

# WANsuite<sup>®</sup> 6450 Reference Manual

March 2004  
34-00326.G



## Emissions Requirements

The WANSuite 6450 has been tested and found to comply with the limits for a Class A digital device, pursuant to EN 55022 and Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. This device must also accept any interference received, including interference that may cause undesired operation.



---

**NOTICE:** *This WANSuite 6450 was tested and found compliant with EN 55022 using the modular cable (9-1544-619-009) and ferrite core (21-00111) placed on the cable end nearest the unit. Both of these items are shipped with the WANSuite 6450. Release the plastic latch on the outside of the core assembly, place around the cable, and close.*

---



---

**WARNING:** *To reduce the risk of electrical shock, do not remove the cover. There are no user-serviceable parts inside. Refer servicing to qualified personnel. This unit contains a lithium battery that is not intended to be field-replaceable. There is risk of explosion if the wrong battery is installed or if the battery is installed incorrectly.*

---



---

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

---

## Canadian Emissions Requirements

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.

## FCC Requirements

This equipment has been tested and found to comply with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: GICDLNAN6450. If requested, provide this number to the telephone company.



---

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

---

- 1 All direct connections to the network lines must be made using standard plugs and jacks that must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug are provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. The table below presents a list of applicable registration jack USOCs, facility interface codes (FICs), and service order codes (SOCs). These are required when ordering service from the telephone company.

Port ID	REN/SOC	FIC	USOC
1.544 Mbps SF	6.0F	04DU9-BN	RJ11C jack
1.544 Mbps SF, B8ZS		04DU9-DN	
1.544 Mbps ANSI ESF		04DU9-1KN	
1.544 Mbps ANSI ESF, B8ZS		04DU9-1SN	

- 2 If this WANSuite product causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. However, if

advance notice is not practical, the telephone company will notify you as soon as possible. Also, you will be advised of your right to file a complaint with the FCC.

- 3 The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice so you can make the modifications necessary to maintain uninterrupted service.
- 4 Parties responsible for equipment requiring AC power should consider including an advisory notice in their customer information suggesting the customer use a surge arrestor. Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem.

## Canadian Emissions Requirements

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.

## Safety Precautions

When handling this equipment, follow these basic safety precautions to reduce the risk of electric shock and injury:

- Follow all warnings and instructions marked on the product and in the manual.
- Unplug the hardware from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a slightly damp cloth for cleaning.
- Do not place this product on an unstable cart, stand, or table. It may fall, causing serious damage to the product.
- Slots in the unit are provided for ventilation to protect it from overheating. These openings must not be blocked or covered. Never place this product near a radiator or heat register.
- This product should be operated only from the type of power source indicated on the marking label and manual. If you are unsure of the type of power supply you are using, consult your dealer or local power company.
- Do not allow anything to rest on the power cord. Do not locate this product where the cord interferes with the free movement of people.
- Do not overload wall outlets and extension cords, as this can result in fire or electric shock.
- Never push objects of any kind into the unit. They may touch dangerous voltage points or short out parts that could result in fire or electric shock. Never spill liquid of any kind on this equipment.
- Unplug the equipment from the wall outlet and refer servicing to qualified service personnel under the following conditions:
  - When the power supply cord or plug is damaged or frayed.
  - If liquid has been spilled into the product.
  - If the product has been exposed to rain or water.
  - If the product has been dropped or if the housing has been damaged.

## Safety Certifications

**IEC 60950 CB Scheme:** The WANsuite 6450 from Verilink was tested to the International Electrotechnical Commission (IEC) CB Scheme (IEC 60950) which is recognized by more than 30 participating countries. This allows Verilink customers around the world to feel confident that Verilink products comply with their relevant international standards.



# Table of Contents

## *Preface*

About this Manual .....	xi
Manual Organization .....	xi
Typographic Conventions .....	xi
Customer Service and Technical Support .....	xii
Support from Your DSL Service Provider .....	xii
Support from Verilink .....	xii
Telephone .....	xii
E-mail .....	xii
Internet .....	xiii
Returning a Unit to Verilink .....	xiii

## *Chapter 1 About the WANsuite 6450*

Introduction .....	1-1
Features of the WANsuite 6450 .....	1-3
Performance .....	1-3
SNMP Management .....	1-3
Intelligent WAN Access Architecture .....	1-3
Overview and Advantages .....	1-3
Features Summary .....	1-4
Front Panel .....	1-6
Rear Panel Connections .....	1-7
Power Port .....	1-7
Power Failure .....	1-7
Supervisory Port .....	1-8
10/100 Ethernet Port .....	1-8
Ethernet LED Indicators .....	1-8
Serial Port .....	1-8
CBR Port .....	1-9
Network Port .....	1-9

## *Chapter 2 Installation*

Unpacking and Inspection .....	2-1
Supplied Materials .....	2-1
Installation Wizard .....	2-2

## Chapter 3 Web Server Interface

Web Server Access .....	3-2
Layout of Interface Screens .....	3-2
Unit Screen .....	3-2
Maintenance Reset .....	3-4
Save and Restart .....	3-5
Interfaces .....	3-6
Network .....	3-6
Configuration Profile Table Screen .....	3-7
Alarm Profile Table Screen .....	3-9
Span Endpoints Screen .....	3-11
CBR .....	3-14
Error Status and Alarm Thresholds Table .....	3-16
Serial .....	3-19
DTR Alarm Control and Status Table .....	3-23
10/100 Ethernet (IP Service Details) .....	3-23
Supervisory .....	3-26
Services .....	3-27
Service Details Screen .....	3-27
Interface Details Button .....	3-28
Type Details Button .....	3-28
IP Service Details Screen .....	3-28
Frame Relay Service Details Screen .....	3-28
Status and Alarms Table .....	3-32
Frame Relay Port Statistics Screen .....	3-33
DLCI Table Screen .....	3-34
DLCI Details Screen .....	3-35
ATM Service Details Screen .....	3-39
ATM Statistics Screen .....	3-41
ATM Virtual Channels Screen .....	3-43
Quality of Service (QoS) Table Screen .....	3-48
CES Service Details Screen .....	3-53
Status .....	3-57
Channel Table Details Screen .....	3-59
Serial CES Configuration .....	3-61
Valid Channel Ranges for Serial and CBR Interfaces .....	3-61
HDLC/PPP Service .....	3-62
Applications .....	3-62
Service Aware .....	3-62
Rule Details Screen .....	3-63
Traffic Meter Statistics Screen .....	3-65
SNMP .....	3-66
Trap Log .....	3-67
Top Talkers .....	3-67
IP Gateway .....	3-69
RIP Parameters .....	3-70
OSPF Parameters .....	3-70
Circuit Table Screen .....	3-70

Static Route Table Screen .....	3-73
Static ARP Table Screen .....	3-76
Trusted Neighbor Table Screen .....	3-77
Area Table Screen .....	3-78
Virtual Link Table Screen .....	3-80
Originate Ping .....	3-82
Network Address Translation (NAT) .....	3-83
NAT Details Screen .....	3-83
Static TCP Translation Table Screen .....	3-85
Static UDP Translation Table Screen .....	3-86
NAT Port Table Screen .....	3-87
Dynamic Host Configuration Protocol (DHCP) .....	3-89
DHCP Server Details Screen .....	3-89
DHCP Host Table Screen .....	3-90
Static Entry Table Screen .....	3-91
IP Address List Table Screen .....	3-92
IP Address Status Table Screen .....	3-93
Bridge .....	3-93
Simple Mail Transfer Protocol (SMTP) .....	3-97
Utilities .....	3-98
Upload/Save .....	3-98
TFTP Configuration .....	3-98
Password .....	3-99
Log Out .....	3-100

## ***Chapter 4 VT100 Interface***

Introduction .....	4-1
Screen Components .....	4-1
Cursor Controls .....	4-1
Field Types .....	4-2
Menu Structure .....	4-3
System Screen .....	4-4
Maintenance Reset .....	4-5
Maintenance Reset .....	4-5
Save and Restart .....	4-6
Interfaces .....	4-7
Network .....	4-7
Configuration Profiles Screen .....	4-9
Alarm Profiles Screen .....	4-11
Span Endpoints Screen .....	4-13
CBR .....	4-17
Error Status and Alarm Thresholds Table .....	4-18
Performance Screens .....	4-20
Serial .....	4-22
10/100 Ethernet (IP Details) .....	4-26
Supervisory .....	4-28
Services .....	4-29

Adding a Service .....	4-29
Service Details Screen .....	4-29
IP Service Details Screen .....	4-30
Frame Relay Service Details Screen .....	4-30
Frame Relay Statistics Screen .....	4-34
DLCI Table Screen .....	4-36
DLCI Details Screen .....	4-37
ATM Service Details Screen .....	4-41
ATM Statistics Screen .....	4-43
ATM Virtual Channel Table Screen .....	4-44
Quality of Service (QoS) Profile Screen .....	4-48
CES Service Details Screen .....	4-54
Status .....	4-57
Channel Table Details Screen .....	4-58
Serial CES Configuration .....	4-61
Valid Channel Ranges for Serial and CBR Interfaces .....	4-61
HDLC/PPP Service .....	4-62
Applications .....	4-62
Service Aware .....	4-63
Rule Config Screen .....	4-64
Traffic Meter Statistics Screen .....	4-65
Trap Log .....	4-66
IP Gateway .....	4-66
RIP Parameters .....	4-67
OSPF Parameters .....	4-68
Circuit Table Screen .....	4-68
Static Route Table Screen .....	4-71
Static ARP Table Screen .....	4-73
Trusted Neighbors Screen .....	4-75
Area Table Screen .....	4-75
Virtual Link Table Screen .....	4-77
Network Address Translation (NAT) .....	4-79
NAT Details Screen .....	4-79
Bridge .....	4-86
TFTP Configuration .....	4-89
SNMP .....	4-90
Top Talkers .....	4-91
Originate Ping .....	4-93
Dynamic Host Configuration Protocol (DHCP) .....	4-94
DHCP Server Details Screen .....	4-94
Simple Mail Transfer Protocol (SMTP) .....	4-98

## ***Appendix A Specifications***

Network Interface - SHDSL Port .....	A-1
CBR Interface .....	A-1
E1 .....	A-1
T1 .....	A-2



Serial Interface .....	A-2
IP Gateway .....	A-2
10/100 Ethernet (IP Gateway or Management) .....	A-2
Management Interfaces .....	A-2
Embedded Operations Channel .....	A-2
10/100 Ethernet .....	A-2
Supervisory Port .....	A-2
Diagnostics .....	A-3
Alarms .....	A-3
Power .....	A-3
Mechanical .....	A-3
Environmental .....	A-3
Industry Listings .....	A-3
Standards .....	A-4
Ordering Information .....	A-4
Standard Equipment .....	A-4
Optional Equipment .....	A-5
Connector Pin Assignments .....	A-6
Serial Interface Pin Assignments, DTE Mode (Packet Use Only) .....	A-6
Serial Interface Pin Assignments, DCE Mode .....	A-7
Ethernet Connection Pin Assignments .....	A-8
Network Interface Pin Assignments .....	A-8
CBR Interface Pin Assignments .....	A-8
Supervisory Port Pin Assignments .....	A-9

## ***Appendix B SNMP Agent***

Introduction .....	B-1
SNMP Configuration Parameters .....	B-1
SNMP MIBs .....	B-1
SNMP Trap Configuration .....	B-2
Generic MIB Loading Instructions .....	B-2



# PREFACE

## About this Manual

---

This reference guide for the WANsuite 6450 ATM integrated access device (IAD) describes unit features and specifications, configuration, and cabling. It is *not* a users guide containing step-by-step procedures. Rather, this manual is designed to be used as a reference regarding commands, interface ports, configuration parameters, and other specific information about the WANsuite 6450.




## Manual Organization

The chapters and appendices in this manual are arranged for quick reference when you need it. You do not have to read previous chapters to understand the subsequent chapters. Appendices are designed to complement the main chapters.

- *Chapter 1, About the WANsuite 6450* – This chapter describes product features and capabilities.
- *Chapter 2, Installation* – This chapter describes unit port connections and powering information.
- *Chapter 3, Web Server Interface* – This chapter describes the menu screens and configuration parameters accessed through the Web server interface.
- *Appendix A, Specifications* – This appendix defines the specifications for the WANsuite 6450. In addition, this section provides ordering information and all the connector pin assignments for the interfaces on the rear panel of the WANsuite 6450.
- *Appendix B, SNMP Agent* – This appendix defines which Management Information Base (MIB) files are supported by the WANsuite 6450 SNMP agent. In addition, instructions are provided for loading these MIB files into most SNMP management stations.

## Typographic Conventions

The following table lists the graphic conventions used throughout this guide.

Convention	Description
	A <i>Notice</i> calls attentions to important features or instructions.
	A <i>Caution</i> alerts you to serious risk of data loss or other results that may cause you or the unit trouble if the warning is not heeded.
	A <i>Warning</i> alerts you to the risk of serious damage to the unit or injury and possible death to the end user.

## Customer Service and Technical Support

---

Verilink provides easy access to customer support through a variety of services. This section describes these services.

### Support from Your DSL Service Provider

If assistance is required, contact your service provider. When you contact your service provider for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

### Support from Verilink

If you are unable to receive support from your service provider or want to contact us directly, Verilink offers worldwide customer support by telephone, e-mail, and through Verilink's Internet Web site.

#### Telephone

Customer support is available by telephone 24 hours a day, 7 days a week. To speak directly with a Verilink customer service representative, you may dial one of the following numbers:

- Sales and Marketing: 800-VERILINK (837-4546)
- Technical Support: 800-285-2755 (toll-free)  
1-256-327-2255 (international)

#### E-mail

You can request sales and marketing information or pose a technical support question about your Verilink product by contacting us at the e-mail addresses provided below. Verilink will respond to e-mailed requests for support during regular business hours (8–5 CST, Monday–Friday).

- Sales and Marketing: info@verilink.com
- Technical Support: support@verilink.com

## Internet

Visit Verilink's Web site to access the latest Verilink product information, technical publications, news releases, contact information, and more:

<http://www.verilink.com>

If this reference manual is revised to reflect code changes or other updates, the most recent version will be posted to the Verilink Web site.

## Returning a Unit to Verilink

---

If for any reason you must return your Verilink product, it must be returned with the shipping prepaid, and packaged to the best commercial standard for electronic equipment. Verilink will pay shipping charges for delivery on return. You are responsible for mode and cost of shipment to Verilink.

You must have a Return Material Authorization (RMA) number marked on the shipping package. Products sent to Verilink without RMA numbers will be returned to the sender unopened, at the sender's expense.

A product sent directly to Verilink for repair must first be assigned an RMA number. You may obtain an RMA number by calling Customer Service at 800-926-0085, extension 3002 (international number: 1-800-256-327-2255).

When calling Verilink for an RMA, please have the following information available:

- Model number and serial number for each unit
- Reason for return and symptoms of problem
- Purchase order number to cover charges for out-of-warranty items
- Name and phone number of person we can contact if we have questions about the unit(s)

The address for you to use when returning a unit to Verilink will be provided when the RMA is issued. The standard delivery method for return shipments is Standard Ground for domestic returns and International Economy for international returns (unless otherwise specified).



# ABOUT THE WANSUITE 6450

## Introduction

---

Verilink's WANSuite 6450 is a feature-rich, intelligent integrated access device (IAD) that manages voice and data applications in an ATM network. The WANSuite 6450 terminates a standards-based Symmetric High-Bit Rate Digital Subscriber Line (SHDSL) that originates from a Digital Subscriber Line Access Multiplexer (DSLAM) and provides interfaces for the end user's communications equipment.

The WANSuite 6450 is **ServiceAware**<sup>TM</sup> IAD with the following hardware: an SHDSL network interface; a Constant Bit Rate (CBR) port configurable as T1 or E1; a Serial port software-configurable for V.35, V.36, X.21, RS-232, RS-449, or EIA-530; a 10/100Base-T Ethernet port; an asynchronous Supervisory port; five tri-color status LEDs; and front panel reset and factory configuration buttons.

The Circuit Emulation Service (CES) support provides for the encapsulation of TDM traffic from end-user equipment into ATM cells for transport across the WAN to the DSLAM and on to the ATM network. This allows for the continued use of existing TDM equipment at the premise while the ATM network continues to grow and move further out to the edge. This unit supports CES over the CBR port and the Serial port.

A router or bridge using PPP/HDLC or Frame Relay protocol connects to the WANSuite 6450's Serial port. The unit encapsulates the PPP data into ATM cells using Internet Engineering Task Force (IETF) RFC 1483. Any router/bridge supporting PPP over ATM (PPPoA) RFC 1483 encapsulation can be used at the other end of this ATM connection.

The IP Gateway feature enables IP packet routing throughout a LAN/WAN network architecture using static routing configuration or dynamic routing protocols (Routing Information Protocol – RIP 1 and RIP 2, or Open Shortest Path First – OSPF), Dynamic Host Communications Protocol – DHCP, and Network Address Translation – NAT.

RIP 1 and RIP 2 allow routers to exchange routing information. The WANSuite 6450 then uses this information exchange to build routing tables

for IP Packet routes. After building the routing tables, the unit periodically broadcasts the contents to neighboring routers so your network can choose the most efficient routes available.

OSPF uses link-state routing algorithms to calculate routes based on the number of routers, transmission speeds, delays, and route costs. Using the OSPF protocol, the WANsuite 6450 works with other routers in your telecommunications fabric to dynamically change routes “on the fly” to make use of the most efficient and cost-effective transit across your network.

Bridging separate LANs together is another option for the IP traffic. Using the IEEE Standard 802.1D Transparent Bridging specification, the WANsuite 6450 can simplify your network architecture by allowing you to bridge separate LANs across a WAN so they operate as a single LAN.

Because IP Gateway enables the WANsuite 6450 to route IP traffic either statically or dynamically or to bridge IP traffic across your LAN/WAN architecture, your need for costly routers is substantially reduced. This one-stop solution can help you meet the requirements of your many different applications.

DHCP uses a server-client architecture to assign IP Addresses to PCs and workstations on the LAN. The DHCP server dynamically assigns these IP Addresses, which can be either temporary or permanent, to each PC or workstation (DHCP client). These IP Addresses are "housed" on the DHCP server. The flexibility to reassign IP Addresses saves the end user money by eliminating the need for a single IP Address for each piece of equipment on the LAN.

NAT enables an enterprise to set up two sets of IP Addresses – one set for internal network use (or LAN traffic) and one set for external use (or Internet traffic). This can provide a layer of security for a company by eliminating outside access to internal IP Addresses from the Internet.

The WANsuite 6450 gives service providers and enterprise customers the capability to monitor end-to-end network performance (with support of up to 16 virtual channels); isolate performance problems to the LAN, local loop, or ATM network; determine appropriate bandwidth needs; and monitor network trends to aid in future capacity planning.

All of the WANsuite 6450's installation, performance configuration, traffic monitoring, alarm reporting, and diagnostic capabilities can be configured through the unit's embedded Web server interface using Microsoft® Internet Explorer™. The Web server interface can be accessed locally through the Ethernet port or the Supervisory port, or remotely through the Network port. Especially advantageous is WANsuite's advanced monitoring and control capability that gives network administrators the ability to plan future capacity requirements.

The unit's built-in Service Aware technology lets network managers maximize available WAN bandwidth and verify SLAs. This management platform lets the end user see network activity (performance) and problems (diagnostics) on any permanent virtual circuit (PVC), access line, or physical circuit.



# Features of the WANsuite 6450

---

## Performance

Historically, WAN access devices have tended to perform well as single-function devices such as CSU/DSUs, but have not been optimized to address higher-level traffic issues such as service levels and integration. Verilink's architecture and Web-based user interface work together to address all access issues such as services and applications, rather than as circuits and protocols, for exceptional WAN management performance.

To further leverage its Web browser interface, Verilink's new architecture also allows firmware to be upgraded via the Web from a standard browser, with password control, if desired.

## SNMP Management

With integrated SNMP in-band management, enterprise managers can now manage Verilink WANsuite units and their integral CSU/DSUs as a single unit. With only one LAN segment in the network, the WANsuite 6450 can be managed by SNMP. By downloading all configuration parameters from the central site, no interaction is required at remote sites to establish connectivity. The unit allows any port to be configured for any of its available service technologies through simple software configuration. Network managers can now fine tune the enterprise network for the lowest cost and highest performance.

## Intelligent WAN Access Architecture

Verilink's next-generation WAN access architecture is built around a PowerPC™ processor with 50 MIPS of processing power and 16 Mbytes of onboard memory, and works with non-proprietary network management solutions via SNMP. An embedded Web server supplies a simple-to-use interface for configuration and statistics collection, with a service table for mapping services to ports and a user table for monitoring and controlling traffic.

## Overview and Advantages

---

Verilink's WANsuite 6450 is an innovative, highly intelligent, software-based WAN access device optimized for ATM over SHDSL access. This unit provides network managers with all the tools necessary to monitor and troubleshoot voice, data, and network transmission systems. The ability to use the WANsuite 6450 unit as an IP Gateway greatly increases its flexibility, while reducing networking costs. In addition, the WANsuite 6450 is a valuable tool for the following:

- Measuring and reporting performance

- Managing network resources to ensure optimum performance
- Analyzing trends to aid in network planning

WANsuite 6450 advantages include the following:

- Enables a new class of xDSL technologies – the internationally standard SHDSL.
- Allows for continued use of existing TDM equipment by supporting CES via AAL1.
- Reduces the need for costly routers with its IP Gateway feature.
- Offers easy installation and configuration, reducing maintenance and sparing costs.
- Controls recurring ATM access costs – WANsuite products quickly pay for themselves by allowing enterprises and service providers to optimize the use of valuable bandwidth.
- Allows for use of existing routers without changing the external router's configuration by running PPP over an ATM network.

## Features Summary

---

- **Powerful core architecture**
  - SHDSL network port for symmetrical data rates ranging from 192 kbps to 2.312 Mbps
  - T1 or E1 circuit emulation
  - 10/100Base-T Ethernet port and asynchronous Supervisory port
  - Serial data port, user-selectable V.35, V.36, RS-232, or EIA-530
  - Intuitive Web browser for management
- **CES**
  - Constant Bit Rate (CBR) port configurable for T1 or E1 supporting the following modes:
    - Unframed T1 – 1.544 Mbps raw bit stream
    - T1 ESF
    - T1 D4
    - Unframed E1 (G.703) framing – 2.048 Mbps raw bit stream
    - E1 CCS framing
    - E1 CAS framing
  - AAL1 ATM encapsulation
    - Structured Nx64 basic service supporting full or partial T1/E1 circuits
    - Structured Nx64 service with Channel Associated Signaling (CAS) supporting the following:
      - E1 CAS signaling
      - T1 robbed bit signaling

- Full or partial T1/E1 circuits with signaling
- Unstructured service (2.048 Mbps E1 or 1.544 Mbps T1)
- Configurable for synchronous or adaptive timing
- User-configurable Cell Delay Variation
- User-configurable partial cell fill
- User-configurable automatic channel configuration for E1 CCS or E1 CAS services
- User-configurable scrambling/descrambling of ATM cell Payload using an  $x^{43}+1$  polynomial
- User-configurable time slot multiplexing between the CBR port and the Serial port
  - For Nx64 basic and CAS services, the user can individually configure the CES channels for the CBR port or for the Serial port
  - For Unstructured E1 service, the user can configure all channels for either the CBR port or for the Serial port
- **IP Gateway**
  - 10/100Base-T Ethernet port
  - Static routes
  - Static Address Resolution Protocol (ARP)
  - Dynamic routing protocols, including RIP 1, RIP 2, and OSPF
  - Un-numbered network
  - Address Management: NAT and DHCP
  - Bridging
  - Programmable alarm thresholds
  - IPoA
- **Serial Port Configurable for PPP, Frame Relay, or CES**
  - Supports V.35, V.36, EIA-530, or RS-232
  - PPPoA
- **Management Interfaces**
  - An innovative Web-based user interface
    - Embedded HTTP server for remote configuration and real-time reporting via Web browser
    - Decreased installation and configuration time for service employees
    - Simplified troubleshooting and fault isolation of network problems
    - Optimal management of ATM-based services
    - Saves and downloads configuration files from remote server
  - EOC for SHDSL-related parameters
  - SNMP
  - VT100

- **Frame Relay-to-ATM Network/Service Interworking**

- Supports FRF.8 Frame/ATM service interworking and maps Frame datalink connection identifiers (DLCIs) to ATM permanent virtual circuits (PVCs); up to 20 VCs can be configured.
- Provides network interworking functionality that allows Frame Relay end users to communicate over an intermediate ATM network that supports FRF.5.
- Benefits Internet service providers that need to link Frame Relay and ATM networks, especially those networks with ATM backbones and Frame Relay end users.

## Front Panel

The front panel of the WANsuite 6450 is shown below in Figure 1.1.

**Figure 1.1** Front Panel of WANsuite 6450



The front panel's five LED status indicators are described below:

Indicator	Description
<b>MODE</b>	Normally, this indicator lights <i>green</i> . The indicator lights <i>amber</i> while configuration is being set by the front panel buttons or when the configuration is changed by SNMP or through the Web interface. The indicator will remain amber until the changed configuration is saved; it will revert to green when the new configuration has been saved.
<b>CBR</b>	The indicator is off (not illuminated) when the CBR port has not been configured. The indicator lights <i>green</i> when the CBR port link is up and is receiving AAL1 cells. The indicator lights <i>red</i> when the CBR port has been configured and no AAL1 cells are received. The indicator lights <i>amber</i> when the CBR port link is up but AAL1 cells are not being received.
<b>NET</b>	The indicator is off (not illuminated) when the Network port has not been configured. The indicator lights <i>green</i> when the Network port link is up and the ATM protocol is established. The indicator lights <i>red</i> when the Network port link is down and the ATM protocol is not established. The indicator lights <i>amber</i> when the Network port link is up, but the ATM protocol is not established.
<b>ALARM</b>	The indicator lights <i>red</i> if an alarm condition exists. The indicator lights <i>amber</i> if a "yellow" alarm condition exists.
<b>POWER</b>	The indicator lights <i>green</i> when power is applied to the unit. The indicator lights <i>amber</i> when the unit is in a test mode loopback.

The user-activated input control buttons are described below:

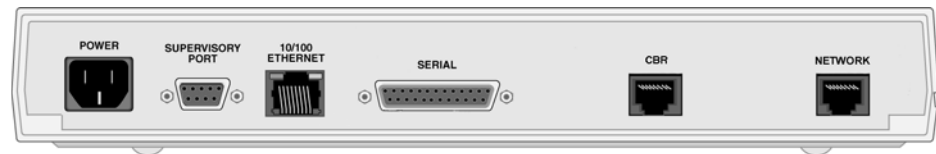
Button	Description
<b>RESET</b>	Provides a hardware reset to the unit.
<b>CONFIG</b>	Sets the unit back to its factory default Ethernet or HDLC configuration; this is the same as a maintenance reset. To initiate this function, you must press and hold the <b>CONFIG</b> button during a power-up sequence.*

\*The **CONFIG** button must be held until the **MODE** LED lights amber and remains illuminated for the default configuration to take effect.

## Rear Panel Connections

The rear panel of the WANsuite 6450 has five connectors. From left to right, these are as follows: **POWER**, **SUPERVISORY PORT**, **10/100 ETHERNET**, **SERIAL**, **CBR**, and **NETWORK** as shown in Figure 1.2 below.

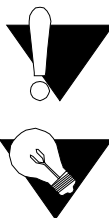
Figure 1.2 WANsuite 6450 Rear Panel



### Power Port

The **POWER** port on the WANsuite 6450 unit is a standard, grounded, three-prong connector. This 110/220 VAC power receptacle is rated at 50–60 Hz, 0.2 A/0.1 A. To apply power to the unit, simply plug the supplied power cord into the unit's **POWER** port and then connect the wall plug to an appropriate electrical outlet. The unit has no power switch.

When power is applied to any WANsuite 6450 unit, the front panel indicators flash for approximately 10 to 15 seconds as the unit initializes. The green **POWER** LED on the front panel will remain illuminated as long as the unit receives power. This LED turns amber when the unit is in test mode.



**CAUTION:** Always connect the power cord to a grounded electrical outlet.

**NOTICE:** Per UL 1950 and CSA 60950 Clause 1.7.2, if the power supply cord is intended to serve as a disconnect device, an easily accessible socket must be installed near the equipment.

### Power Failure

If the indicator does not illuminate, check the power connections and the primary circuit breaker.

The WANsuite 6450 units provide nonvolatile memory retention of the unit configuration in case of a power failure. The unit will automatically restore normal service following a power loss and will retain pre-existing time and date information.

## Supervisory Port

The **SUPERVISORY** port is a DB-9 female DCE connector configured for 8 bits, no parity, and 1 stop bit. Bit rates are configured through the Web server interface. (See *Unit Access Details* on page 3-26.) The Supervisory port speed can be set to 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 bps. The initial default rate of the Supervisory port is 19200 bps.

On power-up, the Supervisory port sends out diagnostic messages at the bit rate of 115.2 kbps until the Supervisory service acquires the Supervisory port, after which the port speed is changed to the setting in the Supervisory interface screen.



---

**NOTICE:** *For information on pinout assignments for this connector, refer to Supervisory Port Pin Assignments on page A-9. See Standard Equipment on page A-4 for information on cables for this connector.*

---

## 10/100 Ethernet Port

The WANsuite 6450 provides a single **10/100 ETHERNET** interface port for IP Gateway, SNMP, and Web browser access. This interface is an eight-pin modular jack that complies with standard twisted-pair, 10/100Base-T requirements. The 10/100Base-T cable is supplied by the end user. Refer to *Ethernet Connection Pin Assignments* on page A-8 for pin assignments and cable descriptions.

### Ethernet LED Indicators

There are two unlabeled indicator LEDs on either side of the 10/100 Ethernet jack. The LED on the left side of the jack pulses amber to indicate data activity (either transmit or receive). The LED on the right side of the jack lights green to indicate that the link layer is operational.

## Serial Port

The **SERIAL** interface port located on the WANsuite 6450 rear panel is a multi-protocol interface presented physically as a DB-25 connection. The protocols supported by this interface are RS-232, V.35, V.36, EIA-530, X.21, and RS-449.

Cables that adapt the DB-25 interface to the 34-pin V.35 interface are available. DB-25 to DB-25 cables are also available if your installation needs require them. See *Standard Equipment* on page A-4 for details. Pin assignments for the Serial interface are listed in *Serial Interface Pin*

*Assignments, DTE Mode (Packet Use Only)* on page A-6 and *Serial Interface Pin Assignments, DCE Mode* on page A-7.



---

**CAUTION:** *FCC rules require that interconnecting cables carrying high-speed data be shielded appropriately to minimize radio frequency interference.*

---

## CBR Port



---

**CAUTION:** *The T1/E1 CBR port is not a standalone port. Connect the T1/E1 CBR port only to the "private" side of the network on the customer premises, never to the "public" side.*

---

The CBR interface port located on the WANsuite 6450 rear panel is an RJ11C, eight-pin modular jack that can be software-selectable for T1 or E1. As a T1 port, it terminates as 100 ohms, and as an E1 port at 120 ohms. This port is used to transport TDM traffic using a T1/E1 framer to provide ATM adaptation Layer 1 with Circuit Emulation Services (AAL1-CES).

To view the pinout assignments for this interface, refer to *CBR Interface Pin Assignments* on page A-8.

## Network Port

The WANsuite 6450 has one rear panel **NETWORK** interface port. This connection is a standard RJ11C, eight-pin modular jack that terminates as 135 ohms.

To view the pinout assignments for this interface, refer to *Network Interface Pin Assignments* on page A-8.





# INSTALLATION

This chapter describes the contents of your WANsuite 6450 shipment and provides information on connecting and installing the unit.

The WANsuite 6450 uses an “Installation Wizard” to help you automatically install the unit quickly and correctly. Procedures for using this Installation Wizard are also described in this chapter.

## Unpacking and Inspection

---

The WANsuite 6450 is shipped in cardboard cartons with foam inserts for shock and vibration protection. When your shipment arrives, inspect the shipping container and contents, and compare all items with those on the packing list.

If the contents of the shipment are incomplete or if there is mechanical damage or defect, notify Verilink. (Refer to *Support from Verilink* on page xii.) If the shipping container or cushioning material is damaged, notify the carrier and Verilink immediately and make a notation on the delivery receipt that the container was damaged. (If possible, obtain the signature and name of the person making delivery.) Retain the packaging material until the contents of the shipment have been checked for completeness and the unit has been checked both mechanically and electrically.

## Supplied Materials

---

The WANsuite 6450 ships with the following standard items:

- Serial (Supervisory) cable
- Network cable
- Power cord
- Verilink Documentation CD

For specific applications, see *Connector Pin Assignments* on page A-6 for additional optional cables and adapters. Contact Verilink Technical Support (page xii) for further assistance.

## Installation Wizard

The WANsuite 6450 can be configured and monitored through the Web server interface. To gain access to this interface, the unit must be configured with an IP Address. Verilink provides a DOS-based program – the Verilink Configuration Wizard – to aid in this initial configuration.



**NOTICE:** *You may also access the Verilink Configuration Wizard on the Verilink Web site: [www.verilink.com](http://www.verilink.com).*

To configure the IP Address using the Verilink Configuration Wizard, perform the following steps:

- 1 Using the supplied cable, connect the unit's DB-9 Supervisory port to a COM port on your PC. (Take note of which COM port is connected.)
- 2 Insert the Verilink CD (provided with the WANsuite 6450) into your PC's CD-ROM drive.
- 3 Use Windows "Explore" to view the contents of the CD and select the folder labeled "Utilities." In this folder will be a file named `ipwiz.exe`; this executable file is the Verilink Configuration Wizard application. Double-click on this file to launch the program. After the program is fully launched, you will see the following screen:



- 4 Using the Tab key to move from field to field, move the cursor to the "COM Port" field. Using the Spacebar, toggle between the available options until the correct COM port is shown (COM1, COM2, COM3, or COM4). Be sure to choose the same COM port as the port to which the unit is connected.
- 5 By default, the "Baud Rate" field will display 115200 (bits per second). For the purpose of this installation, do not change the displayed baud rate from its default. Proceed directly to the next step.

- 6** Using the Tab key again, move the cursor to the “IP Address” field and enter the appropriate IP Address for the unit (*xxx.xxx.xxx.xxx*). If necessary, repeat this process for the “Subnet Mask” and “Gateway Address” fields.
- 7** Next, move the cursor to the “Write To Unit” field and press the Enter key. The program will prompt you to reset the unit.
- 8** To reset the unit, press the **RESET** button on the unit’s front panel. The Configuration Wizard will then automatically download the configuration information to the unit.
- 9** Note the status messages displayed at the bottom of the Configuration Wizard screen. When the download is complete, your PC will beep and the status message bar will display “Finished.”
- 10** Finally, move the cursor to the “Exit” prompt and press Enter. The Configuration Wizard program will close.



## WEB SERVER INTERFACE

The WANsuite 6450 has an innovative, embedded Web-based user interface for remote configuration and real-time reporting via Microsoft Internet Explorer 5.0 or higher. Access to the Web server interface and how the interface is used to configure the WANsuite 6450 unit are described in detail below.



---

**NOTICE:** *Verilink recommends the use of Microsoft's Internet Explorer 5.0 or higher because if you use other Internet browsers to access the Web server interface, some screen elements will not display as described in this manual.*

---



---

**NOTICE:** *The material presented in this chapter follows the order listed in the navigation bar on the left side of the Web Server interface screen. However, because the parameters you specify in the Service Table attach protocols to interfaces, you must configure the Service Table first. (See Services as described on page 3-27.) You will not be able to allocate channels (see Channel Table Details Screen as described on page 3-59) until the Service Table has been configured.*

---

Configuration through the VT100 interface is covered in Chapter 4.

# Web Server Access

---

You can access the Web Server interface by connecting to its IP address. This connection can be directly through the 10/100 Ethernet port, in-band via PPP over any port, or in-band via encapsulated IP traffic on the ATM WAN circuit.



---

**NOTICE:** *Any changes to the unit's configuration **MUST** be followed by a "Submit" if there is a "Submit" button on the menu. If you change the Service Table, you must perform a "Save and Restart."*

---

To access the Web Server interface, type the unit's IP address in the browser's Address (or Location) field and press the "Enter" key.

## Layout of Interface Screens

When you first access the Web Server interface, your browser will display a screen that is divided into three frames. The upper frame forms a border across the top of the screen; it identifies the Verilink unit in service and displays the hardware and software revision and serial numbers under which the unit is operating. The far right corner of the upper frame displays whether or not a "Save and Restart" is necessary when parameters are changed on the currently displayed screen.

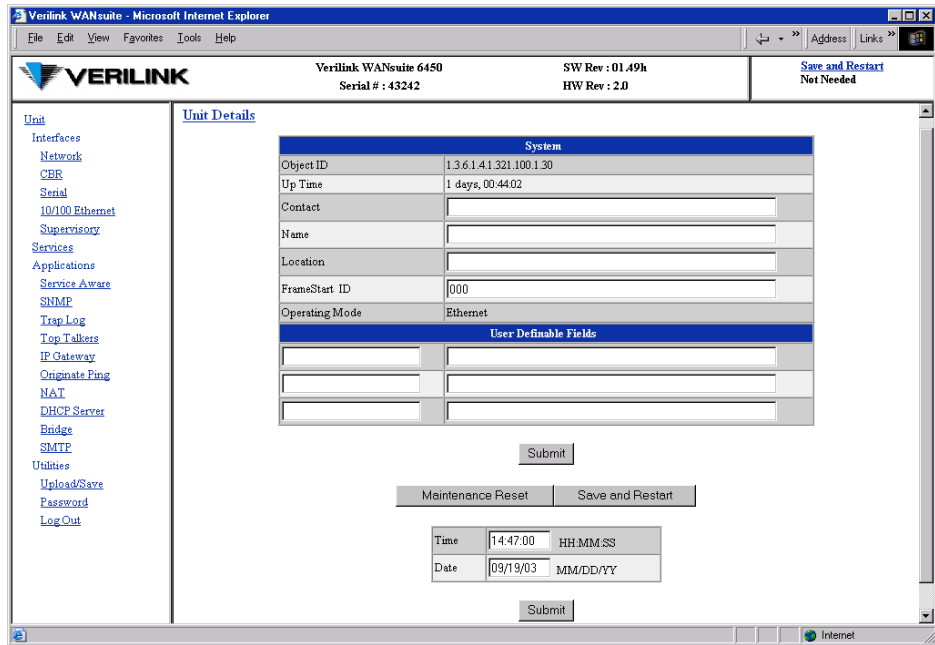
The area beneath the upper frame is divided into two side-by-side frames. The frame on the left side of this area depicts a hierarchical "tree" structure used to navigate through the various interface screens. Each "branch" on the tree guides you to more specific upper-level information about the unit and its configuration. Note that the Interfaces, Applications, and Utilities branches do not link to a page – these branches simply provide structure for navigation. The frame on the right side of the screen will display the actual configuration screen. The screen captures throughout this chapter show only the configuration portion of the screen, except in the case of the Unit screen, which shows all three frames. The Unit screen represents the top of the navigation tree.

## Unit Screen

---

The first screen displayed by the unit's Web Server interface is the Unit screen (Figure 3.1). This screen lets you view and set specific information about the unit in service.

**Figure 3.1** Unit Screen



The Unit screen displays the following fields:

Field	Function
Object ID	Display-only field used to point an SNMP agent to this ID.
Up Time	Displays the amount of time the unit has been up and running.
Contact	Stores the name of a point-of-contact for system failure.
Name	Read/write field that holds the unit's name.
Location	Read/write field that holds the unit's location.
FrameStart ID	Not used for ATM. Read/write field that holds the unit's ID that uniquely identifies the unit and is used in the FrameStart applications.
Operating Mode	Displays most recently executed Maintenance Reset option.
Blank Fields	Read/write fields for user-specific labels and values. Information resides in non-volatile memory.
Time	Read/write field that holds the unit's internal time setting in standard 24-hour HH:MM:SS format.
Date	Read/write field that holds the unit's internal date setting in standard MM/DD/YY format.

The Unit screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed. Use the top "Submit" button to set unit parameters changed in the upper section of the screen, and the lower "Submit" button to set the real-time clock.

Button	Function
Maintenance Reset	Resets unit to its default configuration.
Save and Restart	Saves the current configuration and restarts the unit.

## Maintenance Reset

Use this button to perform a Maintenance Reset. All configurations will be lost and the unit will be set back to an initial factory configuration. The options for a Maintenance Reset are shown in the table below.

Configuration Choice	RFC 1483 Encapsulated Data	IP Encapsulated in ATM	Serial HDLC Encapsulated in ATM	T1 CBR Channels	E1 CBR Channels	Serial CBR Channels
Ethernet	Yes	Yes	No	None	None	None
Serial HDLC	Yes	No	Yes	None	None	None
E1 CCS*	Yes	Yes	No	None	1–31	None
E1 CAS	Yes	Yes	No	None	1–15, 17–31	None
Unframed E1	Yes	Yes	No	None	0–31	None
T1 ESF	Yes	No	Yes	1–24	None	None
T1 SF	Yes	No	Yes	1–24	None	None
T1 ESF CAS/RBS	Yes	No	Yes	1–24	None	None
T1 SF CAS/RBS	Yes	No	Yes	1–24	None	None
Unframed T1	Yes	No	Yes	1–24**	None	None
Serial CES	Yes	Yes	No	None	None	1–31
Unstructured Serial CES	Yes	Yes	No	None	None	0–31
PPoA-IPCP	No	Yes	No	None	None	None
PPoA-NAPT	No	Yes	No	None	None	None

\* Factory default configuration

\*\* Unframed T1 CES service uses an additional 8 kbps of bandwidth for framing

All the factory configurations set up an ATM service on the Network port with one configured virtual channel (VPI=0, VCI=32). Management data received on this channel (either WEB or SNMP) will be processed at the unit if it is encapsulated using RFC 1483 and directed to the unit's IP address. (A Maintenance Reset will not change the unit's IP address.)

The Serial HDLC configuration and the T1 ESF configuration will also accept PPPoA encapsulated data and deliver it to the Serial port.

The T1 SF, T1 ESF CAS/RBS, T1 SF CAS/RBS, Unframed T1, Serial CES, and Unstructured Serial CES configurations set up a CES service between the Network port and the T1/E1 CBR port or the Serial port using VPI=0, VCI=33. The T1 options configure the CBR port for the desired framing mode, and configure the CES service for 24 channels. For unframed T1 service, the CES service provides 1.544 Mbps of bandwidth for the service

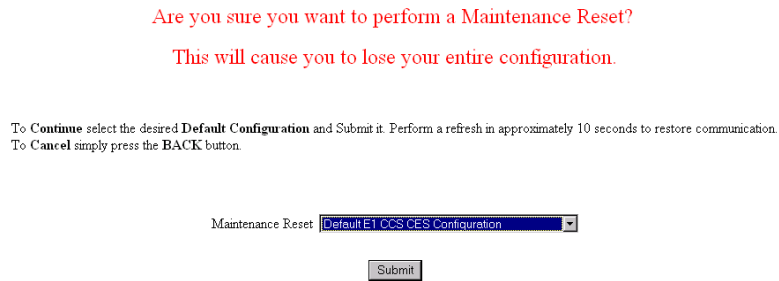


(1.536 Mbps for the T1 channels and 8 kbps for framing). The E1 configurations set up the CBR port to run E1 and have 30, 31, or 32 channels delivered to the CES service. The Serial CES configurations set up the CBR port to run E1 CCS or Unframed E1, but allocates all 31 or 32 channels to the Serial port.

The PPOA-IPCP and PPOA-NAPT set up a PPP connection over ATM using the VPI=0, VCI=32. The resulting PPP interface then uses PPP negotiation to obtain the IP address, mask, and DNS address. After successful negotiation, the DHCP server starts on the Ethernet Lan. For PPOA-IPCP, the negotiated IP address is applied to the LAN, whereas in the case of PPOA-NAPT, the negotiated IP address is applied to the WAN.

Clicking the “Maintenance Reset” button will display a selection screen, as shown in Figure 3.2, with a drop-down list of the available configurations, which are listed in the table above.

**Figure 3.2** *Maintenance Reset Screen*

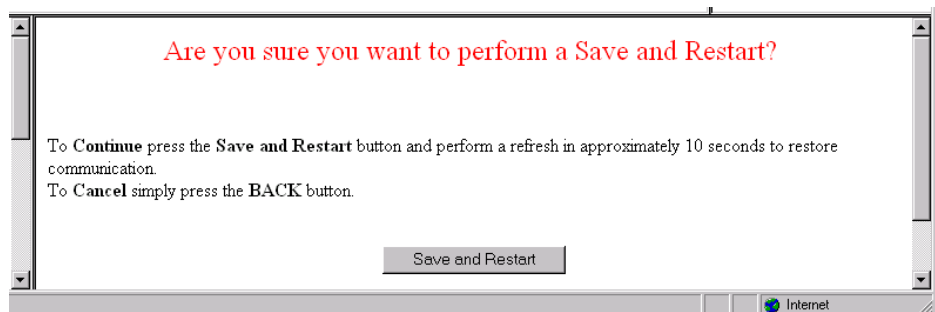


**NOTICE:** *Performing a “Maintenance Reset” or a “Save and Restart” will terminate communications with the unit.*

## Save and Restart

The Save and Restart button on the Unit screen will display the confirmation screen shown in Figure 3.3.

**Figure 3.3** *Save and Restart Screen*



Click the “Save and Restart” button on the confirmation screen to proceed with the action. To cancel, simply invoke your browser’s “Back” function.

# Interfaces

The WANSuite 6450 unit has five available interfaces: Network, CBR, Serial, Ethernet 10/100, and Supervisory. These interfaces are described below.

## Network

The WANSuite 6450 Network screen (Figure 3.4) lets you view and make changes to the Network interface's configuration.

**Figure 3.4** Network Screen

Unit Type	TU-R
Expected Repeaters	0
Span Configuration	DEFVAL
Span Alarm Configuration	DEFVAL
Pair-1 Mode	Data Data Mode
Pair-2 Mode	Idle No Activity
EOC In	24408
EOC Out	24408
Discovered Repeaters	0
Line Rate	2312000
Maximum Line Rate	2320000
Transmission Mode	Annex-B

Submit

Configuration Profiles   Alarm Profiles   Span Endpoints

The Network screen status and configuration parameters are described in the following paragraphs.

**Unit Type** Selects the unit type. TU-R represents a CPE terminal unit; TU-C represents a CO terminal unit.

Values: TU-R, TU-C  
Default: TU-R

**Expected Repeaters** Provisions the number of repeaters in the selected span.

Values: 0 (zero)  
Default: 0 (zero)

**Span Configuration** Represents a span configuration profile in the Span Configuration Profile Table, which applies to this span. By default, this object will have the value "DEFVAL" (the index of the default profile).

Values: User Span Profile 1, User Span Profile 2, DEFVAL (Default Value)  
Default: DEFVAL

- Span Alarm Configuration** Represents an Alarm configuration profile in the Endpoint Alarm Configuration Profile Table. The alarm threshold configuration in the referenced profile will be used by default for all segment endpoints in this span. By default, this object will have the value 'DEFVAL' (the index of the default profile).  
 Values: User Alarm Profile 1, User Alarm Profile 2, User Alarm Profile 3, DEFVAL (Default Value)  
 Default: DEFVAL
- Pair-1 Mode** Represents the status and detail status information of the span for two-wire operation.
- Pair-2 Mode** Represents the status and detail status information of the span for four-wire operation. This mode is not supported by the WANsuite 6450.
- EOC In** Displays the number of messages received on the Embedded Operations Channel.
- EOC Out** Displays the number of messages transmitted on the Embedded Operations Channel.
- Discovered Repeaters** Displays the number of discovered repeaters in this span.
- Line Rate** Displays the actual negotiated line rate.
- Maximum Line Rate** Displays the maximum physical line rate with respect to the current span configuration.
- Transmission Mode** Displays the actual transmission mode (Annex-A or Annex-B).

The Network screen provides the user-activated buttons described below.

Button	Function
Submit	Sets any values that have been changed.
Configuration Profiles	Displays the three configuration profiles that can be used.
Alarm Profiles	Displays the four alarm profiles that can be used.
Span Endpoints	Lists the currently available span endpoints.



**CAUTION:** *Performance data will be lost upon power cycle or after performing a Maintenance Reset/Restart.*

## Configuration Profile Table Screen

Clicking on the “Configuration Profiles” button on the Network screen will display the table shown in Figure 3.5.

**Figure 3.5** Configuration Profile Table Screen

Profile Name	Wire Mode	Data Rate(Min)	Data Rate(Max)	Remote	Transmission Mode
<a href="#">DEFVAL</a>	Two-Wire	192000 (3*64k)	2312000 (36*64k+8k)	Enabled	Annex-B
<a href="#">User Span Profile 1</a>	Two-Wire	192000 (3*64k)	2312000 (36*64k+8k)	Enabled	Annex-B
<a href="#">User Span Profile 2</a>	Two-Wire	192000 (3*64k)	2312000 (36*64k+8k)	Enabled	Annex-B

This table displays the information the user specifies in the Configuration Profile Details screen (Figure 3.6), which is accessed by clicking on the specific Profile Name hyperlink in the table above.

