbour ATM Address	39.840F8000000000024900005.0000C1478498.04
Return	More
Return to previous menu	

Neighbor Last Seen

Displays the time in milliseconds since a Hello Message was last received from the corresponding switch for the DSRR group in question. For the local switch, this value is always displayed a zero.

More

Displays the next entry (sorted by MAC Address).

Return

Closes the screen and returns to the **DSRR Status Tables** screen.

DSRR Acting as Backup Table Screen

Open this menu from the main menu by selecting **Statistics** → **DSRR Status**. Then select **View Backup**. You will be prompted for the Index (Ix) value of the group, then the screen will appear.

This screen contains an entry for each switch for which the local switch is presently acting as active backup. The items on the screen are described.

```

DSRR Acting as Backup Table for Port 2, Group 1

Backup for MAC Address      000083:E24140
Backup for Bridge Number    9
Time Acting as Backup       536040
Backup for ATM Address      39.840F80000000000024900005.0000C1CB7098.04

Return      More

Return to previous menu

```

Time Acting as Backup

Displays the time in milliseconds since the local switch started forwarding frames on behalf of the switch represented by the entry.

More

Displays the next entry (sorted by MAC Address).

Return

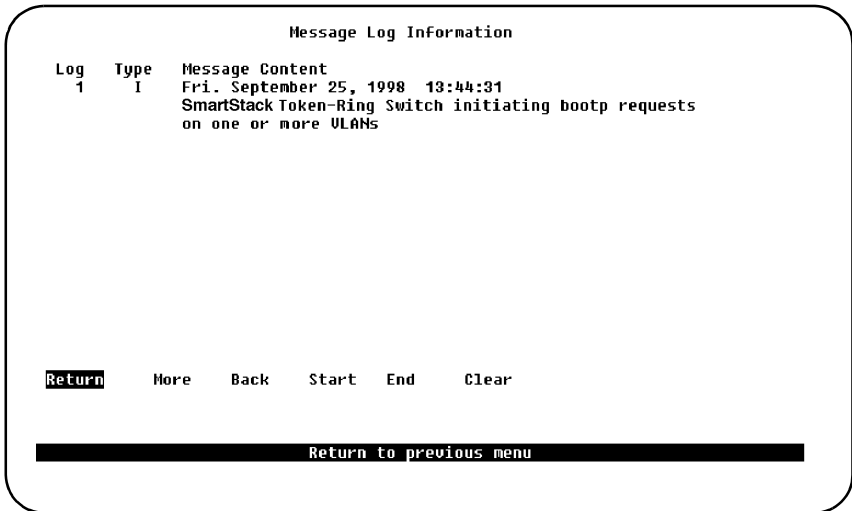
Closes the screen and returns to the **DSRR Status** menu.

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. The message log will be preserved through resets, but will be cleared after a configuration download. The messages in the log can also be sent to a syslog receiver see page 139 in Chapter 6, “Switch Configuration”.

Whenever there are unread messages in the Message log a "*" will be shown in the upper right corner of the console.



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.

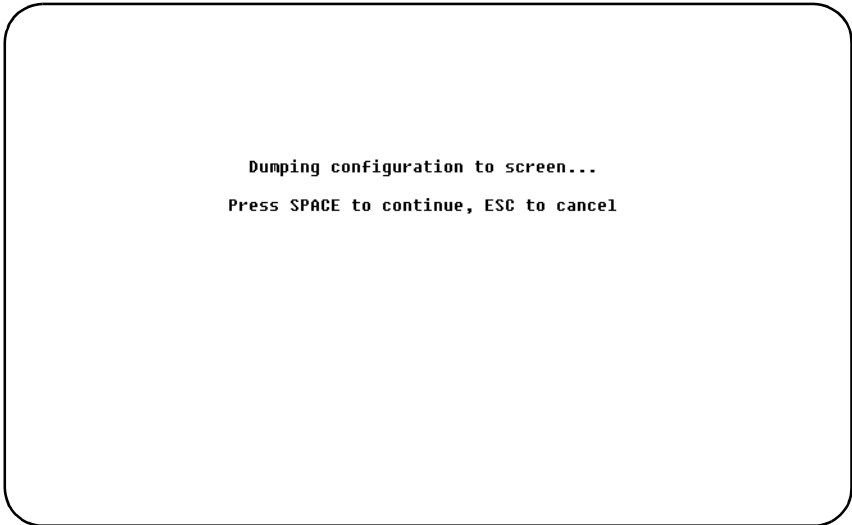
Clear

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 in a summary form. The information is suitable for saving to an ASCII file by means of a capture function in the terminal emulation program used. This file will often be requested by the Cabletron Systems 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.