**Figure 3.6** Configuration Profile Details Screen

Profile : User\_Span\_Profile\_1

Wire Mode	Two-Wire
Data Rate (Min)	192000 (3*64k)
Data Rate (Max)	2312000 (36*64k+8k)
Remote	Enabled
Transmission Mode	Annex-B
PSD Type	Symmetric
Line Probe	Enabled

Submit

This screen lets you configure or change the following information about the selected configuration profile:

- Wire Mode** Displays the type of wire interface used by the span. The WANsuite 6450 supports only the two-wire mode.
- Data Rate (Min)** Sets the minimum attainable data rate in the span.
- Data Rate (Max)** Sets the maximum attainable data rate in the span. Note that the line rate will be 8 kbps above the data rate.
- Remote** Enables/disables support for remote management of the units in an SHDSL line from the STU-R via the EOC.  
 Values: Enabled, Disabled  
 Default: Enabled
- Transmission Mode** Sets the regional setting of the span represented as a bit-map of possible settings.  
 Values: Annex-A (*ITU-T G.991.2*), Annex-B (*ITU-T G.991.2*)  
 Default: Annex-B



**NOTICE:** When the WANsuite 6450 is operating with Unit Type set to TU-R, it supports Annex-A or Annex-B. The configuration of the TU-C unit determines the actual transmission mode used.

**PSD Type** Sets the use of symmetric Power Spectral Density (PSD) mask.

Values: Symmetric

Default: Symmetric

**Line Probe** Enables or disables rate adaptation line probe.

Values: Enabled, Disabled

Default: Enabled

To set any configuration profile parameter, enter the desired value/information in a field or select the desired parameter from one of the pull-down lists, and then click on the “Submit” button.

## Alarm Profile Table Screen

Clicking on the “Alarm Profiles” button on the Network screen will display the screen shown in Figure 3.7.

**Figure 3.7** Alarm Profile Table Screen

Profile Name	Loop Attn Thresh	SNR Margin Thresh	ES Thresh	SES Thresh	CRC Thresh	LOSWS Thresh	UAS Thresh
<a href="#">DEFVAL</a>	0	0	1	1	1	1	1
<a href="#">User Alarm Profile 1</a>	0	0	1	1	1	1	1
<a href="#">User Alarm Profile 2</a>	0	0	1	1	1	1	1
<a href="#">User Alarm Profile 3</a>	0	0	1	1	1	1	1

The Alarm Profiles screen displays the current values of SHDSL alarm thresholds. Click on the specific hyperlink under “Profile Name” to configure the alarm threshold values to be used for the selected segment endpoint in the “Alarm Profile Details” screen shown in Figure 3.8.

**Figure 3.8** Alarm Profile Details Screen

The screenshot shows a web browser window titled "Alarm Profile Details". Below the title, it says "Profile Name : User\_Alarm\_Profile\_1". The main content is a table with two columns: "Type" and "Threshold". The table contains the following rows:

Type	Threshold
Loop Attenuation	<input type="text" value="0"/>
SNR Margin	<input type="text" value="0"/>
ES	<input type="text" value="1"/>
SES	<input type="text" value="1"/>
CRC	<input type="text" value="1"/>
LOSWS	<input type="text" value="1"/>
UAS	<input type="text" value="1"/>

Below the table is a "Submit" button. The browser's status bar at the bottom shows "Internet".

- Loop Attenuation** Sets the loop attenuation alarm threshold. If the current value reaches or exceeds this threshold, a crossing trap is generated. A value of 0 (zero) disables the trap.
- SNR Margin** Sets the Signal-to-Noise Ratio margin alarm threshold. When the current SNR value reaches or drops below this threshold, a crossing trap is generated. A value of 0 (zero) disables the trap.
- ES** Sets the threshold for the number of Errored Seconds within any given 15-minute performance data collection interval. If the value of ES in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- SES** Sets the threshold for the number of Severely Errored Seconds within any given 15-minute performance data collection interval. If the value of SES in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- CRC** Sets the threshold for the number of Cyclic Redundancy Check anomalies within any given 15-minute performance data collection interval. If the value of CRC anomalies in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- LOSWS** Sets the threshold for the number of Loss of Sync Word Seconds within any given 15-minute performance data collection interval. If the value of LOSW in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- UAS** Sets the threshold for the number of Unavailable Seconds within any given 15-minute performance data collection interval. If the value of UAS in a

particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.



**NOTICE:** Any changes to the above-listed parameters must be followed by a “Submit” for the changes to take effect.

## Span Endpoints Screen

Clicking on the “Span Endpoints” button on the Network screen will display the screen shown in Figure 3.9.

**Figure 3.9** *Span Endpoint Table Screen*

Type	Endpoint Side	Endpoint Wire Pair
TU-R	Network	Wire Pair 1

This screen displays each endpoint of the span. If the SHDSL link is not up, only the local side of the span is displayed. The EOC channel is used to access the remote end unit

Clicking on the highlighted (linking) Type identifier in the table on the Span Endpoints screen will display the Span Endpoints Details screen (Figure 3.10). This table supports retrieval of unit inventory information available via the EOC from units on an SHDSL line, and provides details regarding the parameters listed below.

**Figure 3.10** *Span Endpoint Details Screen*

Span Endpoint Details	
Unit TU-C	
Vendor ID	B5 00 56 52 4C 4B 00 00
Model Number	6450
Serial Number	53
EOC Software Version	1
Standard Version	1
List Number	000
Issue Number	00
Software Version	01.49h
Equipment Code	unassigned
Transmission Mode Capability	Annex-B
Endpoint Side	Customer
Wire Pair	Wire Pair 1

**Vendor ID** Displays the Vendor ID as reported in an Inventory Response message.

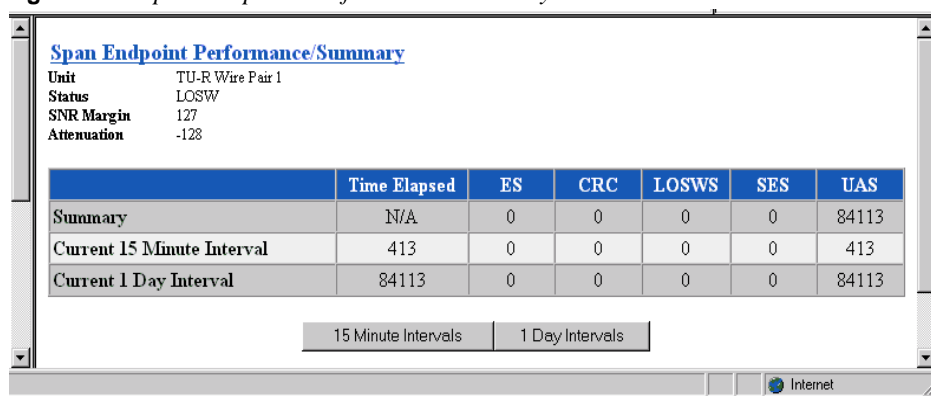
**Model Number** Vendor model number as reported in an Inventory Response message.

**Serial Number** Vendor serial number as reported in an Inventory Response message.

- EOC Software Version** Vendor EOC version as reported in a Discovery Response message.
- Standard Version** Version of the SHDSL standard implemented as reported in an Inventory Response message.
- List Number** Vendor list number as reported in an Inventory Response message.
- Issue Number** Displays the Vendor issue number as reported in an Inventory Response message.
- Software Version** Displays the Vendor software version as reported in an Inventory Response message.
- Equipment Code** Equipment code conforming to ANSI T1.213, Coded Identification of Equipment Entities.
- Transmission Mode Capability** Transmission mode capability of the SHDSL unit.
- Endpoint Side** Defines which direction the SHDSL port is pointing. Normal operation will use the TU-R configuration, and the endpoint will be “Network.” When unit type is TU-C, endpoint will be “Customer.”
- Wire Pair** Always “Wire Pair 1.”

Clicking on the “Span Endpoint Performance/Summary” button on the Span Endpoint Details screen will display the screen shown in Figure 3.11.

**Figure 3.11** *Span Endpoint Performance/Summary Screen*



This screen displays information on the performance and error status of a span endpoint. This information is provided in summary form for complete totals as well as for current 15-minute and 1-day intervals.

**Status** Current state of the endpoint. This is a string indicating possible conditions. The various string components are as follows:

OK – There no defects on the line.

SNR – Indicates that the SNR margin has dropped below the alarm threshold.



Attenuation – Indicates that the loop attenuation has exceeded the alarm threshold.

LOSW – Indicates an LOSW alarm.

Loopback – A loopback is currently active at this Segment Endpoint.

<b>SNR Margin</b>	Current Signal-to-Noise Ratio margin for this endpoint as reported in a Status Response/SNR message.
<b>Loop Attenuation</b>	Current loop attenuation for this endpoint as reported in a Network or Customer Side Performance Status message.
<b>Time Elapsed</b>	Total elapsed seconds in the current 15-minute interval.
<b>ES</b>	Count of Errored Seconds on this endpoint since the unit was last restarted.
<b>CRC</b>	Count of Cyclic Redundancy Check anomalies on this endpoint since the unit was last restarted.
<b>LOSWS</b>	Count of Loss of Sync Word Seconds on this endpoint since the unit was last restarted.
<b>SES</b>	Count of Severely Errored Seconds on this endpoint since the unit was last restarted.
<b>UAS</b>	Count of Unavailable Seconds on this endpoint since the unit was last restarted.

### ***15-Minute and 1-Day Intervals***

Also included on this screen are buttons used to display the span endpoint performance summaries for 15-minute intervals and for 1-day intervals. These screens display only a summary of the errors (ES, SES, CRC, LOSWS, UAS) that have occurred on the span during the interval selected.

The 15-Minute Intervals table provides one row for each endpoint performance data collection 15-minute interval. The 1-Day Intervals screen provides one row for each endpoint performance data collection 24-hour interval.

### ***Span Endpoint Maintenance Screen***

Clicking on the “Span Endpoint Maintenance” button from the Span Endpoint Details screen will display the screen shown in Figure 3.12. This table supports maintenance operations (e.g., loopbacks) to be performed on segment endpoints.

**Figure 3.12** *Span Endpoint Maintenance Screen*

Span Endpoint Maintenance	
Unit TU-C	
Loopback Timeout (minutes)	3
Loopback	No Loopback
Restart Endpoint	Ready
Tip Ring Reversal	Reversed
Power Source	Local

The Span Endpoint Maintenance parameters are described below.

- Loopback Timeout (minutes)** Specifies the timeout value in minutes for loopbacks initiated at this endpoint. A value of 0 disables the timeout.
- Loopback** Specifies loopbacks for the associated segment endpoint.  
Values: No Loopback, Normal Loopback  
Default: No Loopback
- Restart Endpoint** Enables the manager to trigger a soft restart of the SHDSL line at the associated segment endpoint. Set this object to “restart” to initiate a restart. A restart will occur after approximately 5 seconds.  
Values: Ready, Restart  
Default: Ready
- Tip Ring Reversal** Indicates the state of the tip/ring pair at the associated segment endpoint.
- Power Source** Indicates the DC power source being used by the associated unit.

## CBR



---

**CAUTION:** *The T1/E1 CBR port is not a standalone port. Connect the T1/E1 CBR port only to the "private" side of the network on the customer premises, never to the "public" side.*

---

Click on the CBR link on the navigation pane on the left-hand side of the Unit screen to display the CBR screen (Figure 3.13). The CBR screen (Figure 3.13) lets you view and make changes to the CBR interface’s configuration as described below. In addition, this screen provides a table that displays error status and alarm thresholds for the CBR interface.

**Figure 3.13 CBR Screen**

The screenshot shows the CBR configuration interface. At the top, there are several configuration fields:

- T1/E1 Framing: E1 CCS
- T1 Mode: Short-Haul
- T1/E1 Coding: HDB3
- T1 Line Build Out: 0 dB
- T1 PRM: Disable
- T1 DSX Level: 0-110 feet
- T1 Zero Suppression: Disable
- E1 CRC4 Mode: Disable

Below these fields is a table with the following data:

	Status	Alarm	Count	Threshold
ES	---	OK	0	45
SES	---	OK	0	5
LOSS	---	OK	0	5
UAS	---	OK	0	0
CSS	---	OK	0	5
BPVS	---	OK	0	0
OOFS	---	OK	0	5
AISS	---	OK	0	0
RAS	---	OK	0	0
Reset Timer	---	---	---	30

At the bottom of the screen, there are buttons for "Submit", "Clear Alarms", and "Performance".

**T1/E1 Framing** Selects the framing for the network side of the DSU/CSU.

Values T1 ESF, T1 D4, E1 CCS, E1 CAS

E1 Unframed, T1 Unframed

Default: T1 ESF



**NOTICE:** To set unit to Signaling mode, you must first configure the following: on the CBR screen (page 3-14), configure Framing; on the Channel Table Details screen (page 3-59), set Rate to 56k/Signaling, and on the CES Service Details screen (page 3-53), configure AAL1 Format.

**T1/E1 Coding** Sets the CBR interface line coding.

Values: HDB3, AMI, B8ZS

Default: B8ZS



**NOTICE:** For a T1 CBR Maintenance Reset, the default is T1 ESF. The T1/E1 coding default is B8ZS.

**T1 PRM** Lets you establish which performance messaging standard will be employed to initiate Performance Report Message (PRM) functions. Setting this field to “Enable” instructs the unit to use ANSI T1.403, which sends a PRM once every second. Setting this field to “Disable” instructs the unit to use AT&T TR54016, which provides performance reporting on request only.

Values: Disable, Enable

Default: Disable

- T1 Zero Suppression** Determines whether ones density insertion is activated after 15 zeros. This parameter is ignored if the Coding parameter is set to “B8ZS.”  
 Values: Disable, Enable  
 Default: Disable
- T1 Mode** As a T1, the unit will operate in either long-haul or short-haul mode.  
 Values: Short-Haul, Long-Haul  
 Default: Short-Haul
- T1 Line Build Out** Sets the transmit Line Build Out (LBO) for the CBR interface.  
 Values: 0, -7.5, -15.0, -22.5 dB  
 Default: 0 dB
- T1 DSX Level** Specifies the T1 DSX output level.  
 Values: 0–110, 111–220, 221–330, 331–440, 441–550, 551–660, >661 ft  
 Default: 0–110 ft
- E1 CRC4 Mode** Provides line integrity detection to determine if bit errors are present on the line.  
 Values: Disable, Enable  
 Default: Disable

## Error Status and Alarm Thresholds Table

The unit can be programmed to generate an alarm condition based on a specific level of performance degradation. The CBR screen presents a table that provides current error status and alarm threshold information.

Acceptable alarm thresholds are set for periods of 15 minutes (900 seconds) and sampled every second. The error types listed in the following paragraphs can be preset to a value between 0 and 900 seconds. Setting a field to “0” (zero) disables the alarm on that statistic. To effectively disable alarm reporting, set all fields to “0” (zero).

The 15-minute time frame is not based on the TR 54016 or T1.403 interval boundaries, but is a time window based on the accumulated counts over the previous fifteen 1-minute intervals. In all cases, if the number of actual network errored seconds in the previous 15 minutes reaches the preset threshold for the specified error type, an alarm condition is declared.

The four columns of the status table are as follows:

- **Status:** Displays the current status of the CBR port.
- **Alarm:** Displays the alarm value of the network port. The unit declares an alarm as soon as the count exceeds the threshold set.
- **Count:** Displays the number of events or occurrences of this statistic that have been detected.
- **Threshold:** Displays a read/write field that can be set to a desirable threshold.

The table provides error status and alarm threshold information for the following error parameters:

- ES** Sets the Errored Seconds (ES) threshold. An ES is a 1-second period in which at least one logic error occurred. The default value is 45 seconds.
- SES** Sets the Severely Errored Seconds (SES) threshold. An SES is a 1-second period in which at least 320 CRC errors or one Out-of-Frame (OOF) error occurred. The default value is 5 seconds.
- LOSS** Sets the Loss of Signal Seconds (LOSS) threshold. A LOSS is 1-second period in which the T1/E1 received signal is interrupted. The default value is 5 seconds.
- UAS** Sets the Unavailable Seconds (UAS) threshold. A UAS is a 1-second period in which consecutive severely errored seconds cause an unavailable state. The default is 0 seconds (Disabled).
- CSS** Sets the Controlled Slip Seconds (CSS) threshold. The default is 0 seconds (Disabled).
- BPVS** Sets the Bipolar Violation Errored Seconds (BPVS) threshold. A BPVS is a 1-second period in which at least one bipolar violation occurred. The default is 0 seconds (Disabled).
- OOFS** Sets the Out of Frame Seconds (OOFS) threshold. An OOFS is a 1-second period in which a frame sync loss occurred. The default value is 5 seconds.
- AISS** Sets the Alarm Indication Signal Seconds (AISS) threshold. An AIS is a 1-second period when unframed all ones are received. The default is 0 seconds (Disabled).
- RAS** Sets the Remote Alarm Seconds (RAS) threshold. An RAS is generated by the terminal equipment when an improper signal is received from the facility (or upon receipt of unframed all ones). The default is 0 seconds (Disabled).
- Reset Timer** Sets the Reset Timer threshold. This field is the contiguous number of seconds that an alarm parameter must be clear before the alarm is reset. Applicable values range from 000 through 900. A value of "000" means the alarm will never be reset.

The CBR screens provide the user-activated buttons described below.

Button	Function
Submit	Sets any values that have been changed.
Clear Alarms	Resets the alarm conditions and counts to zero.
Performance	Displays a Performance/Summary screen that shows a current count of the number of error events that have occurred over the past 24 hours and the past 30 days.



**CAUTION:** *Performance data will be lost upon power cycle or after performing a Maintenance Reset/Restart.*

Figure 3.14 Performance/Summary Screen

**Performance/Summary**  
Interface: CBR

	Current 15 Minutes	24 Hour Summary	30 Day Summary
ES	0	0	0
BES	0	0	0
SES	0	0	0
UAS	387	84558	0
CSS	0	0	0
CRCES	0	0	0
OOFs	387	84558	0
LOSS	387	84558	0
AISS	0	0	0
RAS	0	0	0
BPVS	0	0	0
LOFC	0	0	0

Performance 24 Hour    Performance 30 Day

Clear Statistics

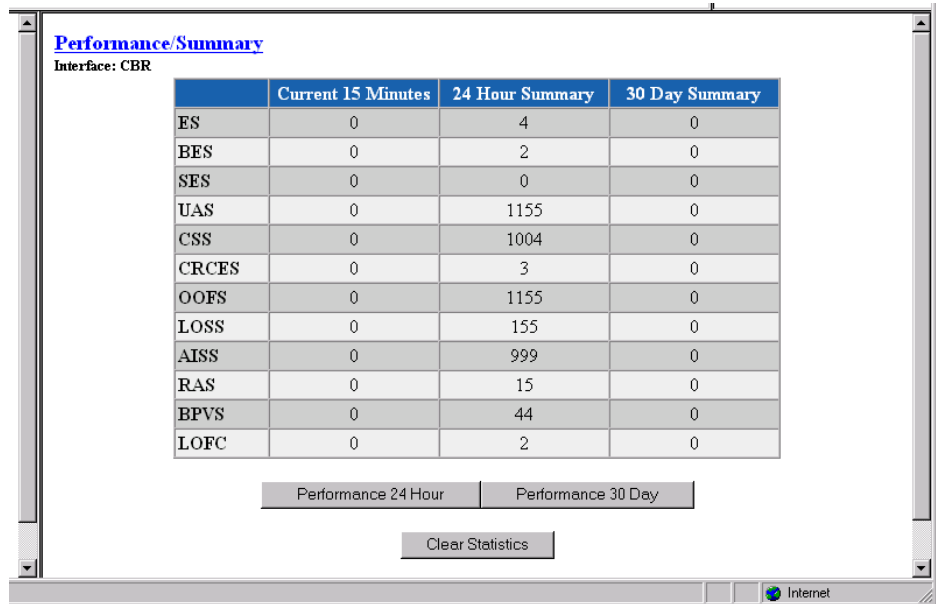
Internet

In addition to the error parameters found in the *Error Status and Alarm Thresholds Table* as described on page 3-16, the following error parameters are included on the Performance/Summary table:

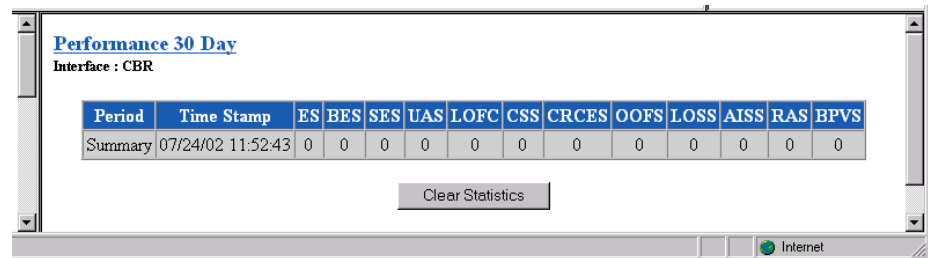
- BES** Sets the Bursty Error Seconds (BES) threshold. A BES is a 1-second period during which at least more than one but fewer than 320 CRC6 errors occurred.
- LOFC** The Loss of Frame Count (LOFC) represents the number of time a loss of frame is declared. A loss of frame is declared after 2.5 seconds of continuous loss of signal or OOF.
- CRCES** Sets the Cyclic Redundancy Check Errored Seconds (CRCES) threshold. A CRC is a method of confirming the integrity of received data.

Beneath the Performance/Summary table are two buttons: “Performance 24 Hour” and “Performance 30 Day.” Clicking either of these buttons will display a detailed summary of the error events that have occurred during each 15-minute interval of the past 24 hours (Figure 3.15) or during each interval (day) of the past 30 days (Figure 3.16).

**Figure 3.15** Performance 24 Hour Screen



**Figure 3.16** Performance 30 Day Screen



## Serial

The Serial screen (Figure 3.17) lets you view and make changes to the unit's Serial interface configuration as described in the paragraphs below. To make changes to any Serial port parameter, simply set the parameter to the desired selection and press the "Submit" button.

Figure 3.17 Serial Screen

The screenshot shows a 'Serial' configuration window with the following settings:

Type	V.35	Flow Control	None
Mode	DCE	Character Size	Eight
Packet Rate	2048 Kbps	Parity	None
Bundling	Contiguous	Stop Bit	1
Start Channel	1	RTS	Normal
Number of Channels	0	RTS/CTS Delay	Normal
		CTS	Forced True
Format	Sync	DCD	Forced True
Tx Clock	Internal	DSR	Forced True
Tx Invert Clock	Disable		
Current Pin Status	DTR:OFF DSR:ON RTS:OFF CTS:ON DCD:ON Mode:DCE		

Below the table are two buttons: 'DTR Alarm Control' (set to 'Disable') and 'DTR Alarm Status' (set to 'OK'). A 'Submit' button is at the bottom.

**Type** Selects the type of interface (based on its electrical signal characteristics) used by the equipment connected to the Serial port.  
Values: V.35, V.36, RS-232, EIA-530, and X-21  
Default: V.35



**NOTICE:** V.35 requires the use of an optional cable. Refer to "Connector Pin Assignments" on page A-6 for ordering information.

**Mode** By default, the Serial port serves as a DCE port. However, the Serial port can serve as a DTE port.  
If the Serial port connects to a DTE device (such as a FRAD or a router), the Mode parameter must be set to "DCE." If this port connects to a DCE device (such as a DSU/CSU), this parameter must be set to "DTE."  
Values: DCE, DTE  
Default: DCE



**NOTICE:** DTE mode requires the use of an optional DTE cable. Refer to "Connector Pin Assignments" on page A-6 for ordering information.



**NOTICE:** When you configure the Serial port for CES, you must set the port mode to DCE.

**Packet Rate** Packet Rate must be configured to the desired port speed (in bits per second). This parameter is only applicable when the Serial port service type is *not* CES.  
Values: 64–2304 kbps  
Default: 2048 kbps



**Bundling** Selects whether the DTE channel assignment is made as a “Contiguous” group or as “Alternate” channels. Selecting “Alternate” ensures ones density. Because the unit allows individual channels to be configured for a service, a value of “Arbitrary” will be returned for this parameter if the current channel allocation is not contiguous or Alternate. The “Arbitrary” value can only be supplied by the unit – it cannot be set by the user.

Values: Contiguous, Alternate, Arbitrary

Default: Contiguous



---

**NOTICE:** *Because “Alternate” Bundling assigns every other channel, only half the channels are available.*

---

**Start Channel** Selects the starting channel in the CES Channel Table. (Refer to *Channel Table Details Screen* as described on page 3-59.) Starting with the specified channel, the unit automatically assigns the channels that follow.

Values: 1–24 for T1; 0–31 for E1

Default: 1

**Number of Channels** Specifies the number of channels to be assigned to CES.

Values: 0–24 for T1; 0–32 for E1

Default: 0



---

**NOTICE:** *Bundling, Start Channel, and Number of Channels apply only when the Serial port service type is CES.*

---

**Format** Selects the port’s operating mode.

Values: Sync, Async

Default: Sync

**Tx Clock** Selects the clock the unit uses to sample the data transmitted from the DTE. When set to “Internal,” the data is sampled directly with the transmit data clock that is also supplied to the DTE as Transmit Clock. The “External” option uses the external clock from the DTE.

Values: Internal, External

Default: Internal



---

**NOTICE:** *The “External” option is valid only in Packet mode.*

---

**Tx Invert Clock** Changes the clock edge used to sample data received from the DTE.

Values: Disable, Enable

Default: Disable

**Flow Control** Selects the type of flow control to be used if the port is asynchronous.

Values: None, Xon/Xoff, RTS/CTS

Default: None

- Character Size** Selects the number of bits required to make up one asynchronous character.  
 Values: Five, Six, Seven, Eight  
 Default: Eight
- Parity** Sets the parity bit.  
 Values: None, Odd, Even  
 Default: None
- Stop Bit** Selects the number of bits required to end the asynchronous character.  
 Values: 1, 2  
 Default: 1
- RTS** Request To Send determines the source from which the unit reads the RTS signal status. If set to “Normal,” the unit gets RTS from the DTE on the Serial interface. If set to “Forced True,” RTS is always perceived as “On.”  
 Values: Normal, Forced True  
 Default: Normal
- RTS/CTS Delay** Request To Send/Clear To Send determines how long the unit waits before it changes the level of CTS to match RTS when the CTS parameter is set to “Internal.”  
 Values: Normal (~30 ms delay), Long (~100 ms delay)  
 Default: Normal
- CTS** The Clear To Send can be set to “Forced True,” “Forced False,” or “Internal.” If this parameter is set to “Internal,” the CTS control lead follows the Request to Send (RTS) control lead from the DTE after a delay of a duration established by the RTS/CTS Delay parameter (see *RTS/CTS Delay* as described on page 3-22).  
 Values: Forced True, Forced False, Internal  
 Default: Forced True
- DCD** Data Carrier Detect can be set to “Forced True,” “Forced False,” or “Internal.” If set to “Internal,” DCD is “On” when network carrier is being received from the remote end, and is “Off” when network carrier is not being received from the far end.  
 Values: Forced True, Forced False, Internal  
 Default: Forced True
- DSR** Data Set Ready can be set to “Forced True,” “Forced False,” or “Internal.” The “Internal” option sets DSR “On” if the port is enabled and “Off” if the port is disabled.  
 Values: Forced True, Forced False, Internal  
 Default: Forced True
- Current Pin Status** Displays the Current Pin Status of the DTE Serial port pins.

## DTR Alarm Control and Status Table

In addition to the configurable fields, the Serial screen displays a table that lets you set the Data Terminal Ready (DTR) Alarm Control parameters and view the current DTR Alarm Status.

Choices for DTR Alarm Control are “Enable” and “Disable”; the default setting is “Disable.” Setting DTR Alarm Control to “Enable” allows the unit to generate an alarm upon loss of DTR, which occurs when the Serial port detects that the DTR signal is low. The DTR Status field indicates the current state of the DTR alarm.

To make changes to a Serial port parameter, simply set the parameter to the desired selection and press the “Submit” button.

## 10/100 Ethernet (IP Service Details)

The 10/100 Ethernet (IP Service Details) screen (Figure 3.18) lets you configure the IP parameters described below.

**Figure 3.18** 10/100 Ethernet (IP Service Details) Screen

10/100 Ethernet (IP Service Details)	
Unit IP Address	192.94.46.72
Subnet Mask	255.255.255.0
Gateway IP Address	192.94.46.1
DHCP Client	Disable
Client Identifier	Verilink WANsuite: 00:C0:E6:A0:1E:E6
Ethernet	Auto-Neg

Physical Address  
00 C0 E6 A0 1E E6

Change IP Service Details

Ethernet Stats    Unit Access Table

**Unit IP Address** A unique Network address assigned to this unit.

**Subnet Mask** Defines the Network portion of the unit’s IP Address.

**Gateway IP Address** IP Address of the default gateway (router) on the LAN side of the unit.

**DHCP Client** If DHCP Client is enabled at power-up, the unit will request its IP, Mask, and Gateway addresses from a DHCP server located on the LAN side of the unit, and the unit will use these addresses. If the DHCP request is unsuccessful, the unit will use the configured addresses shown on this screen.

**Client Identifier** Displays a unique identifier for a specific IP address.

**Ethernet** Enables or disables a remote unit’s Ethernet port.

**Physical Address** Displays unique MAC address.



---

**NOTICE:** *The first three address parameters above can also be configured using the Installation Wizard as described on page 2-2.*

---

The “Change IP Service Details” button will take you to an IP Service Details screen (Figure 3.19) where you can view any changes you have made and verify your settings before submitting them by clicking the “Submit IP Service Changes” button. The “Discard Changes” button allows you to discard any changes you have made, and return to the previous screen to reset the parameters.

**Figure 3.19** *IP Service Details Screen*

The screenshot shows a window titled "IP Service Details" with a table of configuration parameters and two buttons below it.

Unit IP Address	192.94.46.72
Subnet Mask	255.255.255.0
Gateway IP Address	192.94.46.1
DHCP Client	Disable
Client Identifier	Verlink WANsuite: 00:C0:E6:A0:1E:E6
Ethernet	Auto-Neg

**Physical Address**  
00 C0 E6 A0 1E E6

Note: Please verify that all parameters are correct. Changes take place immediately. Incorrect settings may result in loss of communication with this unit.

Submit IP Service Changes

Discard Changes

To view details about the current condition of IP, ICMP (In and Out), TCP, and UDP parameters, click on the “Ethernet Stats” button at the bottom of the screen. The Ethernet Stats screen (Figure 3.20) contains no user-selectable fields or options; it is simply a representation of the applicable MIB II parameters.

**Figure 3.20 Ethernet Stats Screen**

**10/100 Ethernet Statistics**

IP	ICMP				TCP		UDP		
	IN	Out							
Forwarding	1	InMsgs	1	OutMsgs	16	RtoAlgorithm	4	InDatagrams	9761
DefaultTTL	64	InErrors	0	OutErrors	0	RtoMin	1000	NoPorts	15
InReceives	11920	InDestUnreachs	0	OutDestUnreachs	15	MaxConn	4294967295	InErrors	0
InHdrErrors	0	InTimeExcds	0	OutTimeExcds	0	ActiveOpens	0	OutDatagrams	0
InAddrErrors	0	InPamProbs	0	OutPamProbs	0	PassiveOpens	260		
ForwDatagrams	0	InSrcQuenchs	0	OutSrcQuenchs	0	AttemptFails	147		
InUnknownProtos	0	InRedirects	0	OutRedirects	0	EstabResets	107		
InDiscards	0	InEchos	1	OutEchos	0	CurrEstab	1		
InDelivers	11925	InEchoReps	0	OutEchoReps	1	InSegs	2149		
OutRequests	2045	InTimestamps	0	OutTimestamps	0	OutSegs	2030		
OutDiscards	0	InTimestampReps	0	OutTimestampReps	0	RetransSegs	1		
OutNoRoutes	0	InAddrMasks	0	OutAddrMasks	0	InErrs	0		
ReasmTimeout	30	InAddrMaskReps	0	OutAddrMaskReps	0	OutRsts	0		
ReasmOKs	0								
ReasmFails	0								
FragCreates	0								
RoutingDiscards	0								

Internet

Click on the Unit Access Table button on the Ethernet (IP Details) screen to view the Unit Access Table (Figure 3.21), which specifies up to 10 different IP networks that may access the unit's parameters. If no IP networks are supplied, any host may access the unit. Select any Index number on the table to view the Unit Access Details (Figure 3.22) that correspond with that Index number.

**Figure 3.21 Unit Access Table**

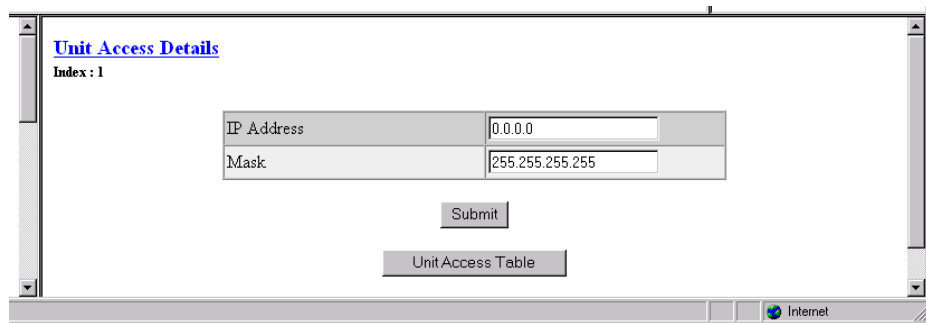
**Unit Access Table**

Index	IP Address	Address Mask
<a href="#">1</a>	0.0.0.0	255.255.255.255
<a href="#">2</a>	0.0.0.0	255.255.255.255
<a href="#">3</a>	0.0.0.0	255.255.255.255
<a href="#">4</a>	0.0.0.0	255.255.255.255
<a href="#">5</a>	0.0.0.0	255.255.255.255
<a href="#">6</a>	0.0.0.0	255.255.255.255
<a href="#">7</a>	0.0.0.0	255.255.255.255
<a href="#">8</a>	0.0.0.0	255.255.255.255
<a href="#">9</a>	0.0.0.0	255.255.255.255
<a href="#">10</a>	0.0.0.0	255.255.255.255

IP Service Details

Internet

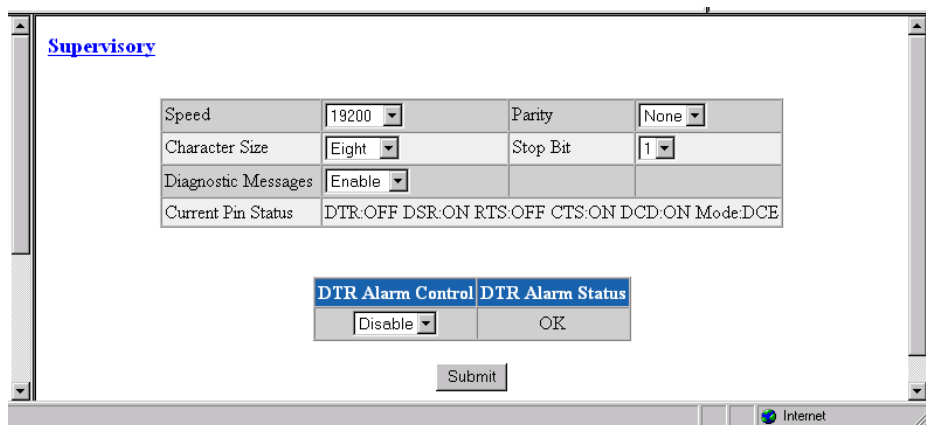
**Figure 3.22** *Unit Access Details*



## Supervisory

The Supervisory screen (Figure 3.23) displays the current speed of the Supervisory port interface along with other parameters as described below. The Supervisory port supports only asynchronous character formats.

**Figure 3.23** *Supervisory Screen*



**Speed** Changes the Supervisory port speed (in bits per second).

Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200  
Default: 19200

**Character Size** Selects the number of bits required to make up one asynchronous character.

Values: Five, Six, Seven, Eight  
Default: Eight

**Diagnostic Messages** Enables the Supervisory port to send out diagnostic messages upon power-up.

Values: Enable, Disable  
Default: Enable

**Parity** Sets the parity bit.

Values: None, Odd, Even  
Default: None

**Stop Bit** Selects the number of bits required to end the character.

Values: 1, 2

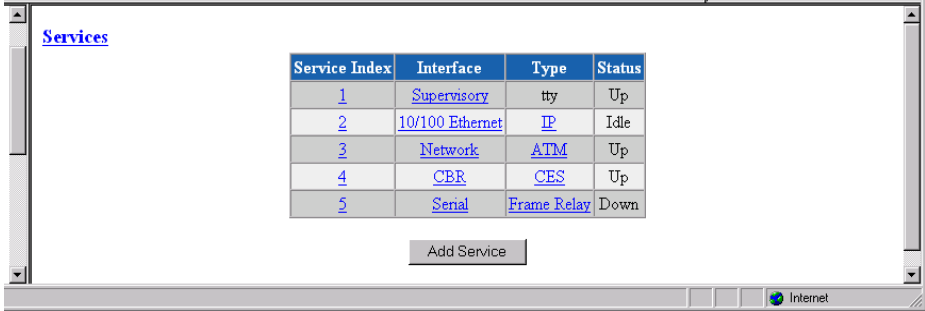
Default: 1

**Current Pin Status** The Current Pin Status, which shows the state of the RS-232 pins, is also displayed on the Supervisory interface screen.

## Services

The Services screen (Figure 3.24) provides a view of the unit's defined services and displays the Interface and Type parameters for each service.

**Figure 3.24** *Services Screen*



The screenshot shows a web browser window titled "Services". Inside the window, there is a table with four columns: "Service Index", "Interface", "Type", and "Status". The table contains five rows of data. Below the table is a button labeled "Add Service". The browser's status bar at the bottom shows "Internet".

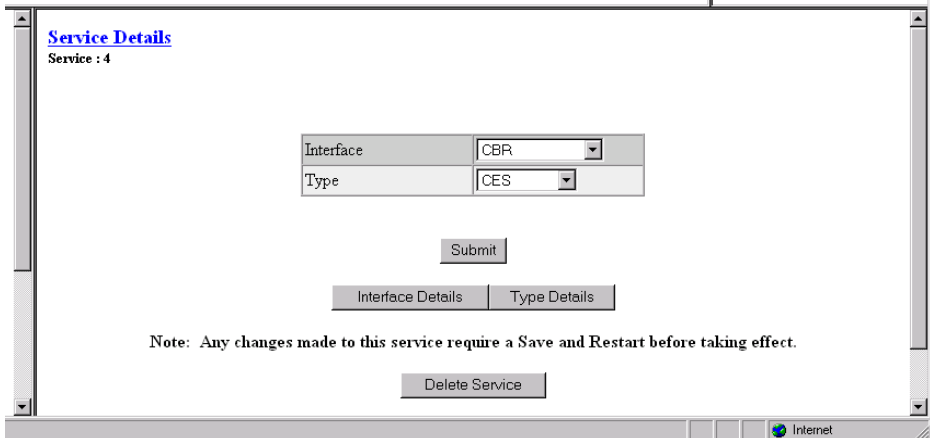
Service Index	Interface	Type	Status
<a href="#">1</a>	<a href="#">Supervisory</a>	tty	Up
<a href="#">2</a>	<a href="#">10/100 Ethernet</a>	<a href="#">IP</a>	Idle
<a href="#">3</a>	<a href="#">Network</a>	<a href="#">ATM</a>	Up
<a href="#">4</a>	<a href="#">CBR</a>	<a href="#">CES</a>	Up
<a href="#">5</a>	<a href="#">Serial</a>	<a href="#">Frame Relay</a>	Down

The table in the center of the screen displays the available services listed by index number.

## Service Details Screen

Clicking on an index number under the Service Index column will display a Service Details screen such as the one shown below (Figure 3.25). (In this example, the selected service type is CES.)

**Figure 3.25** *Service Details Screen*



The screenshot shows a web browser window titled "Service Details". Below the title, it says "Service : 4". There are two dropdown menus: "Interface" with "CBR" selected and "Type" with "CES" selected. Below these are buttons for "Submit", "Interface Details", and "Type Details". A note at the bottom states: "Note: Any changes made to this service require a Save and Restart before taking effect." At the very bottom is a "Delete Service" button. The browser's status bar at the bottom shows "Internet".

From this screen, you can access and change the parameters listed below. The new parameters are saved when you click on "Submit" and return to the previous screen.

**Interface** Selecting one of the interfaces will bring up a screen where you can view interface parameters. These screens are the same ones displayed when you select a sub-menu from the Interfaces screen described earlier on page 3-6.

**Type** Selecting one of the services listed under the “Type” column will bring up a screen where you can view (and, in some cases, change) parameters for each type of service. The details displayed depend on the type of service currently in effect. These screens are shown and described below according to each type of service.

In addition, the Service Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Interface Details	Opens the Details screen for the Interface of the currently selected service.
Type Details	Opens the Details screen for the Type of the currently selected service.

### Interface Details Button

Clicking the “Interface Details” button on the Service Details screen lets you view interface parameters for the selected service. You will also see the interface parameters for the selected service if you click on the interface under the Interface column on the Services screen.

### Type Details Button

Clicking the “Type Details” button on the Service Details screen will let you view (and, in some cases, change) interface parameters for the specified service. The details displayed depend on the type of service currently in effect for the selected service. You will see this same screen if you click on the service under the Type column on the Services screen. Type Details screens

## IP Service Details Screen

Access the IP Service Details screen by clicking the IP link under the Type column on the Services screen. Both the IP Service Details and the Ethernet Stats screens are described on page 3-23.

## Frame Relay Service Details Screen

Click on “Frame Relay” under the “Type” column on the Services screen to access the Frame Relay Service Details screen (Figure 3.26). This screen lets you access the configuration parameters described in the paragraphs below.



**Figure 3.26** *Frame Relay Service Details Screen*

**Frame Relay Service Details**  
 Service : 3 Pair : 4  
 Interface : Network 1

Interface Type	UNI	Default CIR (bps)	0
Link Management	Auto	Default Be Rate (bps)	0
Max Frame Size	2500	Enforce CIR and Be	No
N1	5	Management DLCI	0
N2	3	Management Auto IP DLCI	No
N3	4	LMI Sourcing	Yes
T1	10	FrameStart Auto Discovery	No
RFC1315 Trap	Disable	Round Trip Delay Size (bytes)	16
Normal Tx Queue Size	28	Round Trip Delay Rate (secs)	15

Active	LMI Type	FrameStart Status	Rx Invalid Threshold	Rx Invalid Alarm	Tx Threshold	Tx Alarm	Rx Threshold	Rx Alarm
No	Unknown	0	0	OK	0	OK	0	OK

Submit

Frame Relay Statistics | DLCI Table | Clear Alarms

Pair Type Details

**Interface Type** If this service is connected to a Frame Relay network, the Interface Type should be set to “UNI” as it is the user side of a User-to-Network interface. If it is connected to a FRAD/Router, the Interface Type should be set to “NI” as it is the network side of a User-to-Network interface. If it is connected to an equipment set for Network-to-Network interface, the Interface Type should be set to “NNI.”

Values: UNI, NI, NNI

Default: UNI if interface is Network, NI if interface is Serial

**Link Management** Set this parameter to the link management used by the equipment connected to it. If set to “Auto,” the unit will learn the link management type and display it on the status portion of this screen.

Once it discovers the link management type, the unit should be set to the discovered value so that subsequent unit or network re-initialization will be faster.

Values: Auto, ANSI, CCITT, LMI, None

Default: ANSI

**Max Frame Size** If Auto Diagnostic is set to “Yes,” the unit will discard received frames that are larger than the maximum frame size. If Auto Diagnostic is set to “No,” these large received frames will be sent, but will be counted in the Rx Invalid statistics.

Values: 64–4096

Default: 2500

**N1** There are two types of status inquiries: keep alive and full status requests. Set this parameter to determine how many “keep alives” are sent between full

status requests. (For example, if set to 5, every fifth status inquiry will be a full status inquiry.)

Values: 1–255

Default: 5 if interface is Network (UNI), 6 if interface is Serial (NI).

**N2** The N2 counter specifies the total number of link reliability errors and protocol errors that can occur during the sliding event monitor count defined by N3. If this count is exceeded, the port is declared inactive.

Values: 1–255

Default: 3

**N3** This counter represents a Monitored Events Count. For a network, a monitored event is the receipt of a status inquiry message or the expiration of the polling verification timer T2. For a FRAD, a monitored event is the transmission of a status enquiry message. This parameter defines the size of the sliding window used by the unit to determine whether a channel or user device is active.

Values: 1–255

Default: 4

**T1** This parameter specifies the number of seconds the unit waits between issuing status inquiry messages.

Values: 5–30

Default: 10

**RFC1315 Trap** When this parameter is set to “Enable,” the unit will send the standard RFC1315 frame relay DTE circuit state change trap every time a DLCI changes state, provided at least one destination IP address for trap is configured in the SNMP configuration.

Values: Disable, Enable

Default: Disable

**Normal Tx Queue Size** Each Frame Relay service has two distinct transmit queues: one for normal-priority traffic and one for high-priority traffic. This parameter defines how many normal priority frames can be put in front of a high-priority frame. The software always checks for high-priority frames before placing normal-priority frames in the transmit queue. However, once the frames are in the hardware transmit queue, their order of transmission cannot be changed.

**Default CIR (bps)** This is the Committed Information Rate (in bits per second) provided by your frame relay service provider. The unit will apply this value to each DLCI learned from the network side to gather statistics and to perform CIR enforcement, if required. If a DLCI is configured with a CIR different from the default, the DLCI configuration will be used instead.

Values: 0–1536000

Default: 0

**Default Be Rate (bps)** This is the Excess Burst Rate (in bits per second) provided by your frame relay service provider. The unit will apply this value to each DLCI learned

from the network side to gather statistics and to perform CIR enforcement, if required. If a DLCI is configured with a different Excess Burst from the default, the DLCI configuration will be used instead.

Values: 0–1536000  
Default: 0

**Enforce CIR and Be** If this parameter is set to “Yes,” the unit will enforce Committed Information Rate and Excess Burst.  
Values: No, Yes  
Default: No



---

**NOTICE:** *The Auto Diagnostic parameter must be set to “Yes” to enforce CIR and Be.*

---

**Management DLCI** If there is a DLCI entered (and submitted) in this field, it will be the only DLCI that looks for in-band management packets. If a value of “0” (zero) is entered in this field, all DLCIs will look for management packets.

**Management Auto IP DLCI** If this parameter is set to “Yes,” the unit will monitor the specified management DLCI for 5 pings over 5 seconds, after which the unit uses the destination address as its management IP address.

**LMI Sourcing** If this parameter is set to “Yes,” the unit will source LMI messages for that service. Set this parameter to “Yes” if the service is not paired.  
When set to “No,” the unit will not be the source of LMI messages for that service. LMI messages will be exchanged transparently between the paired services.

Values: No, Yes  
Default: No



---

**NOTICE:** *If either side of the Frame Relay connection goes down, you will be unable to remotely access any connected units.*

---

**FrameStart Auto Discovery** When this parameter is set to “Yes,” the unit will send FrameStart discovery and delay frames to each DLCI it learns as soon as the DLCIs are set active. This is required to calculate round trip delay as well as to discover remote WANSuite units. This parameter should be set to “Yes” only on services that have a WANSuite at the far end of the frame relay connection. Also if set to “Yes,” the unit will gather SLA parameters such as frame and data delivery ratio as defined in the Frame Relay Forum Implementation, FRF.13. Those gathered statistics are then displayed on the DLCI Statistics screen as shown on page 3-39.

Values: No, Yes  
Default: No

**Round Trip Delay Size (bytes)** Specifies the frame size (in bytes) of packets making the round-trip.

**Round Trip Delay Rate (secs)** Specifies the rate (in seconds) at which Round Trip Delay packets are sent.

## Status and Alarms Table

The table displayed at the bottom of the Frame Relay Service Details screen reports on the status and condition of LMI parameters and on Receive/Transmit alarms and thresholds. Alarm threshold levels may be changed by entering a new threshold value in the appropriate field of the table and clicking the “Submit” button. Table fields are described below.

**Active** Read-only field shows whether or not (Yes or No) an alarm is active.

**LMI Type** Read-only status indicates ANSI, CCITT, LMI rev. 1, or Unknown.

**FrameStart Status** Read-only status indicates Sourcing, Monitoring, or 0.

**Rx Invalid Threshold** Number of invalid frames received during a 15-minute interval after which an invalid alarm will be triggered. Default of “0” disables this alarm.

**Rx Invalid Alarm** Status of this alarm indicates OK or Alarmed.

**Tx Threshold** Number of bits per second sent during a 15-minute interval after which a Tx alarm will be triggered. Default of 0 disables this alarm.

**Tx Alarm** Status of this alarm indicates OK or Alarmed.

**Rx Threshold** Number of bits per second sent during a 15-minute interval after which an Rx alarm will be triggered. Default of 0 disables this alarm.

**Rx Alarm** Status of this alarm indicates OK or Alarmed.

The Frame Relay Service Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Frame Relay Statistics	Opens the Frame Relay Port Statistics screen for the current Frame Relay service.
DLCI Table	Opens the DLCI Table screen, which displays all the DLCIs on the current service.
Clear Alarms	Clears all Frame Relay alarms.
Pair Type Details	Opens another Frame Relay Service Details screen that reverses the service and the pair so that you can view both sides of the pair.



**NOTICE:** When a “Submit” command is executed, the Frame Relay link will be re-initialized with the new parameters, causing a brief interruption in data transfer.