8. Monitoring the Network with SNMP

This chapter explains how to monitor the SmartStack STS16-20D Token Ring Switch and the SmartStack STS16-20R Token Ring 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

1. Attach the switch to the console and start a console session as described in Chapter 5, “Accessing Switch Management”.
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 menus.

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 6, “Switch Configuration” for a complete description on how to configure the **IP Configuration** menu.

Trap Receivers Screen

To open this screen from the main menu, select **Configuration** → **SNMP Configuration** → **Trap Receivers**.

Trap receiver tables tell the SmartStack STS16-20D/STS16-20R where to send traps. The table contains the IP address associated with an SNMP trap manager.

Trap Receivers						
Index	IP Address	Community Name	TrBRF			
Return	More	Add Entry	Delete Entry	Change Entry	Clear Table	Zoom
Return to previous menu						

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.

Index

Sequential number of entries in the table.

IP Address

The IP address associated with an SNMP trap receiver.

Community Name

The community name sent with the trap.

BRF

VLANs to which this trap is sent.

More

Used to view next page of table.

An authenticationFailure trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.

Enterprise specific traps - from STS16.MIB

STS16StackCfgChange

This trap is generated when there is a change in the stack configuration, that is, when either a new switch is added to the stack or a switch leaves a stack.

STS16NumSwitches 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.

STS16StackStackMatrixChange

This trap is generated when the stack switches over from primary to secondary Matrix or from secondary back to primary Matrix.

STS16StackTempChange

This trap is generated when the temperature in a switch exceeds normal or returns to normal.

STS16PowerSupply

This trap is generated when the status of the power supply units changes.

Per Port Traps

STS16PortStrNFwdEntry

This trap is generated when a port automatically enters store and forward mode when the error rate exceeds the threshold.

STS16PortCfgLossTrap

This trap occurs when a port is disabled because it has exceeded its Configuration Loss Threshold within the configured Sampling Period.

STS16BeaconStart

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 beaoning.

STS16BeaconEnd

This trap is generated when the ring status change indicates that a ring is no longer beaoning. This trap only occurs only once when the status actually changes.

STS16DuplicateMACAddr

This trap is generated when a duplicate MAC address is detected on a port in a CRF which already has learned that MAC address.

STS16DuplicateBridge

This trap is generated when a duplicated bridge number is detected on a port in a CRF.

STS16RingNumberMismatch

This trap is generated when a mismatch in ring numbers is detected on a port in a CRF.

Traps for the Spanning Tree Protocol*STS16TrCRFNewRoot*

This trap is a CRF 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, for example, upon expiration of the Topology Change Timer immediately subsequent to its election.

STS16TrCRFTopologyChange

This trap is a CRF 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.

STS16TrBRFNewRoot

This trap is a BRF 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, for example, upon expiration of the Topology Change Timer immediately subsequent to its election.

STS16TrBRFTopologyChange

This trap is a BRF 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.

► **Note:** On the SmartStack STS16-20D, only ports 17 to 20 support the spanning tree protocol.

Traps for CrossLinks*STS16CrossLinkFailed*

This trap is sent when one of the links in an CrossLink fail. The variable STS16CLPorts contains the ports which are operational in the CrossLink.

- ▶ **Note:** On SmartStack STS16-20D only ports 17 to 20 allow CrossLinks to be configured.



9. Monitoring Port Traffic

The SmartStack STS16-20D/STS16-20R allows you to configure a Switched Port Analyzer function for monitoring traffic on a port. An *analyzer* port is a port on which an external probe can observe traffic from any other port, that is a *monitored* port. The monitoring function does not interfere in any way with the normal traffic flow in the switch.

The external probe (for example, a protocol analyzer) is not supplied with the switch.

You can monitor traffic going through a monitored port in two different ways, by using either:

- active monitoring or
- passive monitoring.