## Frame Relay Port Statistics Screen

Clicking the “Frame Relay Statistics” button brings up a table (Figure 3.27) that reports on the status and condition of LMI parameters and on Receive/Transmit alarms and thresholds. Alarm threshold levels may be changed by entering a new threshold value in the appropriate field on the Frame Relay Service Details screen and clicking the “Submit” button.

**Figure 3.27** Frame Relay Port Statistics Screen

The screenshot shows a web interface for Frame Relay Port Statistics. At the top, it displays 'Service : 3' and 'Pair : 0'. Below that, it shows 'Period : Summary' and 'Time Stamp : 23:35:48'. The main content is a table with three sections: Transmit, Receive, and Throughput (bits/sec). The Transmit section shows 7711 Frames, 107954 Octets, 0 Mgmt Frames, 0 Mgmt Octets, 7711 Stat Inquiries, and 0 Stat Responses. The Receive section shows 0 for all metrics. The Throughput section shows a Peak of 16 and an Average of 8 bits/sec. At the bottom, there is a 'Submit' button and a 'Period Index' dropdown menu set to 'Summary'. The interface also includes navigation buttons for 'All Frame Relay Intervals', 'Type Details', and 'Clear Stats'.

Transmit	
Frames	7711
Octets	107954
Mgmt Frames	0
Mgmt Octets	0
Stat Inquiries	7711
Stat Responses	0

Receive	
Frames	0
Octets	0
Mgmt Frames	0
Mgmt Octets	0
FECN	0
BECN	0
Invalids	0
Stat Inquiries	0
Stat Responses	0
Invalid LMIs	5784

Throughput (bits/sec)	
Peak	16
Average	8

Period Index:

All Frame Relay Intervals | Type Details | Clear Stats

### *Transmit*

**Frames** Number of frames transmitted by the port.

**Octets** Number of octets transmitted by the port.

**Mgmt Frames** Number of management frames transmitted by the port.

**Mgmt Octets** Number of management octets transmitted by the port.

**Stat Inquiries** Number of octets transmitted in frame relay LMI status inquiries.

**Stat Responses** Number of octets transmitted in frame relay LMI status responses.

### *Receive*

<b>Frames</b>	Number of frames received by the port.
<b>Octets</b>	Number of octets received by the port.
<b>Mgmt Frames</b>	Number of management frames received by the port.
<b>Mgmt Octets</b>	Number of management octets received by the port.
<b>FECN</b>	Number of Forward Explicit Congestion Notification frames received.
<b>BECN</b>	Number of Backward Explicit Congestion Notification frames received.
<b>Invalids</b>	Number of invalid frames received.
<b>Stat Inquiries</b>	Number of octets received in frame relay LMI status inquiries.
<b>Stat Responses</b>	Number of octets received in frame relay LMI status responses.
<b>Invalid LMIs</b>	Number of invalid Local Management Interface frames received.

### *Throughput (bits/sec)*

<b>Peak</b>	Peak bandwidth (in bps) as measured over a 10-second period.
<b>Average</b>	Average bandwidth (in bps) used by the port.
<b>Period Index</b>	Selects the interval (Current, Summary, or 1-96) to be viewed on the Frame Relay Port Statistics screen.

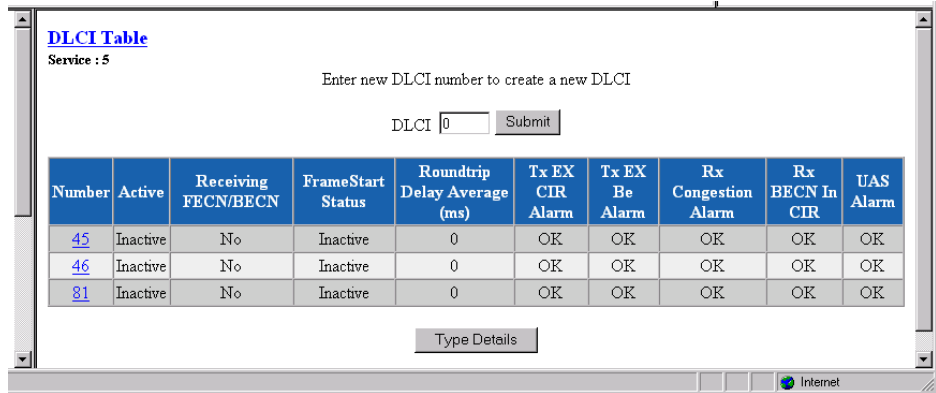
The Frame Relay Port Statistics screen provides the following user-activated buttons:

<b>Button</b>	<b>Function</b>
Submit	Sets any values that have been changed.
All Frame Relay Intervals	Opens the Frame Relay Statistics screen that shows all statistics for all parameters.
Type Details	Returns you to the Frame Relay Service Details screen.
Clear Stats	Clears all Frame Relay statistics.

### **DLCI Table Screen**

Clicking the “DLCI Table” button on the Frame Relay Service Details screen to display a table of all DLCIs (Figure 3.28) on a specific frame relay service along with their state and alarm conditions. You may create a new DLCI by entering the DLCI name in the DLCI field at the top of the screen and clicking the “Submit” button.

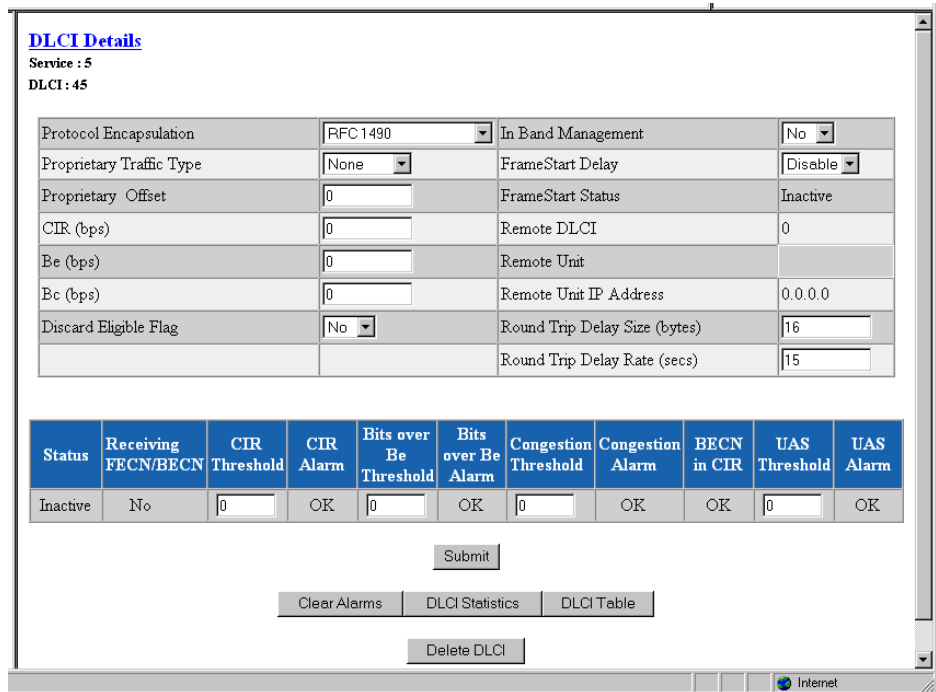
**Figure 3.28** *DLCI Table Screen*



### DLCI Details Screen

The DLCI Details screen (Figure 3.29) lets you access the configuration parameters described in the paragraphs below. To bring up this screen, click on a specific DLCI under the “DLCI” column on the DLCI Table screen.

**Figure 3.29** *DLCI Details Screen*



The unit uses the first three configuration parameters (Protocol Encapsulation, Proprietary Traffic Type, and Proprietary Offset) displayed on this screen to gather statistics. For in-band management, “RFC 1490” must be the encapsulation method.

**Protocol Encapsulation** Type of encapsulation used by the FRAD/Router connected to the unit.

Values: RFC 1490, Proprietary, RFC 1490-Encryption

Default: RFC 1490

<b>Proprietary Traffic Type</b>	When Protocol Encapsulation is set for “Proprietary,” the Proprietary Traffic Type parameter defines which protocol is encapsulated. Values: IP, IPX, Ethertype, None Default: None
<b>Proprietary Offset</b>	When Protocol Encapsulation is set for “Proprietary,” the Proprietary Offset parameter defines the number of octets after the frame relay header where the proprietary traffic type starts. Values: 0–64 Default: 0
<b>CIR (bps)</b>	If a Committed Information Rate is configured here, its value will be used instead of the default CIR of the Frame Relay service. Values: 0–2048000 Default: 0
<b>Be (bps)</b>	If an Excess Burst Rate is configured here, its value will be used instead of the default excess burst of the Frame Relay service. Values: 0–2048000 Default: 0
<b>Bc (bps)</b>	If CIR enforcement is configured to “Yes,” the unit will throttle the committed burst down to this value when frames are received with the BECN bit set. Values: 0–2048000 Default: 0
<b>Discard Eligible Flag</b>	If this parameter is set to “Yes” and CIR enforcement is also set to “Yes,” the unit will set the Discard Eligible (DE) bit for frames sent over CIR. Values: Yes, No Default: No
<b>In Band Management</b>	If the unit is to be used as a gateway to reach a remote WANSuite 6450 through this DLCI, this parameter should be set to “Yes,” and the remote IP address and Mask should be configured in the corresponding endpoint. Values: Yes, No Default: No
<b>FrameStart Delay</b>	If this parameter is set to “Enable,” the unit will send FrameStart discovery and delay frames on this DLCI, and will report the state of the remote Verilink unit with FrameStart technology. It will also send SOS frames when the FRAD/router connected to this unit goes inactive. Values: Enable, Disable Default: Enable if Auto Discovery is set to “Yes”; Disable otherwise
<b>FrameStart Status</b>	If the remote unit is a Verilink unit with FrameStart technology and FrameStart Auto Discovery is enabled, the FrameStart Status field will show the status of the remote unit. The status is “Active” if both the local and



remote DLCIs are active and the remote unit answers to the discovery frames sent by this unit. The status is “SOS” if the remote unit is active but the FRAD/Router connected to it is inactive. The status is “Inactive” in all other cases.

Values: Active, Inactive, SOS  
Default: Inactive

**Remote DLCI** If the remote unit is a Verilink unit with FrameStart technology, and FrameStart Auto Discovery is enabled, this displays the DLCI number used on the remote end of this DLCI.

Values: 16–1023  
Default: 0

**Remote Unit** If the remote unit is a Verilink unit with FrameStart technology, and FrameStart Auto Discovery is enabled, this parameter gives the first three digits of the unit ID configured on the remote end of this DLCI.

Values: 000–999  
Default: 000

**Remote Unit IP Address** Displays the IP address of the remote Verilink unit with FrameStart technology if FrameStart Auto Discovery is enabled.

**Round Trip Delay Size (bytes)** Specifies the frame size (in bytes) of packets making the round-trip. If the Round Trip Delay Size is not configured, the Frame Relay Details values will be used.

**Round Trip Delay Rate (secs)** Specifies the rate (in seconds) at which Round Trip Delay packets are sent. If the Round Trip Delay Rate is not configured, the Frame Relay Details values will be used.

### *DLCI Status Table*

The bottom portion of the screen displays a table detailing the actual status of DLCI and alarm threshold information as follows:

**Status** If this DLCI is up, the status will be “Active”; otherwise, the status will be “Inactive.”

Values: Active, Inactive  
Default: Inactive

**Receiving FECN/ BECN** When a frame is received with congestion bit set, this parameter is set to “Yes.” It is set back to “No” when a frame is received without congestion bit set.

Values: Yes, No  
Default: No

**CIR Threshold** Sets the Tx over CIR alarm threshold. This threshold is the number of bits per second in excess of CIR during a 15-minute interval. Setting this field to “0” (zero) disables the alarm.

- CIR Alarm** Reports if the Tx over CIR threshold has been exceeded.
- Bits Over Be Threshold** Sets the Tx over Be alarm threshold. This threshold is the number of bits per second in excess of CIR + Be during a 15-minute interval. Setting this field to “0” (zero) disables the alarm.
- Bits Over Be Alarm** Reports if the Tx over Be threshold has been exceeded.
- Congestion Threshold** Sets the Rx Congestion alarm threshold. This threshold is the number of frames received with BECN/FECN. Setting this field to “0” (zero) disables the alarm.
- Congestion Alarm** Reports if the Rx Congestion threshold has been exceeded.
- BECN in CIR** Reports if Backward Explicit Congestion Notification (BECN) has been received within CIR.
- UAS Threshold** Sets the Unavailable Seconds (UAS) alarm threshold. This threshold occurs after the DLCI is unavailable for a specified number of seconds. Setting this field to “0” (zero) disables the alarm.
- UAS Alarm** Reports if the UAS threshold has been exceeded.

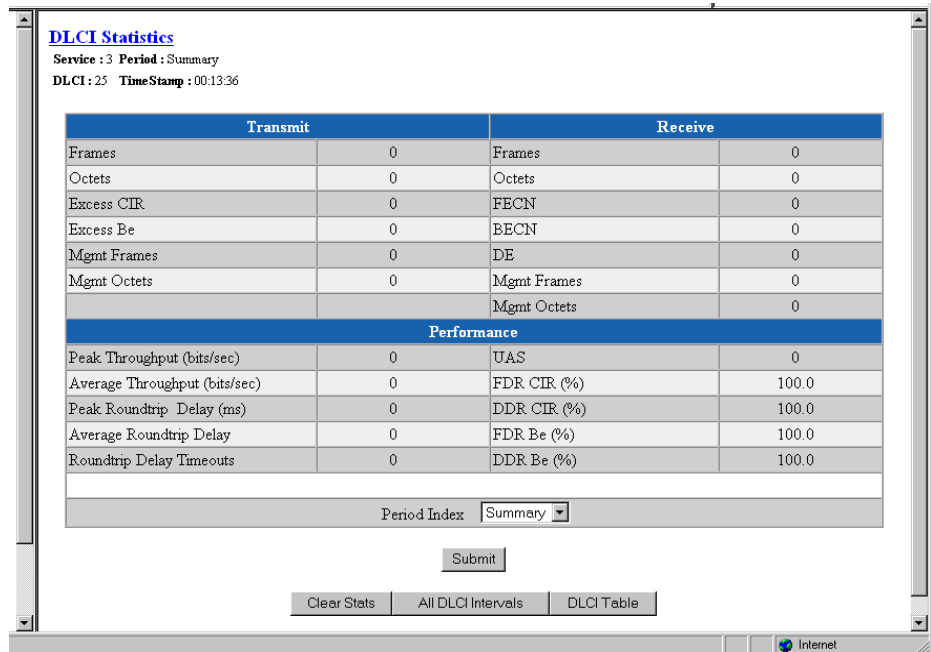
The DLCI Details screen provides the user-activated buttons defined below.

Button	Function
Submit	Sets and activates newly defined DLCI parameters.
Clear Alarms	Clears all DLCI alarms.
DLCI Statistics	Displays a table of the statistics for this DLCI.
DLCI Table	Displays a table of all DLCIs on a specific frame relay service, with their state and alarm conditions.
Delete DLCI	Lets you delete a specific DLCI.

### ***DLCI Statistics Screen***

Clicking the “DLCI Statistics” button on the DLCI Details screen will display a summary (Figure 3.30) of the Transmit, Receive, and Performance statistics for the selected DLCI for a specific period.

**Figure 3.30** *DLCI Statistics Screen*



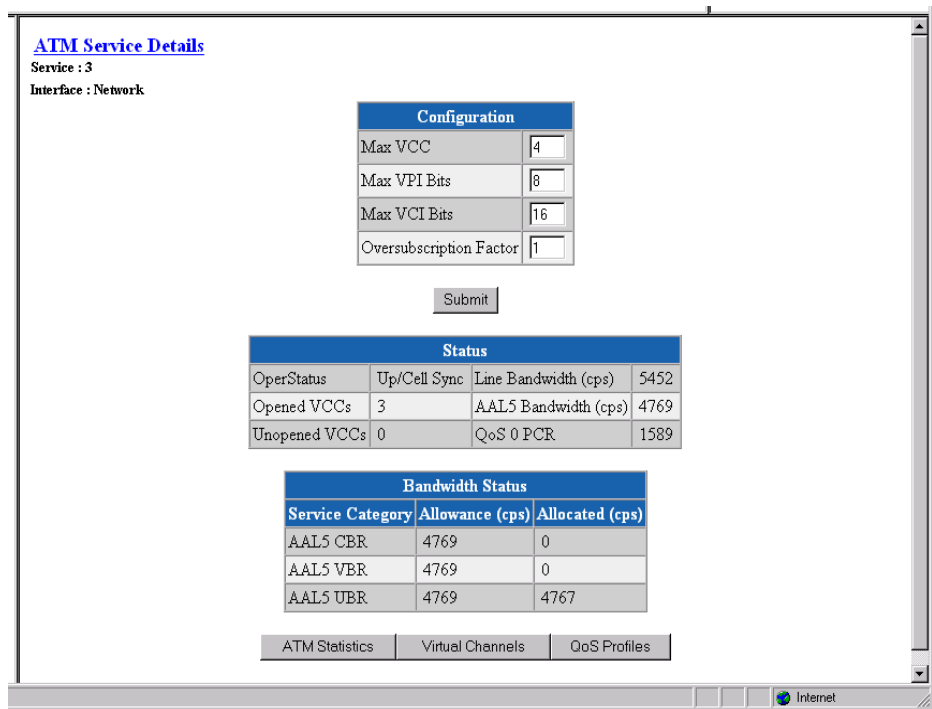
There are ninety-six 15-minute buckets (sampled every second) available for DLCI statistics. If the unit is powered on at 01:00 PM, the first interval will be completed at 01:15 PM; subsequent intervals would be completed at xx:30, xx:45, xx:00 and xx:15. Interval 1 is always the latest (most recent) interval, and interval 96 will always be the oldest.

The DLCI Statistics screen in the preceding figure shows a summary that includes all 96 buckets. You can choose to see the statistics for any given bucket by selecting the desired Period Index from the pull-down menu and clicking the “Submit” button. Alternatively, you can display all intervals at once by clicking the “All DLCI Intervals” button beneath the table. The MIB (ipadv2.mib) describes each available statistic. “FDR” on the screen above refers to Frame Delivery Ratio, which is the ration of successful frame receptions to attempted frame transmissions. “DDR” refers to Data Delivery Ratio or the ratio of successful payload bytes received to attempted payload bytes transmitted. “DE,” or Discard Eligible, refers to the data that is first eligible to be discarded when network congestion occurs.

## ATM Service Details Screen

Access the ATM Service Details screen (Figure 3.31) by clicking on ATM under the Type column on the Services screen. The ATM Service Details screen lets you access the configuration parameters described in the paragraphs below.

**Figure 3.31** ATM Service Details Screen



The Configuration table on the ATM Service Details screen is used to set the following configuration parameters:

- Max VCC (Virtual Channel Connection) – maximum number of Virtual Channel Connections on this ATM link. The default value is 4.
- Max VPI Bits – default Max Virtual Path Identifier Bits value is 8 for VPI values ranging from 0 to 255.
- Max VCI Bits – default Max Virtual Channel Identifier Bits value is 16 for VCI values ranging from 32 to 65535.
- Oversubscription Factor – current over-subscription factor for this ATM interface. Used for VBR and UBR VC connection admission control to allow either the VBR or UBR service category connections to collectively use more bandwidth than is available to make use of the statistical multiplexing of the connections. Values range from 1 to 10. A value of 1 indicates no oversubscription. A value of 5 indicates 5 times oversubscription of both VBR and UBR is permitted.



**NOTICE:** *CBR connections cannot be oversubscribed. Also, if CES is in use on the interface, PCR is limited for all AAL5 connections to the amount the line rate can support above the commitment for CES, and the oversubscription applies only to bandwidth above the CES commitment.*

To change an ATM Service configuration, enter the desired value for each parameter and click on the “Submit” button.

The Status table provides the following status information on the circuits:

- OperStatus (Operation Status) – current operational status for the ATM interface.

- Opened VCCs – current number of open virtual channel connections.
- Unopened VCCs – current number of unopen virtual channel connections.
- Line Bandwidth – current line bandwidth on the ATM Network interface expressed in cells per second.
- AAL5 Bandwidth – current ATM bandwidth available for AAL5 traffic. This value is the line bandwidth less the bandwidth needed for AAL1 CES.
- QoS 0 PCR – current peak cell rate for any virtual channels using default QoS profile.

The Bandwidth Status table provides bandwidth information for three service categories showing the allowed and allocated bandwidth for each.

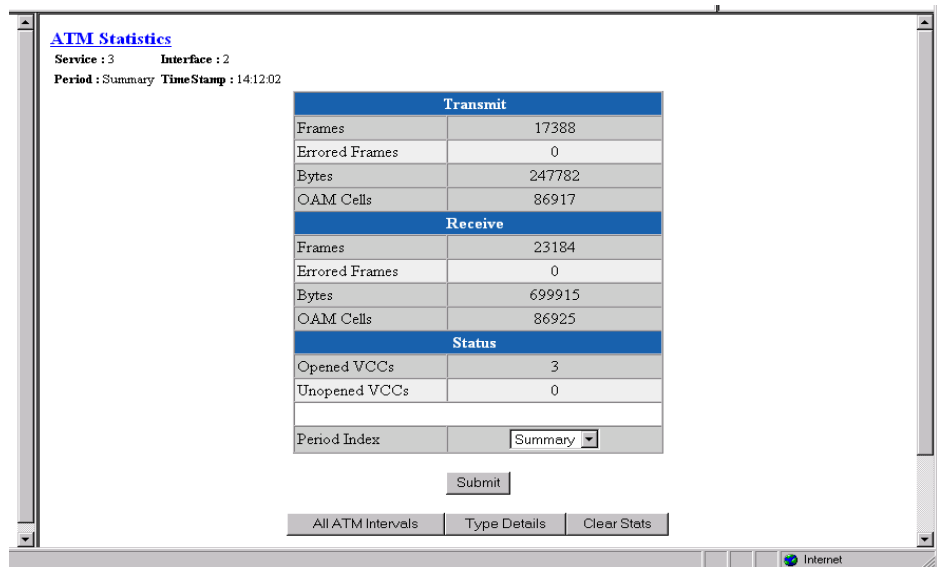
The ATM Service Details screen provides the user-activated buttons described below.

Button	Function
Submit	Sets any values that have been changed.
ATM Statistics	Displays the current ATM statistics.
Virtual Channels	Displays configured VCCs.
QoS Profiles	Displays configured QoS profiles.

## ATM Statistics Screen

Clicking on the “ATM Statistics” button on the ATM Service Details screen will display the screen shown in Figure 3.32.

**Figure 3.32** *ATM Statistics Screen*



There are ninety-six 15-minute “buckets” available for ATM statistics. If the unit is powered on at 01:00 PM, the first interval will be completed at 01:15 PM; subsequent intervals would be completed at xx:30, xx:45, xx:00 and

xx:15. Interval 1 is always the latest (most recent) interval, and interval 96 will always be the oldest.

The table on the ATM Statistics screen shows a summary that includes all 96 buckets. You can choose to see the statistics for any given bucket by selecting the desired Period Index from the pull-down menu and clicking the “Submit” button. Alternatively, you can display all intervals at once by clicking the “All ATM Intervals” button beneath the table. The MIB (ipad.mib) describes each available statistic.

The ATM Statistics table is divided into three sections: Transmit, Receive and Status. Each section provides real-time updates on the following statistics:

- Transmit section
  - Frames – current number of good frames transmitted
  - Errored Frames – current number of frames in error
  - Bytes – current number of bytes sent
  - OAM Cells – current number of OAM cells sent
- Receive
  - Frames – current number of good frames received
  - Errored Frames – current number of frames in error
  - Bytes – current number of bytes received
  - OAM Cells – current number of OAM cells received
- Status
  - Opened VCCs – number of opened VCCs
  - Unopened VCCs – number of unopened VCCs

Use the pull-down menu in the Period Index row of the table to select the interval for which you want to see ATM statistics. You may choose any of the 96 intervals, the current statistics, or a summary of the past 24-hour period. The default setting is a Summary of all intervals.

### ***ATM Statistics (All Intervals) Screen***

Clicking on the “All ATM Intervals” button on the ATM Statistics screen will display a table (Figure 3.33) that summarizes the transmit and receive statistics for the current time interval and all intervals recorded during the current 24-hour reporting period.

**Figure 3.33 ATM Statistics Table (All Intervals) Screen**

<b>ATM Statistics Table</b>									
Service : 3 Interface: Network									
Period Index	Time Stamp	Tx Frames OK	Tx Frames Error	Tx Bytes OK	Tx OAM	Rx Frames OK	Rx Frames Error	Rx Bytes OK	Rx OAM
Summary	10:02:51	0	0	0	71869	0	0	0	4
Current	10:02:51	0	0	0	171	0	0	0	0
Interval 1	10:00:00	0	0	0	900	0	0	0	0
Interval 2	09:45:00	0	0	0	900	0	0	0	0
Interval 3	09:30:00	0	0	0	900	0	0	0	0
Interval 4	09:15:01	0	0	0	901	0	0	0	0
Interval 5	09:00:00	0	0	0	900	0	0	0	0
Interval 6	08:45:00	0	0	0	900	0	0	0	0
Interval 7	08:30:00	0	0	0	900	0	0	0	0
Interval 8	08:15:00	0	0	0	900	0	0	0	0
Interval 9	08:00:00	0	0	0	900	0	0	0	0
Interval 10	07:45:00	0	0	0	900	0	0	0	0
Interval 11	07:30:00	0	0	0	901	0	0	0	0
Interval 12	07:14:59	0	0	0	900	0	0	0	0
Interval 13	06:59:59	0	0	0	900	0	0	0	0
Interval 14	06:44:59	0	0	0	900	0	0	0	0
Interval 15	06:29:59	0	0	0	900	0	0	0	0
Interval 16	06:14:59	0	0	0	900	0	0	0	0
Interval 17	05:59:59	0	0	0	900	0	0	0	1
Interval 18	05:44:59	0	0	0	901	0	0	0	0

## ATM Virtual Channels Screen

Clicking the “Virtual Channels” button on the ATM Service Details screen will display a table (Figure 3.34) of all Virtual Channels on a specific ATM service along with their state and alarm conditions.

**Figure 3.34 ATM Virtual Channels Screen**

<b>ATM Virtual Channel Table</b>								
VPI	VCI	Admin Status	Operation Status	Last Change	QoS Profile	Encapsulation Type	Traffic Type	Row Status
0	32	Up	Up	0 days, 00:00:23	0	LLC-MUX	ubr	Active
0	57	Up	Up	0 days, 00:00:23	0	FRF5	ubr	Active
0	87	Up	Up	0 days, 00:00:23	0	FRF8	ubr	Active

Enter new VPI/VCI to create a new Virtual Channel

VPI  VCI

The ATM Virtual Channels screen displays status information on the following parameters listed below. The QoS Profile and Admin Status are configured or changed on the Virtual Channel Details screen (Figure 3.35).

**VPI** Virtual Path Identifier number.

**VCI** Virtual Channel Identifier number.

**Admin Status** Current Admin Status.

Values: Up, Down, Testing

<b>Operation Status</b>	Current Operation Status. Values: Up, Down, Testing
<b>Last Change</b>	Time and date of the Last Change.
<b>QOS Profile</b>	Current QOS profile in use. The default profile is 0 (zero), which is used for UBR traffic.  When QOS profile “0” is used, the available bandwidth will be equally shared among all configured channels. QOS “0” cannot be modified.  If one virtual channel requires more bandwidth than others, configure another QOS profile and set its peak cell rate (PCR) to the required value. However, the sum of the PCRs of all configured channels must be no greater than the available AAL5 bandwidth. The available PCR on an SHDSL-ATM link with a line rate of 2304 kbps is about 5433 cells per second. When oversubscription is used, the sum of the PCRs for VBR or UBR channels may exceed the AAL5 bandwidth.
<b>Encapsulation Type</b>	Encapsulation Type used. Default is LLC-MUX, which uses RFC 1483 LLC encapsulation. If Serial PPP is selected, PPP traffic received from the Serial port will be sent over the ATM port using RFC 1483 PPPoA encapsulation. There can be only one VCI configured for Serial PPP.  Serial HDLC is similar to Serial PPP except, when you select Serial HDLC, data is encapsulated transparently. Any type of HDLC traffic will be supported. Because this is not a standard encapsulation, a WANSuite unit must reside at each end of the connection. Even if Serial HDLC or Serial PPP encapsulation is configured, routed IP traffic received on this channel will be forwarded to the IP Gateway, if IP Gateway is configured.  VC-MUX is used for a null encapsulation around user data, as in the case of a WAN PPP connection terminated in the WANSuite.  If FRF5 is used, the ATM channel implements FRF.5 Network Interworking, providing a Frame Relay link that can transport data for one or more DLCIs. If FRF8 is used, the ATM channel implements FRF.8.1 Service Interworking, providing a conversion from a Frame Relay PVC to this ATM PVC. Values: Serial PPP, VC-MUX, LLC-MUX, Serial HDLC, FRF5, FRF8
<b>Traffic Type</b>	Traffic type used. This is a read-only parameter determined by the QoS Profile in use for the channel. Values: CBR, UBR, VBR
<b>Row Status</b>	Current status of the VCC. Values: Active, Not In Service, Not Ready

### ***Adding a New Virtual Channel***

To create a new virtual channel, enter the desired VPI/VCI values in the appropriate fields near the bottom of the screen and click on the “Add Virtual Channel” button.



If the newly added virtual channel is within the maximum VCC parameter, it will be activated immediately.



**NOTICE:** When adding a Virtual Channel, the value for VPI may be 0 and above, but for VCI, must be 32 and above.

Click on a listed VPI to bring up the Virtual Channel Details screen (Figure 3.35) where you can view and/or change parameters.

**Figure 3.35** Virtual Channel Details Screen

**Virtual Channel Details**  
 Service : 3  
 VPI/VCI : 0/57  
 Interface : Network

Configuration			
QoS Profile	0		
Encapsulation Type	FRF5		
Traffic Type	ubr		
SLA Verification Timer (s)	0		

Status			
Admin Status	Up	Remote Active	Inactive
Oper Status	Up	Remote VPI	0
Last Change	0 days, 00:00:23	Remote VCI	0
Row Status	Active	Remote Unit ID	
		Remote IP Addr	0.0.0.0

Submit

Virtual Channel Statistics | Virtual Channel OAM | Type Details | QoS Profiles | FRF5 Service Details

Delete Virtual Channel

**SLA Timer (s)** In addition to the above-described parameters, there is an SLA Timer(s) parameter that may be set on the ATM Virtual Channel Details screen. When this timer expires (in seconds), the unit sends a proprietary frame over this virtual circuit. The timer validates Service Level Agreements by calculating the Frame Delivery Ratio, the Data Delivery Ratio, and the Round Trip Delay. When enabled, this timer also determines the IP address of the far-end unit, which must also be a WANsuite unit. A setting of “0” disables SLA measurements.

The following user-activated buttons are included on the Virtual Channel Details Screen:

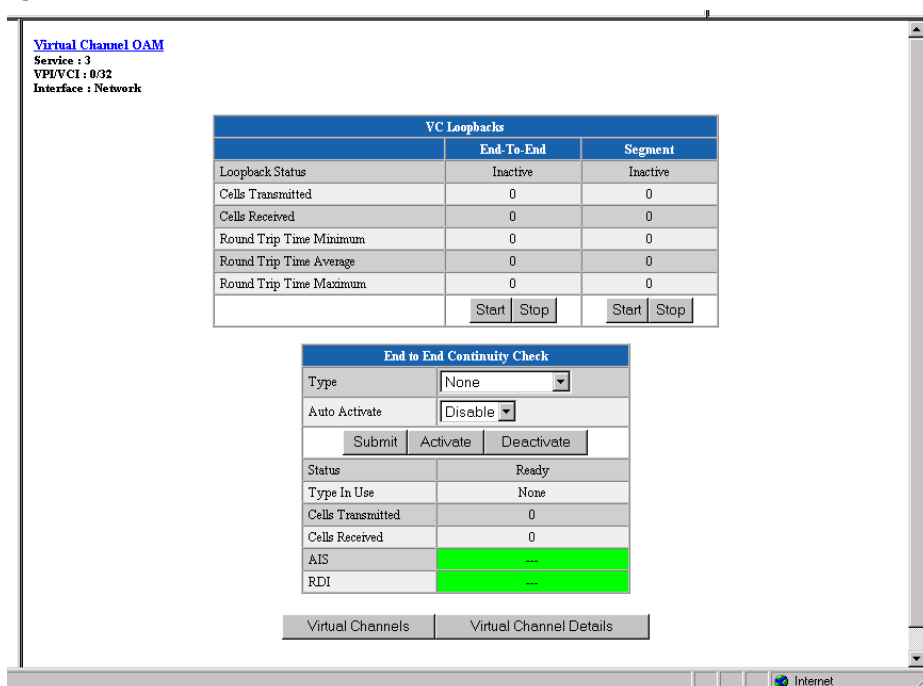
Button	Function
Submit	Sets any values that have been changed.
Virtual Channel Statistics	Displays the current Virtual Channel statistics.
Virtual Channel OAM	Displays Virtual Channel Operations and Maintenance Screen.
Type Details	Returns you to the ATM Service Details screen.

Button	Function
QoS Profiles	Displays configured QOS profiles.
FRF5 [FRF8] Service Details	Displays FRF5 or FRF8 details. <i>(This button is only displayed when FRF5 or FRF8 is the Encapsulation Type.)</i>
Delete Virtual Channel	Displays a confirmation screen.

### Virtual Channel OAM

Click the Virtual Channel OAM button on the Virtual Channel Details screen to view the menu shown in Figure 3.36. Using this menu, you can initiate either an End-to-End or a Segment OAM F5 ATM loopback to check the ATM layer setup of a virtual circuit (VC). An active ATM loopback sends one cell every 5 seconds. When the cells received equal the cells transmitted, the loopback is successful. Use the Start and Stop buttons in the End-to-End and Segment columns to start or to terminate an OAM F5 VCC loopback.

**Figure 3.36** Virtual Channel OAM



**Loopback Status** The state of the current VCC loopback function. When a loopback is activated from a user interface, the Loopback Status will be “Active,” and OAM F5 loopback cells will be sent from this endpoint once every 5 seconds. If a loopback is activated from the other endpoint or segment endpoint, the Loopback Status will be “Loopback.” The Loopback Status will be “Inactive” when no loopback is in place.

**Cells Transmitted** The number of OAM loopback cells transmitted for this VCC.

**Cells Received** The number of OAM loopback cells received for this VCC.

<b>Round Trip Time Minimum</b>	The minimum round-trip time in milliseconds between sending and receiving returned loopback cells.
<b>Round Trip Time Average</b>	The average round-trip time in milliseconds between sending and receiving returned loopback cells.
<b>Round Trip Time Maximum</b>	The maximum round-trip time in milliseconds between sending and receiving returned loopback cells.

The Round-trip Time values are set to zero any time the Loopback Status changes from Inactive to Active or Loopback. The Round-trip Time values are updated only when Loopback Status is Active and response loopback cells are received. When the loopback is initiated from the other ATM endpoint, the Round-trip Time values remain at zero.

### **Continuity Check**

The Virtual Channel OAM menu includes an End to End Continuity Check that, when activated, will continuously check for the purpose of detecting ATM layer defects in real time. Continuity Check may be activated in one or both directions. The ATM endpoint that activates the Continuity Check selects which direction applies. To activate an End-to-End Continuity Check, select the Type and click “Submit.” Then click “Activate.” If activated successfully, the Status will indicate “Active.” If unsuccessful, the Status will indicate “Activation Failed.” The Status is “Ready” when no continuity check (CC) is active. The three types of CCs include the following:

- Sink – a unidirectional CC where one endpoint is the Sink.
- Source – a unidirectional CC where one endpoint is the Source.
- Sink and Source – a bidirectional CC where each endpoint sends one CC cell every second (the Source) and each endpoint (the Sink) expects to receive one CC cell every second.

When the CC Sink does not receive user cells or a CC cell within 3.5 seconds, the AIS will show Active, which is an Alarm indication, and one AIS cell will be generated once per second toward the other endpoint.

To automatically activate an End to End Continuity Check when a VC is first connected, select the Type and set Auto Activate to “Enable.” The next time the VC Oper Status changes from Down to Up, the CC will automatically be activated.

Remote Defect Indication, or RDI, indicates “Receiving” if RDI cells are being received. The RDI state will clear after about 3.5 seconds of no received RDI cells.

Alarm Indication Signal, or AIS, shows “Active” if the VC is receiving AIS cells. The AIS state will clear after about 3.5 seconds of no received AIS cells when no CC is active. When CC is active, the AIS state will clear on receipt of a CC cell or a user cell.

## Quality of Service (QoS) Table Screen

Clicking on the “QoS Profiles” button on the ATM Service Details screen will display the screen shown in Figure 3.37.

**Figure 3.37** ATM Quality of Service Profile Table Screen

Profile	Service Category	Param 1 (PCR)	Param 2 (SCR)	Param 3 (MBS)	Row Status
<a href="#">1</a>	VBR	1200	1000	200	Active

The table displayed on this screen contains information on ATM traffic descriptor type and the associated parameters.

- Service Category** ATM service category. Possible values include CBR, VBR, and UBR.
- Param 1 (PCR)** Peak cell rate in cells per second.
- Param 2 (SCR)** Sustainable cell rate in cells per second. Applicable only to VBR service category.
- Param 3 (MBS)** Maximum burst size in cells. Applicable only to VBR service category.
- Row Status** Current status of the VCC.

Clicking on one of the available “Traffic Description Parameters Index” entries on the ATM Quality of Service Profiles screen will display a screen similar to the screen shown in Figure 3.38. Use this screen to configure or change the QoS parameters listed below.

**Figure 3.38** ATM Quality of Service Details Screen

**ATM Quality of Service Details**  
Profile : 1

Service Category	VBR
Parameter 1 (PCR)	1000
Parameter 2 (SCR)	800
Parameter 3 (MBS)	150
Row Status	Active

- Parameter 1 (PCR)** Peak cell rate in cells per second to use for all channels using this QoS profile.

**Parameter 2 (SCR)** Sustainable cell rate in cells per second to use for all channels using this QoS profile. Applicable to VBR only.

**Parameter 3 (MBS)** Maximum burst size to use for all channels using this QoS profile. Applicable to VBR only.

**Service Category** ATM service category.  
Values: CBR, VBR, UBR  
Default: UBR

**Row Status** Current status of the profile.

The following user-activated buttons are included on the ATM Quality of Service Details Screen:

Button	Function
Submit	Sets any values that have been changed.
Virtual Channels	Displays configured virtual channels.
QoS Profiles	Displays configured QoS profiles.
Delete Profile	Deletes this QoS profile if it is currently unused.

### ***FRF5 Service Details Screen***



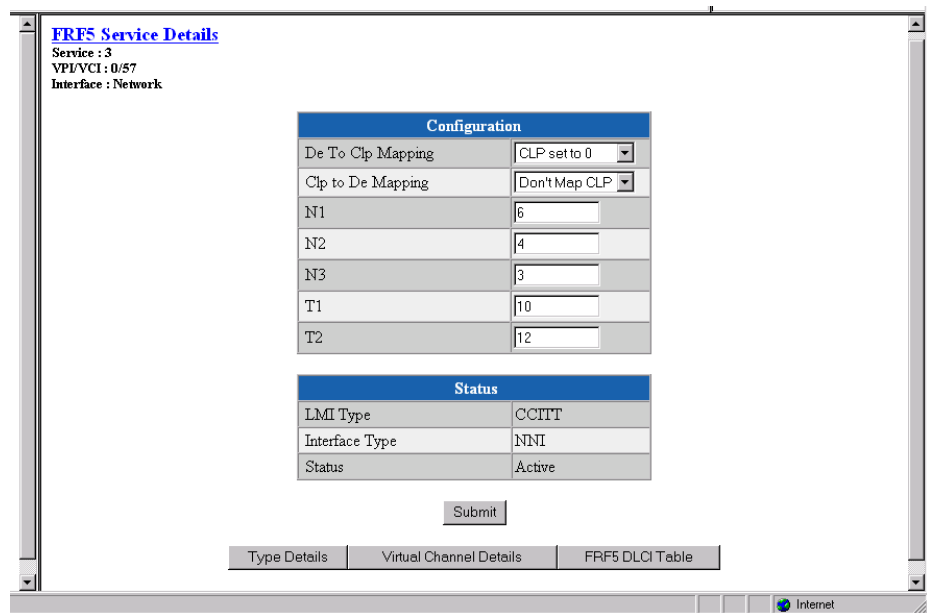
---

**NOTICE:** *The FRF5 Service Details screen is only accessible when FRF5 is the Encapsulation Type as shown on the Virtual Channel Details Screen (see Figure 3.35).*

---

Clicking on the FRF5 Service Details button will bring up the FRF5 Service Details screen as shown in Figure 3.39.

**Figure 3.39** FRF5 Service Details Screen



**DE to CLP Mapping** Indicates whether the Discard Eligibility in the Frame Relay header is mapped to Cell Loss Priority in the ATM cell header when transmitting data in the ATM to Frame Relay direction.

Values: Map DE to CLP, CLP set to 0, CLP set to 1  
Default: CLP set to 0

**CLP to DE Mapping** Indicates whether the Cell Loss Priority in the ATM cell header is mapped to the Discard Eligibility in the Frame Relay header when transmitting data in the ATM to Frame Relay direction.

Values: Map CLP to DE, Don't Map CLP to DE  
Default: Don't Map CLP to DE

**N1** There are two types of status inquiries: keep alive and full status requests. Set this parameter to determine how many “keep alives” are sent between full status requests. (For example, if set to 5, every fifth status inquiry will be a full status inquiry.)

Values: 1–255  
Default: 6

**N2** The N2 counter specifies the total number of link reliability errors and protocol errors that can occur during the sliding event monitor count defined by N3. If this count is exceeded, the port is declared inactive.

Values: 1–10  
Default: 4

**N3** This counter represents a Monitored Events Count. For a network, a monitored event is the receipt of a status inquiry message or the expiration of the polling verification timer T2. This parameter defines the size of the sliding

window used by the unit to determine whether a channel or user device is active.

Values: 1–10

Default: 3

**T1** This parameter specifies the number of seconds the unit waits between issuing status inquiry messages.

Values: 5–240

Default: 10

**T2** This parameter specifies the number of seconds the unit allows before counting non-receipt of a status inquiry message as an error.

Values: 5–245

Default: 12

The following user-activated buttons are included on the FRF5 Service Details Screen:

Button	Function
Type Details	Returns you to the ATM Service Details screen.
Virtual Channel Details	Returns you to the Virtual Channel Details screen.
FRF5 DLCI Table	Displays the FRF5 DLCI Table (see Figure 3.40).

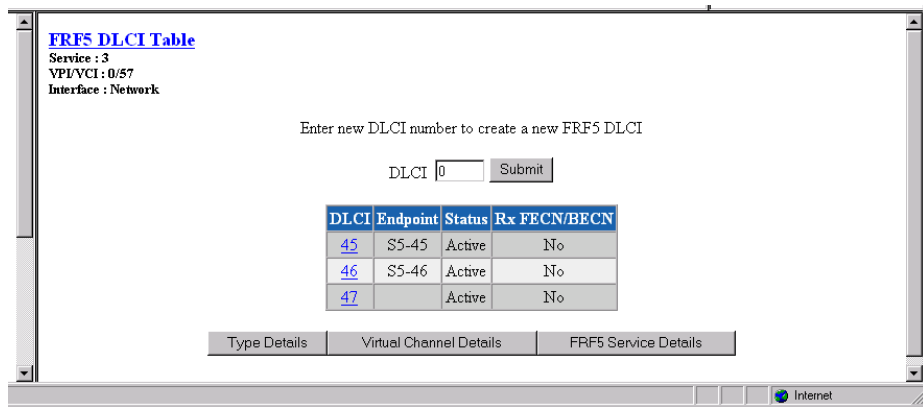
### **FRF5 DLCI Table**

One or more DLCIs may be created for the Frame Relay link carried over ATM for an FRF5 VC. When a DLCI is intended to transport Frame traffic to a Frame Relay link on the Serial port, an endpoint is associated with that DLCI. It is advisable, but not necessary, to use the same DLCI number on the Serial port for the FRF5 DLCI.

If an FRF5 DLCI has no associated endpoint name, that DLCI's Frame traffic will terminate inside the WANsuite 6450. One application for having no associated endpoint is to use the DLCI for router traffic, which is set up by an IP circuit whose endpoint names the FRF5 endpoint for this VPI/VCI/DLCI beginning with the letter "I."

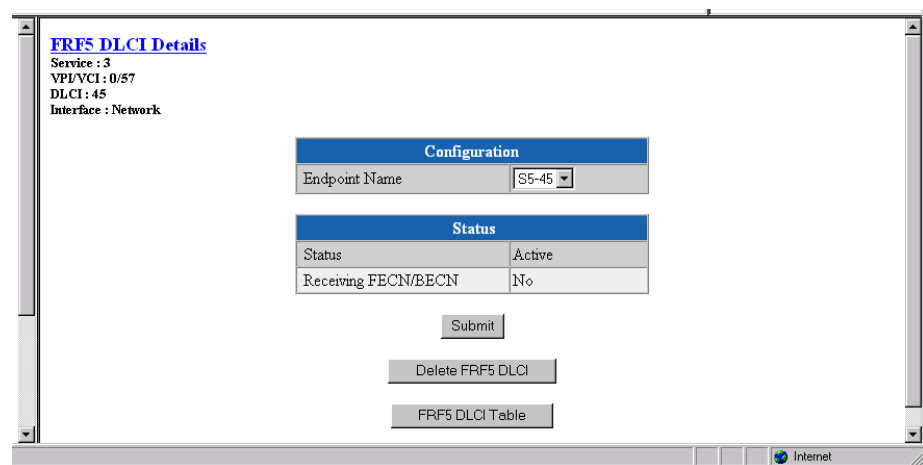
The Received FECN/BECN column shows whether the current frames are indicating Forward Explicit Congestion Notification or Backward Explicit Congestion Notification.

**Figure 3.40** FRF5 DLCI Table



Click on one of the DLCIs listed to view the FRF5 DLCI Details screen as shown in Figure 3.41.

**Figure 3.41** FRF5 DLCI Details Screen



The Endpoint Name specifies which Serial port Frame Relay endpoint is associated with this FRF5 DLCI.

### FRF8 Service Details Screen

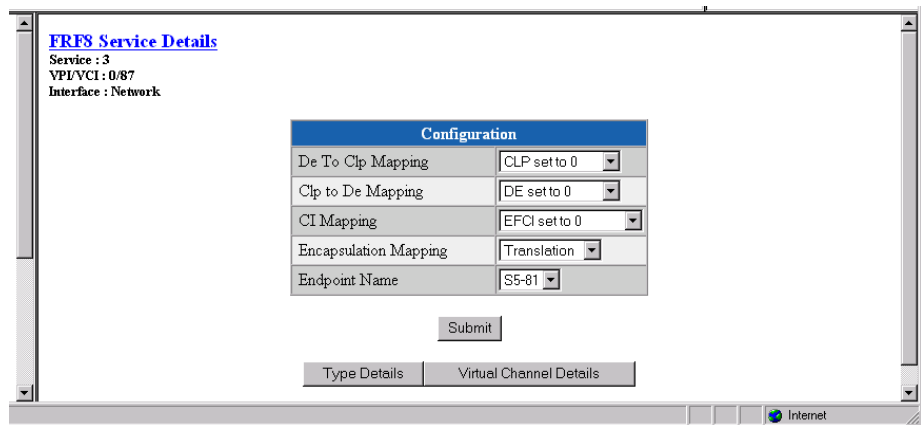


**NOTICE:** The FRF8 Service Details screen is only accessible when FRF8 is the Encapsulation Type as shown on the Virtual Channel Details Screen (see Figure 3.35).

The FRF8 Service Details Screen is shown in Figure 3.42.



**Figure 3.42** FRF8 Service Details Screen



**DE to CLP Mapping** Indicates whether the Discard Eligibility in the Frame Relay header is mapped to Cell Loss Priority in the ATM cell header when transmitting data in the ATM to Frame Relay direction.

Values: Map DE to CLP, CLP set to 0, CLP set to 1

Default: CLP set to 0

**CLP to DE Mapping** Indicates whether the Cell Loss Priority in the ATM cell header is mapped to the Discard Eligibility in the Frame Relay header when transmitting data in the ATM-to-Frame Relay direction.

Values: Map CLP to DE, DE set to 0, DE set to 1

Default: DE set to 0

**CI Mapping** Indicates whether FECN in the Frame Relay header is mapped to EFCI in the ATM cell header when transmitting data in the Frame Relay to ATM direction.

Values: Map FECN to EFCI, EFCI set to 0

Default: EFCI set to 0

**Encapsulation Mapping** Indicates the handling of upper layer user protocol encapsulation. When Encapsulation Mapping is set to Translation, the FRF8 Interworking function maps between the two encapsulations, translating between RFC1490 and RFC1483. When Encapsulation Mapping is set to Transparent, the data is transported without translation between Frame Relay and the ATM PVC.

Values: Transparent, Translation

Default: Translation

**Endpoint Name** Identifies the Serial Frame Relay service DLCI that is to be connected with this FRF8 ATM VC.

## CES Service Details Screen

Clicking on CES under the "Type" column of the table in the Services screen will display the CES Service Details screen shown in Figure 3.43.

**Figure 3.43 CES Service Details Screen**

The screenshot shows a web interface titled "CES Service Details" for an "ATM Interface : Network". It contains two main tables: "Configuration" and "Status".

Configuration			
VPI	0	Partial Cell Fill Byte Count	0
VCI	33	Rx Cell Delay Variation (10 $\mu$ s)	100
Service Type	Structured	Cell Loss Integration (ms)	2500
Timing	Adaptive	Auto Channel Configuration	Disable
AAL1 Format	Basic	Administrative Status	Up
Payload Scrambling	Enable	Operational Status	Down

Status			
Reassembly Cells	125994256	Lost Cells	0
Header Errors	0	Misinserted Cells	0
Pointer Reframes	15749282	Buffer Underflows	0
Pointer Parity Errors	0	Buffer Overflows	0
AAL1 Seq Errors	0	Cell Loss Status	No Loss

Below the status table are two buttons: "Submit" and "Channels".

From this screen, you can access and change the parameters listed below. The new parameters are saved when you click on “Submit” and then perform a Save and Restart.

**VPI** Determines VPI used for this CES Internet Working Function (IWF). The default is 0.

**VCI** Determines VCI used for this CES IWF. The default is 33.

**Service Type** Determines if T1/E1 service is structured (Nx64 kbps with or without signaling) or unstructured (2.048 or 1.544 Mbps raw data stream). You must configure the Service Type to correspond with the desired CBR port framing and Signaling in accordance with the table on page 3-58.

**Timing** Determines the CES services clocking mode, which maps to the transmit clock source of the CBR interface and Serial interface (if configured for a CES service). When “Adaptive” timing is selected, the receive AAL1 payload buffer is monitored for predetermined threshold levels to control the frequency of the interface clocks. When the buffer depth exceeds the predetermined upper threshold, the interface clock frequency is increased to cause the buffer to drain more quickly. If the buffer depth falls below the predetermined lower buffer threshold, the interface clock frequency is decreased to cause the buffer to drain less quickly. Both lower and upper threshold levels are used in conjunction with Cell Delay Variation to provide hysteresis around threshold levels.

Values: Synchronous, Adaptive

Default: Adaptive

- AAL1 Format** Specifies AAL1 format – Basic, E1Cas, Ds1SfCas, or Ds1EsfCas. This value must be set in accordance with the table on page 3-58 for proper operation.
- Payload Scrambling** The WANsuite 6450 scrambles/descrambles cell payload bytes at the physical layer interface using an  $x^{43} + 1$  polynomial. You may enable/disable the scrambling function on the CES Service Details Screen. (Normal operation will have Payload Scrambling enabled, which is the default.) (See Figure 3.43 on page 3-54.)
- Partial Cell Fill Byte Count** Sets the number of user octets per cell. Setting this parameter to 0 disables Partial Cell Fill, and all cells are completely filled before being sent.
- Rx Cell Delay Variation (10  $\mu$ s)** Maximum cell arrival jitter in 10- $\mu$ s increments that the reassembly process will tolerate in the cell stream without producing errors on the CBR service interface. Default is 100 for a 1000- $\mu$ s Cell Delay Variation (CDV).
- Cell Loss Integration (ms)** Time in milliseconds for the cell loss integration period. If cells are continuously lost during the specified period of time, Cell Loss Status is set to “Loss.” Default is 2500 ms.
- AutoChannel Configuration** This feature applies only to circuit emulation of E1 CCS, E1 CAS, and Serial CES services. When enabled, the WANsuite 6450 will automatically configure the number of channels (N) allocated to the service according to the negotiated SHDSL line rate. Channels are allocated starting with channel/time slot 1 in consecutive order until N channels have been allocated to the service. An emulated E1 CCS or Serial service may allocate channels/time slots 1–31. Refer to the table below that shows E1 Nx64 Basic Service Without Signaling (E1 CCS).

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
192	1	171	119.496	281
256	2	342	110.992	261
320	3	512	102.912	242
384	4	683	94.408	222
448	5	854	85.904	202
512	6	1024	77.824	183
576	7	1195	69.320	143
640	8	1366	60.816	143
704	9	1536	52.736	124
768	10	1707	44.232	104
832	11	1878	35.728	84
896	12	2048	27.648	65
960	13	2219	19.144	45
1024	14	2390	10.640	25
1088	15	2560	2.560	6
1152	15	2560	66.560	156
1216	16	2731	58.056	136

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
1280	17	2902	49.552	116
1344	18	3072	41.472	97
1408	19	3243	32.968	77
1472	20	3414	24.464	57
1536	21	3584	16.384	38
1600	22	3755	71.880	18
1664	22	3755	71.880	169
1728	23	3926	63.376	149
1792	24	4096	55.296	130
1856	25	4267	46.792	110
1920	26	4438	38.288	90
1984	27	4608	30.208	71
2048	28	4779	21.704	51
2112	29	4950	13.200	31
2176	30	5120	5.120	12
2240	30	5120	69.120	163
2304	31	5291	60.616	142
2312	31	5291	68.616	161

An emulated E1 CAS service may allocate channels/time slots 1–15 and 17–31 (refer to the table below). Channel/time slot 16, which carries the signaling information, will not be allocated as a voice channel. Refer to the table below for E1 Nx64 Basic Service With Signaling (E1 CAS).

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
192	1	182	114.832	270
256	2	352	106.752	251
320	3	534	93.584	220
384	4	704	85.504	201
448	5	886	72.336	170
512	6	1056	64.256	151
576	7	1238	51.088	120
640	8	1408	43.008	101
704	9	1590	29.840	70
768	10	1760	21.760	51
832	11	1942	8.592	20
896	12	2112	0.512	1
960	12	2112	64.512	152
1024	13	2294	51.344	121
1088	14	2464	43.264	102
1152	15	2646	30.096	70
1216	16	2816	22.016	51
1280	17	2998	8.848	20

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
1344	18	3168	0.768	1
1408	18	3168	64.768	152
1472	19	3350	51.600	121
1536	20	3520	43.520	102
1600	21	3702	30.352	71
1664	22	3872	22.272	52
1728	23	4054	9.104	21
1792	24	4224	1.024	2
1856	24	4224	65.024	153
1920	25	4406	51.856	122
1984	26	4576	43.776	103
2048	27	4758	30.608	72
2112	28	4928	22.528	53
2176	29	5110	9.360	22
2250	30	5280	1.280	3
2304	30	5280	65.280	153
2312	30	5280	73.280	172

**Administrative Status** Sets the Administrative Status of the CES IWF. “Up” indicates traffic flow is enabled, and “Down” indicates traffic flow is disabled across the CES IWF.




---

**NOTICE:** *To enable a new parameter, rather than saving and restarting, set the Administrative Status to “Down,” and click on the “Submit” button at the bottom of the screen. Then set the Administrative Status to “Up,” and click on the “Submit” button once again.*

---

**Operational Status** Displays the Operational Status of the CES IWF. The state will be “Down” or “Unknown” if the supporting CBR or ATM interface is down or unknown.

### Status

**Reassembly Cells** Displays the number of cells received by the CES IWF. This number excludes cells that have been discarded for any reason, including cells not used due to their being misinserted or discarded while the reassembler was awaiting synchronization.

**Header Errors** Displays the number of AAL1 header errors detected, including those that have been corrected. Header errors include correctable and uncorrectable CRCs and bad parity.

**Pointer Reframes** Displays the number of events in which the AAL1 reassembler found a Structured Data Pointer (SDT pointer) where it was not expected, making it necessary to reacquire the pointer.

- Pointer Parity Errors** Displays the number of events in which the AAL1 reassembler has detected an SDT pointer parity check failure.
- AAL1 Seq Errors** Displays the number of times the sequence number of an incoming AAL1 frame causes a transition from the “sync” state to the “out of sequence” state.
- Lost Cells** Displays the number of cells detected as lost in the network prior to reaching the destination CES IWF AAL1 layer processing. As an example, the number of lost cells may be detected as a result of AAL1 sequence number processing.
- Misinserted Cells** Displays the number of AAL1 sequence violations, which the AAL Convergence Sublayer interprets as “misinserted cells.”
- Buffer Underflows** Displays the number of times the CES reassembly buffer underflows.
- Buffer Overflows** Displays the number of times the CES reassembly buffer overflows.
- Cell Loss Status** Displays “Loss” when cells are continuously lost during the specified Cell Loss Integration Period. When a valid cell(s) is received, this condition is cleared, and “No Loss” will be displayed.

Configuring the WANsuite 6450 for CES involves setting parameters not only on the CES Service Details screen (Figure 3.43 on page 3-54), but also on the CBR screen (Figure 3.13 on page 3-15); in some cases, the Serial screen (Figure 3.17 on page 3-20); and the Channel Table Details screen (Figure 3.44 on page 3-59). The table below shows the settings required to maintain the proper relationships among CBR framing, the CES Service Type, the CES AAL1 format, and the Signaling.

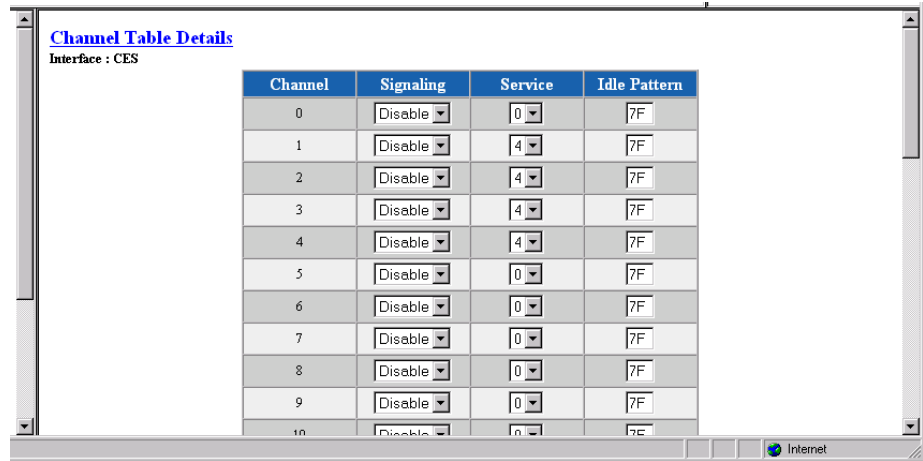
CES Service Description	CBR Framing	CES Service Type	CES AAL1 Format	Signaling
Basic E1 (CCS)	E1 CCS	Structured	Basic	Disable
Serial	E1 CCS	Structured	Basic	Disable
Basic T1 (ESF)	T1 ESF	Structured	Basic	Disable
Basic T1 (D4)	T1 D4	Structured	Basic	Disable
E1 w/Signaling (CAS)	E1 CAS	Structured	E1Cas	Enable*
T1 w/Signaling (ESF)	T1 ESF	Structured	Ds1EsfCas	Enable*
T1 w/Signaling (D4)	T1 D4	Structured	Ds1SfCas	Enable*
Unstructured E1	E1 Unframed	Unstructured	Basic	Disable
Unstructured Serial	E1 Unframed	Unstructured	Basic	Disable
Unstructured T1	T1 Unframed	Unstructured	Basic	Disable

\*Only channels allocated to the CBR interface should have Signaling set to “Enable.” When configuring the Serial interface for CES service (see *Serial CES Configuration* as described on page 3-61), you must set the Signaling to “Disable for allocated channels.”

## Channel Table Details Screen

To allocate Channels, or time slots, for CES services, click on the “Channels” button at the bottom of the CES Service Details screen to bring up the Channel Table Details screen shown in Figure 3.44.

**Figure 3.44** Channel Table Details Screen



Channel	Signaling	Service	Idle Pattern
0	Disable	0	7F
1	Disable	4	7F
2	Disable	4	7F
3	Disable	4	7F
4	Disable	4	7F
5	Disable	0	7F
6	Disable	0	7F
7	Disable	0	7F
8	Disable	0	7F
9	Disable	0	7F
10	Disable	0	7F

The Channel Table Details screen lets you establish the Signaling, Service, and Idle Pattern parameters for any available channel. The screen parameters are described below.

**Signaling** The unit can operate with Signaling enabled or disabled on channels. You must set this value in accordance with the table above for proper operation.

Values: Disable, Enable

Default: Disable

**Service** Specifies the service to which this channel is allocated. Service Index “0” indicates the channel is not used or is idle. Service Index “4” indicates the channel is allocated to the CBR interface. Service Index “5” indicates the channel is allocated to the Serial interface.

**Idle Pattern** Selects the idle pattern sent by the unit and lets the unit determine if the idle pattern has been sent by the other end.

Values: 0–FF (Hex)

Default: 7F



**NOTICE:** Only channels with a non-zero Service parameter value are assembled into ATM cells and transported across the SHDSL network. Similarly, received ATM cells should only contain data for channels with a non-zero Service parameter value. When reassembling the data stream from the received ATM cells, only the channels with a non-zero Service parameter will be assigned data from the ATM cells. The non-active channels with a Service parameter of “0” will be filled with an idle pattern.

The number of channels you can allocate for the CES service depends on the available SHDSL bandwidth. The table below shows the maximum number of channels you can allocate for CES for each possible SHDSL data rate. If the required CES bandwidth exceeds the available SHDSL bandwidth, the unit will not allow you to configure the CES service.

SHDSL Data Rate (kbps)	Maximum Number of CES Channels		
	Structured Nx64 Basic Service	Structured Nx64 with E1 CAS Service	Structured Nx64 with T1 CAS Service
192	2	2	2
256	3	3	3
320	4	4	4
384	5	5	5
448	6	6	6
512	7	6	6
576	7	7	8
640	8	8	8
704	9	9	9
768	10	10	10
832	11	11	11
896	12	12	12
960	13	12	12
1024	14	13	14
1088	15	14	14
1152	15	15	16
1216	16	16	16
1280	17	17	18
1344	18	18	18
1408	19	18	19
1472	20	19	20
1536	21	20	20
1600	22	21	22
1664	22	22	22
1728	23	23	24
1792	24	24	24
1856	25	24	24
1920	26	25	24
1984	27	26	24
2048	28	27	24
2112	29	28	24
2176	30	29	24



SHDSL Data Rate (kbps)	Maximum Number of CES Channels		
	Structured Nx64 Basic Service	Structured Nx64 with E1 CAS Service	Structured Nx64 with T1 CAS Service
2240	30	30	24
2304	31	30	24
2312*	31	30	24

\*This rate is proprietary to the GlobeSpan chipset and is required for unstructured E1 CES service.

To allocate a channel for the CBR interface, set the channel's "Rate" parameter according to the table shown on page 3-58 and the Service parameter to the Service Index for the CBR interface (4). To allocate a channel for the Serial Interface, refer to the paragraphs below.

## Serial CES Configuration

The WANsuite 6450 has the capability to multiplex/demultiplex the Serial interface data stream with the CBR interface data stream. The multiplexing/demultiplexing is external to the AAL1 SAR; the user controls it by designating time slots for the CES service on the CBR or Serial port. To configure the Serial interface for CES service, perform the following steps:

- 1 On the Services screen (Figure 3.24 on page 3-27), click on the Service Index associated with the Serial interface (5). This will cause the unit to display the Service Details screen for the Serial interface. On the Service Details screen (Figure 3.25 on page 3-27), select "CES" from the "Type" pull-down menu.
- 2 On the Serial screen (Figure 3.17 on page 3-20), configure the Serial interface to your requirements. You *must* set the "Mode" parameter to "DCE." If the required time slots for the Serial interface are contiguous and not already allocated to the CBR port, you may allocate the required channels on the Serial screen. If you have not allocated channels for the Serial interface on the Serial screen, use the Channel Table Details screen (Step 3 below) to specify the channels for the Serial CES service.
- 3 On the Channel Table Details screen (Figure 3.44 on page 3-59), set the desired channel's "Rate" parameter to "64K," and the "Service" parameter to the Service Index for the Serial interface (5).

## Valid Channel Ranges for Serial and CBR Interfaces

The range of channels available to the Serial interface depends on the type of CES service. The table below shows the range of channels available to the Serial and CBR interfaces for each type of CES service. The type of CES

service and the SHDSL data rate shown in the table on page 3-60 limit the total number of channels that can be allocated to the Serial interface.

CES Service Type Description	Available Serial Interface Channel Range	Available CBR Interface Channel Range	Comments
Basic E1 (CCS)/Serial	1–31	1–31	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Basic T1 (ESF)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Basic T1 (D4)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
E1 w/Signaling (CAS)	1–31*	1-15, 17-31	Serial interface channels may be any arbitrary set within the available channel range. CBR interface channels may not include Channel 16.**
T1 w/Signaling (ESF)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
T1 w/Signaling (D4)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Unstructured E1/ Unstructured Serial	0–31	0–31	Multiplexing channels between the CBR and Serial interface is not allowed for an unstructured service. All channels may be allocated to either the Serial interface (Service parameter “5”), or the CBR interface (Service parameter “4”), or disabled (Service parameter “0”).
Unstructured T1	None***	1–24	All channels must be allocated to the CBR interface (Service parameter “4”) or disabled (Service parameter “0”).

\*Channel 16 (time slot 6) can be used for the Serial CES service without affecting E1 signaling. The E1 signaling information is extracted from the CBR interface data stream prior to multiplexing it with the Serial interface stream. Therefore, replacing channel 16 (time slot 16) with Serial interface data will not affect the assembly or reassembly of the signaling data in the CES data stream.

\*\*The signaling information in the channel is automatically extracted in this mode and assembled in the signaling substructure of the ATM payload. Including channel 16 in the CBR interface data stream would duplicate the data transmitted in the signaling substructure and is therefore not needed.

\*\*\*An Unstructured T1 CES service is not compatible with a Serial interface CES service because the Serial interface does not support a 1.544 MHz clock rate. However, you may use a Basic T1 CES service and allocate all 24 channels to the Serial interface CES service resulting in a 1.536 MHz clock rate.

## HDLC/PPP Service

This service has no configurable parameters.

## Applications

The Applications screens describe configuration tables and statistics for Layer 3 and above that do not map to a specific service or interface.

## Service Aware

The Service Aware function recognizes IP traffic on the WAN and counts the number of frames and bytes passed for a specific service based on filters by VPI/VCI, by DLCI, by IP Address, and by IP Port. Each row of the Service

Aware table represents a specific set of filter parameters known as a “rule.” Each rule is established through the Rule Config screen, which is accessed by clicking the “Rule Details” button at the bottom of the Service Aware screen.

The Service Aware screen (Figure 3.45) provides a table showing these filtered packet counts for up to 10 rules. This table indicates which Service Aware filters are enabled or disabled, and shows the specific VPI/VCI, DLCI, IP Address, IP Mask, and IP Port by which the IP traffic is filtered. In addition, this table shows the Tx Alarm Threshold and the current Tx Alarm status (if enabled) for each rule.

**Figure 3.45** *Service Aware Screen*

Index	Statistics	Service	VPI	VCI	Filter By VPI/VCI	DLCI	Filter By DLCI	IP Address	IP Mask	Filter By IP Address	IP Port	Filter By IP Port	Tx Alarm Threshold	Tx Alarm
<a href="#">1</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">2</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">3</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">4</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">5</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">6</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">7</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">8</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">9</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK
<a href="#">10</a>	<a href="#">Statistics</a>	0	0	0	Disabled	0	Disabled	0.0.0.0	0.0.0.0	Disabled	0	Disabled	0	OK

Clear Alarms

The Service Aware screen provides a “Clear Alarms” user-activated buttons:

### Rule Details Screen

Access the Rule Details screen (Figure 3.46), where you can establish Service Aware parameters, by selecting the appropriate hyperlink from the “Index” column in the above screen. To establish a rule, select the desired rule configuration options, provide the appropriate filter information where required, and click on the “Submit” button at the bottom of the screen.

**Figure 3.46** Rule Details Screen

**Rule Details**  
Rule : 8

Service	0
VPI	0
VCI	0
Filter By VPI/VCI	Disabled
DLCI	0
Filter By DLCI	Disabled
IP Address	0.0.0.0
IP Mask	0.0.0.0
Filter By IP Address	Disabled
IP Port	0 Enter or select from list -->
Filter By IP Port	Disabled
TX Alarm Threshold (bps)	0
TX Alarm	OK

Note: If the Service parameter is changed a Submit must be made before the appropriate DLCIs are shown.

Submit

IP Port List  
0  
Enter

The paragraphs below describe the rule configuration parameters and their options.

**Service** Selects the service to which the rule applies. Select from a pull-down menu that lists available services.



**NOTICE:** *If you change the Service parameter, you must click on “Submit” to see the appropriate DLCIs.*

**VPI** Selects the VPI to which the rule applies.

**VCI** Selects the VCI to which the rule applies.

**Filter By VPI/VCI** Enables or disables filtering of the IP traffic in accordance with the specified VPI/VCI.



**NOTICE:** *To use this filter, you must specify both the Service and VPI/VCI parameters in the Rule Config screen.*

**DLCI** Selects the DLCI to which the rule applies from a pull-down list of applicable DLCIs.

**Filter By DLCI** Enables or disables filtering of the IP traffic by the DLCI specified in the DLCI pull-down list.



**NOTICE:** *To use this filter, you must specify both the Service and DLCI parameters in the rule configuration.*

**IP Address** Establishes the IP Address by which the rule will filter IP traffic (if enabled).

**IP Mask** Represents a range of IP Addresses defined so that only machines with IP Addresses within the range defined by the mask are allowed to access an Internet service. To mask a portion of the IP Address, replace it with the wild card character “0” (zero). (For example, an IP Address Filter of 192.44.0.0 and an IP Mask Filter of 255.255.0.0 represent every computer on the Internet with an IP Address beginning with 192.44.)

**Filter By IP Address** Enables or disables filtering of the IP traffic by the IP Address specified in the IP Address or IP Mask field.

**IP Port** Establishes the IP port by which the rule will filter IP traffic (if enabled).

**Filter By IP Port** Enables or disables filtering of the IP traffic by the IP port specified in the IP Port field.

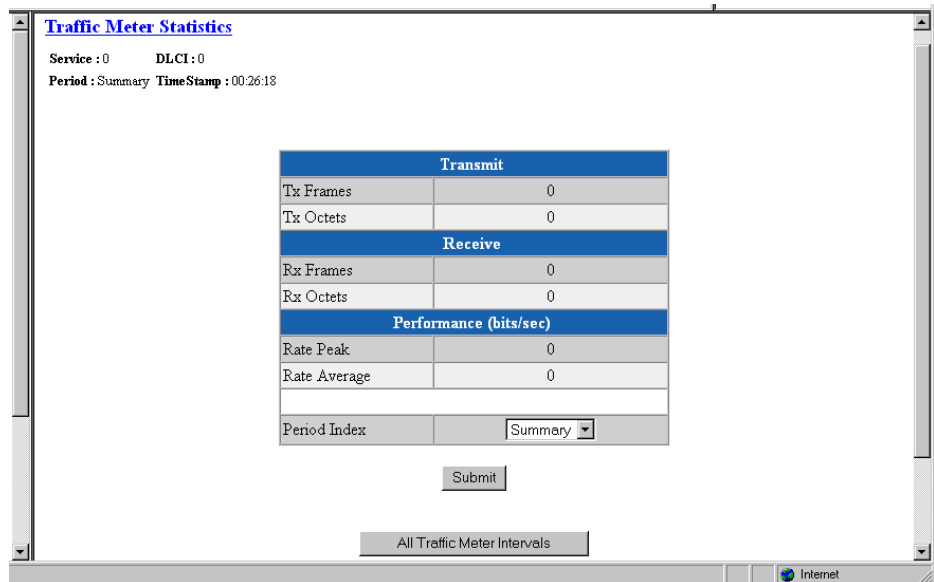
**Tx Alarm Threshold** Specifies the threshold (in bps) for the Transmit Alarm on this rule.

**Tx Alarm** Displays the current status of the Transmit Alarm.

## Traffic Meter Statistics Screen

The Traffic Meter Statistics (Figure 3.47) screen displays the number of frames and octets that have been counted in accordance with the Service Aware “rule” that has been established for a Service. In addition, this screen provides data rate performance information for the period of time specified in the Period Index field (see below). Access this screen by clicking on the appropriate “Statistics” hyperlink on the Service Aware screen.

**Figure 3.47** Traffic Meter Statistics Screen



The Traffic Meter Statistics screen reports Transmit, Receive, and Performance statistics on the following parameters:

- Tx Frames

- Tx Octets
- Rx Frames
- Rx Octets
- Rate Peak – the peak data rate for the viewed period (see below)
- Rate Average – the average data rate for the viewed period (see below)

The Period Index field is used to define the period of time for which the Traffic Meter statistics will be reported. It represents the 24-hour, 15-minute buckets index. Selecting a period and then clicking the “Submit” button will display the traffic meter statistics for that period. The user-selectable options are listed below.

Click on the “All Traffic Meter Intervals” button to see the screen shown below in Figure 3.48.

**Figure 3.48** All Traffic Meter Stats (All Intervals) Screen

Period	Time Stamp	Tx Frames	Tx Octets	Rx Frames	Rx Octets	Tx Rate Peak	Tx Rate Average
Summary	00:27:38	0	0	0	0	0	0
Current	00:27:38	0	0	0	0	0	0
Interval 1	00:15:01	0	0	0	0	0	0

Clear Stats

## SNMP

The unit detects and reports E1 network alarms and provides several options for reporting them, one of which is SNMP traps. When a network alarm occurs, the unit sends a trap message to as many as eight destinations on your network. The unit will report each alarm by transmitting an SNMP “trap” to each non-zero Trap IP Address. The SNMP Details screen (Figure 3.49) lets you configure the SNMP parameters described below.

**Figure 3.49** SNMP Details Screen

Read Community	public
Write Community	private
Trap Community	public
Trap IP Address 1	0.0.0.0
Trap IP Address 2	0.0.0.0
Trap IP Address 3	0.0.0.0
Trap IP Address 4	0.0.0.0
Trap IP Address 5	0.0.0.0
Trap IP Address 6	0.0.0.0
Trap IP Address 7	0.0.0.0
Trap IP Address 8	0.0.0.0

Submit

- Read Community** Accepts a character string identifying the group authorized to perform read operations. The default setting is “Public.”
- Write Community** Accepts a character string identifying the group authorized to perform write operations. The default setting is “Private.”
- Trap Community** Accepts a character string, which is included in SNMP traps generated by the unit. The default setting is “Public.”
- Trap IP Address** Accepts the IP Address of a network device where alarm reporting traps are to be sent.

## Trap Log

A trap is a mechanism that permits a device to send an alarm for certain network events to an SNMP management station. The Trap Log screen (Figure 3.50) shows all generated traps.

The table shown in this screen lists each trap by its Index number, and displays the type of error captured by the trap (Trap Number) and the date and time that the trap was stored (Time Stamp).

Click the hyperlink at the top of the screen to display the latest trap information in the table. To remove all trap information stored in memory, click the “Delete All Traps” button at the bottom of the screen (not shown in the figure below).

**Figure 3.50** Trap Log Screen

Index	Trap Number	Time Stamp	Description	Value
1	ShdsIPerfESThresh	Mon Jul 22 16:15:46 2002	ShdsEndpointCurr15MinES.2.2.1.1	2
2	ShdsIPerfSESThresh	Mon Jul 22 16:15:46 2002	ShdsEndpointCurr15MinSES.2.2.1.1	2
3	ShdsIPerfLOSWSThresh	Mon Jul 22 16:15:46 2002	ShdsEndpointCurr15MinLOSWS.2.2.1.1	2
4	tle1SESAAlarmDeclared	Mon Jul 22 16:15:47 2002	tle1SESCount.1.0.3	5
5	tle1OOFSAAlarmDeclared	Mon Jul 22 16:15:47 2002	tle1OOFSCount.1.0.3	5
6	tle1LOSSAlarmDeclared	Mon Jul 22 16:15:47 2002	tle1LOSSCount.1.0.3	5
7	ShdsIPerfUASThresh	Mon Jul 22 16:15:52 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	10
8	ShdsIPerfUASThresh	Mon Jul 22 16:30:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
9	ShdsIPerfUASThresh	Mon Jul 22 16:45:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
10	ShdsIPerfUASThresh	Mon Jul 22 17:00:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
11	ShdsIPerfUASThresh	Mon Jul 22 17:15:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
12	ShdsIPerfUASThresh	Mon Jul 22 17:30:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
13	ShdsIPerfUASThresh	Mon Jul 22 17:45:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
14	ShdsIPerfUASThresh	Mon Jul 22 18:00:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
15	ShdsIPerfUASThresh	Mon Jul 22 18:15:45 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
16	ShdsIPerfUASThresh	Mon Jul 22 18:30:44 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
17	ShdsIPerfUASThresh	Mon Jul 22 18:45:44 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
18	ShdsIPerfUASThresh	Mon Jul 22 19:00:44 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
19	ShdsIPerfUASThresh	Mon Jul 22 19:15:44 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2
20	ShdsIPerfUASThresh	Mon Jul 22 19:30:44 2002	ShdsEndpointCurr15MinUAS.2.2.1.1	2

## Top Talkers

Clicking on the “Top Talkers” link in the navigation tree displays a screen (Figure 3.51) used to set the parameters for and initiate the generation of a list of IP Addresses ranked in terms of the number of frames and octets they have transmitted during a specified reporting period. This report allows MIS managers to determine who is generating the most traffic on a WAN based on IP Addresses.

**Figure 3.51** *Top Talkers Screen*

The screenshot shows a web interface titled "Top Talkers". It contains three input fields: "Duration (s)" with value 0, "Time Remaining (s)" with value 0, and "Requested Report Size" with value 0. Below these is a "Submit" button. At the bottom, there is a table with the following data:

Report # 0		
Size	Start Time	System Up Time
0	0 days, 00:00:00	1 days, 00:04:29
No entries in table.		

To generate a Top Talkers report, enter the desired report size in the appropriate field, and then click the “Submit” button.

**Duration** Establishes the amount of time (in seconds) for which the Top Talkers report will capture IP traffic; typically this value is 900 seconds (15 minutes).

**Time Remaining** Establishes the amount of time (in seconds) for which the Top Talkers report will capture IP traffic; typically this value is 900 (15 minutes). As soon as you initiate generation of the report by pressing the “Submit” button, the Duration value is copied over to the Time Remaining field. Click on the hyperlink to see how much time is left before the report is completed.

**Requested Report Size** Establishes how many IP Addresses will be reported as the “Top Talkers.”



---

**NOTICE:** *While you may request any number, the unit is internally limited to a maximum of 20.*

---

As soon as the specified Duration for the report has elapsed, the screen will refresh itself and the resulting report-specific information will be displayed in the outlined box at the bottom of the screen. This report comprises elements as defined in the following paragraphs.

**Report #** This field displays a unique number used to identify the generated report. This number is generated automatically, is incremented sequentially for each report, and can be used by management stations for automatic polling (via the ipadv2.mib).

**Size** Displays the actual number of IP Addresses identified as Top Talkers in the generated report. The maximum report size is 20.

**Start Time** Displays the time at which the Top Talkers report was initiated (based on System Up Time).

**System Up Time** Displays the amount of time that the unit has been operational since it was turned on or last reset.



The Top Talkers table reports in descending order the IP Addresses that have generated the most traffic during the requested report's duration. For each IP Address listed, the report displays the number of Rx frames, Rx octets, Tx frames, and Tx octets that have been passed across it. In addition, the Timestamp field indicates the time at which a packet was examined for the specified IP Address.

## IP Gateway

The IP Gateway is a feature that allows routing of IP packets from one network to another using *static routes* configuration and/or *dynamic routing*. The IP Gateway uses Routing Information Protocol (RIP) 1 or RIP 2 or Open Shortest Path First (OSPF) routing.

RIP 1 and RIP 2 are protocols that allow exchange of routing information between two routers. With that information exchange, a router can build its own routing tables that later can be used for "routing" IP packets.

OSPF is a shortest path first (SPF) or link-state protocol. OSPF is also an internal gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least cost path as the best path.

While RIP is ideal for small- to medium-sized networks, OSPF is more suitable for complex networks with a large number of routers. OSPF provides equal cost multipath routing where packets to a single destination can be sent via more than one interface simultaneously.

Figure 3.52 IP Gateway Details Screen

The screenshot displays the 'IP Gateway Details' configuration interface. It features two main sections: 'RIP Parameters' and 'OSPF Parameters'. The 'RIP Parameters' section includes fields for 'RIP Enable' (set to 'Enable RIP2'), 'RIP Trust Neighbors' (set to 'Enable'), 'RIP Interval' (set to '30'), and 'RIP Domain' (set to '0'). Below these are buttons for 'Static Route Table', 'Static ARP Table', and 'Trusted Neighbors'. The 'OSPF Parameters' section includes 'OSPF Enable' (set to 'Disable') and 'OSPF Router ID' (set to '192.94.46.71'). Below these are buttons for 'Area Table' and 'Virtual Link Table'. At the bottom of the form are 'Submit' and 'Circuit Table' buttons. The interface is presented in a windowed format with a standard Windows-style title bar and taskbar at the bottom.

RIP Parameters	
RIP Enable	Enable RIP2
RIP Trust Neighbors	Enable
RIP Interval	30
RIP Domain	0

OSPF Parameters	
OSPF Enable	Disable
OSPF Router ID	192.94.46.71

## RIP Parameters

- RIP Enable** Globally enables RIP 1, RIP 2, or No RIP.  
 Values: Disable, Enable RIP1, Enable RIP2  
 Default: Enable (RIP2)
- RIP Trust Neighbors** Globally enables the trusted neighbors feature. If there is a list of trusted neighbors in an IP Gateway, only RIP packets coming from those trusted neighbors will be used to build the internal routing table.  
 Values: Enable, Disable  
 Default: Enable
- RIP Interval** Interval for RIP packet to be sent. Default is 30 seconds.
- RIP Domain** Value representing the RIP domain. Default is 0.

## OSPF Parameters

- OSPF Enable** This Protocol is suitable for complex networks with a large number of routers. If a large network is involved, OSPF may be the solution for the user.  
 Values: Disable, Enable  
 Default: Disable
- OSPF Router ID** This 32-bit number assigned to each router running the OSPF protocol uniquely identifies the router within an autonomous system. Each router requires a unique router ID. Default is the LAN IP Address of the unit.

The IP Gateway screen provides the following user-activated buttons:

Button	Function
<b>RIP Parameters</b>	
Static Routes Table	Displays static routes and dynamic routes information.
Static ARP Table	Displays static ARP information.
Trusted Neighbors	Displays trusted neighbors information.
<b>OSPF Parameters</b>	
Area Table	Displays area information.
Virtual Link Table	Displays virtual link information.
Submit	Submits to the unit information specific to IP Gateway.
Circuit Table	Lets you access to circuit-related information/operation.

## Circuit Table Screen

Access this menu by clicking on the “Circuit Table” button at the bottom of the IP Gateway menu. This screen shows the configured circuit. Endpoints that begin with “P,” such as Px-Cy, are for ATM VPI x, VCI y. For example, P0-C32 is VPI 0, VCI 32. Endpoints that begin with “S,” such as Sx-yy, are for

Frame Relay Service x, DLCI yy. For example, S5-45 is Service 5, DLCI 45. Endpoints that begin with “I” such as Ix-y-z are FRF5 Interworking Frame Relay endpoints for VPI x, VCI y, DLCI z. For example I0-87-45 would be FRF5 Interworking endpoint for VPI 0, VCI 87, DLCI 45.

**Figure 3.53** *Circuit Table Screen*

Index	Endpoint	IP Address	IP Mask	RIP Status	OSPF Status
1	LAN	192.94.46.72	255.255.255.0	Disable	Disable

Add New

To configure a new circuit, click on "Add New."

### **Circuit Details Screen**

Access this menu (Figure 3.54) by clicking on the appropriate numbered link under the “Index” column on the Circuit Table screen.



**NOTICE:** A “Submit” on this screen will activate a newly created circuit. It is not necessary to perform a “Save and Restart” for the circuit to take effect.

**Figure 3.54** *Circuit Details Screen*

**Circuit Details**  
Circuit : 1

Endpoint	LAN
IP Address	192.94.46.72
IP Mask	255.255.255.0
Max Transmit Unit	1500
Cost	1
RIP Status	Disable
Multicast Status	Enable
OSPF Status	Disable
OSPF Area	0.0.0.0
OSPF LSA Timer	5
OSPF LSU Delay	1
OSPF Router Priority	1
OSPF Hello Interval	10
OSPF Dead Interval	40
OSPF Auth Key	

Submit

Circuit Table

**Endpoint** Endpoint name. By default, the first circuit is always the LAN circuit. WAN circuit endpoint names are taken from the VPI/VCI number. For example, VPI 0/VCI 32 will have “P0-C32” for an endpoint name. The pull-down menu will display a list of VPI/VCI’s actually configured. A given circuit will

receive/transmit data on the VPI/VCI combination corresponding to its endpoint name.

- IP Address** IP Address of the circuit.
- IP Mask** IP Mask of the circuit.
- Max Transmit Unit** Maximum transmit unit this circuit will send at any one time.
- Cost** Represents the relative time of treatment of an IP packet. This value is used when there are multiple routes to the same destination. When two or more routes are available, the one with the lowest circuit cost is selected. An ATM circuit should have a higher value than a LAN circuit.
- RIP Status** Indicates whether or not RIP is enabled on this circuit.  
Values: Disable, Listen and Talk, Talk Only, Listen Only  
Default: Listen and Talk
- Multicast Status** Indicates whether or not Multicast is enabled on this circuit.  
Values: Enable, Disable  
Default: Enable
- OSPF Status** Indicates whether or not OSPF is enabled on this circuit.  
Values: Enable, Disable  
Default: Disable
- OSPF Area** Represents the area that this circuit is part of.
- OSPF LSA Timer** Determines how often the Link State Acknowledgment (LSA) packet is sent.  
Values: 1–3600  
Default: 5
- OSPF LSU Delay** The estimated number of seconds it takes to transmit a Link State Update (LSU) packet over this circuit interface.  
Values: 1–3600  
Default: 1
- OSPF Router Priority** This 8-bit unsigned integer ranges from 1 to 255 and assigns priority to one of two routers attached to the same network; without an assigned priority, both routers attempt to become the designated router.  
Values: 1–255  
Default: 1
- OSPF Hello Interval** The time in seconds between the Hello packets that a router sends on a circuit. This value is also advertised in the router's Hello packets and must be identical for all routers on the same network. The smaller the Hello Interval, the sooner topological changes are detected (but then more traffic is created).  
Values: 1–65535  
Default: 10

**OSPF Dead Interval** The number of seconds that a router's Hello's have not been received before its neighbors declare the router down. The value must be the same as the value on the network.

Values: 1–65535  
 Default: 40

**OSPF Auth Key** When configured, this parameter allows an authentication procedure to be executed on the OSPF header. If the 64-bit (8 character) password does not correspond, the packet is thrown away.

Values: 64 bits (8 characters)  
 Default: 8 spaces (no authentication)

The Circuit Details screen provides the following user-activated buttons:

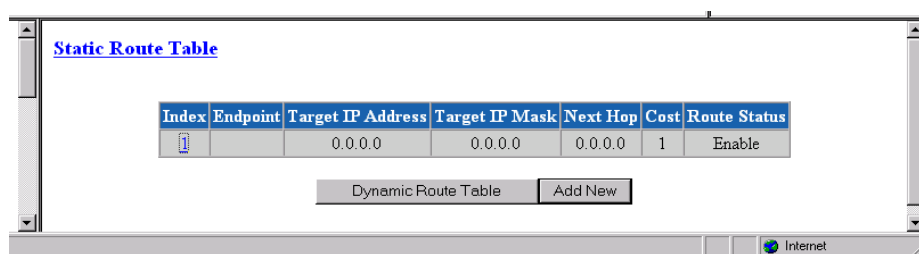
Button	Function
Submit	Sets any values that have been changed.
Circuit Table	Returns you to the previous screen.

## Static Route Table Screen

Under some circumstances, it may not be necessary for a router to learn a route using ordinary means such as RIP or OSPF. It is possible under these circumstances for you to add a route to the route table of a router.

The Static Route Table is always associated with a circuit. Access this menu by selecting the Static Route Table from the RIP Parameters Table on the IP Gateway menu.

**Figure 3.55** *Static Route Table Screen*



**Endpoint** Endpoint name (or interface) through which to send the IP packet to reach the Target IP Address. By default, the first circuit is always the LAN circuit. WAN circuit endpoint names are taken from the VPI/VCI number. For example, VPI 0/VCI 32 will have “P0-C32” for an endpoint name. The pull-down menu will display a list of VPI/VCI's actually confirmed. A given circuit will receive/transmit data on the VPI/VCI combination corresponding to its endpoint name.

**Target IP Address** Represents the target network that you want this router to reach.

**Target IP Mask** Mask of the target network.

**Next Hop** IP Address of the next device in the route.

**Cost** Cost of using that route.

**Route Status** Indicates whether a route is enabled or disabled.

The Static Routes Table screen provides the following user-activated buttons:

Button	Function
Dynamic Route Table	Displays routes learned via RIP or OSPF.
Add New	Adds a new static route.

### ***Route Details Screen***

Access the Route Details screen (Figure 3.56) by clicking on the appropriate numbered link under the “Index” column on the Static Route Table screen.

To establish a new route or to change the parameters of an existing route, enter the desired values in the available parameter fields and press the “Submit” button.



**NOTICE:** A “Submit” on this screen will activate a newly created route. It is not necessary to perform a “Save and Restart” for the route to take effect.

**Figure 3.56** *Route Details Screen*

The screenshot shows a web-based interface titled "Route Details" for "Route : 1". It contains a form with the following fields and values:

Endpoint	LAN
Target IP Address	0.0.0.0
Target IP Mask	0.0.0.0
Next Hop IP Address	0.0.0.0
Cost	1
Route Status	Enable

Below the form are three buttons: "Submit", "Static Route Table", and "Delete Route". The interface is displayed in a browser window with a taskbar at the bottom showing "Internet".

**Endpoint** Endpoint name (or interface) through which to send the IP packet to reach the Target IP Address.

**Target IP Address** Represents the target network that you want this router to reach.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Target IP Mask** Mask of the target network.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0



**NOTICE:** Setting the Target IP Address and Target IP Mask to 0.0.0.0 defines *the* default route for this unit. Because a unit can have only one default route, if a default route is configured as a WAN route on the above screen, the Gateway address configured on the 10/100 Ethernet screen must be left blank. Likewise, if a Gateway is configured on the 10/100 Ethernet screen, it becomes *the* default route, and no WAN default route can be configured on a Static Route.

**Next Hop IP Address:** IP Address of the next device in the route.

**Cost** Cost of using that route.  
 Values: 0–65535  
 Default: 1

**Route Status** Indicates whether or not the current route is enabled.  
 Values: Enable, Disable, Enable and Advertise  
 Default: Enable

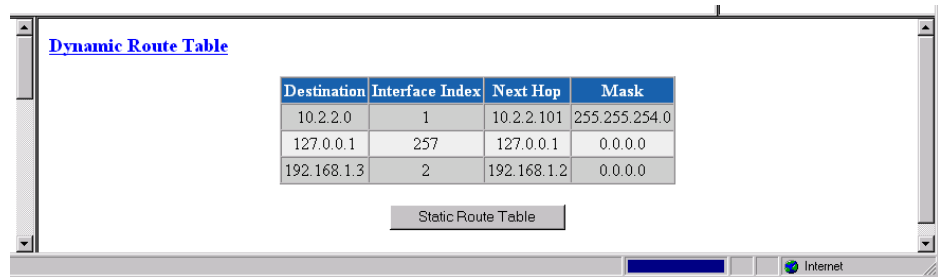
The Route Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Static Route Table	Returns you to the previous screen.
Delete Route	Deletes the route currently displayed.

### Dynamic Route Table Screen

Access this menu by clicking on “Dynamic Route Table” on the Static Routes menu. This table shows both dynamic and static routes. Please note that not all parameters are necessarily defined, depending on whether or not the routes were learned dynamically. Primarily, the most useful information is included in "Destination," "Interface Index," and "Mask" columns.

**Figure 3.57** Dynamic Route Table Screen



**Destination** Network to be reached.

**Interface Index** Interface internal number.

**Next Hop** IP Address used to reach the destination network.

**Mask** Mask of the destination network.

## Static ARP Table Screen

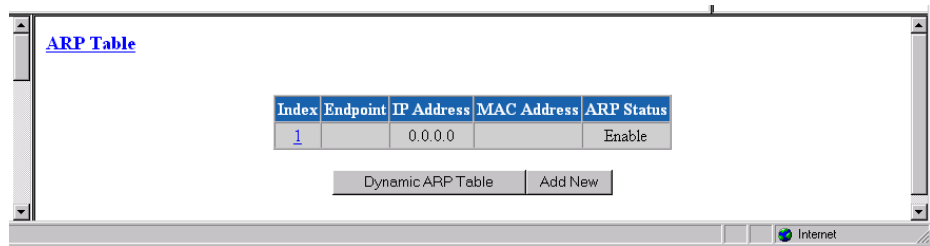
Address Resolution Protocol (ARP) is used by the router to dynamically associate a high-level IP Address to a low-level physical hardware address. ARP packets are only sent across a single physical network.

There are some cases when an IP-compatible device does not support ARP or ARP is deliberately disabled (for security). In these cases, instead of using ARP to dynamically update the router internal MAC <-> IP Address Table, you can use this menu can to *force* an entry into that table. This entry never times out.

At least one circuit must be defined to create a Static ARP Table entry because an ARP entry is always associated with a circuit.

The static ARP table is useful when a Host does not respond to an ARP request. Access this menu by selecting “Static ARP Table” from the RIP Parameters screen on the IP Gateway menu.

**Figure 3.58** *ARP Table Screen*



**Endpoint** Endpoint name (or Interface) through which to send the IP packet to reach the defined IP Address. The default is the LAN.

**IP Address** The IP Address of the unit for which you want to define the MAC Address.

**MAC Address** The MAC Address of the host to be reached.

**ARP Status** Displays whether this static ARP entry is enabled or disabled.

The Static ARP Table screen provides the following user-activated buttons:

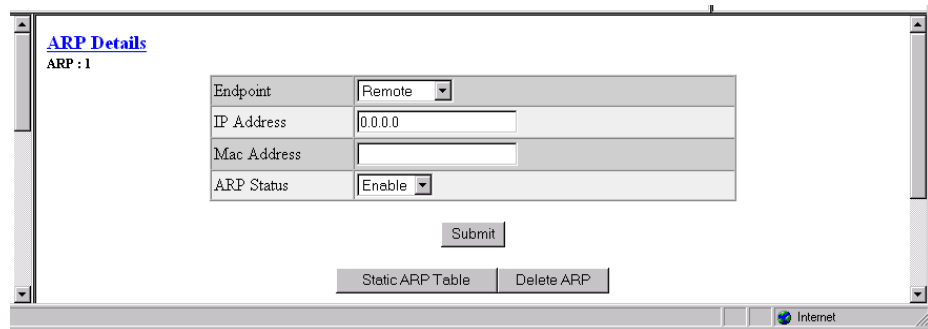
Button	Function
Dynamic ARP Table	Displays the dynamically learned MAC <-> IP Address.
Add New	Adds a new static ARP.

### *ARP Details Screen*

Access the ARP Details screen (Figure 3.59) by clicking on the appropriate numbered link under the “Index” column on the ARP Table screen.



**Figure 3.59** ARP Details Screen



**Endpoint** Endpoint name (or Interface) through which to send the IP packet to reach the defined IP Address. Currently, this is always the LAN.

**IP Address** IP Address of the circuit.  
 Values: 0.0.0.0–255.255.255.255  
 Default: 0.0.0.0

**MAC Address** MAC Address of the Host to be reached.  
 Values: A 6-byte value  
 Default: 00-00-00-00-00-00

**ARP Status** Displays whether this ARP is enabled or disabled.  
 Values: Enable, Disable  
 Default: Enable

The ARP Details screen provides the following user-activated buttons:

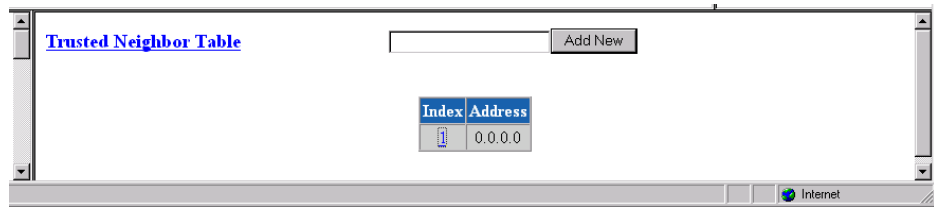
Button	Function
Submit	Sets any values that have been changed.
Static ARP Table	Returns you to the previous screen.
Delete ARP	Deletes this static ARP.

## Trusted Neighbor Table Screen

The Trusted Neighbors feature can be used to store RIP information only from specific routers. This allows the router to reject any RIP information coming from non-Trusted Neighbors. Only information coming from Trusted Neighbors is kept by the router.

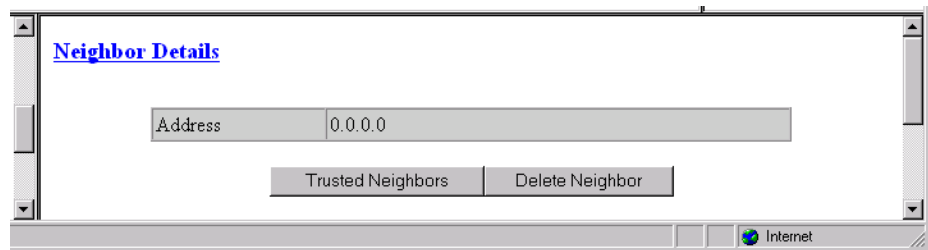
Access the Trusted Neighbor Table screen (Figure 3.60) by selecting Trusted Neighbors from the RIP Parameters on the IP Gateway menu. This table is useful when the Network Administrator wants to listen to RIP of specific router(s).