Active Monitoring

This mode copies traffic switched to and from the monitored port to the analyzer port. Since MAC frames never are switched between ports, they will not be seen on the analyzer port. To prevent spurious frames, the analyzer port must be a Token-Ring port on the same box as the monitored port. It is recommended that you put the analyzer port into a separate VLAN. The monitored port can be any type of port (Token-Ring, ATM, HSTR, and Fast Ethernet)

- **Note!** The analyzer port works as a normal port. This means it can be in FDX/HDX mode, Station/Port 4 or 16 Mbps. Moreover, you can use any external probe. The frames will be buffered normally, that is, if you try to monitor a FDX 16 MB line with a 4 MB HDX port, data loss can occur.

When the monitored port is in HDX mode, the frames sent to the analyzer port will be the frames received on the Token-Ring of the monitored ports (that is, a true copy apart from MAC frames). When monitoring a FDX port, it is the forwarding port that is responsible for the copy. As a consequence, packets may be seen on the analyzer port in a different order than on the monitored port. Moreover, since it is the monitored port itself that expands Source Route Explorer frames, the last ring and bridge number will be missing from explorer frames passing a BRF in the switch.

Passive Monitoring

This mode makes a physical connection from the monitored port to the analyzer port. Both the monitored and the analyzer port must be Token-Ring ports. You can choose to connect either the transmit or the receive wire from the monitored port to the analyzer port. That is, if the monitored port is in HDX mode, the analyzer port

Switched Port Analyzer Screen

To open this screen from the main menu, select **Configuration** → **Switched Port Analyzer**.

Box 1 Switched Port Analyzer

Active Monitoring

Analyzer Port Number 0
 Monitored Port Number 0

Passive Monitoring

Analyzer Port Number 0 Monitors receive traffic for a FDX port
 Monitored Port Number 0 or all traffic for a HDX port

Analyzer Port Number 0 Monitors transmit traffic for a FDX port
 Port to Monitor 0 or all traffic for a HDX port

Return

Return to previous menu

The following information is displayed on this screen:

Analyzer Port Number

The port to which the network analyzer or probe will be attached.

- ▶ **Note:** This port should be assigned to its own CRF. For information about assigning ports to a CRF, see “VLAN Configuration” on page 86.

Monitored Port Number

The port that will be monitored. To change a setting select it and specify the new value. To disable the Switched Port Analyzer port, select **Port to Monitor** and set it to 0. To save the changes, select **Return**

- ▶ **Note:** The analyzer port and the monitored port must be on the same physical switch, not on different switches in the stack.



10. Troubleshooting

This chapter contains procedures that help you troubleshoot problems with a switch and its connections to other devices.

Obtaining Service

There are no serviceable parts inside the SmartStack STS16-20D/Sys16-20R. Do not remove the cover for any reason. If you think your switch requires service, please contact Cabletron Systems Technical Support. Please refer to Chapter 11, “Getting in Touch with Technical Support” for instructions.

Troubleshooting in a Network

The switch console and SNMP management agent give you access to important statistics and other information about the network, as seen by the switch. (See Chapter 7, “Monitoring the Network from the Console Statistics Menu”).

The section “Port Statistics Menu” on page 162 can be helpful in isolating network level problems.

The Switched Port Analyzer feature allows a network analyzer to be attached to a port on the switch to monitor, in real time, switch activity of another port. See Chapter 9, “Monitoring Port Traffic” for information on configuring Switched Port Analyzer.

Start of Troubleshooting Process

If one or more devices (such as PCs) connected to a switch are unable to communicate with other devices in the network, use the following steps to start the troubleshooting process:

1. Locate the switch to which the device is connected. Use the network sketch, the label on the cable connected to the device, or other network records to help you locate the switch.
2. If you have set up a console session (see Chapter 5, “Accessing Switch Management”), it can be used to determine whether diagnostics have been completed correctly. A list of normal diagnostic messages is shown on page 73.
3. Observe the LEDs on the switch front panel. Figure 2 on page 5 illustrates the LEDs. For explanations of the LEDs, see the section “Status and Activity LEDs” on page 7. Review this section before proceeding with the troubleshooting process.

- In Table 15, locate the symptom that best describes the communication problem and the LED pattern you observed. Then, go to the section that contains the recommended actions for resolving the problem and follow that procedure.

Choosing a Troubleshooting Procedure

Use Table 15 to determine which troubleshooting procedure you should use. For a description of the status LEDs and their meanings, see “Status and Activity LEDs” on page 7.

Symptom and LED State	Go To:
All of the LEDs are off.	Procedure A
The ERR LED or the DIAG are on.	Procedure B
None of the devices connected to the switch can communicate, the ERR LED is off, and the PWR LED is on.	Procedure C
A single device connected to the switch is having trouble communicating.	Procedure D
<p>Note: Segment refers to a single cable or interconnected cables between a switch port and the device at the other end.</p>	

Table 15. Symptom, LED State and Recommended Procedure

Procedure A

Use this procedure if all of the LEDs are off:

- Verify that the power cord is connected at both ends and that the power outlet is working.
- If the power cord is connected correctly, the outlet is working, and the problem persists, the problem is in the switch. In that case, contact technical support.

Procedure B

Use this procedure if the ERR LED is on:

- Verify that the boot code is at least release 2.3. If not, download the boot code using either TFTP or serial download as described in Chapter 6, “Switch Configuration”.

2. Reset the switch by disconnecting the power cord, waiting 10 seconds, and then reconnecting it to the electrical outlet. If the problem goes away, resume using the switch.
3. If you have just downloaded new microcode, clear NVRAM and reset the switch using the instructions in “Reset Screen” on page 152.

► **Note:** Clearing NVRAM returns all configuration parameters to their default values.

If the problem is corrected, resume using the switch.

4. One or more bad ports can cause this symptom, and the remaining ports might continue to operate.
 - Reset the switch and monitor the diagnostic messages that appear for port failures. The section “Diagnostic Screen” on page 73 includes a sample diagnostic screen. Try to correct any individual port problems that are detected.
 - If the problem is corrected, resume using the switch.
5. If the problem does not go away, the problem is in the switch.

Procedure C

Use this procedure if all devices connected to the switch are having communication problems, the ERR LED is off, and the PWR LED is on:

1. Reset the switch by disconnecting power cord for 10 seconds.
 - If the problem goes away, resume using the switch.
 - If the status LEDs indicate a failure, go to “Procedure B”.
 - If the problem persists, check all the configuration parameters.
 - If the problem has still not been resolved, go to “Procedure D” and try to get individual ports working.

Procedure D

Use this procedure if one device connected to the switch is having a communication problem. The ERR LED and the DIAG LEDs are off, and other attached devices can communicate through the switch:

1. Check the port LEDs.
 - If the port INSRT LED is on, the problem is probably external to the switch. Go to Step 2.

- **Note:** If a switch port is configured to “speed auto sense” mode, and is connected to shared-media where there are no active stations, the port will not open until another station becomes active and sets the ring speed. If necessary, this can be avoided by configuring the port to “fixed speed” mode.
6. For each device that is having a communication problem, connect its segment to another token-ring port on the switch. Try each of the remaining ports to determine whether the problem will go away.
 - If the problem goes away, the problem might be in the switch. Contact your dealer.
 - If the problem persists, continue with step 7.
 7. The problem does not appear to be in the switch and the cables and devices connected to the switch. The problem might be in the network applications or other software running on the devices. See the software documentation for software problem determination procedures, or consult your network administrator for assistance.



11. Getting in Touch with Technical Support

For additional support related to this device or document, contact Cabletron Systems using one of the following methods:

World Wide Web	http://www.cabletron.com/
Phone	(603) 332-9400
Internet mail	support@cabletron.com
FTP	ftp://ftp.cabletron.com/
Login	<i>anonymous</i>
Password	<i>your email address</i>
<p>To send comments or suggestions concerning this document, contact the Cabletron Systems Technical Writing Department via the following email address: TechWriting@cabletron.com <i>Make sure to include the document Part Number in the email message.</i></p>	

Before calling Cabletron Systems, have the following information ready:

- Your Cabletron Systems service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Cabletron Systems products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

Problem Description

Blank area for problem description.

Network Installation Sketch

Blank area for 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
DIS	Disabled
DSAP	Destination Service Access Point
DSRR	Dynamic Source Route Recovery
DTE	Data Terminal Equipment
DTR	Dedicated Token Ring
EIA	Electronic Industry Association
EPROM	Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
FDX	Full-duplex
FSM	Finite State Machine
FTP	File Transfer Protocol
FWD	Forwarding
HDX	Half-duplex

SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SRB	Source Route Bridging
SRS	Source Route Switching
SRT	Source Route Transparent Bridging
SSIM	SmartStack Interface Module
STE	Spanning Tree Explorer
STP	Shielded Twisted Pair <i>or</i> Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
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
WAN	Wide Area Network



Appendix B. Cable and Pin Information

This appendix provides information on cables that can be used with the SmartStack STS16-20D/STS16-20R. It also provides minimum pin-out information to be used to verify that the cables are correctly wired.