**Figure 3.60** *Trusted Neighbor Table Screen*



The Trusted Neighbor Table screen provides an “Add New” user-activated button that allows you to specify a new Trusted Neighbor. To see details regarding the Trusted Neighbor feature (Figure 3.61), click on an Index number on the above screen.

**Figure 3.61** *Neighbor Details Screen*



The Neighbor Details screen provides the following user-activated buttons:

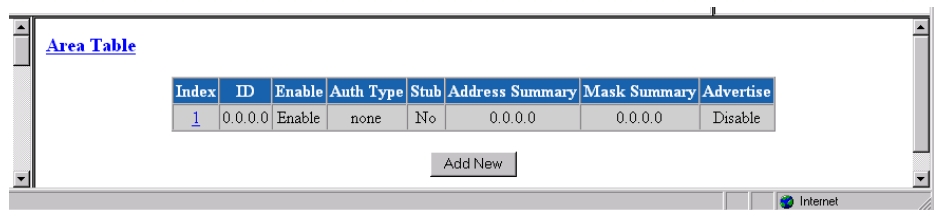
Button	Function
Trusted Neighbors	Returns you to the previous screen.
Delete Neighbors	Deletes this Trusted Neighbor.

## Area Table Screen

An Area allows growth and makes the networks at a site easier to manage. An area is self-contained; knowledge of an area’s topology remains hidden from other areas. Thus, multiple groups within a given site retain the ability to change their internal network topology independently.

Access the Area Table screen from the OSPF Parameters table on the IP Gateway screen.

**Figure 3.62** *Area Table Screen*



**ID** Displays the ID of the Area (represented by an IP Address).

**Enable** Displays whether the defined Area is enabled or disabled.

**Auth Type** Indicates Area validation.

**Stub** Displays whether or not the defined area is a Stub Area.

**Address Summary** Displays the Address Summary of the defined Area.

**Mask Summary** Displays the Mask Summary of the defined Area.

**Advertise** Displays whether advertising is enabled or disabled for this Area.

The “Add New” button on this screen allows you to define a new Area.

### ***Area Details Screen***

Access this screen (Figure 3.63) by clicking on a specific Index number on the Area Table screen.

**Figure 3.63** *Area Details Screen*

The screenshot shows a web browser window titled "Area Details". The page content includes a header "Area : 1" and a form with the following fields and values:

Area ID	0.0.0.0
Enable	Enable
Auth Type	none
Stub	No
Address Summary	0.0.0.0
Mask Summary	0.0.0.0
Advertise	Disable

Below the form are three buttons: "Submit", "Area Table", and "Delete Area". The browser's status bar at the bottom shows "Internet".

**Area ID** This parameter has the same format as the IP Address of the Mask Address.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Enable** Displays whether or not this Area is enabled.  
Values: Enable, Disable  
Default: Enable

**Auth Type** Indicates type of Authentication.  
Values: Simple, None  
Default: None

**Stub** An area can be configured as stub when there is a single exit point from the area, or when the choice of exit point need not be made on a per-external-destination basis.  
Values: Yes, No  
Default: No

**Address Summary** A configured address range specifies what addresses are contained within an area. When summarizing the routes in an area to inform other areas, all routes falling within the configured range are described by a single LSA, thus decreasing the size of the LSA database.

Values: 0.0.0.0–255.255.255.255

Default: 0.0.0.0

**Mask Summary** IP Mask of the summary to be added.

Values: 0.0.0.0–255.255.255.255

Default: 0.0.0.0

**Advertise** Describes the local state of a router or network. This includes the state of the route's interfaces and adjacencies. Each link state advertisement is flooded throughout the routing domain. The collected link state advertisements of all routers and networks form the protocol's topological database.

Values: Yes, No

Default: No

The Area Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Area Table	Returns you to the previous screen.
Delete Area	Deletes the currently defined Area.

## Virtual Link Table Screen

To permit maximum flexibility, OSPF allows the configuration of *virtual* links to enable the backbone area to appear contiguous despite the physical reality.

In OSPF, the backbone is defined as an Area ID of 0.0.0.0. This backbone cannot be disconnected in any way or some areas of the Autonomous System become unreachable. This is because all inter-area traffic must go through the backbone. In fact, the backbone is responsible for all inter-area routing information distribution.

It is possible that an area cannot be connected directly to the backbone; in this case a virtual link is used (see Figure 3.64). To establish or maintain the connectivity of the backbone, virtual links can be configured through non-backbone areas. Basically, virtual links are used to connect components that are otherwise not connected to the backbone.

A virtual link is treated by OSPF as a point-to-point unnumbered network joining two area border routers. The virtual link must be configured in both of the area border routers.

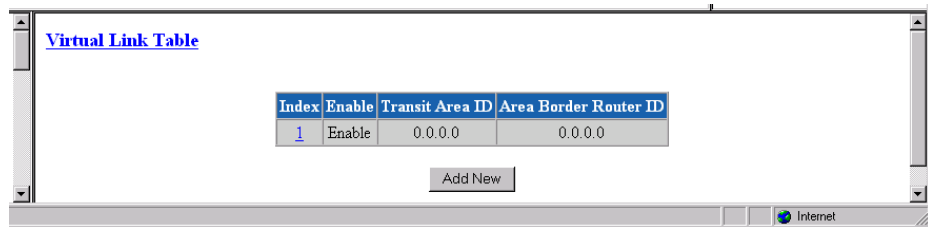
A virtual link is defined by the following two parameters:

- The Router ID of the virtual link's other endpoint

- The non-backbone area across which the virtual link goes through.

Access this screen by selecting the Virtual Link Table from the OSPF Parameters table on the IP Gateway screen.

**Figure 3.64** *Virtual Link Table Screen*



**Enable** Enables this definition of a virtual link.

**Transmit Area ID** The non-backbone area that the virtual link goes through.

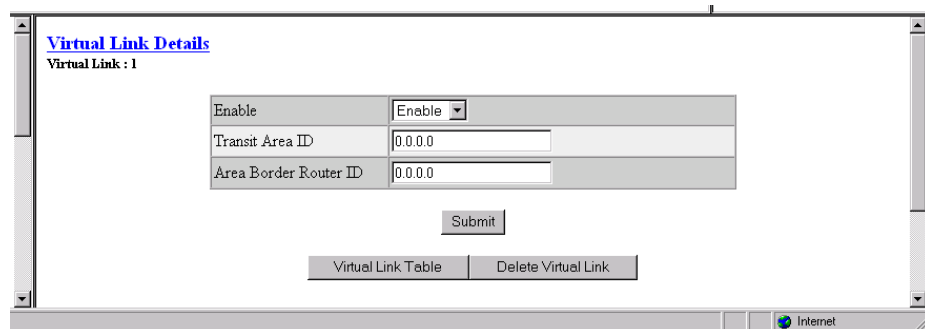
**Area Border Router ID** The Router ID of the virtual link’s other endpoint.

The Virtual Link Table screen provides an “Add New” user-activated button, which lets you define a new Virtual Link.

### ***Virtual Link Details Screen***

Access this screen (Figure 3.65) by clicking on the appropriate Index number under the “Index” column on the Virtual Link Table screen.

**Figure 3.65** *Virtual Link Details Screen*



The Virtual Link Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Virtual Link Table	Returns you to the previous screen.
Delete Virtual Link	Deletes currently defined Virtual Link.

## Originate Ping

The WANsuite 6450 Originate Ping (Figure 3.66) function helps telephone companies determine if a network is properly configured and also helps them maintain SLAs.

**Figure 3.66** *Originate Ping Screen*

The screenshot shows a web-based interface titled "Originate Ping". It contains a table with five rows for configuration: "Destination IP Address" with value "0.0.0.0", "Number To Send" with value "5", "Ping Size (Bytes)" with value "100", "Ping Reply Timeout (sec)" with value "1", and "Ping Status" with value "Ping IP Address required". Below the table is a "Submit" button. At the bottom of the interface are three buttons: "Start Ping", "Stop Ping", and "Reset Stats". The browser's address bar shows "Internet".

**Destination IP Address** Destination IP Address of sent Ping request messages.

**Number to Send** Number of Ping request messages to send.

Values: 1–10,000

Default: 5

**Ping Size (Bytes)** Number of bytes in a Ping request message.

Values: 100–4096 bytes

Default: 100 bytes

**Ping Reply Timeout** Number of seconds to wait for a reply to a Ping request message.

(sec) Values: 1–60 s

Default: 1 s

**Ping Status** Shows the number of pings returned versus the number requested, and providing minimum, average, and maximum statistics.

The Originate Ping screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Start Ping	Starts sending Ping messages.
Stop Ping	Stops sending Ping messages.
Reset Stats	Clears all counts activity.

# Network Address Translation (NAT)

NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP Address. This lets users cost-effectively and efficiently connect their networks to the Internet.

Whether on a global or local port, NAT provides translation only upon receipt of a packet, which NAT will translate, not translate, or filter, depending on the user-specified parameters (further described below). If the decision is made to “translate,” the packet will be modified internally, and eventually sent on to the IP Gateway to be processed. If the decision is made not to “translate,” the packet will not be modified in any way. If the decision is made to “filter,” the packet will be discarded without any further action required.



**NOTICE:** *You must Save and Restart for any changes in NAT configuration parameters to take effect.*

## NAT Details Screen

The NAT Details screen (Figure 3.67) lets the user configure the NAT global parameters described below.

**Figure 3.67** NAT Details Screen

NAT Details			
Enable	Disable ▾	TCP Connection Timer	300
Mode	NAPT ▾	TCP Closing Timer	0
Global IP Addr	192.168.25.12	TCP Disconnected Timer	120
Global Mask	255.255.255.0	TCP Sequence Delta Timer	180
ICMP Default Addr	192.168.25.12	UDP Timer	120
Filter Non Local Addr	Enable ▾	ICMP Timer	120
IP Entry Timer	120		

**Enable** Enables or disables NAT. Default is “Disable.”

**Mode** Selects the Network Address Port Translation (NAPT) mode or the Basic NAT mode. In NAPT mode, all hosts on the Global (public) side view all hosts on the Local (private) side as a single internet host (one IP Address). In Basic NAT mode, the Global IP Address is assigned as a Class C host address (Mask of 255.255.255.0). Each private IP Address on the Local side is mapped to a Class C public address on the Global side. In other words, if there are 30 hosts on the private (Local) side, 30 public (Global) addresses are required. The default is NAPT.

**Global IP Addr** Global IP Address used in NAPT mode. Must be a valid Class C address. Default is LAN IP Address.

**Global Mask** IP Mask associated with defined Global IP Address. Default is LAN IP Mask.

**ICMP Default Addr** Default source address used to answer any ICMP request. Default is LAN IP Address. ICMP requests are not transferred from the Global to the Local side. Rather they are answered by the unit itself since Local addresses are private and do not receive unsolicited requests.

**Filter Non Local Address** Discards any packet with “non corporate” source address. Default is “Enable.”

The screen parameters listed below are related to the NAT Control Block Timer. Note that default values should be in accordance with most NAT applications. The timers’ values minimize NAT resources. Generally, when a timer has expired, the resources used are no longer needed. Those resources will then be available for other connection resources.

**IP Entry Timer** The maximum time (in seconds) NAT will use resources when not using TCP, UDP, or ICMP.  
Values: 0–65535  
Default: 120

**TCP Connection Timer** The maximum time (in seconds) NAT will use resources when attempting to establish a TCP connection.  
Values: 0–65535  
Default: 300

**TCP Closing Timer** The maximum time (in seconds) NAT will use resources when attempting to close a TCP connection.  
Values: 0–65535  
Default: 0

**TCP Disconnected Timer** The maximum time (in seconds) NAT will use resources when attempting to disconnect from TCP.  
Values: 0–65535  
Default: 120

**TCP Sequence Delta Timer** The maximum time (in seconds) NAT will use resources when managing TCP Packet Sequencing.  
Values: 0–65535  
Default: 180

**UDP Timer** The maximum time (in seconds) NAT will use resources for a UDP port in use.  
Values: 0–65535  
Default: 120

**ICMP Timer** The maximum time (in seconds) NAT will use resources for any ICMP request.  
Values: 0–65535  
Default: 120



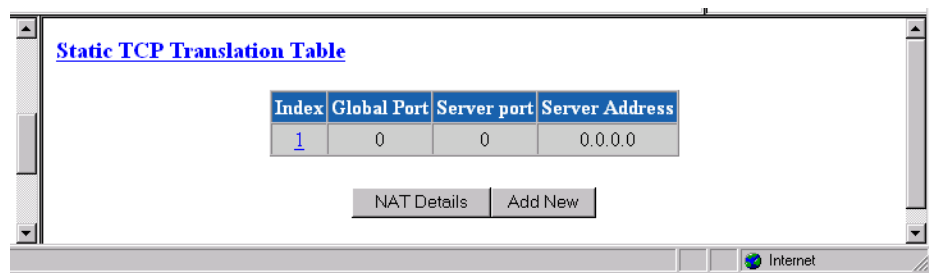
The NAT Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Static TCP Translation Table	Allows static mapping of global TCP Server ports to a local host IP Address/port combination.
Static UDP Translation Table	Allows static mapping of global UDP Server ports to a local host IP Address/port combination.
Table	Defines NAT global/Internet and local/corporate ports.

## Static TCP Translation Table Screen

The Static TCP Translation Table screen allows static mapping of global TCP Server ports to a local host IP Address/port combination. The parameters described below enable access to TCP servers on the private/corporate network “behind the NAT.” The parameters may be used only when in NAPT mode.

**Figure 3.68** *Static TCP Translation Table Screen*



**Global Port** Decimal IP Port exposed to the global Internet. Default is 0.

**Server Port** Decimal IP Port of the local TCP Server. This port is usually the same as the Global Port. Default is 0.

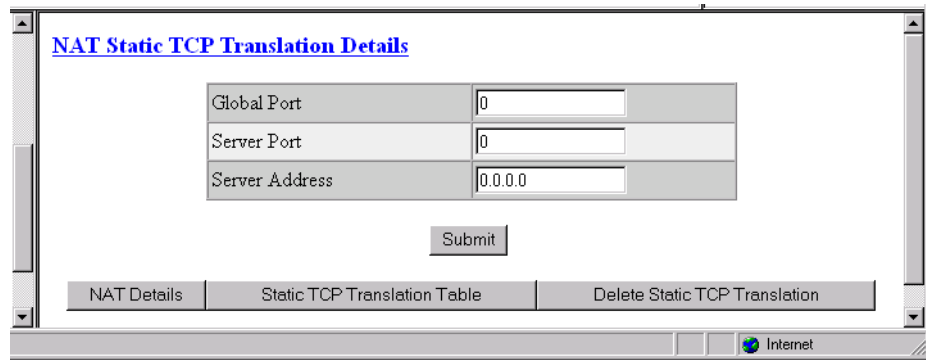
**Server Address** IP Address of the local TCP Server. Default is 0.0.0.0.

The Static TCP Translation Table screen provides the following user-activated buttons:

Button	Function
NAT Details	Returns the user to the previous screen.
Add New	Lets the user add additional addresses.

You can configure or change the above-listed parameters on the Static TCP Translation Details screen (Figure 3.71), which is accessed by selecting the appropriate number under the Index column on the Static TCP Translation Table screen.

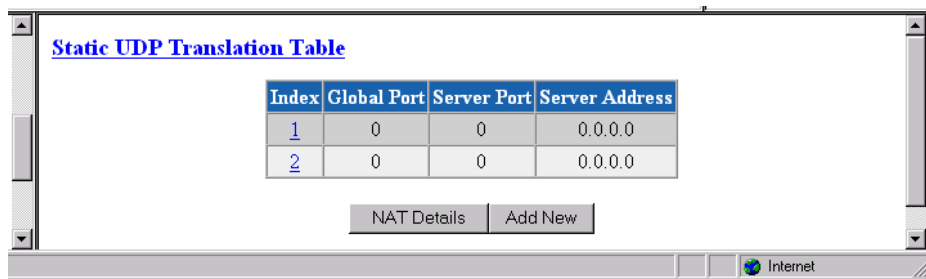
**Figure 3.69** NAT Static TCP Translation Details Screen



## Static UDP Translation Table Screen

The Static UDP Translation Table screen (Figure 3.70) allows static mapping of global UDP Server ports to a local host IP Address/port combination. The parameters described below enable access to UDP Servers on the private/corporate network “behind the NAT.” The parameters may be used only when in NAPT mode.

**Figure 3.70** Static UDP Translation Table Screen



**Global Port** Decimal IP Port exposed to the global Internet. Default is 0.

**Server Port** Decimal IP Port of the local UDP Server. This port is usually the same as the Global Port. Default is 0.

**Server Address** IP Address of the local UDP Server. Default is 0.0.0.0.

The Static UDP Translation Table screen provides the following user-activated buttons:

Button	Function
NAT Details	Returns the user to the previous screen.
Add New	Lets the user add an additional address.

You can configure or change the above-listed parameters on the NAT Static UDP Translation Details screen (Figure 3.71), which is accessed by selecting the appropriate number under the Index column on the Static UDP Translation Table screen.

**Figure 3.71** NAT Static UDP Translation Details Screen

**NAT Static UDP Translation Details**

Global Port	0
Server Port	0
Server Address	0.0.0.0

Submit

NAT Details    Static UDP Translation Table    Delete Static UDP Translation

## NAT Port Table Screen

The parameters on the NAT Port Table screen (Figure 3.72) define the NAT global/Internet and local/Corporate ports. These parameters are configured in the NAT Ports Details screen shown in Figure 3.73. Access the NAT Port Details screen by clicking on the Index number of the desired port on the NAT Port Table screen.

**Figure 3.72** NAT Port Table Screen

**NAT Port Table**

Index	Endpoint	Enable	Default Translation	Type	IP Address	Mask
<a href="#">1</a>	LAN	Enable	Disable	Global	192.94.46.71	255.255.255.0

Add New

**Endpoint** The Endpoint name of the circuit associated with the LAN or WAN port. Default is LAN for the first port.

**Enable** Enables or disables the NAT port. Default is “Enable.”

**Default Translation** Forces translation on a specific IP port regardless of the source IP Address. If Default Translation is set to “Enable,” the packet will never be discarded, but will always pass through the translation path. Therefore, any packets with a destination address different from the global/Internet network address will be processed by the IP Gateway, and may be routed to another port. If this parameter is set to “Disable,” no packet with a destination address different from the global/Internet address will be processed. Setting this parameter to “Disable” will override an “Enable” parameter set under “Filter Non Local Address” on the NAT Details menu.

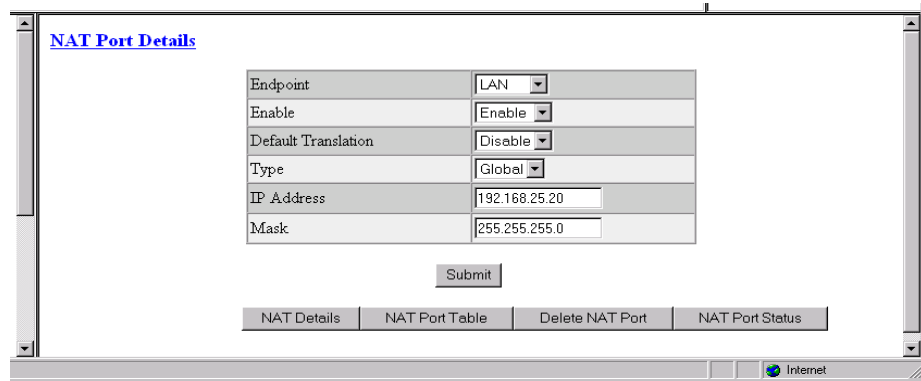
**Type** Defines whether this port is local or global. Default is LAN global. All others are local.

**IP Address** IP Address of this port. Default is the value defined in the IP Gateway Circuit Table.

**Mask** Mask related to the defined IP Address. Default is the value defined in the IP Gateway Circuit Table.

The NAT Port Table screen provides an “Add New” button that lets you add additional addresses.

**Figure 3.73** NAT Port Details Screen

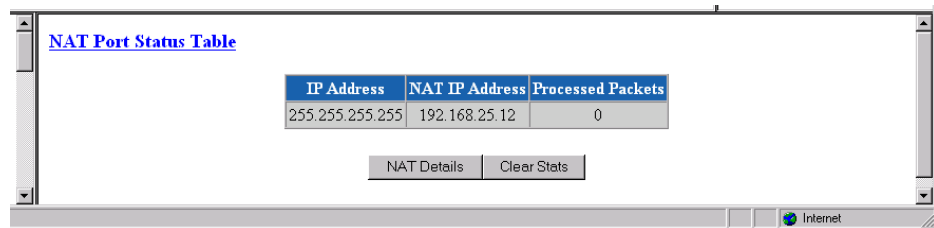


The NAT Port Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
NAT Details	Returns the user to the NAT Details screen.
NAT Port Table	Returns the user to the NAT Port Table screen.
Delete NAT Port	Deletes the specified NAT Port.
NAT Port Status	Displays the NAT Port Status Table screen.

The NAT Port Status Table (Figure 3.74) displays for each port the processed packets from specific IP addresses.

**Figure 3.74** NAT Port Status Table Screen



**IP Address** Original IP Address of the host.

**NAT IP Address** Translated IP Address of the host.

**Processed Packets** Number of packets processed by NAT for this address.

# Dynamic Host Configuration Protocol (DHCP)

DHCP provides a mechanism through which computers using TCP/IP can obtain protocol configuration parameters automatically through the network.

The most important configuration parameter associated with DHCP is the IP Address. A computer must initially be assigned a specific IP Address that is appropriate to the network to which the computer is attached, and that is not assigned to any other computer on that network. If a computer moves to a new network, it must be assigned a new IP Address for that new network. DHCP can be used to manage these assignments automatically.

DHCP has other important configuration parameters also, such as the subnet mask, default router, and Domain Name System (DNS) server. Using DHCP, a network administrator can avoid “hands-on” configuration of individual computers through complex and confusing setup applications. Instead, those computers can obtain all required configuration parameters automatically, without manual intervention, from a centrally managed DHCP server. DHCP is available on the 10/100 Ethernet port only.



---

**NOTICE:** *You must Save and Restart for any changes in DHCP configuration parameters to take effect.*

---

## DHCP Server Details Screen

The DHCP Server Details screen (Figure 3.75) lets you configure the parameters described below.

**Figure 3.75** DHCP Server Details Screen

DHCP Server Details			
Enable	Disable	Primary DNS IP Addr	0.0.0.0
Number of Ports	1	Secondary DNS IP Addr	0.0.0.0
TTL	64	Domain Name	Verilink DHCP Ser
Service Type	1	Router IP Addr	0.0.0.0
Lease Time	600	Primary WINS IP Addr	0.0.0.0
		Secondary WINS IP Addr	0.0.0.0

Submit

Host Table   Static Entry Table   IP Address List Table   IP Address Status Table

Internet

**Enable** Enables or disables the DHCP Server. Default is “Enable.”

**Number of Ports** Defines the number of DHCP ports to be used. In this version, only “1” is a valid value.

**TTL** Time to Live for any DHCP packet. Default is 64.

**Service Type** Type of Service used by the DHCP Server packet. Default is 1.

- Lease Time** Tells the DHCP client the number of seconds it can retain this IP Address. The client should make a new DHCP request within the specified amount of time to ensure the IP Address is not given to another PC. Default is 600 seconds.
- Primary DNS IP Addr** If requested by DHCP client, the client then uses this address to resolve names of IP Addresses. Default is 0.0.0.0.
- Secondary DNS IP Addr** If requested by DHCP client, the client then uses this secondary address to resolve names of IP Addresses. Default is 0.0.0.0.
- Domain Name** Domain name to be used by all DHCP clients. Default is user's server.
- Router IP Addr** IP Address that all clients use for Gateway or Router. Default is 0.0.0.0.

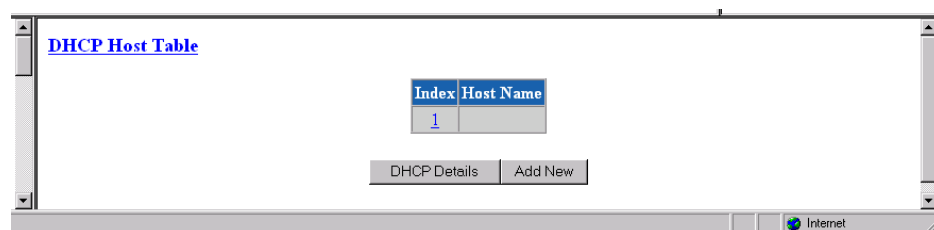
The DHCP Details screen provides the following user-activated buttons:

Button	Function
Submit	Sets any values that have been changed.
Host Table	Lists Host names (DHCP server identification).
Static Entry Table	Creates a list of static IP Addresses associated with MAC Addresses.
IP Address List Table	Defines the addresses available for DHCP clients.
IP Address Status Table	Displays DHCP Server statistics.

## DHCP Host Table Screen

In some cases, it may be necessary to provide an IP station with a specific DHCP server name, which may be used by the IP station when making a DHCP request. That name is included on the DHCP Host Table screen (Figure 3.76), which identifies the DHCP server sending DHCP packets. This parameter is configured on the DHCP Host Details screen (Figure 3.77) accessed by clicking on an "Index" number.

**Figure 3.76** *DHCP Hosts Screen*



- Host Name** The name of the DHCP Server. Default is none.

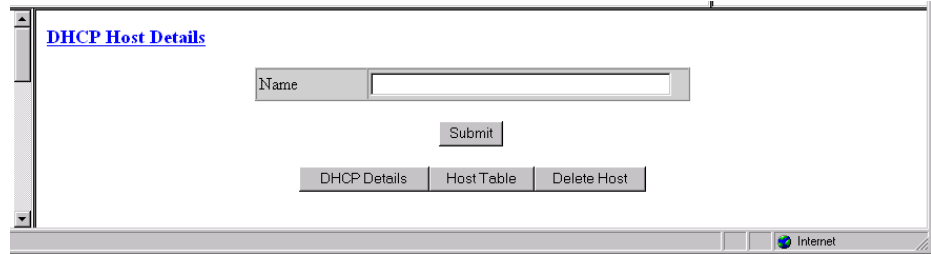
The DHCP Hosts screen provides the following user-activated buttons:

Button	Function
DHCP Details	Returns the user to the previous screen.
Add New	Adds a new Server name.



**NOTICE:** *You must Save and Restart for the new Server name to become active.*

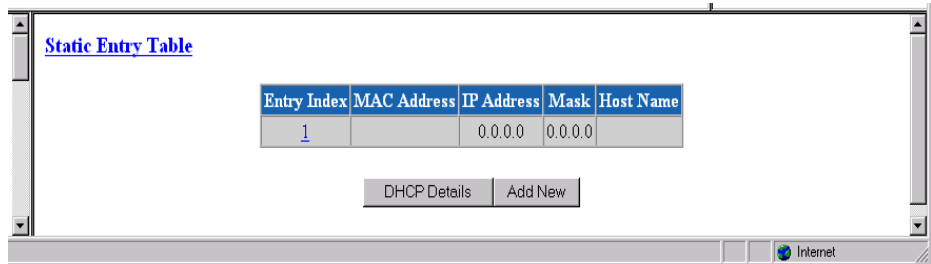
**Figure 3.77** DHCP Host Details Screen



## Static Entry Table Screen

The Static Entry Table screen (Figure 3.78) lists static IP Addresses associated with MAC Addresses. This ensures that the same IP Address will always be used for a given PC provided its MAC Address is known. These parameters are configured on the Static Entry Details screen (Figure 3.79) accessed by selecting a number from the “Entry Index” column.

**Figure 3.78** Static Entry Table Screen



**MAC Address** MAC Address you want to associate with an IP Address.

**IP Address** IP Address given to the DHCP client if that client has the MAC Address defined on this screen.

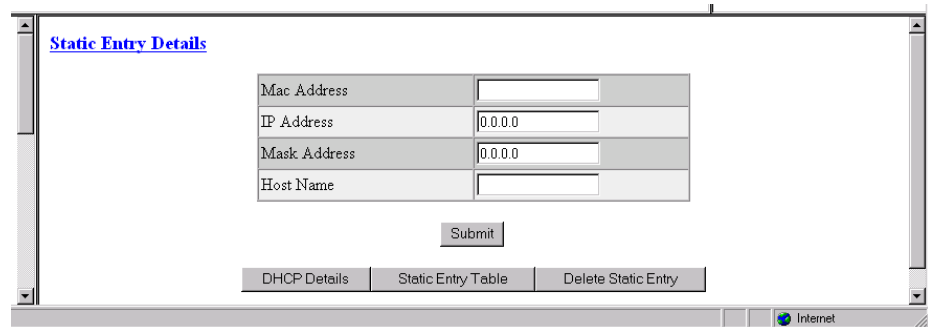
**Mask** Mask associated with the IP Address shown on the screen.

**Host Name** Name given to the DHCP client.

The Static Entries screen provides the following user-activated buttons:

Button	Function
DHCP Details	Returns the user to the previous screen.
Add New	Lets the user add an additional Static Entry.

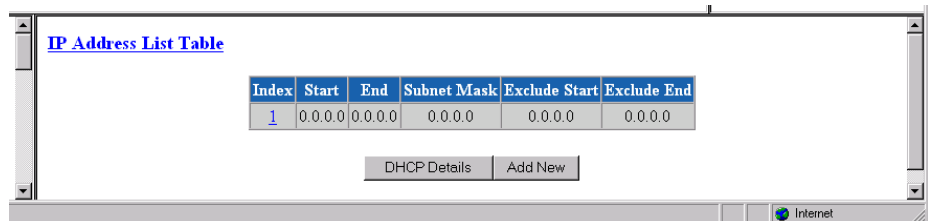
**Figure 3.79** *Static Entry Details Screen*



## IP Address List Table Screen

The IP Address List Table screen (Figure 3.80) displays the “pool” of addresses available for DHCP clients. These parameters are configured on the IP Address Details screen (Figure 3.81) accessed by clicking on an “Index” number.

**Figure 3.80** *IP Address List*



**Start** Starting IP Address of the DHCP client pool.

**End** Ending IP Address of the DHCP client pool.

**Subnet Mask** Subnet Mask associated with the defined range.

**Exclude Start** Beginning of “excluded” range.

**Exclude End** End of “excluded” range.

The IP Address List screen provides the following user-activated buttons:

Button	Function
DHCP Details	Returns the user to the previous screen.
Add New	Lets the user add an additional IP Address.



**Figure 3.81** *IP Address Details Screen*

The screenshot shows a web interface titled "IP Address Details". It contains a table with five rows, each with a label and a text input field containing "0.0.0.0":

IP Start	0.0.0.0
IP End	0.0.0.0
Subnet Mask	0.0.0.0
IP Exclude Start	0.0.0.0
IP Exclude End	0.0.0.0

Below the table is a "Submit" button. At the bottom, there are three navigation tabs: "DHCP Details", "IP Address List Table", and "Delete Address". The browser's address bar shows ".101/border\_sr.htm..." and the status bar shows "Internet".

## IP Address Status Table Screen

The IP Address Status Table screen (Figure 3.82) displays a list of all current DHCP clients.

**Figure 3.82** *IP Address Status Table Screen*

The screenshot shows a web interface titled "IP Address Status Table". The main content area displays the text "No entries in table." Below this text is a "DHCP Details" button. The browser's address bar shows ".101/border\_sr.htm..." and the status bar shows "Internet".

**MAC Address** MAC Address of this DHCP client.

**IP Address** IP Address given to this DHCP client if that client has the MAC Address defined on this screen.

**Status** Provides IP Address Status.

## Bridge

A Bridge operates at the physical network layer, connecting two or more networks and forwarding packets between those networks. For example, a Bridge will connect two or more physical Ethernet cable segments and forward Ethernet packets from one segment to the other.

Bridges differ from routers in that bridges forward packets based on physical addresses rather than on the IP Addresses that routers use to forward packets. Bridges will not “blindly” forward packets from one network to others, however. Rather, it learns all local physical addresses and forwards packets based on those learned “tables.” This greatly reduces the number of broadcasted packets, thus saving valuable bandwidth.

The Bridge Details screen shown in Figure 3.83 lets you access and configure the parameters described below.

**Figure 3.83** *Bridge Details Screen*

Parameter	Value
Enable	Disable
Group Multicast MAC Address	0180C2000000
Bridge ID	0
Hello Timer	10
Max Age Timer	60
Forward Delay	5
Filter Aging Timer	300

Submit

Bridge Port Table    Bridge Lookup Table

From this screen, you may view the parameters described below.

**Enable** Enables or disables Bridging capability.  
Values: Enable, Disable  
Default: Disable

**Group Multicast MAC Address** MAC Address recognized by the Bridge as the group address for the Bridge Protocol Data Unit (BPDU) transfer between bridges.  
Values: Any valid Group Multicast MAC Address  
Default: 0180C2000000

**Bridge ID** Consists of a bridge priority and its own MAC Address.  
Values: 1–65535  
Default: 2

**Hello Timer** Specifies the BPDU broadcasting interval.  
Values: 1–65535 s  
Default: 10 s

**Max Age Timer** Specifies the length of time a bridge will consider the network topology held in memory as valid.  
Values: 1–65535 s  
Default: 60 s

**Forward Delay** Specifies the length of time to delay creation of a temporary loop in the network.  
Values: 1–65535 s  
Default: 5 s

**Filter Ageing Timer** Specifies the length of time an entry in the lookup table will be held if no traffic is received from the specified MAC Address.

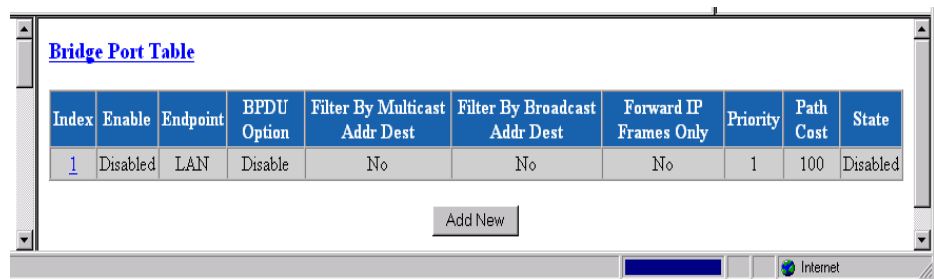
Values: 1–65535 s

Default: 300 s

The Bridge Details screen provides the following user-activated buttons:

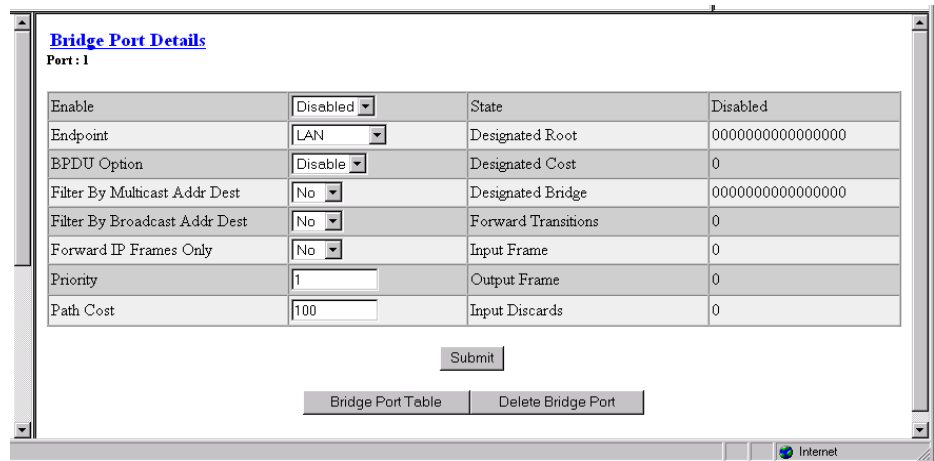
Button	Function
Bridge Port Table	Displays the Bridge Port Table screen (Figure 3.84) that lets the user access and configure the Bridge Port Details screen (Figure 3.85).
Bridge Lookup Table	Displays the Bridge Lookup Table screen (Figure 3.86) that contains all MAC Addresses learned by the Bridge.
Submit	Sets any values that have been changed.

**Figure 3.84** Bridge Port Table



The Bridge Port Table screen lets you view the parameters described below the Bridge Port Details screen. Clicking on a number in the “Index” column of the Bridge Port Table will bring up the Bridge Port Details screen, which displays, and, in some cases, lets you change, the parameters described below.

**Figure 3.85** Bridge Port Details



**Enable** Enables or disables Bridging on this port.

**Endpoint** Endpoint name.

- BPDU Option** Shows if BPDU packet will be sent and received on this port.
- Filter By Multicast Addr Dest** Filters multicast messages received on this port, which reduces the load on the WAN connection.
- Filter By Broadcast Addr Dest** Filters broadcast messages received on this port, which reduces the load on the WAN connection.
- Forward IP Frames Only** Setting this option to “Yes” specifies that only IP frames will be forwarded and all other frames will be filtered.
- Priority** Value of priority associated with this port. The lower the value, the higher the priority.
- Path Cost** Value of efficiency of the path to the port. A higher path cost indicates a lower link.
- State** If Enabled, reflects the state of the port. “Blocking” means there is no data transfer between LANs. “Listening” means the frames received from this port are filtered, but do not modify the Lookup Table. “Learning” means that while the port continues to look at frames without participating in data transfer, the frames received from the port will be used to update the Lookup Table. “Forwarding” means the port participates fully in data transfer and the frames received are used to update the Lookup Table.
- Designated Root** MAC Address of the designated root of the spanning-tree topology.
- Designated Cost** Associated Path Cost to the route for this port.
- Designated Bridge** Designated Bridge MAC Address.
- Forward Transmissions** Number of times this port has changed from any other state to a “Forwarding” state.
- Input Frame** Number of frames received.
- Output Frame** Number of frames transmitted.
- Input Discards** Number of frames discarded.

**Figure 3.86** *Bridge Lookup Table*

Address	Port	Status
00C0E6A000F0	1	Self

**Address** MAC Address learned and included in the forwarding table.

**Port** Port where the MAC Address was learned.

**Status** How the address was included in the forwarding table. (Currently, only “learned” will appear.)

## Simple Mail Transfer Protocol (SMTP)

Use the SMTP Details Screen (Figure 3.87) to configure the SMTP function of the WANsuite 6450. SMTP is used to forward notification of events to a user-definable list of up to five recipients. The even notification is sent as an e-mail in the following format:

From: WANsuite@verilink.com  
To: Event Receiver  
Subject: Even Notification

IP Address: 192.168.60.157  
System Up Time: 0 days, 01:20:02  
System Name:  
System Location:  
System Contact:

Reporting the following event:  
OOFS Threshold Exceeded, ifIndex 3, Count 5

The parameters associated with the SMTP Details screen are described below.

**Figure 3.87** SMTP Details Screen

Mail Server IP Address	0.0.0.0
Domain Name	
Mail From	
Recipient 1	
Recipient 2	
Recipient 3	
Recipient 4	
Recipient 5	

Submit

**Mail Server IP Address** IP address of the mail server to which notifications will be sent.

**Domain Name** Name of domain where the device resides (i.e., Verilink.com)

**Mail From** E-mail address of the device (WANsuite). While the device will not be able to retrieve e-mail from a service, the mail needs to have the “From” address filled in.



---

**NOTICE:** *There can be no blank space(s) in the “Mail From” address.*

---

**Recipient 1...5** E-mail addresses of recipients of event notifications (i.e., sales@verilink.com or support@verilink.com).

# Utilities

The options available under the Utilities branch of the navigation tree serve as utilities for upgrading your unit's software, managing access with passwords, and logging off the system.

## Upload/Save

The Upload/Save screen (Figure 3.88) lets you save a new configuration, upload a former configuration, or install software.

To save a unit's configuration, click on the "HTTP Save Configuration" button. The Web browser will prompt you for a file name where you will store configurations.

To upload a former configuration, click on the "Browse" button to select the file (which must have a ".cfg" extension), then click "HTTP Upload Configuration." The WANsuite unit will reset, after which it will use the uploaded configuration.

To install software, click on the "Browse" button to select the file you want installed. Then click on "HTTP Software Install."



**NOTICE:** *Make sure you allow sufficient time for the installation to occur. Canceling the installation before it has fully executed will result in the new software NOT being installed into the unit.*

Figure 3.88 Upload/Save Screen

HTTP Upload/Save	
File Name	<input type="text"/> Browse...
HTTP Upload Configuration    HTTP Save Configuration    HTTP Software Install	

Note : This upload may take several minutes to complete

TFTP Upload/Save	
TFTP Server IP Address	<input type="text" value="0.0.0.0"/>
File Name	<input type="text"/>
Status	Idle

Get File    Put File    Abort

## TFTP Configuration

A Trivial File Transfer Protocol (TFTP) service on a server can provide remote file access to the WANsuite 6450 to

- Update the firmware on a WANsuite unit
- Save the configuration setup of a WANsuite unit
- Restore a saved configuration setup to a WANsuite unit

To transfer a file to or from a TFTP server from a WANsuite unit, you must indicate the TFTP server's IP address, the file name, and then perform a Get operation to receive a file from the server, or a Put operation to send a file to the server. The file name and its extension determine the type of file transferred.

The table below shows the possible file operations.

Operation	Filename Extension	Action
Update Application Firmware	.CHX or .HEX	Get
Update Boot Firmware	.HEX	Get
Save Configuration Setup	.CFG	Put
Restore Configuration Setup	.CFG	Get

Note that when updating the application software using a .HEX file, the filename should have the form xxAPxxxx.HEX; the AP indicates the file is an application load. When updating the boot software, the filename should have the form xxWBxxxx.HEX; the WB indicates the file is a boot load.

## Password

The Password Details screen (Figure 3.89) is used to modify the password that restricts access to the Web Server interface.

Acceptable characters for use in a password are digits 0–9 and letters A–Z and a–z, for a total of 62 distinct characters.

**Figure 3.89** Password Details Screen

The screenshot shows a web browser window titled "Password Details". It contains the following elements:

- Two text input fields: "New Password:" and "Confirm Password:".
- A note: "Note: Password is case sensitive and must be no more than 10 characters from the following set: (A-Z, a-z, 0-9, #!\$@%&^\*0=-\_+;,:/[]~{} )".
- A warning: "Changing password will perform a Log Out and require a Log In to continue."
- Two buttons: "Change Admin Password" and "Change Read Only Password".
- A "Password Lockout" section with a dropdown menu set to "Disable" and a "Lockout Status" field showing "Disabled".
- A "Submit" button at the bottom.

To change either the Admin or Read-Only password, you must enter it once in the New Password field and then re-enter the same password in the Confirm Password field. After entering the new password in both these fields, click the “Change Admin Password” or the “Change Read Only Password”

button to update and establish the new password. When enabled, the Password Lockout feature denies Login after five unsuccessful attempts.



---

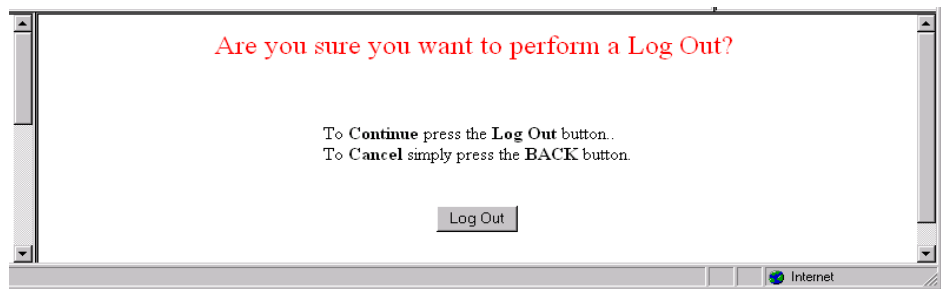
**NOTICE:** *Remember that passwords are case-sensitive. When logging on, password must be entered exactly as it was programmed.*

---

## Log Out

The Log Out screen (Figure 3.90) is used to log the current user off of the Web Server.

**Figure 3.90** *Log Out Screen*



The Log Out function is only available after user password protection has been set. You will be automatically logged out of the system 1 hour after you log on using a password to gain access; after this, you will be required to enter the password to gain write access.



# VT100 INTERFACE

## Introduction

---

This chapter describes the menus and options associated with the WANsuite 6450's VT100 interface. You can access the VT100 interface locally via the Supervisory port or remotely through a TELNET session.

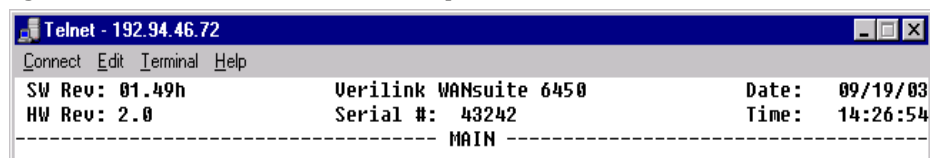
To access the VT100 screens locally, verify the Supervisory type is "tty" and the Supervisory port speed matches the terminal emulation program that's being used. The default for the Supervisory Port is 19200, 8, N, 1. (Port speeds supported include the following: 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.)

You can access the VT100 interface remotely by opening a TELNET session, entering the unit's IP Address, and connecting to the unit. All screens in this chapter were captured during a TELNET session.

## Screen Components

The VT100 terminal screens have components common to all screens (see Figure 4.1 below). These components include the device type (in the example below, Verilink WANsuite 6450), which is centered on the screen, the software and hardware revision numbers (upper left), the date and time (upper right), the menu title ("Main" in the figure below), and the serial number under which the unit is operating.

**Figure 4.1** VT100 Terminal Screen Components



## Cursor Controls

The VT100 interface uses a blinking cursor to select various menus and then to select sub-menus and/or fields within those menus. You can navigate using

this cursor in different ways, depending on the program you use. Most programs allow use of the “Tab” key and the “Shift+Tab” keys. Others allow use of the arrow keys.



---

**NOTICE:** If you are using Hyperterm and are unable to use your arrow keys, access the pull-down menu under “Terminal,” click on “Preferences,” and be sure the “VT100 Arrows” box is checked.

---

For keyboards that do not have these standard keys or have only some of them, an alternative set of cursor control commands is provided. Perform each command by pressing a letter key while holding down the “Ctrl” key. You may use the alternative commands and keyboard commands listed below interchangeably at your discretion.

Keyboard Command	Alternative Command
Left Arrow	Ctrl+S
Right Arrow	Ctrl+D
Up Arrow	Ctrl+E
Down Arrow	Ctrl+X
Backspace	Ctrl+H
Delete	Ctrl+Z

You can navigate further within a menu as described below.

## Field Types

Each menu screen is composed of fields. The two basic field types are user-selectable (most of these are in brackets or parentheses) and display-only (no brackets or parentheses). If you can move the highlighted cursor to a field, that field is user-selectable; all other fields are display-only. User-selectable fields are those in which you can make changes or execute commands. To save changed parameters, press the “Enter” key while on any user-selectable field or link to a submenu (screen). If you make changes to a screen and then “Esc” out of the screen, you will see a prompt at the bottom of the screen: “Save Changes (Y) or Discard Changes (N).” To save changes, press “Y” or “y”; to discard changes, press “N” or “n” or “Esc.” If the VT100 session times out, you will be logged off without the unit’s having saved any changes.

Fields enclosed in brackets [ ] offer a list of selections from which to choose. The selections may be made by pressing your Spacebar to “toggle” between choices. Each time the Spacebar is pressed, a new item appears. When the item you wish to choose is displayed, press the “Esc” key to save it.

Fields enclosed in parentheses ( ) are manipulated by one of the following two methods. The first is to press the “Enter” key to simply execute the function. The most common type of field in parentheses accepts typed input in the form of letters and/or numbers. Typing characters when the field is highlighted causes the current entry to be replaced by the new characters. To

edit an existing entry rather than replace it, press the right arrow key to move the cursor to the point that needs editing. You may insert characters or delete them. Typed data must always be inserted rather than typed over. If the field is full, you must first delete at least one character before you can add another.

The screen captures throughout this chapter show only the configuration portion of the screen, except in the case of the Main Menu, which shows the screen components that will appear at the top of all screens.

The lower right corner of each screen displays whether or not a “Save and Restart” is necessary when parameters are changed on the currently displayed screen.



---

**NOTICE:** *The data on VT100 screens is automatically refreshed every 5 seconds. You may also press Ctrl+U to redisplay the screen.*

---

## Menu Structure

The Main Menu screen (shown in Figure 4.2) lists the functional user-accessible menus. To activate a specific menu, tab to it (or use your arrow keys) and press “Enter.” To exit this or any subsequent menu, press the “Esc” key. If you exit the Main menu, the terminal interface program terminates. This is a valid way to end a session. When you exit any menu other than the Main menu, you will be returned to the previous screen.

**Figure 4.2** *VT100 Main Menu Screen*

```
Telnet - 192.94.46.72
Connect Edit Terminal Help
SW Rev: 01.49h      Verilink WANSuite 6450      Date: 09/19/03
HW Rev: 2.0        Serial #: 43242                Time: 14:26:54
-----
                               MAIN
                               -----
                               System
                               Interfaces
                               Services
                               Applications

                               Save & Restart
                               Not Needed
```



---

**CAUTION:** *If you do not enter a keystroke for 10 minutes, the terminal interface logs off automatically.*

---

# System Screen

The first option on the Main menu screen is the System screen (Figure 4.3). This screen lets you view and set specific information about the unit in service.