Connecting to the Out-of-Band Management Port

Table 16 lists the type of cables that are used when connecting to the OBM port (labeled MANAGEMENT) on the front panel of the switch.

Cable Function	Cable Type or Cable Solution
Connect a modem to the MANAGEMENT port.	Connect one end of a straight-through, TIA/EIA- 232 modem cable to the MANAGEMENT port and the other end to the modem.
Connect a PC or other DTE device to the MANAGEMENT port.	Connect one end of a crossover, TIA/EIA-232 cable to the MANAGEMENT port and the other end to the PC or DTE device <i>or</i> attach a null-modem adapter to the MANAGEMENT port. Then, attach a straight-through modem cable to the null-modem adapter.

Table 16. Connecting to the Management Port

Out-of-Band Management Port and Cable Pin-Outs

The switch's Out-of-Band Management (OBM) port (labeled MANAGEMENT on the front panel) is an TIA/EIA-232 port wired as a DTE. For this reason, you cannot use a straight-through modem cable to directly connect a terminal to the MANAGEMENT port.

For a terminal connection, you can use either a null-modem cable or a modem cable with a null-modem adapter attached. For a modem connection, you can use a standard modem cable.

This section provides pin-out information for the cables you can use to connect to the MANAGEMENT port.

Management Port Pin-Out

Pin	Signal Name
Shell	CHS GND
3	TXD
2	RXD
7	RTS
8	CTS
6	DSR
5	SIG GND
1	DCD
4	DTR
9	RI

Table 17. Pin-out of the Management Port

TIA/EIA-232 Modem Cable Connections

Use a standard straight-through modem cable to connect the switch's MANAGEMENT port to a modem.

TIA/EIA-232 Null-Modem Connections

Use a null-modem (crossover) cable shown in Figure 28 to connect the MANAGEMENT port to a terminal (DTE) with a 25-pin connector. Alternatively, you can use a modem cable and a null-modem adapter. DTR (pin 20) and RTS (pin 4) must be on, or high, on your terminal or in your terminal emulation program.

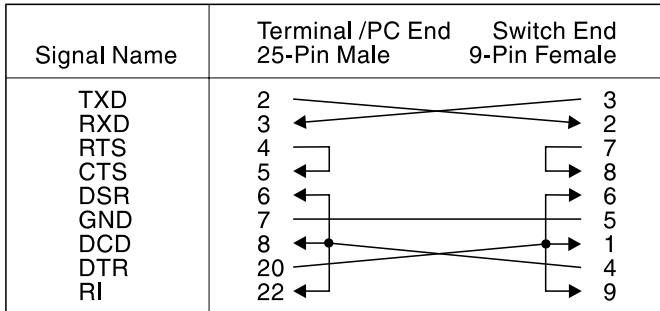


Figure 28. TIA/EIA-232 Null-Modem Cable for 25-pin Connector

Use a null-modem (crossover) cable shown in Figure 29 to connect the MANAGEMENT port to a terminal (DTE) with a 9-pin connector. Alternatively, you can use a modem cable and a null-modem adapter. DTR (pin 4) and RTS (pin 7) must be on, or high, on your terminal or in your terminal emulation program.

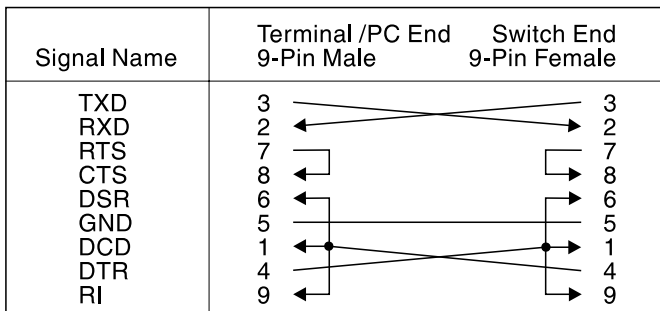


Figure 29. EIA 232 Null-Modem Cable for 9-pin Connector

Cabling Recommendations

The tables in this section contain the maximum supported lobe lengths. The maximum lengths reflect the longest lengths supported by the transmission characteristics of IEEE 802.5-compliant adapters. The recommended distances for the various cable types are set by North American and international commercial building wiring standards. These standards state that standards-compliant horizontal copper cabling shall not exceed 90 m (295 ft) leaving 10 m (33 ft) total for required patch cabling in both the office and telecommunications closet. It is good practice to follow the cabling standards guidelines when installing building cabling to help ensure a longer useful life for your cabling infrastructure, migration to new technologies, and maximum flexibility for the network configuration.