**Figure 4.3** *System Screen*

```

----- SYSTEM -----
Contact      (████████████████████)
Name        ( )
Location    ( )
FrameStart ID (000 )
Operating Mode Ethernet

( )
( )
( )

Time      (14:25:05)
Date      (09/19/03)

New Admin Password  (*****) Password Lockout [Disable]
New Read Only Password (*****) Lockout Status Disabled
(Clear Password Lockout)

(Maintenance Reset)
(Save & Restart)

Ctrl^R PageUp           Save & Restart
Ctrl^C PageDown        Not Needed
  
```

The System screen displays the fields shown below.

Field	Description
Contact	Read/write field used to store the name of a point-of-contact for system failure.
Name	Read/write field that holds the unit's name.
Location	Read/write field that holds the unit's location.
FrameStart ID	Not used for ATM. Read/write field that holds the unit's ID that uniquely identifies the unit and is used in the FrameStart applications.
Operating Mode	Displays most recently executed Maintenance Reset option.
Blank Fields	Read/write fields for user-specific labels and values. Information resides in non-volatile memory.
Time	Read/write field that holds the unit's internal time setting in standard 24-hour HH:MM:SS format.
Date	Read/write field that holds the unit's internal time setting in standard 24-hour MM:DD:YY format.
New Admin Password New Read Only Password	Lets you modify your Admin or Read-only password by typing in a new password. Acceptable characters for use in a password are digits 0-9 and letters A-Z and a-z, for a total of 62 distinct characters.

Field	Description
Password Lockout	Enables or disables the Password Lockout function, which, when enabled, locks out access to the Web or telnet interface if user attempts five invalid passwords in a row. The Supervisory port will not cause a lockout of the Web or telnet interface.
Lockout Status	Shows whether the Password Lockout function is enabled or disabled.

The System screen displays two user-selectable prompts: Maintenance Reset, and Save and Restart. Both are described in the paragraphs below.

## Maintenance Reset

### Maintenance Reset

Use this button to perform a Maintenance Reset. All configurations will be lost and the unit will be set back to an initial factory configuration. The options for a Maintenance Reset are shown in the table below.

Configuration Choice	RFC 1483 Encapsulated Data	IP Encapsulated in ATM	Serial HDLC Encapsulated in ATM	T1 CBR Channels	E1 CBR Channels	Serial CBR Channels
Ethernet	Yes	Yes	No	None	None	None
Serial HDLC	Yes	No	Yes	None	None	None
E1 CCS*	Yes	Yes	No	None	1–31	None
E1 CAS	Yes	Yes	No	None	1–15, 17–31	None
Unframed E1	Yes	Yes	No	None	0–31	None
T1 ESF	Yes	No	Yes	1–24	None	None
T1 SF	Yes	No	Yes	1–24	None	None
T1 ESF CAS/RBS	Yes	No	Yes	1–24	None	None
T1 SF CAS/RBS	Yes	No	Yes	1–24	None	None
Unframed T1	Yes	No	Yes	1–24**	None	None
Serial CES	Yes	Yes	No	None	None	1–31
Unstructured Serial CES	Yes	Yes	No	None	None	0–31
PPoA-IPCP	No	Yes	No	None	None	None
PPoA-NAPT	No	Yes	No	None	None	None

\* Factory default configuration

\*\* Unframed T1 CES service uses an additional 8 kbps of bandwidth for framing

All the factory configurations set up an ATM service on the Network port with one configured virtual channel (VPI=0, VCI=32). Management data received on this channel (either WEB or SNMP) will be processed at the unit

if it is encapsulated using RFC 1483 and directed to the unit's IP address. (A Maintenance Reset will not change the unit's IP address.)

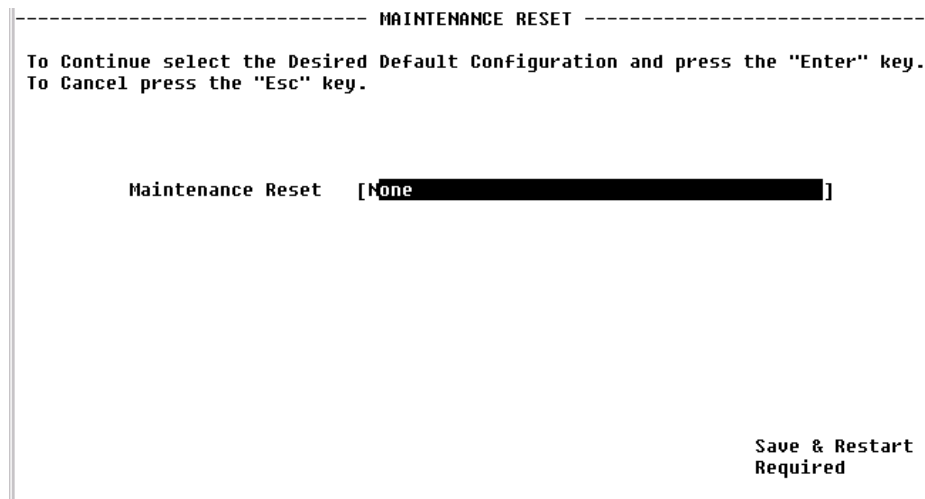
The Serial HDLC configuration and the T1 ESF configuration will also accept PPPoA encapsulated data and deliver it to the Serial port.

The T1 SF, T1 ESF CAS/RBS, T1 SF CAS/RBS, Unframed T1, Serial CES, and Unstructured Serial CES configurations set up a CES service between the Network port and the T1/E1 CBR port or the Serial port using VPI=0, VCI=33. The T1 options configure the CBR port for the desired framing mode, and configure the CES service for 24 channels. For unframed T1 service, the CES service provides 1.544 Mbps of bandwidth for the service (1.536 Mbps for the T1 channels and 8 kbps for framing). The E1 configurations set up the CBR port to run E1 and have 30, 31, or 32 channels delivered to the CES service. The Serial CES configurations set up the CBR port to run E1 CCS or Unframed E1, but allocates all 31 or 32 channels to the Serial port.

The PPOA-IPCP and PPPoA-NAPT set up a PPP connection over ATM using the VPI=0, VCI=32. The resulting PPP interface then uses PPP negotiation to obtain the IP address, mask, and DNS address. After successful negotiation, the DHCP server starts on the Ethernet Lan. For PPPoA-IPCP, the negotiated IP address is applied to the LAN, whereas in the case of PPPoA-NAPT, the negotiated IP address is applied to the WAN.

Selecting the "Maintenance Reset" field will display a selection screen where you can toggle (using the spacebar) among available configurations as shown in Figure 4.4.

**Figure 4.4** Maintenance Reset Screen



## Save and Restart

Selecting "Save and Restart" will display a confirmation menu as shown in Figure 4.5. Select "yes" to save the current configuration settings and proceed with the restart.

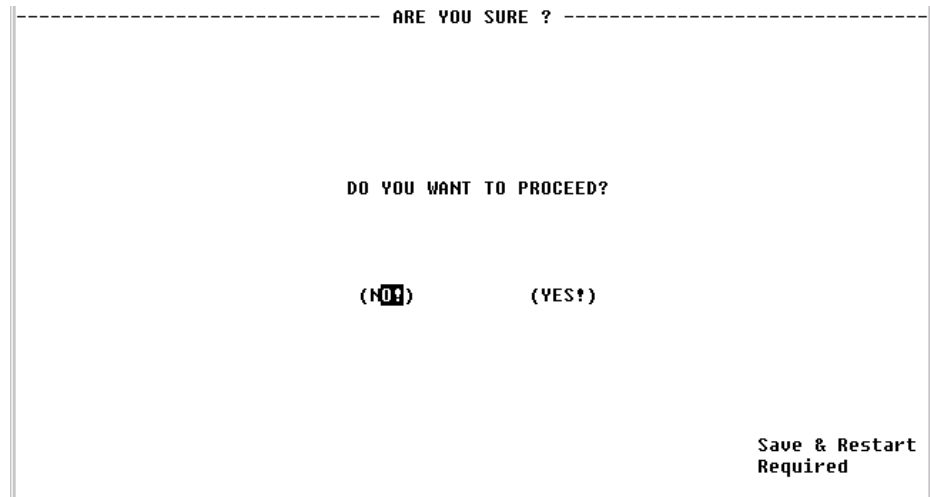


---

**NOTICE:** Performing a “Maintenance Reset” or a “Save and Restart” will terminate communications with the unit. Refresh (by pressing “Ctrl+U”) after approximately 10 seconds to restore communications.

---

**Figure 4.5** Confirmation Screen

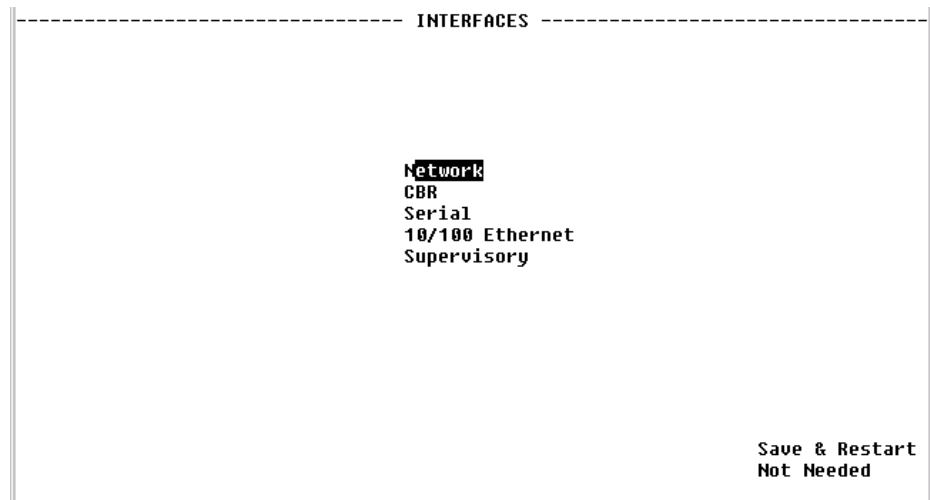


## Interfaces

---

As shown on the Interfaces screen (Figure 4.6), the WANsuite 6450 has five interfaces: Network, CBR, Serial, Ethernet, and Supervisory. Each of these is described in detail below.

**Figure 4.6** Interfaces Screen



## Network

The Network screen (Figure 4.7) lets you view and make changes to the Network interface's configuration.

**Figure 4.7** Network Screen

Network			
Unit Type	[TU-R]	Pair-1 Mode	Data Data Mode
		Pair-2 Mode	Idle
			No Activity
Discovered Repeaters	0	EOC In	24761
Line Rate	2312000	EOC Out	24761
Maximum Line Rate	2320000		
Transmission Mode	Annex-B		
Expected Repeaters	[0]		
Span Configuration	[DEFVAL		]
Span Alarm Configuration	[DEFVAL		]
(Configuration Profiles)			
(Alarm Profiles)			
(Span Endpoints)			
		Save & Restart	Not Needed

The Network screen parameters are described in the following paragraphs.

**Unit Type** Selects the unit type. TU-R represents a CPE terminal unit; TU-C represents a CO terminal unit.  
 Values: TU-R, TU-C  
 Default: TU-R

**Discovered Repeaters** Displays the number of discovered repeaters in this span.

**Line Rate** Displays the actual negotiated line rate.

**Maximum Line Rate** Displays the maximum physical line rate with respect to the current span configuration.

**Transmission Mode** Displays the actual transmission mode (Annex-A or Annex-B).

**Expected Repeaters** Provisions the number of repeaters in the selected span.  
 Values: 0–8  
 Default: 0 (zero)

**Span Configuration** Represents a span configuration profile in the Span Configuration Profile Table, which applies to this span. By default, this object will have the value “DEFVAL” (the index of the default profile).  
 Values: User Span Profile 1, User Span Profile 2, DEFVAL (Default Value)  
 Default: DEFVAL

**Span Alarm Configuration** Represents an Alarm configuration profile in the Endpoint Alarm Configuration Profile Table. The alarm threshold configuration in the referenced profile will be used by default for all segment endpoints in this span. Individual endpoints may override this profile by explicitly specifying



some other profile in the table. By default, this object will have the value 'DEFVAL' (the index of the default profile).

Values: User Alarm Profile 1, User Alarm Profile 2, User Alarm Profile 3, DEFVAL (Default Value)

Default: DEFVAL

**Pair 1 Mode** Represents the status and details status of the span for two-wire operation.

**Pair 2 Mode** Represents the status and details status of the span for four-wire operation. This mode is not supported by the WANsuite 6450.

**EOC In** Displays the number of messages received on the Embedded Operations Channel.

**EOC Out** Displays the number of messages transmitted on the EOC Embedded Operations Channel.

The Network screen provides the user-activated prompts described below.

Prompt	Function
Configuration Profiles	Displays the three configuration profiles that can be used.
Alarm Profiles	Displays the four alarm profiles that can be used.
Span Endpoints	Lists the currently available span endpoints.

## Configuration Profiles Screen

Selecting the “Configuration Profiles” prompt on the Network screen will display the screen shown in Figure 4.8.

**Figure 4.8** Configuration Profiles Screen

```

----- CONFIGURATION PROFILES -----
<Configuration Name> Wire Mode   Data      Data      Remote  Trans Mode
DEFVAL                Two-Wire  192000    2312000   Enabled Annex-B
User_Span_Profile_1  Two-Wire  192000    2312000   Enabled Annex-B
User_Span_Profile_2  Two-Wire  192000    2312000   Enabled Annex-B

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Not Needed
  
```

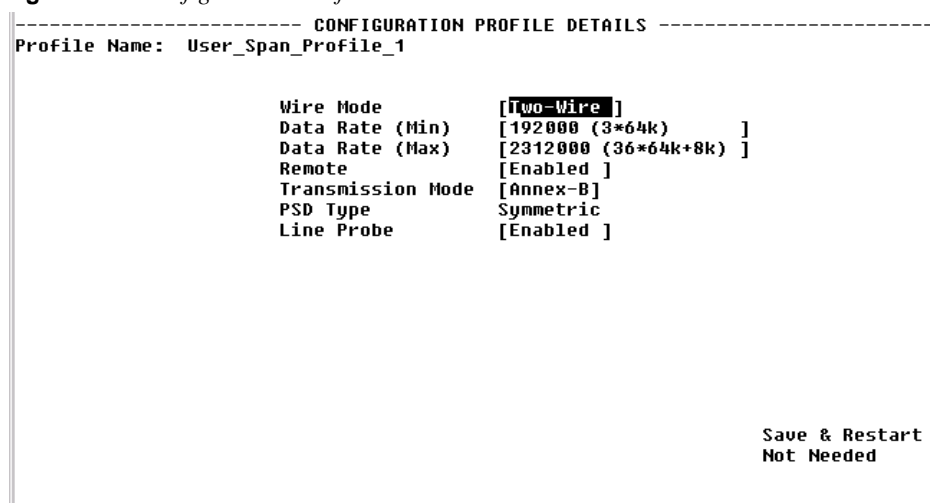
This screen displays the following information for each available Span Configuration Profile:

**Configuration Name** Name of the defined span configuration profile.

- Wire Mode** Type of wire interface used by the span.
- Data Rate (Min)** Minimum attainable data rate in the span.
- Data Rate (Max)** Maximum attainable data rate in the span.
- Remote** Indicates whether the option to span remote is enabled or disabled.
- Trans Mode** Regional setting of the span. The possible settings are Annex-A (ITU-T G.991.2), Annex-B (ITU-T G.991.2).

Select the particular profile for which you want to see details by selecting from the <Configuration Name> on the Configuration Profile screen and then pressing the “Enter” key. The Configuration Details screen (Figure 4.9) supports the overall configuration of the spans.

**Figure 4.9** Configuration Profile Details Screen



This screen lets you configure or change the following information about the selected configuration profile:

- Profile Name** A 32-character string that identifies a Profile Name in the Span Profile table. Each entry represents the complete span in an ATM line.
- Wire Mode** Displays the type of wire interface used by the span). The WANsuite 6450 supports only the two-wire mode.
- Data Rate (Min)** Sets the minimum attainable data rate in the span.
- Data Rate (Max)** Sets the maximum attainable data rate in the span. Note that the line rate will be 8 kbps above the data rate.
- Remote** Enables/disables support for remote management of the units in an SHDSL line from the STU-R via the EOC.  
 Values: Enabled, Disabled  
 Default: Enabled

**Transmission Mode** Sets the regional setting of the span represented as a bit-map of possible settings.

Values: Annex-A (*ITU-T G.991.2*), Annex-B (*ITU-T G.991.2*)

Default: Annex-B

Default: Annex-B



**NOTICE:** *When the WANSuite 6450 is operating with Unit Type set to TU-R, it supports Annex-A or Annex-B. The configuration of the TU-C unit determines the actual transmission mode used.*

**PSD Type** Sets the use of symmetric Power Spectral Density (PSD) mask.

Values: Symmetric

Default: Symmetric

**Line Probe** Enables or disables rate adaptation line probe.

Values: Enabled, Disabled

Default: Enabled

To change any configuration profile parameter, enter the desired value/information in a field or select the desired parameter from one of the pull-down lists, and then press the “Esc” key.

## Alarm Profiles Screen

Selecting the “Alarm Profiles” prompt on the WANSuite 6450’s Network Config screen will display the screen shown in Figure 4.10.

**Figure 4.10** *Alarm Profiles Screen*

```
----- ALARM PROFILES -----
<Alarm Profiles>
DEUAL
User_Alarm_Profile_1
User_Alarm_Profile_2
User_Alarm_Profile_3

      Loop   SNR
      Atten  Margin  ES  SES  CRC  LOSWS  UAS
      0      0      1  1   1   1      1
      0      0      1  1   1   1      1
      0      0      1  1   1   1      1
      0      0      1  1   1   1      1

Ctrl^R PageUp
Ctrl^C PageDown

                        Save & Restart
                        Not Needed
```

The Alarm Profiles screen displays the current values of SHDSL alarm thresholds. Information is displayed for the following alarm parameters:

**Alarm Profiles** Name associated with this Alarm profile.

**Loop Atten** Loop attenuation threshold.

- SNR Margin** Signal-to-Noise Ratio margin threshold.
- ES** Errored Seconds threshold.
- SES** Severely Errored Seconds threshold.
- CRC** Cyclic Redundancy Check anomalies threshold.
- LOSWs** Loss of Sync Word Second threshold.
- UAS** Unavailable Seconds Threshold.

### *Alarm Profile Details Screen*

Select from the <Alarm Profiles> column on the above screen to display a screen similar to the one shown in Figure 4.11. The table on this screen lets you configure the alarm threshold values to be used for the selected alarm profile.

**Figure 4.11** Alarm Profile Details Screen

ALARM PROFILE DETAILS		
Profile Name: User_Alarm_Profile_1		
Type	Threshold	
Loop Attenuation	( 0 )	
SNR Margin	( 0 )	
ES	( 1 )	
SES	( 1 )	
CRC	( 1 )	
LOSWs	( 1 )	
UAS	( 1 )	
Save & Restart Not Needed		

- Profile Name** Displays the name associated with this Endpoint Alarm profile.
- Loop Attenuation** Sets the loop attenuation alarm threshold. If the current value reaches or exceeds this threshold, a crossing trap is generated. A value of 0 (zero) disables the trap.
- SNR Margin** Sets the Signal-to-Noise Ratio margin alarm threshold. When the current SNR value reaches or drops below this threshold, a crossing trap is generated. A value of 0 (zero) disables the trap.
- ES** Sets the threshold for the number of Errored Seconds within any given 15-minute performance data collection interval. If the value of ES in a particular 15-minute collection interval reaches/ exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.

- SES** Sets the threshold for the number of Severely Errored Seconds within any given 15-minute performance data collection interval. If the value of SES in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- CRC** Sets the threshold for the number of Cyclic Redundancy Check anomalies within any given 15-minute performance data collection interval. If the value of CRC anomalies in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- LOSWS** Sets the threshold for the number of Loss of Sync Word Seconds within any given 15-minute performance data collection interval. If the value of LOSW in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.
- UAS** Sets the threshold for the number of Unavailable Seconds within any given 15-minute performance data collection interval. If the value of UAS in a particular 15-minute collection interval reaches/exceeds this value, a trap is generated. One trap will be sent per interval per endpoint. A value of 0 (zero) disables the trap.

## Span Endpoints Screen

Selecting the “Span Endpoints” prompt on the WANsuite 6450 Network screen will display the screen shown in Figure 4.12.

**Figure 4.12** *Span Endpoints Screen*

```

----- SPAN ENDPOINTS -----
                                <Unit>   Side      WirePair
                                TU-C     Customer  Wire Pair 1
                                TU-R     Network   Wire Pair 1

Ctrl1^R PageUp
Ctrl1^C PageDown

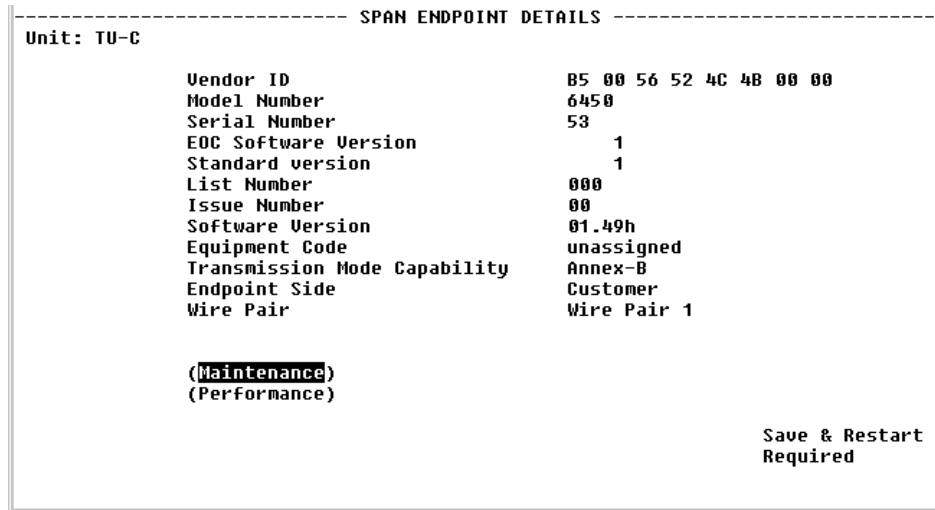
                                Save & Restart
                                Not Needed

```

This screen displays each endpoint of the span. If the SHDSL link is not up, only the local side of the span is displayed. The EOC channel is used to access the remote end unit

The Span Endpoints Details screen (Figure 4.13, accessed by selecting from the <Unit> column) supports retrieval of unit inventory information available via the EOC from units on an SHDSL line, and provides details regarding the parameters listed below.

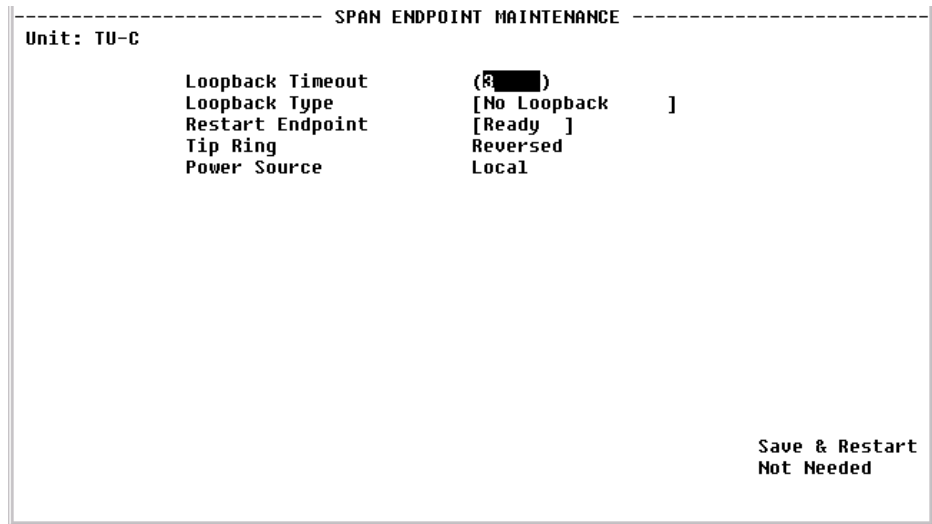
**Figure 4.13** *Span Endpoint Details Screen*



- Vendor ID** Vendor ID as reported in an Inventory Response message.
- Model Number** Vendor model number as reported in an Inventory Response message.
- Serial Number** Vendor serial number as reported in an Inventory Response message.
- EOC Software Version** Vendor EOC version as reported in a Discovery Response message.
- Standard Version** Version of the SHDSL standard implemented as reported in an Inventory Response message.
- List Number** Vendor list number as reported in an Inventory Response message.
- Issue Number** Vendor issue number as reported in an Inventory Response message.
- Software Version** Vendor software version as reported in an Inventory Response message.
- Equipment Code** Equipment code conforming to ANSI T1.213, Coded Identification of Equipment Entities.
- Transmission Mode Capability** Transmission mode capability of the SHDSL unit.
- Endpoint Side** Defines which direction the SHDSL port is pointing. Normal operation will use the TU-R configuration, and the endpoint will be "Network." When unit type is TU-C, endpoint will be "Customer."
- Wire Pair** Always "Wire Pair 1."

Selecting the “Maintenance” prompt from the Span Endpoint Details screen will display the screen shown in Figure 4.14. This table supports maintenance operations (e.g., loopbacks) to be performed on segment endpoints.

**Figure 4.14** *Span Endpoint Maintenance Screen*



The Span Endpoint Maintenance parameters are described below.

- Loopback Timeout** Specifies the timeout value in minutes for loopbacks initiated at this endpoint. A value of 0 disables the timeout.
- Loopback Type** Specifies loopbacks for the associated segment endpoint.  
Values: No Loopback, Normal Loopback  
Default: No Loopback
- Restart Endpoint** Enables the manager to trigger a soft restart of the SHDSL line at the associated segment endpoint. Set this object to “restart” to initiate a restart. A restart will occur after approximately 5 seconds.  
Values: Ready, Restart  
Default: Ready
- Tip Ring** Indicates the state of the tip/ring pair at the associated segment endpoint.
- Power Source** Indicates the DC power source being used by the associated unit.

Selecting the “Performance” prompt on the Span Endpoint Details screen will display the screen shown in Figure 4.15.

**Figure 4.15** *Span Endpoint Performance Screen*

SPAN ENDPOINT PERFORMANCE						
Unit:	TU-C	Wire Pair	1			
Status:	OK					
SNR Margin:	19					
Loop Attenuation:	0					
	Time	ES	CRC	LOSWS	SES	UAS
	Elapsed					
Summary		0	0	0	0	0
Current 15 Min.	260	0	0	0	0	0
Current Day	13760	0	0	0	0	0
<b>(15 Minute Intervals)</b>						
<b>(1 Day Intervals)</b>						
						Save & Restart Required

This screen displays information on the performance and error status of a span endpoint. This information is provided in summary form for complete totals and for the most recent 15 min period or most recent current day period.

**Status** Current state of the endpoint. This is a string indicating possible conditions. The various string components are as follows:

OK – There no defects on the line.

SNR – Indicates that the SNR margin has dropped below the alarm threshold.

Attenuation – Indicates that the loop attenuation has exceeded the alarm threshold.

LOSW – Indicates an LOSW alarm.

Loopback – A loopback is currently active at this Segment Endpoint.

**SNR Margin** Current Signal-to-Noise Ratio margin for this endpoint as reported in a Status Response/SNR message.

**Loop Attenuation** Current loop attenuation for this endpoint as reported in a Network or Customer Side Performance Status message.

**Time Elapsed** Total elapsed seconds in the current 15-minute interval.

**ES** Count of Errored Seconds on this endpoint since the unit was last restarted.

**CRC** Count of Cyclic Redundancy Check anomalies on this endpoint since the unit was last restarted.

**LOSWS** Count of Loss of Sync Word Seconds on this endpoint since the xU was last restarted.

**SES** Count of Severely Errored Seconds on this endpoint since the unit was last restarted.



**UAS** Count of Unavailable Seconds on this endpoint since the xU was last restarted.

### 15-Minute and 1-Day Intervals

Also included on this screen are prompts that, when selected, display the span endpoint performance summaries for 15-minute intervals and for 1-day intervals. These screens display only a summary of the errors (ES, SES, CRC, LOSWS, UAS) that have occurred on the span during the interval selected.

The 15-Minute Intervals table provides one row for each endpoint performance data collection 15-minute interval. The 1-Day Intervals screen provides one row for each endpoint performance data collection 24-hour interval.

## CBR



**CAUTION:** *The T1/E1 CBR port is not a standalone port. Connect the T1/E1 CBR port only to the "private" side of the network on the customer premises, never to the "public" side.*

The CBR screen (Figure 4.16) lets you view and make changes to the CBR interface's configuration as described below. In addition, this screen provides a table that displays error status and alarm thresholds for the CBR interface.

**Figure 4.16** CBR Screen

```

----- CBR -----
T1/E1 Framing      [E1 CCS      ] T1 Mode           [Short-Haul  ]
T1/E1 Line Coding  [HDB3        ] T1 Line Build Out {Long} [0 dB        ]
T1 PRM Enable      [Disable     ] T1 DSX Level {Short}  [0-110 feet  ]
T1 Zero Suppression [Disable     ] E1 CRC4 Mode       [Disable     ]

      Status      Alarm      Count      Threshold
ES      ---      OK         0          ( 45)
SES     ---      OK         0          ( 5)
LOSS   ---      OK         0          ( 5)
UAS    ---      OK         0          ( 0)
CSS    ---      OK         0          ( 5)
BPUS   ---      OK         0          ( 0)
OOF    ---      OK         0          ( 5)
AIS    ---      OK         0          ( 0)
RAS    ---      OK         0          ( 0)
Reset Timer
(Clear Alarms) (Performance)          Save & Restart
                                          Not Needed
  
```

**T1/E1 Framing** Selects the framing for the network side of the DSU/CSU.

Values: T1 ESF, T1 D4, E1 CCS, E1 CAS

E1 Unframed, T1 Unframed

Default: T1 ESF



---

**NOTICE:** *To set unit to Signaling mode, you must first configure the following: on the CBR Configuration screen (page 4-17), configure Framing, on the Channel Table Details screen (page 4-59), set “Rate” to 56k/SIG, and on the CES Service Details screen (page 4-54), configure AAL1 Format.*

---

**T1/E1 Coding** Sets the CBR interface line coding.

Values: HDB3, AMI, B8ZS

Default: B8ZS



---

**NOTICE:** *For a T1 CBR Maintenance Reset, the default is T1 ESF. The T1/E1 coding default is B8ZS.*

---

**T1 PRM** Lets you establish which performance messaging standard will be employed to initiate Performance Report Message (PRM) functions. Setting this field to “Enable” instructs the unit to use ANSI T1.403, which sends a PRM once every second. Setting this field to “Disable” instructs the unit to use AT&T TR54016, which provides performance reporting on request only.

Values: Disable, Enable

Default: Disable

**T1 Zero Suppress** Determines whether ones density insertion is activated after 15 zeros. This parameter is ignored if the Coding parameter is set to “B8ZS.”

Values: Disable, Enable

Default: Disable

**T1 Mode** As a T1, the unit will operate in either long-haul or short-haul mode.

Values: Short-Haul, Long-Haul

Default: Short-Haul

**T1/E1 Line Build Out** Sets the transmit Line Build Out (LBO) for the CBR interface.

Values: 0, -7.5, -15.0, -22.5 dB

Default: 0 dB

**T1 DSX Level** Specifies the T1 DSX output level.

Values: 0–110, 111–220, 221–330, 331–440, 441–550, 551–660, >661 ft

Default: 0–110 ft

**E1 CRC4 Mode** Provides line integrity detection to determine if bit errors are present on the line.

Values: Disable, Enable

Default: Disable

## Error Status and Alarm Thresholds Table

The unit can be programmed to generate an alarm condition based on a specific level of performance degradation. The CBR screen presents a table that provides current error status and alarm threshold information.

Acceptable alarm thresholds are set for periods of 15 minutes (900 seconds) and sampled every second. The error types listed in the following paragraphs can be preset to a value between 0 and 900 seconds. Setting a field to “0” (zero) disables the alarm on that statistic. To effectively disable alarm reporting, set all fields to “0” (zero).

The 15-minute time frame is not based on the TR 54016 or T1.403 interval boundaries, but is a time window based on the accumulated counts over the previous fifteen 1-minute intervals. In all cases, if the number of actual network errored seconds in the previous 15 minutes reaches the preset threshold for the specified error type, an alarm condition is declared.

The four columns of the status table are as follows:

- **Status:** Displays the current status of the CBR port.
- **Alarm:** Displays the alarm value of the network port. The unit declares an alarm as soon as the count exceeds the threshold set.
- **Count:** Displays the number of events or occurrences of this statistic that have been detected.
- **Threshold:** Displays a read/write field that can be set to a desirable threshold.

The table provides error status and alarm threshold information for the following error parameters:

- ES** Sets the Errored Seconds (ES) threshold. An ES is a 1-second period in which at least one logic error occurred. The default value is 45 seconds.
- SES** Sets the Severely Errored Seconds (SES) threshold. An SES is a 1-second period in which at least 320 CRC errors or one Out-of-Frame (OOF) error occurred. The default value is 5 seconds.
- LOSS** Sets the Loss of Signal Seconds (LOSS) threshold. A LOSS is 1-second period in which the T1/E1 received signal is interrupted. The default value is 5 seconds.
- UAS** Sets the Unavailable Seconds (UAS) threshold. A UAS is a 1-second period in which consecutive severely errored seconds cause an unavailable state. The default is 0 seconds (Disabled).
- CSS** Sets the Controlled Slip Seconds (CSS) threshold. The default is 0 seconds (Disabled).
- BPVS** Sets the Bipolar Violation Errored Seconds (BPVS) threshold. A BPVS is a 1-second period in which at least one bipolar violation occurred. The default is 0 seconds (Disabled).
- OOFS** Sets the Out of Frame Seconds (OOFS) threshold. An OOFS is a 1-second period in which a frame sync loss occurred. The default value is 5 seconds.

**AISS** Sets the Alarm Indication Signal Seconds (AISS) threshold. An AIS is a 1-second period when unframed all ones are received. The default is 0 seconds (Disabled).

**RAS** Sets the Remote Alarm Seconds (RAS) threshold. An RAS is generated by the terminal equipment when an improper signal is received from the facility (or upon receipt of unframed all ones). The default is 0 seconds (Disabled).

**Reset Timer** Sets the Reset Timer threshold. This field is the contiguous number of seconds that an alarm parameter must be clear before the alarm is reset. Applicable values range from 000 through 900. A value of “000” means the alarm will never be reset.

The CBR screen provides the user-activated buttons described below.

Button	Function
Clear Alarms	Resets the alarm conditions and counts to zero.
Performance	Displays a current count of the number of error events that have occurred over the past 24 hours and the past 30 days.



---

**CAUTION:** *Performance data will be lost upon power cycle or after performing a Maintenance Reset/Restart.*

---

## Performance Screens

The “Performance” prompt near the bottom of the Network screens displays a Performance 24 Hour screen (Figure 4.17), which provides a summary of the error events that have occurred during each interval of the past 24 hours. In addition to the parameters already defined on the *Error Status and Alarm Thresholds Table* on page 4-18, the following parameters are included on the Performance screens.

**BES** Sets the Bursty Error Seconds (BES) threshold. A BES is a 1-second period during which at least more than one but fewer than 320 CRC6 errors occurred.

**LOFC** The Loss of Frame Count (LOFC) represents the number of time a loss of frame is declared. A loss of frame is declared after 2.5 seconds of continuous loss of signal or OOF. This parameter is on the T1 Performance 24 Hour screen only.

**CRCES** Sets the Cyclic Redundancy Check Errored Seconds (CRCES) threshold. A CRC is a method of confirming the integrity of received data.

Figure 4.17 CBR T1 Performance 24 Hour Screen

```

----- T1 PERFORMANCE 24 HOUR -----
Interface:  CBR

      (Performance 30 Day)      (Clear Statistics)

<Period>    RAS  ES  BES  SES  UAS  LOFC  CSS  CRCES  ODFS  LOSS  AISS  BPUS
Summary      0   0   0   0 86400   0   0   0 86400 86400   0   0
Current      0   0   0   0   46   0   0   0   46   46   0   0
Interval 1   0   0   0   0  900   0   0   0  900  900   0   0
Interval 2   0   0   0   0  900   0   0   0  900  900   0   0
Interval 3   0   0   0   0  900   0   0   0  900  900   0   0
Interval 4   0   0   0   0  900   0   0   0  900  900   0   0
Interval 5   0   0   0   0  900   0   0   0  900  900   0   0
Interval 6   0   0   0   0  900   0   0   0  900  900   0   0
Interval 7   0   0   0   0  900   0   0   0  900  900   0   0
Interval 8   0   0   0   0  900   0   0   0  900  900   0   0
Interval 9   0   0   0   0  900   0   0   0  900  900   0   0
Interval 10  0   0   0   0  900   0   0   0  900  900   0   0
Interval 11  0   0   0   0  900   0   0   0  900  900   0   0
Interval 12  0   0   0   0  900   0   0   0  900  900   0   0
Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown          Not Needed
  
```

Figure 4.18 CBR E1 Performance 24 Hour Screen

```

----- E1 PERFORMANCE 24 HOUR -----
Interface:  CBR

      (Performance 30 Day)      (Clear Statistics)

<Period>    RAS  ES  BES  SES  UAS  CSS  CRCES  ODFS  LOSS  AISS  BPUS
Summary      0   0   0   0 86400   0   0 86400 86400   0   0
Current      0   0   0   0  129   0   0  129  129   0   0
Interval 1   0   0   0   0  900   0   0  900  900   0   0
Interval 2   0   0   0   0  900   0   0  900  900   0   0
Interval 3   0   0   0   0  900   0   0  900  900   0   0
Interval 4   0   0   0   0  900   0   0  900  900   0   0
Interval 5   0   0   0   0  900   0   0  900  900   0   0
Interval 6   0   0   0   0  900   0   0  900  900   0   0
Interval 7   0   0   0   0  900   0   0  900  900   0   0
Interval 8   0   0   0   0  900   0   0  900  900   0   0
Interval 9   0   0   0   0  900   0   0  900  900   0   0
Interval 10  0   0   0   0  900   0   0  900  900   0   0
Interval 11  0   0   0   0  900   0   0  900  900   0   0
Interval 12  0   0   0   0  900   0   0  900  900   0   0
Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown          Required
  
```

Select the “Performance 30 Day” prompt on the above screen to see a detailed summary of the error events that have occurred during each interval of the past 30 days (Figure 4.19).

**Figure 4.19** CBR T1 Performance 30 Day Summary Screen

```

----- T1 PERFORMANCE 30 DAY SUMMARY -----
Interface:  CBR

  (Clear Statistics)

<Period>      ES      UAS      OOFs      LOSS      AISS
Summary       0      85773    85773     85773     0
Day 1         0      85773    85773     85773     0

Ctrl^R PageUp                               Save & Restart
Ctrl^C PageDown                              Not Needed
  
```

**Figure 4.20** CBR E1 Performance 30 Day Summary Screen

```

----- E1 PERFORMANCE 30 DAY SUMMARY -----
Interface:  CBR

  (Clear Statistics)

<Period>      ES      UAS      OOFs      LOSS      AISS
Summary       0      85773    85773     85773     0
Day 1         0      85773    85773     85773     0

Ctrl^R PageUp                               Save & Restart
Ctrl^C PageDown                              Required
  
```




---

**NOTICE:** Any changes to settings in the channel map require a “Save and Restart” for them to take effect.

---

## Serial

The Serial screen (Figure 4.21) lets you view and make changes to the unit’s Serial interface configuration as described in the paragraphs below. To make changes to any Serial parameter, simply set the parameter to the desired selection and press the “Esc” key.

**Figure 4.21** *Serial Screen*

Serial			
Type	[V.35]	Flow Control	[None]
Mode	[DCE]	Character Size	[Eight]
Packet Rate	[2048 Kbps]	Parity	[None]
Bundling	[Contiguous]	Stop Bit	[1]
Start Channel	( 1)	RTS	[Normal]
# of Channels	( 0)	RTS/CTS Delay	[Normal]
Format	[Sync]	CTS	[Forced True]
Tx Clock	[Internal]	DCD	[Forced True]
Tx Invert Clock	[Disable]	DSR	[Forced True]
DTR Alarm Control	[Disable]		
DTR Alarm Status	OK		
Cur. Pin Status: DTR:OFF DSR:ON RTS:OFF CTS:ON DCD:ON Mode:DCE			
Save & Restart Not Needed			

**Type** Selects the type of interface (based on its electrical signal characteristics) used by the equipment connected to the Serial port.

Values: V.35, V.36, RS-232, EIA-530, and X.21

Default: V.35



**NOTICE:** *V.35 requires the use of an optional cable. Refer to Connector Pin Assignments on page A-6 for ordering information.*

**Mode** By default, the Serial port serves as a DCE port. However, the Serial port can serve as a DTE port.

If the Serial port connects to a DTE device (such as a FRAD or a router), the Mode parameter must be set to “DCE.” If this port connects to a DCE device (such as a DSU/CSU), this parameter must be set to “DTE.”

Values: DCE, DTE

Default: DCE



**NOTICE:** *DTE mode requires the use of an optional DTE cable. Refer to Connector Pin Assignments on page A-6 for ordering information.*



**NOTICE:** *When you configure the Serial port for CES, you must set the port mode to DCE.*

**Packet Rate** Packet Rate must be configured to the desired port speed (in bits per second). This parameter is only applicable when the Serial port service type is *not* CES.

Values: 64–2304 kbps

Default: 2048 kbps

**Bundling** Selects whether the DTE channel assignment is made as a “Contiguous” group or as “Alternate” channels. Selecting “Alternate” ensures ones density. Because the unit allows individual channels to be configured for a service, a value of “Arbitrary” will be returned for this parameter if the current channel allocation is not contiguous or Alternate. The “Arbitrary” value can only be supplied by the unit – it cannot be set by the user.

Values: Contiguous, Alternate, Arbitrary

Default: Contiguous



---

**NOTICE:** *Because “Alternate” Bundling assigns every other channel, only half the channels are available.*

---

**Start Channel** Selects the starting channel in the CES Channel Table. (Refer to *Channel Table Details Screen* on page 4-58.) Starting with the specified channel, the unit automatically assigns the channels that follow.

Values: 1–24 for T1; 0–31 for E1

Default: 1

**# of Channels** Specifies the number of channels to be assigned to CES.

Values: 0–24 for T1; 0–32 for E1

Default: 0



---

**NOTICE:** *Bundling, Start Channel, and # of Channels apply only when the Serial port service type is CES.*

---

**Format** Selects the port’s operating mode.

Values: Sync, Async

Default: Sync

**Tx Clock** Selects the clock the unit uses to sample the data transmitted from the DTE. When set to “Internal,” the data is sampled directly with the transmit data clock that is also supplied to the DTE as Transmit Clock. The “External” option uses the external clock from the DTE.

Values: Internal, External

Default: Internal



---

**NOTICE:** *The “External” option is valid only in Packet mode.*

---

**Invert Clock** Changes the clock edge used to sample data received from the DTE.

Values: Disable, Enable

Default: Disable



- DTR Alarm Control** Lets you set DTR Alarm Control parameters. Selecting “Enable” allows the unit to go into alarm on loss of DTR, which occurs when the Serial port detects that the DTR signal is low.  
Values: Enable, Disable  
Default: Disable
- DTR Alarm Status** Lets you view the current DTR Alarm status.
- Flow Control** Selects the type of flow control to be used if the port is asynchronous.  
Values: None, Xon/Xoff, RTS/CTS  
Default: None
- Character Size** Selects the number of bits required to make up one asynchronous character.  
Values: Five, Six, Seven, Eight  
Default: Eight
- Parity** Sets the parity bit.  
Values: None, Odd, Even  
Default: None
- Stop Bit** Selects the number of bits required to end the asynchronous character.  
Values: 1, 2  
Default: 1
- RTS** Request To Send determines the source from which the unit reads the RTS signal status. If set to “Normal,” the unit gets RTS from the DTE on the Serial interface. If set to “Forced True,” RTS is always perceived as “On.”  
Values: Normal, Forced True  
Default: Normal
- RTS/CTS Delay** Request To Send/Clear To Send determines how long the unit waits before it changes the level of CTS to match RTS when the CTS parameter is set to “Internal.”  
Values: Normal (~30 ms delay), Long (~100 ms delay)  
Default: Normal
- CTS** Clear to Send can be set to “Forced True,” “Forced False,” or “Internal.” If this parameter is set to “Internal,” the CTS control lead follows the RTS control lead from the DTE after a delay of a duration established by the RTS/CTS Delay parameter (see above).  
Values: Forced True, Forced False, Internal  
Default: Forced True
- DCD** Data Carrier Detect parameter can be set to “Forced True,” “Forced False,” or “Internal.” If set to “Internal,” DCD is “On” when network carrier is being

received from the remote end, and is “Off” when network carrier is not being received from the far end.

Values: Forced True, Forced False, Internal

Default: Forced True

**DSR** Data Set Ready can be set to “Forced True,” “Forced False,” or “Internal.” The “Internal” option sets DSR “On” if the port is enabled and “Off” if the port is disabled.

Values: Forced True, Forced False, Internal

Default: Forced True

**Cur. Pin Status** Shows the status of the DTE Serial port pins.

## 10/100 Ethernet (IP Details)

If you select “10/100Ethernet” from the Interfaces screen, you will bring up an IP Details screen (Figure 4.22) that lets you view and/or modify the IP parameters listed below.

**Figure 4.22** *IP Details Screen*

```
----- IP DETAILS -----
IP Address      (192.094.046.072)
Subnet Mask     (255.255.255.000)
Gateway Address (192.094.046.001)
DHCP Client     [Disable]
Client Identifier (Verilink WANSuite: 00:C0:E6:A0:1E:E6 )
Ethernet       [Auto-Neg ]

Physical Address 00 C0 E6 A0 1E E6
                (Unit Access Table)

Note: Please verify that all parameters are correct.
Changes take place immediately. Incorrect settings
may result in loss of communication with this unit.

Save & Restart
Not Needed
```

**IP Address** A unique network address assigned to this unit.

**Subnet Mask** Defines the network portion of the unit’s IP Address.

**Gateway IP Address** IP Address of the default gateway (router) on the LAN side of the unit.

**DHCP Client** If DHCP Client is enabled at power-up, the unit will request its IP, Mask, and Gateway addresses from a DHCP server located on the LAN side of the unit, and the unit will use these addresses. If the DHCP request is unsuccessful, the unit will use the configured addresses shown on this screen.

**Client Identifier** Displays a unique identifier for a specific IP address.



**NOTICE:** Always verify that a DHCP server is available on the network before enabling DHCP Client. If, on power-up, a DHCP server is not found, a 60-second timeout will occur.

**Ethernet** Enables or disables a remote unit's Ethernet port.

**Physical Address** Displays unique MAC address.

Select the Unit Access Table prompt on the IP Details screen to view the Unit Access Table (Figure 4.23), which specifies up to 10 different IP networks that may access the unit's parameters. If no IP networks are supplied, any host may access the unit. Select any Index number on the table to view the Unit Access Details (Figure 4.24) that correspond with that Index number.

**Figure 4.23** Unit Access Table Screen

```

----- UNIT ACCESS TABLE -----
<Ndx>  IP Address      Mask
1      000.000.000.000  255.255.255.255
2      000.000.000.000  255.255.255.255
3      000.000.000.000  255.255.255.255
4      000.000.000.000  255.255.255.255
5      000.000.000.000  255.255.255.255
6      000.000.000.000  255.255.255.255
7      000.000.000.000  255.255.255.255
8      000.000.000.000  255.255.255.255
9      000.000.000.000  255.255.255.255
10     000.000.000.000  255.255.255.255

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Recommended
  
```

**Figure 4.24** Unit Access Details Screen

```

----- UNIT ACCESS DETAILS -----

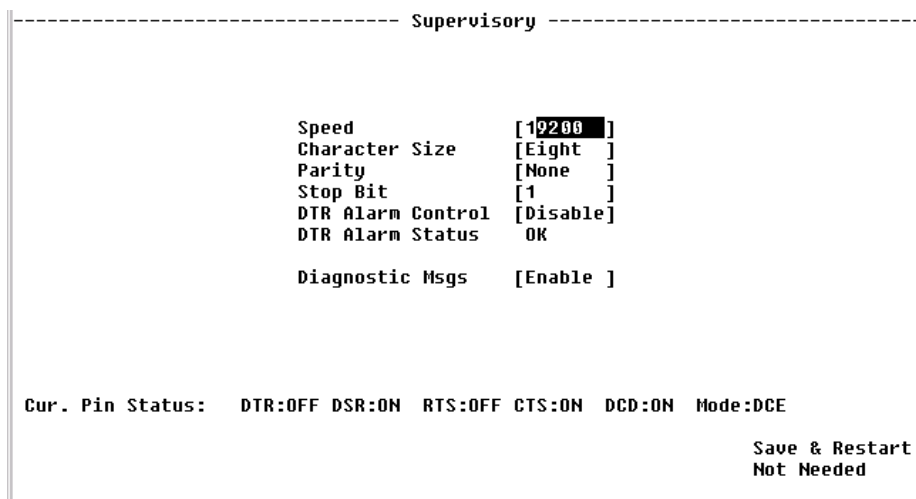
Index      1      IP Address(000.000.000.000)  Mask (255.255.255.255)

Save & Restart
Recommended
  
```

# Supervisory

The Supervisory screen (Figure 4.25) displays the current speed of the Supervisory port interface along with other parameters as described below. The Supervisory port supports only asynchronous character formats.