Cable Type	Impedance
Types 1 and 1A	150 Ohm
Types 2 and 2A	150 Ohm
Type 8	150 Ohm
Type 9	150 Ohm
Type 3	100 Ohm
Category 3	100 and 120 Ohm
Category 4	100 and 120 Ohm
Category 5	100 and 120 Ohm

Table 18. Copper Cable Types

- If you are installing new cabling for data applications, it is recommended that you For lobe cabling from the telecommunications closet to the wall outlet, it is recommended that 150-ohm STP or four-pair Category 5 cable that meets the international cable standard (ISO/IEC 11801) or North American cabling standard (EIA/TIA 568A).
- For backbone cabling, it is recommended that 62.5/125-micron multimode optical fiber cable that meets the international cable standard (ISO/IEC 11801) or the North American cabling standard (EIA/TIA 568A).

Number Of Attaching Devices

A Token Ring network supports up to 255 attaching devices or nodes on a single network when using 150 Ohm shielded media (type 1, 1A, 2, or 2A). When cable segments in the network are 100 or 120 Ohm, this number is decreased to 132 (72

if using any 4 Mbps only adapters or filters).

Cable Length and Lobe Wiring Rules for Dedicated-Media LAN Segments

The Cabletron Systems Token Ring network dedicated-media (full-duplex) connections support only one attached entity (workstation or switch) per connection. In a Token Ring network, the section of cable that attaches a device to an access unit is called a lobe.

The tables in this section specify the maximum supported lobe lengths for the types of cables listed. An additional 10 m (33 ft) per lobe length is allowed to accommodate patch cables, unless otherwise specified.

Ring Speed	Types 1 and 1A	Types 2 and 2A	Type 8	Type 9
4 Mbps	750 m (2460 ft)	750 m (2460 ft)	376 m (1234 ft)	500 m (1640 ft)
16 Mbps	430 m (1410 ft)	430 m (1410 ft)	215 m (705 ft)	295 m (968 ft)
100 Mbps	90 m (295 ft) See the Note!	Not Supported	Not Supported	Not Supported
<p>Note: An additional 10 m (33 ft) UTP 100 Ohm CAT.5 lobe length and a maximum of two UTP/STP converters without impedance transformation is allowed to accommodate connection to the STP cabling. The UTP/STP converter must be specified for 100 MHz operation.</p>				

Table 19. Lobe Length for 150 Ohm Shielded Media

Ring Speed	100 Ohm Type 3	100 Ohm Category 3
4 Mbps	100 m (328 ft)	250 m (820 ft)
16 Mbps	Not Supported	100 m (328 ft)
100 Mbps	Not Supported	Not Supported

Table 20. Lobe Lengths for 100 Ohm Shielded or Unshielded Cable

Ring Speed	100 or 120 Ohm Category 4	100 or 120 Ohm Category 5
4 Mbps	350 m (1148 ft)	350 m (1148 ft)
16 Mbps	200 m (656 ft)	200 m (656 ft)
100 Mbps	Not Supported	90 m (295 ft)

Table 21. Lobe Lengths for 100 or 120 Ohm Shielded or Unshielded Cable

Cable Length and Lobe Wiring Rules for Shared-Media LAN Segments

The types of cables that can be used in shared-media segments (half-duplex) are the same as those described for dedicated-media segments on page 234.

- **Note:** The acceptable cable lengths are defined by the hub or concentrator attached to the switch port, but in general the distances are half of that stated in the tables above for dedicated-media segments.



Index

Numerics

- 802.5 17
- 802.5 DTR MAC Information menu 172
- 802.5 State Information screen 170
- 802.5 Statistics screen 167

A

- address
 - unknown 20
- address aging 126
- Address Aging menu 127
- address filtering 116
- address tables 20
- Address Tables menu 177
- addresses
 - management 20
 - master address table 178
- advanced 10
- airflow recommendations 43
- AMP 225
- ARE 225
- ARP 225
- ATM 225
- auto 25

B

- BLK 225
- BootP requests and parameters 96
- bottlenecks 2
- BPDU 225
- BRF 225
- broadcast packets 18
- built-in port counters 39

C

- cabinet 58
- Cable Length 235
- Cable Pin-Outs 229
- cable pin-outs 229
- cable wiring 229
- Cables 232
- cabling
 - building wiring 60, 61
 - guidelines 60
 - labeling 60, 61, 62
 - token-ring connections 60, 61
 - types 60

- cabling length recommendations 234
- cabling recommendations 233
- capacity 13
- CAU 225
- characteristics 15
- chassis 58
- chassis accessibility 43
- chassis overheat caution 43
- checking 62
- cold boot 73
- communication problems 72
- Community Strings screen 203
- concentrator relay functions 21
- configuration 75
- Configuration menu 79
- Configure Filters screen 118
- Configure Port Security Mode screen 120
- congestion control 24
- connecting
 - a network management console 69
- connecting the console 70
- connecting to end-node devices 60
- connecting to hubs 60
- console
 - connecting 69
 - guidelines for using 76
 - terminal emulation 72
- Console Configuration menu 132
- Console/Telnet sessions 132
- conversations, multiple 18
- cooling recommendations 43
- CRF 21, 225
- CrossLink 110
 - procedure for setting up 114
- CrossLink Configuration screen 113
- CrossLink Connections 29
- CrossLink menu 112
- Current CrossLink Information screen 115
- Current Spanning Tree Information for a CRF screen 188
- Current Spanning Tree Information screen 185
- current spanning tree information screen 105
- Cut-Through 25

D

- diagnostic screen 73
- Diagnostic Test Results screen 196
- DIS 225
- Display Summary screen 199

- Filters and Port Security 117
 - navigation 77
 - Password 130
 - Protocol Filters 122
 - Statistics 156
 - VLAN Configuration 87
- Message Log Information screen 197
- MIB 226
- modem
 - creating a console session 134
- modem cable connections 230
- Module Information screen 84
- monitoring port traffic 211
- monitoring the network 155
- mounting instructions 58
- MTU 226
- multicast packets 18
- multiple 18, 21
- multiple conversations 18

N

- network management console
 - connecting 69
- network management system 201
- NMS 226
- NSR 226
- null-modem cable connections 230
- number of attaching devices 233

O

- opening the switch
 - not allowed 41
- operation modes 26
- Out-of-Band Management Port 229
- out-of-band management port 229

P

- packets
 - broadcast 18
 - multicast 18
- Password menu 130
- performance 10, 14
- performance bottlenecks 2
- Pin Information 229
- Port Address Table Aging screen 127
- Port Configuration screen 106
- Port Filtering Attributes screen 124
- Port Pin-Outs 229
- Port Spanning Tree Parameters screen 104
- Port Status screen 160

- port traffic
 - monitoring 211
- ports
 - MANAGEMENT 5
- power 43
 - Power Supply Information screen 159
- power supply 40
- problem report form 222
- PROM 226
- Protocol Class Assignment screen 123
- Protocol Filters menu 122
- protocols supported 17

R

- rack 58
- rack mounting instructions 58
- reset button 6
- Reset screen 152
- RI/RO-Like Connection 27
- RJ-45 ports 17
- RMON 226
- RMON Support 37

S

- safety 41
 - electricity 41
 - ESD 42
 - general guidelines 41
- scalability 11
- screens
 - 802.5 State Information 170
 - 802.5 Statistics 167
 - Community Strings 203
 - Configure Filters 118
 - Configure Port Security Mode 120
 - CrossLink Configuration 113
 - Current CrossLink Information 115
 - Current Spanning Tree Information 185
 - Current Spanning Tree Information for a CRF 188
 - Diagnostic Test Results 196
 - Display Summary 199
 - DSRR Acting as Backup Table 195
 - DSRR Configuration 144
 - DSRR Group Configuration 143
 - DSRR Neighbour Table Screen 194
 - DSRR Status Tables 193
 - General Statistics 163
 - guidelines for using 76
 - IP Configuration 94, 201
 - Master Address Table 178