**Figure 4.25** *Supervisory Screen*



**Speed** Used to change the Supervisory port speed (in bits per second).  
Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200  
Default: 19200

**Character Size** Selects the number of bits required to make up one asynchronous character.  
Values: Five, Six, Seven, Eight  
Default: Eight

**Parity** Sets the parity bit.  
Values: None, Odd, Even  
Default: None

**Stop Bit** Selects the number of bits required to end the character.  
Values: 1, 2  
Default: 1

**DTR Alarm Control** Lets you set DTR Alarm Control parameters. Selecting “Enable” allows the unit to go into alarm on loss of DTR, which occurs when the Supervisory port detects that the DTR signal is low.  
Values: Enable, Disable  
Default: Disable

**DTR Alarm Status** Lets you view the current DTR Alarm status.

**Diagnostic Messages** Enables the Supervisory port to send out diagnostic messages upon power-up.  
Values: Enable, Disable  
Default: Enable

**Current Pin Status** The Current Pin Status, which shows the state of the RS-232 pins, is also displayed on the Supervisory interface screen.

## Services

The Service Table screen (Figure 4.26) provides a view of the unit's defined services and displays the Interface, Type, and Pair parameters for each service.

**Figure 4.26** Service Table Screen

```
----- SERVICE TABLE -----
(Add Service)

<Index> <Interface>           <Type>           Status
  1  Supervisory             tty              Up
  2  10/100 Ethernet         IP               Idle
  3  Network                 ATM              Up
  4  CBR                     CES              Up
  5  Serial                 Frame Relay     Down

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Not Needed
```

### Adding a Service

To add a service, select the “Add Service” prompt on the Service Table screen. A new service listed by the next incremental index number will appear on the screen. The Interface for the newly added service will be “Unassigned.” To assign an interface for the new service, select its index number, which will take you to the Service Details screen where you can specify parameters as described below.

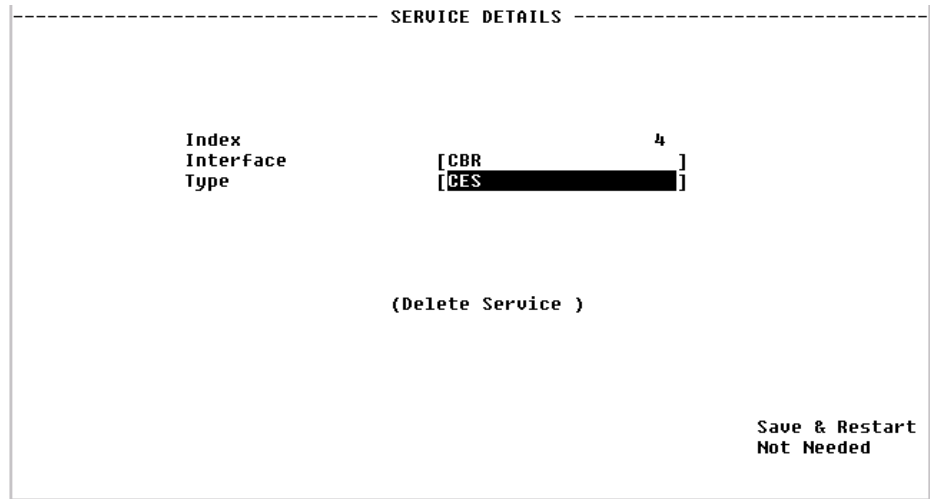


**NOTICE:** Any changes to settings in the Service Table require a “Save and Restart” for them to take effect.

### Service Details Screen

Selecting a number from the <Index> column will display a Service Details screen such as the one shown below (Figure 4.27). (In this example, the selected service type is CES.)

**Figure 4.27** Service Details Screen



From this screen, you can access and change the parameters listed below. The new parameters are saved when you press the “Esc” key and return to the previous screen.

- Interface** Selecting one of the interfaces will bring up a screen where you can view interface parameters. These screens are the same ones displayed when you select a sub-menu from the Interfaces screen described earlier on page 4-7.
- Type** Selecting one of the services listed under the “Type” column will bring up a screen where you can view (and, in some cases, change) parameters for each type of service. The details displayed depend on the type of service currently in effect. These screens are shown and described below according to each type of service.

## IP Service Details Screen

The IP Service Details screen (Figure 4.22), accessed by selecting “IP” from the <Type> column in the IP Service screen, lets you configure the IP parameters described on page 4-26.

To change any of the available parameters, you must enter new values in the appropriate field(s) and press the “Esc” key to save your changes.



---

**NOTICE:** *To use newly established IP parameters, you must “Save and Restart.” (See “Save and Restart” on page 4-6.)*

---

## Frame Relay Service Details Screen

Select “Frame Relay” under the “Type” column on the Services screen to access the Frame Relay Service Details screen (Figure 4.28). This screen lets you access the configuration parameters described in the paragraphs below.

**Figure 4.28** *Frame Relay Service Details Screen*

```

----- FRAME RELAY SERVICE DETAILS -----
Service: 5 Pair: 0 Interface: Serial

Active      No
LMI Type    Unknown
FrameStart  Sourcing
Status

Round Trip Delay Size (bytes) ( 16 )
Round Trip Delay Rate (sec)   ( 15 )

Interface Type [ NI] Default CIR (bps) ( 0 )
Link Management [ Auto] Default Be Rate (bps) ( 0 )
Max Frame Size ( 2500) Enforce CIR and Be [ No]
N1 ( 6) Management DLCI ( 0 )
N2 ( 3) Management Auto IP DLCI [ No]
N3 ( 4) LMI Sourcing [ Yes]
T1 ( 10) FrameStart Auto Discovery [ No]
Normal Tx Queue Size ( 28 )
Tx Threshold ( 0) RFC1315 Trap [ Disable]
Tx Alarm OK
Rx Threshold ( 0) Rx Invalid Threshold ( 0 )
Rx Alarm OK Rx Invalid Alarm OK

(Frame Relay Statistics) (Clear Alarms) Save & Restart
(DLCI Table) Not Needed

```

The Frame Relay Service Details screen displays Service, Pair, and Interface details across the top of the screen. Fields shown at the top of the Frame Relay Service Details screen are described below.

Field	Description
Active	Read-only status (No, Yes)
LMI Type	Read-only status
FrameStart Status	Read-only status
Round Trip Delay (bytes)	Specifies the frame size of packets making round-trip.
Round Trip Rate (sec)	Specifies the rate at which Round Trip Delay packets are sent.

Screen parameters that can be viewed and/or changed are listed below. To save new parameters, press the “Esc” key.

**Interface Type** If this service is connected to a Frame Relay network, the Interface Type should be set to “UNI” as it is the user side of a User-to-Network interface. If it is connected to a FRAD/Router, the Interface Type should be set to “NI” as it is the network side of a User-to-Network interface. If it is connected to an equipment set for Network-to-Network interface, the Interface Type should be set to “NNI.”

Values: UNI, NI, NNI

Default: UNI if interface is Network, NI if interface is Serial

**Link Management** Set this parameter to the link management used by the equipment connected to it. If set to “Auto,” the unit will learn the link management type and display it on the status portion of this screen.

Once it discovers the link management type, the unit should be set to the discovered value so that subsequent unit or network re-initialization will be faster.

Values: Auto, ANSI, CCITT, LMI, None  
Default: ANSI

**Max Frame Size** If Auto Diagnostic is set to “Yes,” the unit will discard received frames that are larger than the maximum frame size. If Auto Diagnostic is set to “No,” these large received frames will be sent, but will be counted in the Rx Invalid statistics.

Values: 64–4096  
Default: 2500

**N1** There are two types of status inquiries: keep alive and full status requests. Set this parameter to determine how many “keep alives” are sent between full status requests. (For example, if set to 5, every fifth status inquiry will be a full status inquiry.)

Values: 1–255  
Default: 5 if interface is Network (UNI), 6 if interface is Serial (NI).

**N2** The N2 counter specifies the total number of link reliability errors and protocol errors that can occur during the sliding event monitor count defined by N3. If this count is exceeded, the port is declared inactive.

Values: 1–255  
Default: 3

**N3** This counter represents a Monitored Events Count. For a network, a monitored event is the receipt of a status inquiry message or the expiration of the polling verification timer T2. For a FRAD, a monitored event is the transmission of a status enquiry message. This parameter defines the size of the sliding window used by the unit to determine whether a channel or user device is active.

Values: 1–255  
Default: 4

**T1** This parameter specifies the number of seconds the unit waits between issuing status inquiry messages.

Values: 5–30  
Default: 10

**Tx Threshold** Number of bits per second sent during a 15-minute interval after which a Tx alarm will be triggered. A value of “0” (zero) disables this trap.

Values: 0–4294967295  
Default: 0

**Tx Alarm** Status of this alarm (OK, Alarmed).



**Rx Threshold** Number of bits per second sent during a 15-minute interval after which an Rx alarm will be triggered. A value of “0” (zero) disables this trap.

Values: 0–4294967295

Default: 0

**Rx Alarm** Status of this alarm (OK, Alarmed).

**Default CIR (bps)** The Committed Information Rate (in bits per second) provided by your frame relay service provider. The unit will apply this value to each DLCI learned from the network side to gather statistics and to perform CIR enforcement, if required. If a DLCI is configured with a CIR different from the default, the DLCI configuration will be used instead.

Values: 0–1536000

Default: 0

**Default Be Rate (bps)** The Excess Burst Rate (in bits per second) provided by your frame relay service provider. The unit will apply this value to each DLCI learned from the network side to gather statistics and to perform CIR enforcement, if required. If a DLCI is configured with an Excess Burst different from the default, the DLCI configuration will be used instead.

Values: 0–1536000

Default: 0

**Enforce CIR and Be** If this parameter is set to “Yes,” the unit will enforce Committed Information Rate and Excess Burst.

Values: No, Yes

Default: No



---

**NOTICE:** *The Auto Diagnostic parameter must be set to “Yes” to enforce CIR and Be.*

---

**Management DLCI** If this parameter is set to “0,” the unit will look for management traffic on any DLCI. If set to a number associated with a specific DLCI, the unit will look for management traffic on that DLCI only.

**Management Auto IP DLCI** If this parameter is set to “Yes,” the unit will monitor the specified DLCI for 5 pings over 5 seconds, after which the unit uses the destination address as its management IP address.

**LMI Sourcing** If this parameter is set to “Yes,” the unit will source LMI messages for that service. Set this parameter to “Yes” if the service is not paired.

When set to “No,” the unit will not be the source of LMI messages for that service. LMI messages will be exchanged transparently between the paired services.

Values: No, Yes

Default: No

**FrameStart Auto Discovery** When this parameter is set to “Yes,” the unit will send FrameStart discovery and delay frames to each DLCI it learns as soon as the DLCIs are set active. This is required to calculate round-trip delay as well as to discover remote WANSuite units. This parameter should be set to “Yes” only on services that have a WANSuite at the far end of the frame relay connection.

Values: No, Yes  
Default: No

**Normal Tx Queue Size** Each Frame Relay service has two distinct transmit queues: one for normal-priority traffic and one for high-priority traffic.

This parameter defines how many normal priority frames can be put in front of a high-priority frame. The software always checks for high-priority frames before placing normal-priority frames in the transmit queue. However, once the frames are in the hardware transmit queue, their order of transmission cannot be changed.

**RFC1315 Trap** When this parameter is set to “Enable,” the unit will send the standard RFC1315 frame relay DTE circuit state change trap every time a DLCI changes state, provided at least one destination IP address for trap is configured in the SNMP configuration.

Values: Disable, Enable  
Default: Disable

**Rx Invalid Threshold** Number of invalid frames received during a 15-minute interval after which an Rx invalid alarm will be triggered. A value of “0” (zero) disables this trap.

Values: 0–4294967295  
Default: 0

**Rx Invalid Alarm** Status of this alarm (OK, Alarmed).

User prompts at the bottom of the Frame Relay Services Details screen are described in the following table.

Prompt	Function
Frame Relay Statistics	Opens the Frame Relay Statistics screen for the current frame relay service.
Clear Alarms	Clears all Frame Relay alarms.
DLCI Table	Opens the DLCI Table screen, which displays all the DLCIs on the current service. Refer to <i>DLCI Table Screen</i> on page 4-36 for more information.

### Frame Relay Statistics Screen

Select the “Frame Relay Statistics” prompt to bring up a table (Figure 4.29) that reports on the status and condition of LMI parameters and on Receive/Transmit alarms and thresholds. Alarm threshold levels may be changed by entering a new threshold value in the appropriate field on the Frame Relay Service Details screen and pressing the “Esc” key.

**Figure 4.29** *Frame Relay Statistics Screen*

```

----- FRAME RELAY STATS -----
Service: 3 (Clear Statistics)
<Period> Tx Frames Tx Octets Rx Frames Rx Octets Average Peak

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Required
    
```

To view the Port Statistics (Figure 4.30) for a specific interval, select that interval from the Frame Relay Statistics <Period> column.

**Figure 4.30** *Frame Relay Port Statistics Screen*

```

----- FRAME RELAY PORT STATISTICS -----
Service: 3 Pair: 0 Period: Interval 1
Time: 07:30:00

Transmit
Frames 0
Octets 0
Mgmt Frames 0
Mgmt Octets 0
Stat Inquiries 0
Stat Responses 0

Receive
Frames 0
Octets 0
Mgmt Frames 0
Mgmt Octets 0
FECN 0
BECN 0
Invalids 0
Stat Inquiries 0
Stat Responses 0
Invalid LMIs 57

Throughput(bits/sec)
Peak 0
Average 0

(Clear Statistics)

Save & Restart
Required
    
```

***Transmit***

- Frames** Number of frames transmitted by the port.
- Octets** Number of octets transmitted by the port.
- Mgmt Frames** Number of management frames transmitted by the port.
- Mgmt Octets** Number of management octets transmitted by the port.
- Stat Inquiries** Number of octets transmitted in frame relay LMI status inquiries.
- Stat Responses** Number of octets transmitted in frame relay LMI status responses.

### *Receive*

<b>Frames</b>	Number of frames received by the port.
<b>Octets</b>	Number of octets received by the port.
<b>Mgmt Frames</b>	Number of management frames received by the port.
<b>Mgmt Octets</b>	Number of management octets received by the port.
<b>FECN</b>	Number of Forward Explicit Congestion Notification frames received.
<b>BECN</b>	Number of Backward Explicit Congestion Notification frames received.
<b>Invalids</b>	Number of invalid frames received.
<b>Stat Inquiries</b>	Number of octets received in frame relay LMI status inquiries.
<b>Stat Responses</b>	Number of octets received in frame relay LMI status responses.
<b>Invalid LMIs</b>	Number of invalid Local Management Interface frames received.

### *Throughput (bits/sec)*

<b>Peak</b>	Peak bandwidth (in bps) as measured over a 10-second period.
<b>Average</b>	Average bandwidth (in bps) used by the port.

### **DLCI Table Screen**

Select the “DLCI Table” prompt on the Frame Relay Service Details screen to display a table of all DLCIs (Figure 4.31) on a specific frame relay service along with their state and alarm conditions. You may create a new DLCI by entering the DLCI name in the DLCI field at the top of the screen and selecting “Add DLCI.”

**Figure 4.31** *DLCI Table Screen*

```
----- DLCI TABLE -----
Service: 5

Enter new DLCI to create a DLCI
DLCI (0) (Add DLCI)

      Rec      Rdtrip      Tx EX      Rx      Rx
      BECN/    Delay      CIR      Be Alarm Congest In    UAS
<Number> Active FECN  Status  Average (ms) Alarm Be Alarm Alarm CIR  Alm
      45 Inactive 0   Inactive 0   OK   OK   OK   OK   OK
      46 Inactive 0   Inactive 0   OK   OK   OK   OK   OK
      81 Inactive 0   Inactive 0   OK   OK   OK   OK   OK

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Not Needed
```

## DLCI Details Screen

The DLCI Details screen (Figure 4.32) lets you access the configuration parameters described in the paragraphs below. To bring up this screen, select a specific DLCI under the “DLCI” column on the DLCI Table screen.

**Figure 4.32** *DLCI Details Screen*

```

----- DLCI DETAILS -----
Service: 5
DLCI: 45

Protocol Encapsulation [RFC 1490] In Band Management [No ]
Proprietary Traffic Type [None ] FrameStart Delay [Disable ]
Proprietary Offset ( 0) FrameStart Status Inactive
CIR (bps) ( 0) Remote DLCI 0
Be (bps) ( 0) Remote Unit
Bc (bps) ( 0) Remote IP Address 000.000.000.000
Discard Eligible Flag [No ] Round Trip Delay ( 16)
Round Trip Rate ( 15)

Status Inactive Congestion Threshold ( 0)
Receiving FECN/BECN No Congestion Alarm OK
CIR Threshold ( 0) BECN in CIR OK
CIR Alarm OK UAS Threshold ( 0)
Bits over Be Threshold ( 0) UAS Alarm OK
Bits over Be Alarm OK

(DLCI Statistics) Save & Restart
(Delete DLCI) Not Needed
  
```

The unit uses the first three configuration parameters (Protocol Encapsulation, Proprietary Traffic Type, and Proprietary Offset) displayed on this screen to gather statistics. For in-band management, “RFC 1490” must be the encapsulation method.

- Protocol Encapsulation** Type of encapsulation used by the FRAD/Router connected to the unit.  
 Values: RFC 1490, Proprietary, RFC 1490-Encryption  
 Default: RFC 1490
- Proprietary Traffic Type** When Protocol Encapsulation is set for “Proprietary,” the Proprietary Traffic Type parameter defines which protocol is encapsulated.  
 Values: IP, IPX, Ethertype, None  
 Default: None
- Proprietary Offset** When Protocol Encapsulation is set for “Proprietary,” the Proprietary Offset parameter defines the number of octets after the frame relay header where the proprietary traffic type starts.  
 Values: 0–64  
 Default: 0
- CIR (bps)** If a Committed Information Rate is configured here, its value will be used instead of the default CIR of the Frame Relay service.  
 Values: 0–2048000  
 Default: 0

- Be (bps)** If an Excess Burst Rate is configured here, its value will be used instead of the default excess burst of the Frame Relay service.  
 Values: 0–2048000  
 Default: 0
- Bc (bps)** If CIR enforcement is configured to “Yes,” the unit will throttle the committed burst down to this value when frames are received with the BECN bit set.  
 Values: 0–2048000  
 Default: 0
- Discard Eligible Flag** If this parameter is set to “Yes” and CIR enforcement is also set to “Yes,” the unit will set the Discard Eligible (DE) bit for frames sent over CIR.  
 Values: Yes, No  
 Default: No
- In Band Management** If the unit is to be used as a gateway to reach a remote WANsuite 6450 through this DLCI, this parameter should be set to “Yes,” and the remote IP address and Mask should be configured in the corresponding endpoint.  
 Values: Yes, No  
 Default: No
- FrameStart Delay** If this parameter is set to “Enable,” the unit will send FrameStart discovery and delay frames on this DLCI, and will report the state of the remote Verilink unit with FrameStart technology. It will also send SOS frames when the FRAD/router connected to this unit goes inactive.  
 Values: Enable, Disable  
 Default: Enable if Auto Discovery is set to “Yes”; Disable otherwise
- FrameStart Status** If the remote unit is a Verilink unit with FrameStart technology and FrameStart Auto Discovery is enabled, the FrameStart Status field will show the status of the remote unit. The status is “Active” if both the local and remote DLCIs are active and the remote unit answers to the discovery frames sent by this unit. The status is “SOS” if the remote unit is active but the FRAD/Router connected to it is inactive. The status is “Inactive” in all other cases.  
 Values: Active, Inactive, SOS  
 Default: Inactive
- Remote DLCI** If the remote unit is a Verilink unit with FrameStart technology, and FrameStart Auto Discovery is enabled, this displays the DLCI number used on the remote end of this DLCI.  
 Values: 16–1023  
 Default: 0

<b>Remote Unit</b>	If the remote unit is a Verilink unit with FrameStart technology, and FrameStart Auto Discovery is enabled, this parameter gives the first three digits of the unit ID configured on the remote end of this DLCI. Values: 000–999 Default: 000
<b>Remote Unit IP Address</b>	Displays the IP address of the remote Verilink unit with FrameStart technology if FrameStart Auto Discovery is enabled.
<b>Round Trip Delay Size (bytes)</b>	Specifies the frame size (in bytes) of packets making the round-trip. If the Round Trip Delay Size is not configured, the Frame Relay Details values will be used.
<b>Round Trip Delay Rate (secs)</b>	Specifies the rate (in seconds) at which Round Trip Delay packets are sent. If the Round Trip Delay Rate is not configured, the Frame Relay Details values will be used.

### ***DLCI Status Table***

The bottom portion of the screen displays a table detailing the actual status of DLCI and alarm threshold information as follows:

<b>Status</b>	If this DLCI is up, the status will be “Active”; otherwise, the status will be “Inactive.” Values: Active, Inactive Default: Inactive
<b>Receiving FECN/ BECN</b>	When a frame is received with congestion bit set, this parameter is set to “Yes.” It is set back to “No” when a frame is received without congestion bit set. Values: Yes, No Default: No
<b>CIR Threshold</b>	Sets the Tx over CIR alarm threshold. This threshold is the number of bits per second in excess of CIR during a 15-minute interval. Setting this field to “0” (zero) disables the alarm.
<b>CIR Alarm</b>	Reports if the Tx over CIR threshold has been exceeded.
<b>Bits Over Be Threshold</b>	Sets the Tx over Be alarm threshold. This threshold is the number of bits per second in excess of CIR + Be during a 15-minute interval. Setting this field to “0” (zero) disables the alarm.
<b>Bits Over Be Alarm</b>	Reports if the Tx over Be threshold has been exceeded.
<b>Congestion Threshold</b>	Sets the Rx Congestion alarm threshold. This threshold is the number of frames received with BECN/FECN. Setting this field to “0” (zero) disables the alarm.
<b>Congestion Alarm</b>	Reports if the Rx Congestion threshold has been exceeded.

**BECN in CIR** Reports if Backward Explicit Congestion Notification (BECN) has been received within CIR.

**UAS Threshold** Sets the Unavailable Seconds (UAS) alarm threshold. This threshold occurs after the DLCI is unavailable for a specified number of seconds. Setting this field to “0” (zero) disables the alarm.

**UAS Alarm** Reports if the UAS threshold has been exceeded.

The DLCI Details screen provides the user-activated prompts defined below.

Prompt	Function
DLCI Statistics	Displays a table of the statistics for this DLCI.
Delete DLCI	Lets you delete a specific DLCI.

### *DLCI Statistics Screen*

Selecting the “DLCI Statistics” prompt on the DLCI Details screen will display a summary (Figure 4.33) of the Transmit, Receive, and Performance statistics for the selected DLCI for a specific period.

**Figure 4.33** *DLCI Statistics Screen*

```

----- DLCI STATISTICS -----
Service: 5
DLCI: 45

(Clear Statistics)

<Period>      Tx      Tx      Tx      Rx      Rx      Rx
              Frames  Octets  Excess  Frames  Octets  BECN
Summary      0         0        0         0         0         0
Current      0         0        0         0         0         0
Interval 1   0         0        0         0         0         0
Interval 2   0         0        0         0         0         0
Interval 3   0         0        0         0         0         0
Interval 4   0         0        0         0         0         0
Interval 5   0         0        0         0         0         0
Interval 6   0         0        0         0         0         0
Interval 7   0         0        0         0         0         0
Interval 8   0         0        0         0         0         0

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Not Needed
  
```

This screen displays all ninety-six 15-minute buckets available for DLCI statistics. If the unit is powered on at 01:00 PM, the first interval will be completed at 01:15 PM; subsequent intervals would be completed at xx:30, xx:45, xx:00 and xx:15. Interval 1 is always the latest (most recent) interval, and interval 96 will always be the oldest.

The first row of the DLCI Statistics screen shows a summary that includes all 96 buckets. You can choose to see the statistics for any given bucket by selecting the desired <Period> and pressing the “Enter” key, which displays the DLCI Statistics Details screen. The MIB (ipadv2.mib) describes each available statistic.



### DLCI Statistics Details Screen

Select from the <Period> column to display the DLCI Statistics Details screen (Figure 4.34) for a specific period or interval. The parameters on this screen are described below.

**Figure 4.34** *DLCI Statistics Details Screen*

```
----- DLCI STATISTICS DETAILS -----
Service: 5  DLCI: 46  Period: Interval 1
Time: 09:44:53

          Transmit                               Receive
Frames                0  Frames                0
Octets                0  Octets                0
Mgmt Frames           0  FECN                 0
Mgmt Octets           0  BECN                 0
Excess CIR            0  DE                   0
Excess Be             0  Mgmt Frames          0
                               Mgmt Octets          0

          Performance
Peak Throughput(bits/sec)                0
Average Throughput(bits/sec)             0
Peak Roundtrip Delay(ms)                 0
Average Roundtrip Delay                   0
Roundtrip Delay Timeouts                  0
UAS                                        0
FDR CIR (%)                             100.0
DDR CIR (%)                             100.0
FDR Be (%)                              100.0
DDR Be (%)                              100.0

                                         Save & Restart
                                         Required
```

The DLCI Statistics screen in Figure 4.33 shows a summary that includes all 96 buckets. You can choose to see the statistics for any given bucket by selecting a specific interval under the <Period> column on the DLCI Statistics screen. The MIB (ipadv2.mib) describes each available statistic. “FDR” on the screen above refers to Frame Delivery Ratio, which is the ration of successful frame receptions to attempted frame transmissions. “DDR” refers to Data Delivery Ratio or the ratio of successful payload bytes received to attempted payload bytes transmitted. “DE,” or Discard Eligible, refers to the data that is first eligible to be discarded when network congestion occurs.

## ATM Service Details Screen

Access the ATM Service Details screen (Figure 4.35) by selecting the ATM link under the Type column on the Services screen. The ATM Service Details screen lets you access the configuration parameters described in the paragraphs below.

**Figure 4.35** ATM Service Details Screen

```

----- ATM SERVICE DETAILS -----
Interface: Network

Max VCC      ( 4 )      Operation Status   Up/Cell Sync
Max VPI Bits [  8 ]      Opened VCCs       3
Max VCI Bits [ 16 ]      Unopened VCCs    0
Oversubscription Factor ( 1 ) Line Bandwidth (cps) 5452
QoS 0 PCR    1589      AAL5 Bandwidth (cps) 4769

----- Bandwidth Status -----
Category  Allowance(cps)  Allocated(cps)
AAL5 CBR      4769           0
AAL5 UBR      4769           0
AAL5 UBR      4769           4767

(ATM Statistics)
(Virtual Channels)
(QoS Profiles )

Save & Restart
Not Needed

```

The Configuration table on the ATM Service Details screen is used to set the following configuration parameters:

- Max VCC (Virtual Channel Connection) – Represents the maximum number of Virtual Channel Connections on this ATM link. The default value is 4.
- Max VPI Bits – The default Max Virtual Path Identifier Bits value is 8 for VPI values ranging from 0 to 255.
- Max VCI Bits – The default Max Virtual Channel Identifier Bits value is 16 for VCI values ranging from 32 to 65535.
- Oversubscription Factor – The current over-subscription factor for this ATM interface. Used for VBR and UBR VC connection admission control to allow either the VBR or UBR service category connections to collectively use more bandwidth than is available to make use of the statistical multiplexing of the connections. Values range from 1 to 10. A value of 1 indicates no oversubscription. A value of 5 indicates 5 times oversubscription of both VBR and UBR is permitted.



**NOTICE:** *CBR connections cannot be oversubscribed. Also, if CES is in use on the interface, PCR is limited for all AAL5 connections to the amount the line rate can support above the commitment for CES, and the oversubscription applies only to bandwidth above the CES commitment.*

To change an ATM Service configuration, enter the desired value for each parameter and press the “Esc” key.

The Status table provides the following status information on the circuits:

- QoS 0 PCR – current peak cell rate for any virtual channels using default QoS profile.
- Operation Status – current operational status for the ATM interface.
- Opened VCCs – current number of open virtual channel connections.
- Unopened VCCs – current number of unopen virtual channel connections.
- Line Bandwidth – current line bandwidth on the ATM Network interface expressed in cells per second.

- AAL5 Bandwidth – current ATM bandwidth available for AAL5 traffic. This value is the line bandwidth less the bandwidth needed for AAL1 CES.

The Bandwidth Status table provides bandwidth information for three service categories showing the allowed and allocated bandwidth for each.

The ATM Service Details screen provides the user-activated prompts described below.

Prompt	Function
ATM Statistics	Displays the current ATM statistics.
Virtual Channels	Displays configured VCCs.
QoS Profiles	Displays configured QoS profiles.

### ATM Statistics Screen

Selecting the “ATM Statistics” prompt on the ATM Service Details screen will display the screen shown in Figure 4.36.

Figure 4.36 ATM Statistics Screen

```

----- ATM STATISTICS -----
Opened VCCs:          2
Unopened VCCs:       0  (Clear Statistics)

Index   Tx      Tx  Tx Err  Tx   Rx   Rx   Rx Err  Rx   TimeStamp
Summary 0      0      0 073869 0     0     0     0     4 10:36:12
Current 0      0      0  371    0     0     0     0     0 10:36:12
Int 1   0      0      0 900    0     0     0     0     0 10:30:01
Int 2   0      0      0 900    0     0     0     0     0 10:15:01
Int 3   0      0      0 900    0     0     0     0     0 10:00:01
Int 4   0      0      0 900    0     0     0     0     0 09:45:01
Int 5   0      0      0 900    0     0     0     0     0 09:30:01
Int 6   0      0      0 901    0     0     0     0     0 09:15:01
Int 7   0      0      0 900    0     0     0     0     0 09:00:00
Int 8   0      0      0 900    0     0     0     0     0 08:45:00

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Required
  
```

There are ninety-six 15-minute “buckets” available for ATM statistics. If the unit is powered on at 01:00 PM, the first interval will be completed at 01:15 PM; subsequent intervals would be completed at xx:30, xx:45, xx:00 and xx:15. Interval 1 is always the latest (most recent) interval, and interval 96 will always be the oldest.

The table on the ATM Statistics screen shows a summary that includes all 96 buckets. The MIB (ipad.mib) describes each available statistic.

The ATM Statistics table is divided into two sections: Transmit (first three columns), and Receive (next three columns). Each section provides real-time updates (TimeStamp column) on the following statistics:

- Frames – current number of good frames transmitted
- Errored Frames – current number of frames in error
- Bytes – current number of bytes sent
- OAM Cells – current number of OAM cells sent

## ATM Virtual Channel Table Screen

Select the “Virtual Channels” prompt on the ATM Service Details screen to display a table (Figure 4.37) of all Virtual Channels on a specific ATM service along with their state and alarm conditions.

**Figure 4.37** Virtual Channel Table Screen

```

----- VIRTUAL CHANNEL TABLE -----
Enter new VPI/VCI to create a new Virtual Channel
VPI(0) VCI( 0) (Add Virtual Channel)

<VPI>  VCI      Admin  Oper   QoS   Encapsulation  Traffic  Row
      Status Status Status Prof   Encaps          Type     Status
      0    32      Up     Up     0     LLC-MUX        ubr      Active
      0    57      Up     Up     0     FRF5           ubr      Active
      0    87      Up     Up     0     FRF8           ubr      Active

Ctrl^R PageUp          Save & Restart
Ctrl^C PageDown       Not Needed
  
```

The Virtual Channel Table displays status information on the parameters listed below. These parameters are configured on the Virtual Channel Details screen (Figure 4.38):

**VPI** Virtual Path Identifier number.

**VCI** Virtual Channel Identifier number.

**Admin Status** Current Admin Status.  
Values: Up, Down, Testing

**Oper Status** Current Operation Status.  
Values: Up, Down, Testing

**Last Change** Time and date of the Last Change.

**QOS Prof** Current QOS profile in use. The default profile is 0 (zero), which is used for UBR traffic.

When QOS profile “0” is used, the available bandwidth will be equally shared among all configured channels. QOS “0” cannot be modified.

If one virtual channel requires more bandwidth than others, configure another QOS profile and set its peak cell rate (PCR) to the required value. However, the sum of the PCRs of all configured channels must be no greater than the available AAL5 bandwidth. The available PCR on an SHDSL-ATM link with a line rate of 2304 kbps is about 5433 cells per second. When oversubscription is used, the sum of the PCRs for VBR or UBR channels may exceed the AAL5 bandwidth.

**Encapsulation** Encapsulation Type used. Default is LLC-MUX, which uses RFC 1483 LLC encapsulation. If Serial PPP is selected, PPP traffic received from the Serial port will be sent over the ATM port using RFC 1483 PPPoA encapsulation. There can be only one VCI configured for Serial PPP.

Serial HDLC is similar to Serial PPP except, when you select Serial HDLC, data is encapsulated transparently. Any type of HDLC traffic will be supported. Because this is not a standard encapsulation, a WANSuite unit must reside at each end of the connection. Even if Serial HDLC or Serial PPP encapsulation is configured, routed IP traffic received on this channel will be forwarded to the IP Gateway, if IP Gateway is configured.

VC-MUX is used for a null encapsulation around user data, as in the case of a WAN PPP connection terminated in the WANSuite.

If FRF5 is used, the ATM channel implements FRF.5 Network Interworking, providing a Frame Relay link that can transport data for one or more DLCIs. If FRF8 is used, the ATM channel implements FRF.8.1 Service Interworking, providing a conversion from a Frame Relay PVC to this ATM PVC.

Values: Serial PPP, LLC-MUX, VC-MUX, Serial HDLC

**Traffic Type** Traffic type used. This is a read-only parameter determined by the QoS Profile in use for the channel.

Values: CBR, VBR, UBR

**Status** Current status of the VCC.

Values: active, notinService, notReady, createAndGo, createAndWait, destroy

### ***Adding a New Virtual Channel***

To create a new virtual channel, enter the desired VPI/VCI values in the appropriate field(s) at the top of the screen and select the “Add Virtual Channel” prompt.

If the newly added virtual channel is within the maximum VCC parameter, it will be activated immediately.



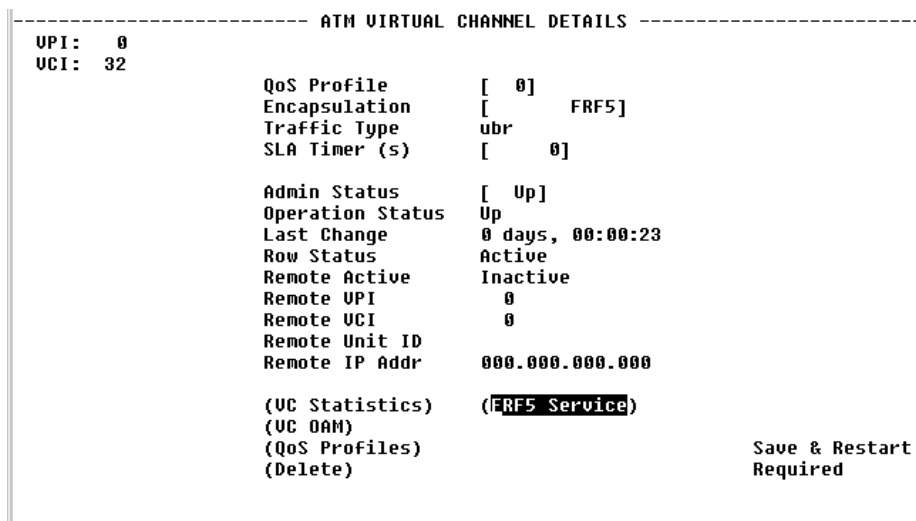
---

**NOTICE:** *When adding a Virtual Channel, the value for VPI may be 0 and above, but for VCI, must be 32 and above.*

---

Select a listed VPI to bring up the ATM Virtual Channel Details Screen (Figure 4.38) where you can configure or change the parameters described above.

**Figure 4.38** *Virtual Channel Details Screen*



**SLA Timer (s)** In addition to the above-described parameters, there is an SLA Timer(s) parameter that may be set on the ATM Virtual Channel Details screen. When this timer expires (in seconds), the unit sends a proprietary frame over this virtual circuit. The timer validates Service Level Agreements by calculating the Frame Delivery Ratio, the Data Delivery Ratio, and the Round Trip Delay. When enabled, this timer also determines the IP address of the far-end unit, which must also be a WANsuite unit. A setting of “0” disables SLA measurements.

The following user-activated prompts are included on the ATM Virtual Channel Details Screen:

Prompt	Function
VC Statistics	Displays the current Virtual Channel statistics.
VC OAM	Displays Virtual Channel Operations and Maintenance Screen.
QoS Profiles	Displays configured QOS profiles.
Delete	Displays a confirmation screen.

### **Virtual Channel OAM**

Select the Virtual Channel OAM prompt on the Virtual Channel Details screen to view the menu shown in Figure 4.39. Using this menu, you can initiate either an End-to-End or a Segment OAM F5 ATM loopback to check the ATM layer setup of a virtual circuit (VC). An active ATM loopback sends one cell every 5 seconds. When the cells received equal the cells transmitted, the loopback is successful. Use the Start and Stop buttons in the End-to-End and Segment columns to start or to terminate an OAM F5 VCC loopback.

**Figure 4.39** *Virtual Channel OAM*

```

----- ATM VCC OAM -----
UPI:  0
UCI: 32

          UC Loopbacks
        End-To-End Segment
          (Start) (Start)
          (Stop)  (Stop)
LB Status Inactive Inactive
Cells Tx   0      0
Cells Rx   0      0
Round Trip Times (msec)
Minimum    0      0
Average    0      0
Maximum    0      0

          End to End Continuity Check
          CC Type [None ]
          CC Auto Activate [Disable ]
          (Activate Continuity Check)
          (Deactivate Continuity Check)

          CC Status      Ready
          CC Type In Use None
          CC Cells Transmitted  0
          CC Cells Received    0

          AIS ---
          RDI ---

                                Save & Restart
                                Not Needed

```

**LB Status** The state of the current VCC loopback function. When a loopback is activated from a user interface, the Loopback Status will be “Active,” and OAM F5 loopback cells will be sent from this endpoint once every 5 seconds. If a loopback is activated from the other endpoint or segment endpoint, the Loopback Status will be “Loopback.” The Loopback Status will be “Inactive” when no loopback is in place.

**Cells Tx** The number of OAM loopback cells transmitted for this VCC.

**Cells Rx** The number of OAM loopback cells received for this VCC.

**Round Trip Times  
(msec)**

**Minimum** The minimum round-trip time in milliseconds between sending and receiving returned loopback cells.

**Average** The average round-trip time in milliseconds between sending and receiving returned loopback cells.

**Maximum** The maximum round-trip time in milliseconds between sending and receiving returned loopback cells.

The Round-trip Time values are set to zero any time the Loopback Status changes from Inactive to Active or Loopback. The Round-trip Time values are updated only when Loopback Status is Active and response loopback cells are received. When the loopback is initiated from the other ATM endpoint, the Round-trip Time values remain at zero.

**Continuity Check**

The Virtual Channel OAM menu includes an End to End Continuity Check that, when activated, will continuously check for the purpose of detecting ATM layer defects in real time. Continuity Check may be activated in one or

both directions. The ATM endpoint that activates the Continuity Check selects which direction applies. To activate and End-to-End Continuity Check, select the Type and “Activate Continuity Check.” If activated successfully, the Status will indicate “Active.” If unsuccessful, the Status will indicate “Activation Failed.” The Status is “Ready” when no continuity check (CC) is active. The three types of CCs include the following:

- Sink – a unidirectional CC where one endpoint is the Sink.
- Source – a unidirectional CC where one endpoint is the Source.
- Sink and Source – a bidirectional CC where each endpoint sends one CC cell every second (the Source) and each endpoint (the Sink) expects to receive one CC cell every second.

When the CC Sink does not receive user cells or a CC cell within 3.5 seconds, the AIS will show Active, which is an Alarm indication, and one AIS cell will be generated once per second toward the other endpoint.

To automatically activate an End to End Continuity Check when a VC is first connected, select the Type and set Auto Activate to “Enable.” The next time the VC Oper Status changes from Down to Up, the CC will automatically be activated.

Alarm Indication Signal, or AIS, shows “Active” if the VC is receiving AIS cells. The AIS state will clear after about 3.5 seconds of no received AIS cells when no CC is active. When CC is active, the AIS state will clear on receipt of a CC cell or a user cell.

Remote Defect Indication, or RDI, indicates “Receiving” if RDI cells are being received. The RDI state will clear after about 3.5 seconds of no received RDI cells.

## Quality of Service (QoS) Profile Screen

Select the “QoS Table” prompt on the ATM Service Details screen to display the screen shown in Figure 4.40.

**Figure 4.40** *Quality of Service Profile Screen*

----- QUALITY OF SERVICE PROFILE -----						
<b>(Add New)</b>						
<Ndx>	Category	Param1 (PCR)	Param2 (SCR)	Param3 (MBS)	Row Status	
1	UBR	1200	1000	200	Active	

Ctrl^R PageUp  
Ctrl^C PageDown

Save & Restart  
Not Needed



The table displayed on this screen contains information on ATM traffic descriptor type and the associated parameters.

- Category** ATM service category. Possible values include CBR, VBR, and UBR.
- Param 1 (PCR)** Peak cell rate in cells per second.
- Param 2 (SCR)** Sustainable cell rate in cells per second. Applicable only to VBR service category.
- Param 3 (MBS)** Maximum burst size in cells. Applicable only to VBR service category.
- Row Status** QoS Profile Row Status. Possible values include Active and Not in Service. Selecting one of the available <Ndx> entries on the Quality of Service Profile screen will display a screen similar to the screen shown in Figure 4.41. Use this screen to configure or change the QoS parameters listed below.

**Figure 4.41** *QoS Profile Details Screen*

```
----- QoS PROFILE DETAILS -----
                                     1
Profile                               [UBR]
Category                             (1000)
Param 1 (PCR)                         ( 800)
Param 2 (SCR)                         ( 150)
Param 3 (MBS)
Row Status                             Active

                                     (Delete)

                                     Save & Restart
                                     Not Needed
```

- Category** ATM service category.  
Values: CBR, VBR, UBR  
Default: UBR
- Param 1 (PCR)** Peak cell rate in cells per second to use for all channels using this QoS profile.
- Param 2 (SCR)** Sustainable cell rate in cells per second to use for all channels using this QoS profile. Applicable to VBR only.
- Param 3 (MBS)** Maximum burst size to use for all channels using this QoS profile. Applicable to VBR only.
- Row Status** Current status of the profile.

## FRF5 Service Details Screen



**NOTICE:** The FRF5 Service Details screen is only accessible when FRF5 is the Encapsulation Type as shown on the Virtual Channel Details Screen (see Figure 4.38).

Selecting the FRF5 Service Details prompt on the Virtual Channel Details Screen will bring up the FRF5 Service Details screen as shown in Figure 4.42.

**Figure 4.42** FRF5 Service Details Screen

```
----- FRF5 SERVICE DETAILS -----
UPI:  0
UCI: 32

DE to CLP Mapping  [CLP set to 0 ]
CLP to DE Mapping  [Don't Map CLP]
N1                 (  6)
N2                 (  4)
N3                 (  3)
T1                 ( 10)
T2                 ( 12)

LMI Type           CCITT
Interface Type     NNI

Status             Inactive

(DLCI Table)

Save & Restart
Required
```

**DE to CLP Mapping** Indicates whether the Discard Eligibility in the Frame Relay header is mapped to Cell Loss Priority in the ATM cell header when transmitting data in the ATM to Frame Relay direction.

Values: Map DE to CLP, CLP set to 0, CLP set to 1  
Default: CLP set to 0

**CLP to DE Mapping** Indicates whether the Cell Loss Priority in the ATM cell header is mapped to the Discard Eligibility in the Frame Relay header when transmitting data in the ATM to Frame Relay direction.

Values: Map CLP to DE, Don't Map CLP to DE  
Default: Don't Map CLP to DE

**N1** There are two types of status inquiries: keep alive and full status requests. Set this parameter to determine how many “keep alives” are sent between full status requests. (For example, if set to 5, every fifth status inquiry will be a full status inquiry.)

Values: 1–255  
Default: 6

- N2** The N2 counter specifies the total number of link reliability errors and protocol errors that can occur during the sliding event monitor count defined by N3. If this count is exceeded, the port is declared inactive.  
Values: 1–10  
Default: 4
- N3** This counter represents a Monitored Events Count. For a network, a monitored event is the receipt of a status inquiry message or the expiration of the polling verification timer T2. This parameter defines the size of the sliding window used by the unit to determine whether a channel or user device is active.  
Values: 1–10  
Default: 3
- T1** This parameter specifies the number of seconds the unit waits between issuing status inquiry messages.  
Values: 5–240  
Default: 10
- T2** This parameter specifies the number of seconds the unit allows before counting non-receipt of a status inquiry message as an error.  
Values: 5–245  
Default: 12

The user-activated prompt at the bottom of the screen will bring up the FRF5 DLCI Table.

#### **FRF5 DLCI Table**

One or more DLCIs may be created for the Frame Relay link carried over ATM for an FRF5 VC. When a DLCI is intended to transport Frame traffic to a Frame Relay link on the Serial port, an endpoint is associated with that DLCI. It is advisable, but not necessary, to use the same DLCI number on the Serial port for the FRF5 DLCI.

If an FRF5 DLCI has no associated endpoint name, that DLCI's Frame traffic will terminate inside the WANsuite 6450. One application for having no associated endpoint is to use the DLCI for router traffic, which is set up by an IP circuit whose endpoint names the FRF5 endpoint for this VPI/VCI/DLCI beginning with the letter "I."

The Received FECN/BECN column shows whether the current frames are indicating Forward Explicit Congestion Notification or Backward Explicit Congestion Notification.

**Figure 4.43** FRF5 DLCI Table

```

----- FRF5 DLCI TABLE -----
UPI:    0   UCI: 32

          New DLCI Number (    0) (Add DLCI)
          <DLCI>   Status      Endpoint      Receiving
          45      Inactive    [REDACTED]   BECN/FECN
                                           No

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Required
    
```

Select on one of the DLCIs listed to view the FRF5 DLCI Details screen as shown in Figure 4.44.

**Figure 4.44** FRF5 DLCI Details Screen

```

----- FRF5 DLCI DETAILS -----
UPI:    0   UCI: 32
DLCI   45

          Endpoint Name      [REDACTED]
          Status              Inactive
          Receiving FECN/BECN No
          (Delete DLCI)

Save & Restart
Required
    
```

The Endpoint Name specifies which Serial port Frame Relay endpoint is associated with this FRF5 DLCI.

**FRF8 Service Details Screen**



**NOTICE:** *The FRF8 Service Details screen is only accessible when FRF8 is the Encapsulation Type as shown on the Virtual Channel Details Screen (see Figure 4.38).*

The FRF8 Service Details Screen is shown in Figure 4.45.

**Figure 4.45** FRF8 Service Details Screen

```
----- FRF8 SERVICE DETAILS -----
UPI:  0
UCI: 32

DE to CLP Mapping  [CLP set to 0 ]
CLP to DE Mapping  [DE set to 0 ]
CI Mapping          [EFCI set to 0 ]
Encapsulation Mapping [Translation]
Endpoint Name       [          ]

Save & Restart
Required
```

**DE to CLP Mapping** Indicates whether the Discard Eligibility in the Frame Relay header is mapped to Cell Loss Priority in the ATM cell header when transmitting data in the ATM to Frame Relay direction.

Values: Map DE to CLP, CLP set to 0, CLP set to 1  
Default: CLP set to 0

**CLP to DE Mapping** Indicates whether the Cell Loss Priority in the ATM cell header is mapped to the Discard Eligibility in the Frame Relay header when transmitting data in the ATM to Frame Relay direction.

Values: Map CLP to DE, DE set to 0, DE set to 1  
Default: DE set to 0

**CI Mapping** Indicates whether FECN in the Frame Relay header is mapped to EFCI in the ATM cell header when transmitting data in the Frame Relay to ATM direction.

Values: Map FECN to EFCI, EFCI set to 0  
Default: EFCI set to 0

**Encapsulation Mapping** Indicates the handling of upper layer user protocol encapsulation. When Encapsulation Mapping is set to Translation, the FRF8 Interworking function maps between the two encapsulations, translating between RFC1490 and RFC1483. When Encapsulation Mapping is set to Transparent, the data is transported without translation between Frame Relay and the ATM PVC.

Values: Transparent, Translation  
Default: Translation

**Endpoint Name** Identifies the Serial Frame Relay service DLCI that is to be connected with this FRF8 ATM VC.

## CES Service Details Screen

Selecting CES under the “Type” column of the table in the Services screen will display the CES Service Details screen show in Figure 4.46.