index-4

- Master Address Table Aging 129
- Master Route Descriptor Table 180
- Message Log Information 197
- Module Information 84
- Port Address Table Aging 127
- Port Configuration 106
- Port Filtering Attributes 124
- Port Spanning Tree Parameters 104
- Port Status 160
- Power Supply Information Screen 159
- Protocol Class Assignment 123
- Reset 152
- Serial Link Configuration 133
- Serial Link Download 148
- SNMP Configuration 202
- Spanning Tree for CRF 101
- Stack Configuration 83
- Station-Cport Information 175
- Switch Configuration 80
- Switch Statistics 157
- Switched Port Analyzer 213
- Syslog Daemon 139
- Telnet Configuration 135
- Telnet Sessions 136
- TFTP Download/Upload 150
- Trap Receivers 205
- TXI Information 173
- View Port Filters 121
- VLAN Address Table 182
- VLAN Configuration 88
- VLAN Parameter Configuration for BRF 91
- VLAN Parameter Configuration for CRF 89
- VLAN Port Configuration 93
- VLAN Route Descriptor Table 183
- VLAN Statistics for BRF 192
- VLAN Statistics for CRF 191
- Serial Link Configuration screen 133
- Serial Link Download screen 148
- servers 19
- Service 215
- service, obtaining 215
- site requirements 43
- SMP 226
- SNA 226
- SNAP 227
- SNMP 35, 227
 - monitoring the network with 201
- SNMP configuration 97
- SNMP Configuration screen 202
- SNMP setup 201
- SNMP trap tables 86
- Source Route Bridging 22
- Source Route Transparent 23
- SPAN 227
- spanning tree
 - VLAN 86
- Spanning Tree for BRF screen screens
 - Spanning Tree for BRF 99
- Spanning Tree for CRF screen 101
- spanning tree information 188
- spanning tree protocol 97
- Spanning Tree Protocol Support 30
 - specifications 13
- SRB 22, 227
- SRS 22, 227
- SRT 23, 227
- SRT/SRB 23
- Stack Configuration screen 83
- stack module 17
- stackable architecture 39
- Start of Troubleshooting Process 215
- static electricity prevention 42
- Station-Cport Information screen 175
- statistics 155
 - master address table 178
 - VLAN address table 182
- Statistics menu 156
- STE 227
- stopping the console session 134
- store and forward 25
- store-and-forward technology 19
- STP 227
- straight-through cable 232
- summary 55
- support 30
- switch configuration 75
- Switch Configuration screen 80
- switch management
 - accessing 69
- switch of desktops 3
- switch of floors and buildings 4
- switch of hubs 3
- switch of routers 4
- switch of servers 3
- switch of switches 2
- Switch Statistics screen 157
- switch theory 17
- Switched Port Analyzer screen 213
- switching 2
- switching modes 25
- switching technology 2
- Syslog Daemon screen 139
- system request button 6

T

table mounting 59
 TCP/IP 227
 Technical Support 221
 Telnet Configuration screen 135
 Telnet Management 36
 Telnet session
 starting 137
 stopping 137
 Telnet Sessions 132
 Telnet Sessions screen 136
 terminal emulation program on console 72
 TFTP 227
 TFTP Download/Upload screen 150
 TKP 227
 Token Passing 26
 token-ring bandwidth 2
 Token-Ring Port operation modes 26
 Token-Ring ports 5
 tools 57
 Transmission Priority Queues 28
 Trap Receivers screen 205
 trap tables 86
 TrBRF 227
 TrCrif 227
 troubleshooting 215
 troubleshooting procedures 216
 twisted-pair cable pinouts 232
 TXI 227
 TXI Information screen 173

U

UAA 227
 UNA 227
 unknown address 20
 unpacking 45
 before installation 56
 UTP 227

V

View Port Filters screen 121
 VLAN 227
 filters 87
 IP 87
 SNMP trap tables 86
 spanning tree 86
 VLAN Address Table screen 182
 VLAN configuration 86
 VLAN Configuration menu 87
 VLAN Configuration screen 88

VLAN Parameter Configuration for BRF
 screen 91
 VLAN Parameter Configuration for CRF
 screen 89
 VLAN Port Configuration screen 93
 VLAN Route Descriptor Table screen 183
 VLAN statistics 191
 VLAN Statistics for BRF screen 192
 VLAN Statistics for CRF screen 191
 VT100 Management 36
 VT100/VT220 137

W

WAN 227
 warm boot 73
 warning
 electricity 41
 Windows 95 36



71001812

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>