**Figure 4.46** CES Service Details Screen

```

----- CES SERVICE DETAILS -----
VPI                ( 0 ) Partial Fill      ( 0 )
VCI                ( 33 ) Rx Cell Delay Var ( 100 )
Service Type      [ Structured] Cell Loss Int    ( 2500 )
Timing            [ Adaptive]  Auto Channel Config [ Disable ]
AAL1 Format        [ Basic]     Admin Status      [ Up ]
Payload Scrambling [ Enable]   Operational Status Down

Reassembly Cells  127431678  Lost Cells        0
Header Errs       0          Misinserted Cells 0
Pointer Reframes  15928959  Buffer Underflows  0
Pointer Parity Errs 0          Buffer Overflows   0
AAL1 Seq Errs     0          Cell Loss Status  No Loss

(Channel(s))

Save & Restart
Not Needed

```

From this screen, you can access and change the parameters listed below. The new parameters are saved when you “ESC” from the screen and perform a Save and Restart.

**VPI** Determines VPI used for this CES Internet Working Function (IWF). The default is 0.

**VCI** Determines VCI used for this CES IWF. The default is 33.

**Service Type** Determines if T1/E1 service is structured (Nx64 kbps with or without signaling) or unstructured (2.048 Mbps or 1.544 Mbps raw data stream). You must configure the Service Type to correspond with the desired CBR port framing and Signaling in accordance with the table on page 4-58.

**Timing** Determines the CES services clocking mode, which maps to the transmit clock source of the CBR interface and Serial interface (if configured for a CES service). When “Adaptive” timing is selected, the receive AAL1 payload buffer is monitored for predetermined threshold levels to control the frequency of the interface clocks. When the buffer depth exceeds the predetermined upper threshold, the interface clock frequency is increased to cause the buffer to drain more quickly. If the buffer depth falls below the predetermined lower buffer threshold, the interface clock frequency is decreased to cause the buffer to drain less quickly. Both lower and upper threshold levels are used in conjunction with Cell Delay Variation to provide hysteresis around threshold levels.

Values: Synchronous, Adaptive

Default: Adaptive

- AAL1 Format** Specifies AAL1 format – Basic, E1Cas, Ds1SfCas, or Ds1EsfCas. This value must be set in accordance with the table on page 4-58 for proper operation.
- Payload Scrambling** The WANsuite 6450 scrambles/descrambles cell payload bytes at the physical layer interface using an  $x^{43} + 1$  polynomial. You may enable/disable the scrambling function on the CES Service Details Screen. (Normal operation will have Payload Scrambling enabled, which is the default.) (See Figure 4.46 on page 4-54.)
- Partial Fill** Sets the number of user octets per cell. Setting this parameter to 0 disables Partial Cell Fill, and all cells are completely filled before being sent.
- Rx Cell Delay Var** Maximum cell arrival jitter in 10- $\mu$ s increments that the reassembly process will tolerate in the cell stream without producing errors on the CBR service interface. Default is 100 for a 1000- $\mu$ s Cell Delay Variation (CDV).
- Cell Loss Int** Time in milliseconds for the cell loss integration period. If cells are continuously lost during the specified period of time, Cell Loss Status is set to “Loss.” Default is 2500 ms.
- AutoChannel Configuration** This feature applies only to circuit emulation of E1 CCS, E1 CAS, and Serial CES services. When enabled, the WANsuite 6450 will automatically configure the number of channels (N) allocated to the service according to the negotiated SHDSL line rate. Channels are allocated starting with channel/time slot 1 in consecutive order until N channels have been allocated to the service. An emulated E1 CCS or Serial service may allocate channels/time slots 1–31. Refer to the table below for E1 Nx64 Basic Service Without Signaling (E1 CCS).

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
192	1	171	119.496	281
256	2	342	110.992	261
320	3	512	102.912	242
384	4	683	94.408	222
448	5	854	85.904	202
512	6	1024	77.824	183
576	7	1195	69.320	143
640	8	1366	60.816	143
704	9	1536	52.736	124
768	10	1707	44.232	104
832	11	1878	35.728	84
896	12	2048	27.648	65
960	13	2219	19.144	45
1024	14	2390	10.640	25
1088	15	2560	2.560	6
1152	15	2560	66.560	156
1216	16	2731	58.056	136

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
1280	17	2902	49.552	116
1344	18	3072	41.472	97
1408	19	3243	32.968	77
1472	20	3414	24.464	57
1536	21	3584	16.384	38
1600	22	3755	71.880	18
1664	22	3755	71.880	169
1728	23	3926	63.376	149
1792	24	4096	55.296	130
1856	25	4267	46.792	110
1920	26	4438	38.288	90
1984	27	4608	30.208	71
2048	28	4779	21.704	51
2112	29	4950	13.200	31
2176	30	5120	5.120	12
2240	30	5120	69.120	163
2304	31	5291	60.616	142
2312	31	5291	68.616	161

An emulated E1 CAS service may allocate channels/time slots 1–15 and 17–31 (refer to the table below). Channel/time slot 16, which carries the signaling information, will not be allocated as a voice channel. Refer to the table below for E1 Nx64 Basic Service With Signaling (E1 CAS).)

SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
192	1	182	114.832	270
256	2	352	106.752	251
320	3	534	93.584	220
384	4	704	85.504	201
448	5	886	72.336	170
512	6	1056	64.256	151
576	7	1238	51.088	120
640	8	1408	43.008	101
704	9	1590	29.840	70
768	10	1760	21.760	51
832	11	1942	8.592	20
896	12	2112	0.512	1
960	12	2112	64.512	152
1024	13	2294	51.344	121
1088	14	2464	43.264	102
1152	15	2646	30.096	70
1216	16	2816	22.016	51
1280	17	2998	8.848	20



SHDSL Data Rate (kbps)	N	PCR	AAL5 Bandwidth	
			kbps	CPS
1344	18	3168	0.768	1
1408	18	3168	64.768	152
1472	19	3350	51.600	121
1536	20	3520	43.520	102
1600	21	3702	30.352	71
1664	22	3872	22.272	52
1728	23	4054	9.104	21
1792	24	4224	1.024	2
1856	24	4224	65.024	153
1920	25	4406	51.856	122
1984	26	4576	43.776	103
2048	27	4758	30.608	72
2112	28	4928	22.528	53
2176	29	5110	9.360	22
2250	30	5280	1.280	3
2304	30	5280	65.280	153
2312	30	5280	73.280	172

**Admin Status** Sets the Administrative Status of the CES IWF. “Up” indicates traffic flow is enabled, and “Down” indicates traffic flow is disabled across the CES IWF.

**Operational Status** Displays the Operational Status of the CES IWF. The state will be “Down” or “Unknown” if the supporting CBR or ATM interface is down or unknown.

## Status

**Reassembly Cells** Displays the number of cells received by the CES IWF. This number excludes cells that have been discarded for any reason, including cells not used due to their being misinserted or discarded while the reassembler was awaiting synchronization.

**Header Errors** Displays the number of AAL1 header errors detected, including those that have been corrected. Header errors include correctable and uncorrectable CRCs and bad parity.

**Pointer Reframes** Displays the number of events in which the AAL1 reassembler found a Structured Data Pointer (SDT pointer) where it was not expected, making it necessary to reacquire the pointer.

**Pointer Parity Errs** Displays the number of events in which the AAL1 reassembler has detected an SDT pointer parity check failure.

**AAL1 Seq Errs** Displays the number of times the sequence number of an incoming AAL1 frame causes a transition from the “sync” state to the “out of sequence” state.

**Lost Cells** Displays the number of cells detected as lost in the network prior to reaching the destination CES IWF AAL1 layer processing. As an example, the number of lost cells may be detected as a result of AAL1 sequence number processing.

**Misinserted Cells** Displays the number of AAL1 sequence violations, which the AAL Convergence Sublayer interprets as “misinserted cells.”

**Buffer Underflows** Displays the number of times the CES reassembly buffer underflows.

**Buffer Overflows** Displays the number of times the CES reassembly buffer overflows.

**Cell Loss Status** Displays “Loss” when cells are continuously lost during the specified Cell Loss Integration Period. When a valid cell(s) is received, this condition is cleared, and “No Loss” will be displayed.

Configuring the WANsuite 6450 for CES involves setting parameters not only on the CES Service Details screen (Figure 4.46 on page 4-54), but also on the CBR screen (Figure 4.16 on page 4-17); in some cases, the Serial screen (Figure 4.21 on page 4-23); and the Channel Table Details screen (Figure 4.47 on page 4-59). The table below shows the settings required to maintain the proper relationships among CBR framing, the CES Service Type, the CES AAL1 format, and the Signaling.

CES Service Description	CBR Framing	CES Service Type	CES AAL1 Format	Signaling
Basic E1 (CCS)/Serial	E1 CCS	Structured	Basic	Disable
Basic T1 (ESF)	T1 ESF	Structured	Basic	Disable
Basic T1 (D4)	T1 D4	Structured	Basic	Disable
E1 w/Signaling (CAS)	E1 CAS	Structured	E1Cas	Enable*
T1 w/Signaling (ESF)	T1 ESF	Structured	Ds1EsfCas	Enable*
T1 w/Signaling (D4)	T1 D4	Structured	Ds1SfCas	Enable*
Unstructured E1/Serial	E1 Unframed	Unstructured	Basic	Disable
Unstructured T1	T1 Unframed	Unstructured	Basic	Disable

\*Only channels allocated to the CBR interface should have Signaling set to “Enable.” When configuring the Serial interface for CES service (see *Serial CES Configuration* on page 4-61), you must set the Signaling to “Disable for allocated channels.”

## Channel Table Details Screen

To allocate Channels, or time slots, for CES services, select the “Channels” prompt at the bottom of the CES Service Details screen to bring up the Channel Table Details screen shown in Figure 4.47.

**Figure 4.47** Channel Table Details Screen

```
----- CHANNEL TABLE DETAILS -----
Interface: CES

      Channel Signaling Service Idle Pattern
      0      [Disable] [0 ] ( 7F)
      1      [Disable] [4 ] ( 7F)
      2      [Disable] [4 ] ( 7F)
      3      [Disable] [4 ] ( 7F)
      4      [Disable] [4 ] ( 7F)
      5      [Disable] [0 ] ( 7F)
      6      [Disable] [0 ] ( 7F)
      7      [Disable] [0 ] ( 7F)

Ctrl^R PageUp                               Save & Restart
Ctrl^C PageDown                             Not Needed
```

The Channel Table Details screen lets you establish the Signaling, Service, and Idle Pattern parameters for any available channel. The screen parameters are described below.

**Signaling** The unit can operate with Signaling enabled or disabled on channels. You must set this value in accordance with the table above for proper operation.

Values: Disable, Enable

Default: Disable

**Service** Specifies the service to which this channel is allocated. Service Index “0” indicates the channel is not used or is idle. Service Index “4” indicates the channel is allocated to the CBR interface. Service Index “5” indicates the channel is allocated to the Serial interface.

**Idle Pattern** Selects the idle pattern sent by the unit and lets the unit determine if the idle pattern has been sent by the other end.

Values: 0–FF (Hex)

Default: 7F



**NOTICE:** Only channels with a non-zero Service parameter value are assembled into ATM cells and transported across the SHDSL network. Similarly, received ATM cells should only contain data for channels with a non-zero Service parameter value. When reassembling the data stream from the received ATM cells, only the channels with a non-zero Service parameter will be assigned data from the ATM cells. The non-active channels with a Service parameter of “0” will be filled with an idle pattern (0xFF).

The number of channels you can allocate for the CES service depends on the available SHDSL bandwidth. The table below shows the maximum number of channels you can allocate for CES for each possible SHDSL data rate. If the

required CES bandwidth exceeds the available SHDSL bandwidth, the unit will not allow you to configure the CES service.

SHDSL Data Rate (kbps)	Maximum Number of CES Channels		
	Structured Nx64 Basic Service	Structured Nx64 with E1 CAS Service	Structured Nx64 with T1 CAS Service
192	2	2	2
256	3	3	3
320	4	4	4
384	5	5	5
448	6	6	6
512	7	6	6
576	7	7	8
640	8	8	8
704	9	9	9
768	10	10	10
832	11	11	11
896	12	12	12
960	13	12	12
1024	14	13	14
1088	15	14	14
1152	15	15	16
1216	16	16	16
1280	17	17	18
1344	18	18	18
1408	19	18	19
1472	20	19	20
1536	21	20	20
1600	22	21	22
1664	22	22	22
1728	23	23	24
1792	24	24	24
1856	25	24	24
1920	26	25	24
1984	27	26	24
2048	28	27	24
2112	29	28	24
2176	30	29	24
2240	30	30	24
2304	31	30	24
2312*	31	30	24

\*This rate is proprietary to the GlobeSpan chipset and is required for unstructured E1 CES service.

To allocate a channel for the CBR interface, set the channel's "Rate" parameter according to the table shown on page 4-58 and the Service parameter to the Service Index for the CBR interface (4). To allocate a channel for the Serial Interface, refer to the paragraphs below.

## Serial CES Configuration

The WANsuite 6450 has the capability to multiplex/demultiplex the Serial interface data stream with the CBR interface data stream. The multiplexing/demultiplexing is external to the AAL1 SAR; the user controls it by designating time slots for the CES service on the CBR or Serial port. To configure the Serial interface for CES service, perform the following steps:

- 1** On the Services Table screen (Figure 4.26 on page 4-29), select the Service Index associated with the Serial interface (5). This will cause the unit to display the Service Details screen for the Serial interface. On the Service Details screen (Figure 4.27 on page 4-30), select "CES" from the options available under "Type."
- 2** On the Serial screen (Figure 4.21 on page 4-23), configure the Serial interface to your requirements. You *must* set the "Mode" parameter to "DCE." If the required time slots for the Serial interface are contiguous and not already allocated to the CBR port, you may allocate the required channels on the Serial screen. If you have not allocated channels for the Serial interface on the Serial screen, use the Channel Table Details screen (Step 3 below) to specify the channels for the Serial CES service.
- 3** On the Channel Table Details screen (Figure 4.47 on page 4-59), set the desired channel's "Rate" parameter to "64K," and the "Service" parameter to the Service Index for the Serial interface (5).

## Valid Channel Ranges for Serial and CBR Interfaces

The range of channels available to the Serial interface depends on the type of CES service. The table below shows the range of channels available to the Serial and CBR interfaces for each type of CES service. The type of CES service and the SHDSL data rate shown in the table on page 4-60 limit the total number of channels that can be allocated to the Serial interface.

CES Service Type Description	Available Serial Interface Channel Range	Available CBR Interface Channel Range	Comments
Basic E1 (CCS)/Serial	1–31	1–31	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Basic T1 (ESF)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Basic T1 (D4)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
E1 w/Signaling (CAS)	1–31*	1-15, 17-31	Serial interface channels may be any arbitrary set within the available channel range. CBR interface channels may not include Channel 16.**
T1 w/Signaling (ESF)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
T1 w/Signaling (D4)	1–24	1–24	Serial or CBR interface channels may be any arbitrary set within the available channel range.
Unstructured E1/ Unstructured Serial	0–31	0–31	Multiplexing channels between the CBR and Serial interface is not allowed for an unstructured service. All channels may be allocated to either the Serial interface (Service parameter “5”), or the CBR interface (Service parameter “4”), or disabled (Service parameter “0”).
Unstructured T1	None***	1–24	All channels must be allocated to the CBR interface (Service parameter “4”) or disabled (Service parameter “0”).

\*Channel 16 (time slot 6) can be used for the Serial CES service without affecting E1 signaling. The E1 signaling information is extracted from the CBR interface data stream prior to multiplexing it with the Serial interface stream. Therefore, replacing channel 16 (time slot 16) with Serial interface data will not affect the assembly or reassembly of the signaling data in the CES data stream.

\*\*The signaling information in the channel is automatically extracted in this mode and assembled in the signaling substructure of the ATM payload. Including channel 16 in the CBR interface data stream would duplicate the data transmitted in the signaling substructure and is therefore not needed.

\*\*\*An Unstructured T1 CES service is not compatible with a Serial interface CES service because the Serial interface does not support a 1.544 MHz clock rate. However, you may use a Basic T1 CES service and allocate all 24 channels to the Serial interface CES service resulting in a 1.536 MHz clock rate.

## HDLC/PPP Service

This service has no configurable parameters.

## Applications

Select “Applications” in the Main Menu screen to display the various WANsuite 6450 applications (Figure 4.48) associated with configuration tables and statistics for Layer 3 and above that do not map to a specific service or interface.

Figure 4.48 Applications Screen



## Service Aware

The Service Aware function recognizes IP traffic on the WAN and counts the number of frames and bytes passed for a specific service based on filters by VPI/VCI, by DLCI, by IP Address, and by IP Port. Each row of the Service Aware table represents a specific set of filter parameters known as a “rule.” Each rule is established through the Rule Config screen, which is accessed by selecting “Rule Details.”

The Service Aware screen (Figure 4.49) provides a table showing these filtered packet counts for up to 10 rules. This table indicates which Service Aware filters are enabled or disabled, and shows the specific VPI/VCI, DLCI, IP Address, IP Mask, and IP Port by which the IP traffic is filtered. In addition, this table shows the Tx Alarm Threshold and the current Tx Alarm status (if enabled) for each rule.

Figure 4.49 Service Aware Screen

```

----- SERVICE AWARE -----

```

<Ndx>	Svc	UPI	UCI	DLCI	IP Address	IP Mask	IP Port	Tx Alarm Thresh	Tx Alarm
1	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
2	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
3	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
4	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
5	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
6	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
7	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
8	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
9	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK
10	0	0	0	0	000.000.000.000	000.000.000.000	0	0	OK

```

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Required
    
```

## Rule Config Screen

Use the Rule Config screen (Figure 4.50) to establish Service Aware parameters. To establish a rule, select the desired rule configuration options, provide the appropriate filter information where required, and press the “Esc” key.

**Figure 4.50** *Rule Config Screen*

```

----- RULE CONFIG -----
Rule: 1
Service          [ 0 ]
UPI              [ 0 ]
UCI              [ 0 ]
Filter By UPI/UCI [Disabled]
DLCI             [ 0 ]
Filter By DLCI   [Disabled]
IP Address       (000.000.000.000)
IP Mask          (000.000.000.000)
Filter By IP Address [Disabled]
Enter IP Port or ( 0 )
Select from list [ 0 ]
Filter By IP Port [Disabled]
Tx Alarm Threshold ( 0 )
Tx Alarm         OK

(Traffic Meter Stats)

Save & Restart
Required
  
```

The paragraphs below describe the rule configuration parameters and their options.

**Service** Selects the service to which the rule applies. Select from a pull-down menu that lists available services.

**VPI** Selects the VPI to which the rule applies.

**VCI** Selects the VCI to which the rule applies.

**Filter By VPI/VCI** Enables or disables filtering of the IP traffic in accordance with the specified VPI/VCI.



**NOTICE:** *To use this filter, you must specify both the Service and DLCI parameters in the rule configuration.*

**DLCI** Selects the DLCI to which the rule applies from a pull-down list of applicable DLCIs.

**Filter By DLCI** Enables or disables filtering of the IP traffic by the DLCI specified in the DLCI pull-down list.



**NOTICE:** *To use this filter, you must specify both the Service and DLCI parameters in the rule configuration.*

**IP Address** Establishes the IP Address by which the rule will filter IP traffic (if enabled).



**IP Mask** Represents a range of IP Addresses defined so that only machines with IP Addresses within the range defined by the mask are allowed to access an Internet service. To mask a portion of the IP Address, replace it with the wild card character “0” (zero). (For example, an IP Address Filter of 192.44.0.0 and an IP Mask Filter of 255.255.0.0 represent every computer on the Internet with an IP Address beginning with 192.44.)

**Filter By IP Address** Enables or disables filtering of the IP traffic by the IP Address specified in the IP Address or IP Mask field.

**Enter IP Port or Select From List** Establishes the IP port by which the rule will filter IP traffic (if enabled).

**Filter By IP Port** Enables or disables filtering of the IP traffic by the IP port specified in the IP Port field.

**Tx Alarm Threshold** Specifies the threshold in bits per second for the Transmit Alarm on this rule.

**Tx Alarm** Displays the current Transmit Alarm status.

## Traffic Meter Statistics Screen

The Traffic Meter Statistics screen displays the number of frames and octets that have been counted in accordance with the Service Aware “rule” that has been established for a Service. In addition, this screen provides data rate performance information for the period of time specified in the <Period> field (see below).

**Figure 4.51** *Traffic Meter Statistics Screen*

```
----- TRAFFIC METER STATISTICS -----
Service: 0 DLCI: 0 Rule: 1
(Clear Statistics)
<Period> Tx Frames Tx Octets Rx Frames Rx Octets Rate Peak Rate Average
Summary 0 0 0 0 0 0 0 0
Current 0 0 0 0 0 0 0 0
Interval 1 0 0 0 0 0 0 0
Interval 2 0 0 0 0 0 0 0
Interval 3 0 0 0 0 0 0 0
Interval 4 0 0 0 0 0 0 0
Interval 5 0 0 0 0 0 0 0
Interval 6 0 0 0 0 0 0 0
Interval 7 0 0 0 0 0 0 0
Interval 8 0 0 0 0 0 0 0

Ctrl^R PageUp Save & Restart
Ctrl^C PageDown Not Needed
```

The Traffic Meter Statistics screen reports on the following parameters:

- Tx Frames
- Tx Octets
- Rx Frames
- Rx Octets

- Rate Peak – the peak data rate for the viewed period (see below)
- Rate Average – the average data rate for the viewed period (see below)

The “Period” refers to the period of time for which the Traffic Meter statistics are reported as listed below.

**Summary** Represents the past 24 hours; reports the additive number of frames/octets, the highest peak encountered for 24 hours, and the average for 24 hours.

**Current** Reports on the current 15-minute interval.

**Interval 1,**  
**Interval 2,...,**  
**Interval 96** Reports on Intervals 1-96, which correspond to the periods completed 15 minutes ago, 30 minutes ago,..., 24 hours ago.

## Trap Log

A trap is a mechanism that permits a device to send an alarm for certain network events to an SNMP management station. The Trap Log screen (Figure 4.52) shows all generated traps.

The table shown in this screen lists each trap by its Index number, and displays the type of error captured by the trap (Trap Number) and the date and time that the trap was stored (Time Stamp).

**Figure 4.52** *Trap Log Screen*

TRAP LOG		
(Delete Traps)		
Index	Trap Number	Time Stamp
1	t1e1SESAlarmDeclared	Thu Jan 8 00:44:49 1970
2	t1e100FSAlarmDeclared	Thu Jan 8 00:44:49 1970
3	t1e1LOSSAlarmDeclared	Thu Jan 8 00:44:49 1970
4	t1e1SESAlarmDeclared	Thu Jan 8 00:44:49 1970
5	t1e100FSAlarmDeclared	Thu Jan 8 00:44:49 1970
6	t1e1LOSSAlarmDeclared	Thu Jan 8 00:44:49 1970

Ctrl^R PageUp  
Ctrl^C PageDown

Save & Restart  
Not Needed

## IP Gateway

The IP Gateway is a feature of the WANsuite 6450 that allows routing of IP packets from one network to another using *static routes* configuration and/or *dynamic routing*. The IP Gateway uses Routing Information Protocol (RIP) 1 or RIP 2 or Open Shortest Path First (OSPF) routing.

RIP 1 and RIP 2 are protocols that allow exchange of routing information between two routers. With that information exchange, a router can build its own routing tables that later can be used for “routing” IP packets.

OSPF is a shortest path first (SPF) or link-state protocol. OSPF is also an internal gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least cost path as the best path.

While RIP is ideal for small- to medium-sized networks, OSPF is more suitable for complex networks with a large number of routers. OSPF provides equal cost multipath routing where packets to a single destination can be sent via more than one interface simultaneously.

**Figure 4.53** IP Gateway Screen

```

----- IP GATEWAY -----
                                RIP Parameters
RIP Enable                       [Enable RIP2]
RIP Trust Neighbors              [Enable ]
RIP Interval                      (          30)
RIP Domain                       (          0)

                                OSPF Parameters
OSPF Enable                       [Disable]
OSPF Router ID                   (010.002.002.101)

(Static Route Table)  (Area Table)
(Static ARP Table)   (Virtual Link Table)
(Trusted Neighbors)
(Circuit Table)

                                Save & Restart
                                Not Needed

```

## RIP Parameters

**RIP Enable** Globally enables RIP1, RIP2, or No RIP. Default is RIP2.

Values: Disable, Enable RIP1, Enable RIP2

Default: Enable RIP2

**RIP Trust Neighbors** Globally enables the trusted neighbors feature. If there is a list of trusted neighbors in an IP Gateway, only RIP packets coming from those trusted neighbors will be used to build the internal routing table.

Values: Enable, Disable

Default: Enable

**RIP Interval** Interval for RIP packet to be sent. Default is 30 seconds.

**RIP Domain** Value representing the RIP domain. Default is 0.

## OSPF Parameters

**OSPF Enable** This Protocol is suitable for complex networks with a large number of routers. If a large network is involved, OSPF may be the solution for the user.

Values: Disable, Enable

Default: Disable

**OSPF Router ID** This 32-bit number assigned to each router running the OSPF protocol uniquely identifies the router within an Autonomous System. Each router requires a unique router ID. Default is the LAN IP Address of the unit.

The IP Gateway screen provides the following user prompts that may be selected by pressing the “Enter” key:

Prompt	Function
<b>RIP Parameters</b>	
Static Route Table	Displays static and dynamic route information.
Static ARP Table	Displays static ARP information.
Trusted Neighbors	Displays trusted neighbors information.
<b>OSPF Parameters</b>	
Area Table	Displays area information.
Virtual Link Table	Displays virtual link information.
Circuit Table	Provides user access to circuit-related information/operation.

## Circuit Table Screen

This menu shows the configured circuit. To configure a new circuit, select "Add New." Endpoints that begin with “P,” such as Px-Cy, are for ATM VPI x, VCI y. For example, P0-C32 is VPI 0, VCI 32. Endpoints that begin with “S,” such as Sx-yy, are for Frame Relay Service x, DLCI yy. For example, S5-45 is Service 5, DLCI 45. Endpoints that begin with “I” such as Ix-y-z are FRF5 Interworking Frame Relay endpoints for VPI x, VCI y, DLCI z. For example I0-87-45 would be FRF5 Interworking endpoint for VPI 0, VCI 87, DLCI 45.

To configure a new circuit, select “Add New.”

**Figure 4.54** *Circuit Table Screen*

```

----- CIRCUIT TABLE -----
      (Add New)
<Index> Endpoint      IP Address      IP Mask      RIP Status  OSPF Status
   1     LAN          192.094.046.072 255.255.255.000 Disable     Disable

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Required
  
```

**Circuit Details Screen**

Access this menu by selecting the appropriate <Index> number from the Circuit Table menu. The screen's parameters are described in the paragraphs that follow.

**Figure 4.55** *Circuit Details Screen*

```

----- CIRCUIT DETAILS -----
Circuit:  1

Endpoint      [LAN]
IP Address    (010.002.002.101)
IP Mask       (255.255.254.000)
Max Transmit Unit ( 1500)
Cost          ( 1)
RIP Status    [Disable]
Multicast Status [ Enable]
OSPF Status   [Disable]
OSPF Area     (000.000.000.000)
OSPF LSA Timer ( 5)
OSPF LSU Delay ( 1)
OSPF Router Priority ( 1)
OSPF Hello Interval ( 10)
OSPF Dead Interval ( 40)
OSPF Auth Key ( )

      (Delete Circuit)

Save & Restart
Not Needed
  
```

**Endpoint** Endpoint name. By default, the first circuit is always the LAN circuit. All other circuits are associated with Endpoint names as defined in the Endpoint Table.

**IP Address** IP Address of the circuit.

**IP Mask** IP mask of the circuit.

**Max Transmit Unit** Maximum transmit unit this circuit will send at any one time.

<b>Cost</b>	Represents the relative time of treatment of an IP packet. This value is used when there are multiple routes to the same destination. When two or more routes are available, the one with the lowest circuit cost is selected. A frame relay circuit should have a higher value than a LAN circuit.
<b>RIP Status</b>	Indicates whether or not RIP is enabled on this circuit. Values: Disable, Listen and Talk, Talk Only, Listen Only Default: Listen and Talk
<b>Multicast Status</b>	Indicates whether or not Multicast is enabled on this circuit. Values: Enable, Disable Default: Enable
<b>OSPF Status</b>	Indicates whether or not OSPF is enabled on this circuit. Values: Enable, Disable Default: Enable
<b>OSPF Area</b>	Represents that area that this circuit is part of.
<b>OSPF LSA Timer</b>	Determines how often The Link State Acknowledgment (LSA) packet is sent. Values: 1–3600 Default: 5
<b>OSPF LSU Delay</b>	The estimated number of seconds it takes to transmit a Link State Update (LSU) packet over this circuit interface. Values: 1–3600 Default: 1
<b>OSPF Router Priority</b>	This 8-bit unsigned integer ranges from 1 to 255 and assigns priority to one of two routers attached to the same network; without an assigned priority, both routers attempt to become the designated router. Values: 1–255 Default: 1
<b>OSPF Hello Interval</b>	The time in seconds between the Hello packets that a router sends on a circuit. This value is also advertised in the router's Hello packets and must be identical for all routers on the same network. The smaller the Hello Interval, the sooner topological changes are detected (but then more traffic is created). Values: 1–65535 Default: 10
<b>OSPF Dead Interval</b>	The number of seconds that a router's "Hellos" have not been received before its neighbors declare the router down. The value must be the same as the value on the network. Values: 1–65535 Default: 40

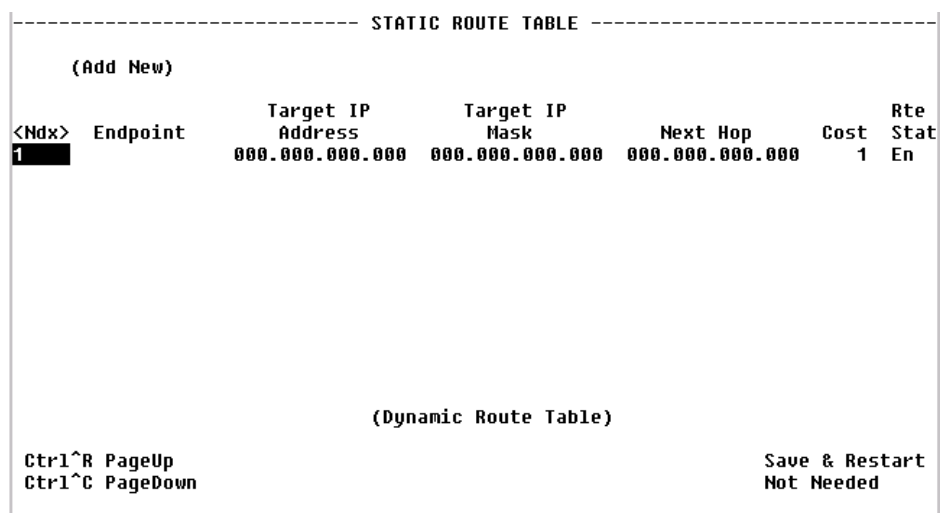
**OSPF Auth Key** When configured, this parameter allows an authentication procedure to be executed on the OSPF header. If the 64-bit (8 character) password does not correspond, the packet is thrown away.

Values: 64 bits (8 characters)  
 Default: 8 spaces (no authentication)

## Static Route Table Screen

Under some circumstances, it may not be necessary for a router to learn a route using ordinary means such as RIP or OSPF. It is possible under these circumstances for you to add a route to the route table of a router. The Static Route menus are always associated with a circuit.

**Figure 4.56** *Static Route Table Screen*



The fields on this screen are described below.

Field	Description
Endpoint	Endpoint name (or interface) through which to send the IP packet to reach the Target IP Address.
Target IP Address	Represents the target network that you want this router to reach.
Target IP Mask	Mask of the target network.
Next Hop	IP Address of the next device in the route.
Cost	Cost of using that route.
Rte Stat	Indicates whether or not a route is enabled or disabled.

## Route Details Screen

This screen (Figure 4.57) displays the details associated with a specific route.

**Figure 4.57** *Route Details Screen*

```
----- ROUTE DETAILS -----
Route:      1

Endpoint    [LAN]
Target IP Address (000.000.000.000)
Target IP Mask  (000.000.000.000)
Next Hop IP Address (000.000.000.000)
Cost        ( 1)
Route Status [          Enable]

          (Delete Route)

Save & Restart
Not Needed
```

**Endpoint** Endpoint name (or interface) through which to send the IP packet to reach the Target IP Address.

**Target IP Address** Represents the target network that you want this router to reach.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Target IP Mask** Mask of the Target IP or network.  
Represents the target network that you want this router to reach.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0



---

**NOTICE:** *Setting the Target IP Address and Target IP Mask to 0.0.0.0. defines THE default route for this unit.*

---

**Next Hop IP Address:** IP Address of the next device in the route.

**Cost** Cost of using that route.  
Values: 0–65535  
Default: 1

**Route Status** Indicates whether or not the current route is enabled.  
Values: Disable, Enable, Enable and Advertise  
Default: Enable

### ***Dynamic Route Table Screen***

Access this menu (Figure 4.58) by selecting the “Static Route Table” on the IP Gateway menu and then selecting Dynamic Route Table. This table shows both dynamic and circuit tables. Please note that not all parameters are necessarily defined, depending on whether or not the routes were learned



dynamically. Primarily, the most useful information is included in "Destination," "If Ndx," and "Mask" columns.

**Figure 4.58** *Dynamic Route Table Screen*

```

----- DYNAMIC ROUTE TABLE -----
Destination      If      Next Hop      Mask
000.000.000.000  1      192.094.046.001  000.000.000.000
127.000.000.001  34     127.000.000.001  000.000.000.000
192.094.046.000  1      192.094.046.072  255.255.255.000

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Required

```

The Dynamic Route Table displays the fields listed below.

Field	Description
Destination	Network to be reached.
If Ndx	Interface internal number.
Next Hop	IP Address used to reach the destination network.
Mask	Mask of the destination network.

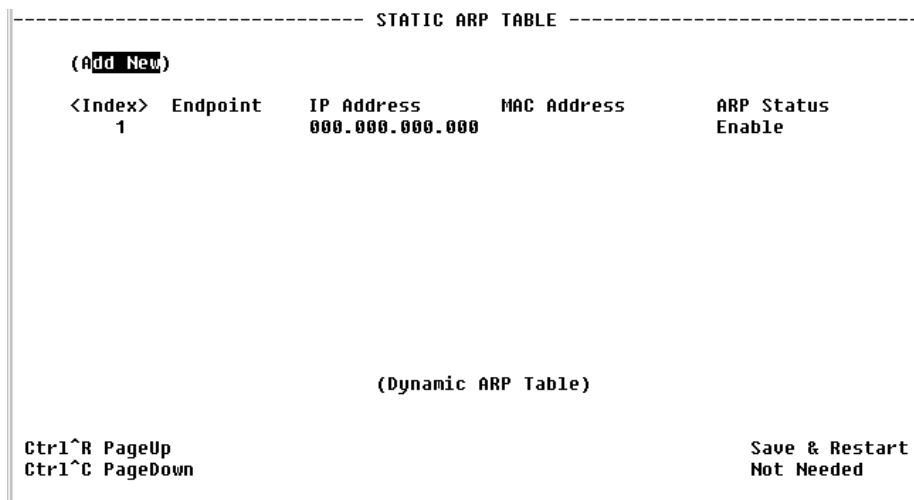
### Static ARP Table Screen

ARP (Address Resolution Protocol) is used by the router to dynamically associate a high-level IP Address to a low-level physical hardware address. ARP packets are only sent across a single physical network.

There are some cases when an IP-compatible device does not support ARP or ARP is deliberately disabled (for security). In these cases, instead of using ARP to dynamically update the router internal MAC <-> IP Address Table, this menu can *force* an entry into that table. This entry never times out.

At least one circuit must be defined to create a Static ARP Table entry because an ARP entry is always associated with a circuit. The static ARP table is useful when a Host does not respond to an ARP request. Access this menu by selecting "Static ARP Table" from the IP Gateway menu.

**Figure 4.59** *Static ARP Table Screen*



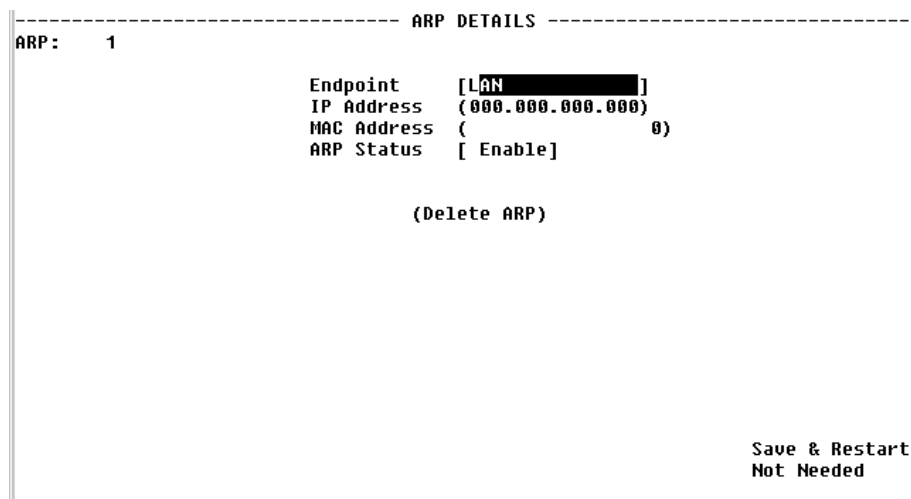
The fields listed below are displayed on the Static ARP Table screen.

Field	Description
Endpoint	Endpoint name (or Interface) through which to send the IP packet to reach the defined IP Address. Currently, this is always the LAN.
IP Address	The IP Address of the unit for which you want to define the MAC Address.
MAC Address	The MAC Address of the host to be reached.
ARP Status	Displays whether this static ARP is enabled or disabled.

**ARP Details Screen**

Access this screen by selecting the applicable <Index> number on the ARP Table screen.

**Figure 4.60** *ARP Details Screen*



**Endpoint** Endpoint name (or Interface) through which to send the IP packet to reach the defined IP Address. The default is the LAN.

**IP Address** IP Address of the circuit.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

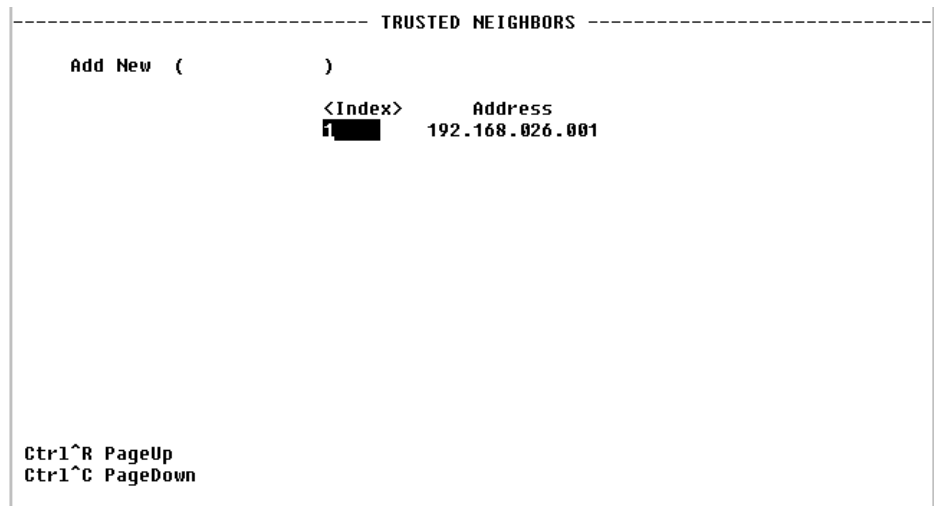
**MAC Address** The MAC Address of the Host to be reached.  
Values: A 6-byte value  
Default: 00-00-00-00-00-00

**ARP Status** Displays whether this static ARP is enabled or disabled.  
Values: Enable, Disable  
Default: Enable

## Trusted Neighbors Screen

The Trusted Neighbors feature can be used to store RIP information only from a specific router. This allows the router to reject any RIP information coming from non-Trusted Neighbors. Only information coming from Trusted Neighbors is kept by the router. Access this menu by choosing Trusted Neighbors from the IP Gateway menu. This table is useful when the Network Administrator wants to listen to RIP of specific router(s).

**Figure 4.61** *Trusted Neighbors Screen*



**Add New** Adds a Trusted Neighbors IP Address.

## Area Table Screen

An Area allows growth and makes the networks at a site easier to manage. An area is self-contained; knowledge of an area's topology remains hidden from other areas. Thus, multiple groups within a given site retain the ability to change their internal network topology independently.

**Figure 4.62** Area Table Screen

```

----- AREA TABLE -----
(Add New)
<Ndx>      Area ID      Ena      Auth      Stub  Addr Summary  Mask Summary  Ad
  1  000.000.000.000  En      none      No    000.000.000.000  000.000.000.000  Dis

Ctrl^R PageUp                               Save & Restart
Ctrl^C PageDown                              Not Needed
  
```

The fields displayed on the Area Table screen are described below.

Field	Description
Area ID	Displays the ID of the Area (represented by an IP Address).
Ena	Displays whether the defined area is enabled or disabled.
Auth Type	Indicates Area validation.
Stub	Displays whether or not the defined area is a Stub Area.
Addr Summary	Displays the Address Summary of the defined Area.
Mask Summary	Displays the Mask Summary of the defined Area.
Ad	Displays whether advertising is enabled or disabled for this Area.

**Area Details Screen**

This screen displays the details associated with a defined Area.

**Figure 4.63** Area Details Screen

```

----- AREA DETAILS -----
Area: 1

Area ID      (000.000.000.000)
Enable      [ Enable]
Auth Type    [ none]
Stub        [ No]
Address Summary (000.000.000.000)
Mask Summary (000.000.000.000)
Advertise    [Disable]

(Delete Area)

Save & Restart
Not Needed
  
```

**Area ID** This parameter has the same format as the IP Address of the Mask Address.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Enable** Displays whether or not this Area is enabled.  
Values: Enable, Disable  
Default: Enable

**Auth Type** Indicates type of Authentication.  
Values: Simple, None  
Default: None

**Stub** An area can be configured as stub when there is a single exit point from the area, or when the choice of exit point need not be made on a per-external-destination basis.  
Values: Yes, No  
Default: No

**Address Summary** A configured address range specifies what addresses are contained within an area. When summarizing the routes in an area to inform other areas, all routes falling within the configured range are described by a single LSA, thus decreasing the size of the LSA database.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Mask Summary** IP Mask of the summary to be added.  
Values: 0.0.0.0–255.255.255.255  
Default: 0.0.0.0

**Advertise** Describes the local state of a router or network. This includes the state of the route's interfaces and adjacencies. Each link state advertisement is flooded throughout the routing domain. The collected link state advertisements of all routers and networks form the protocol's topological database.  
Values: Yes, No  
Default: No

## Virtual Link Table Screen

To permit maximum flexibility, OSPF allows the configuration of *virtual* links to enable the backbone area to appear contiguous despite the physical reality.

In OSPF, the backbone is defined as an Area ID of 0.0.0.0. This backbone cannot be disconnected in any way or some areas of the Autonomous System become unreachable. This is because all inter-area traffic must go through the backbone. In fact, the backbone is responsible for all inter-area routing information distribution.

It is possible that an area cannot be connected directly to the backbone. In this case a virtual link is used. To establish or maintain the connectivity of the backbone, virtual links can be configured through non-backbone areas. Basically, virtual links are used to connect components that are otherwise not connected to the backbone.

A virtual link is treated by OSPF as a point-to-point unnumbered network joining two area border routers. The virtual link must be configured in both of the area border routers.

A virtual link is defined by the following two parameters:

- The Router ID of the virtual link's other endpoint
- The non-backbone area the virtual link goes through.

**Figure 4.64** *Virtual Link Table Screen*

```

----- VIRTUAL LINK TABLE -----
(Add New)

      <Ndx>  Enable      Transit      Area Border
              1  Enable    000.000.000.000  000.000.000.000

Ctrl1^R PageUp          Save & Restart
Ctrl1^C PageDown       Not Needed
  
```

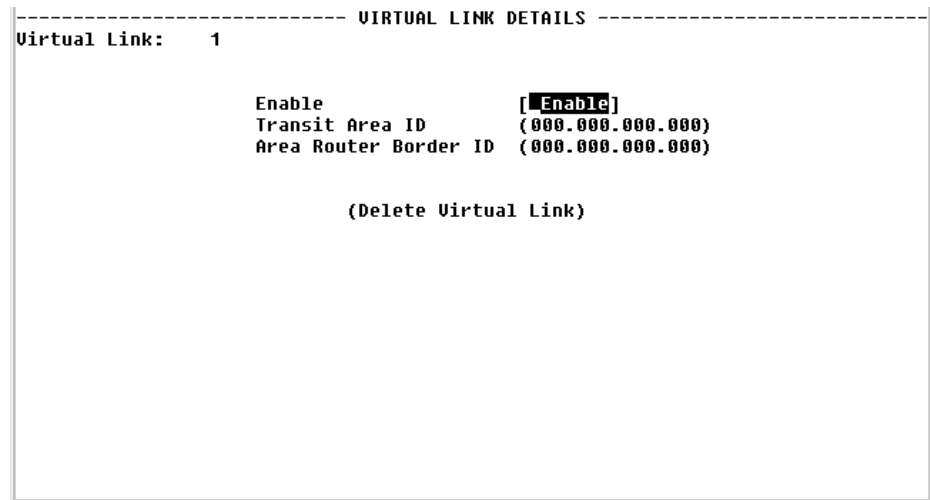
The fields displayed on the Virtual Link Table screen are described below.

Field	Description
Enable	Enables the definition of a virtual link.
Transit Area ID	The non-backbone area the virtual link goes through.
Area Border Router ID	The Router ID of the virtual link's other endpoint.

### ***Virtual Link Details Screen***

This screen displays the details associated with the specific Virtual Link.

**Figure 4.65** *Virtual Link Details Screen*



## Network Address Translation (NAT)

NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP Address. This lets users cost-effectively and efficiently connect their networks to the Internet.

Whether on a global or local port, NAT provides translation only upon receipt of a packet, which NAT will translate, not translate, or filter, depending on the user-specified parameters (further described below). If the decision is made to “translate,” the packet will be modified internally, and eventually sent on to the IP Gateway to be processed. If the decision is made not to “translate,” the packet will not be modified in any way. If the decision is made to “filter,” the packet will be discarded without any further action required.



---

**NOTICE:** *You must Save and Restart for any changes in NAT configuration parameters to take effect.*

---

### NAT Details Screen

The NAT Details screen (Figure 4.66) lets the user configure the NAT global parameters described below.

Figure 4.66 NAT Details Screen

```
----- NAT DETAILS -----
Enable                [Disable]
Mode                  [NAPT ]
Global IP Address     (192.168.025.012)
Global Mask           (255.255.255.000)
ICMP Default Address  (192.168.025.012)
Filter Non Local Address [Enable ]
IP Entry Timer        ( 120)
TCP Connection Timer  ( 300)
TCP Closing Timer     (   0)
TCP Disconnected Timer ( 120)
TCP Sequence Delta Timer ( 180)
UDP Timer             ( 120)
ICMP Timer            ( 120)

(Static TCP Translation Table)
(NAT Ports)
(Static UDP Translation Table)

Save & Restart
Not Needed
```

**Enable** Enables or disables NAT. Default is “Disable.”

**Mode** Selects the Network Address Port Translation (NAPT) mode or the Basic NAT mode. In NAPT mode, all hosts on the Global (public) side view all hosts on the Local (private) side as a single internet host (one IP Address). In Basic NAT mode, the Global IP Address is assigned as a Class C host address (Mask of 255.255.255.0). Each private IP Address on the Local side is mapped to a Class C public address on the Global side. In other words, if there are 30 hosts on the private (Local) side, 30 public (Global) addresses are required. The default is NAPT.

**Global IP Addr** Global IP Address used in NAPT mode. Must be a valid Class C address. Default is LAN IP Address.

**Global Mask** IP Mask associated with defined Global IP Address. Default is LAN IP Mask.

**ICMP Default Addr** Default source address used to answer any ICMP request. Default is LAN IP Address. ICMP requests are not transferred from the Global to the Local side. Rather they are answered by the unit itself since Local addresses are private and do not receive unsolicited requests.

**Filter Non Local Address** Discards any packet with “non corporate” source address. Default is “Enable.”

The screen parameters listed below are related to the NAT Control Block Timer. Note that default values should be in accordance with most NAT applications. The timers’ values minimize NAT resources. Generally, when a timer has expired, the resources used are no longer needed. Those resources will then be available for other connection resources.

**IP Entry Timer** The maximum time (in seconds) NAT will use resources when not using TCP, UDP, or ICMP.

Values: 0–65535

Default: 120



**TCP Connection Timer** The maximum time (in seconds) NAT will use resources when attempting to establish a TCP connection.

Values: 0–65535

Default: 300

**TCP Closing Timer** The maximum time (in seconds) NAT will use resources when attempting to close a TCP connection.

Values: 0–65535

Default: 0

**TCP Disconnected Timer** The maximum time (in seconds) NAT will use resources when attempting to disconnect from TCP.

Values: 0–65535

Default: 120

**TCP Sequence Delta Timer** The maximum time (in seconds) NAT will use resources when managing TCP Packet Sequencing.

Values: 0–65535

Default: 180

**UDP Timer** The maximum time (in seconds) NAT will use resources for a UDP port in use.

Values: 0–65535

Default: 120

**ICMP Timer** The maximum time (in seconds) NAT will use resources for any ICMP request.

Values: 0–65535

Default: 120

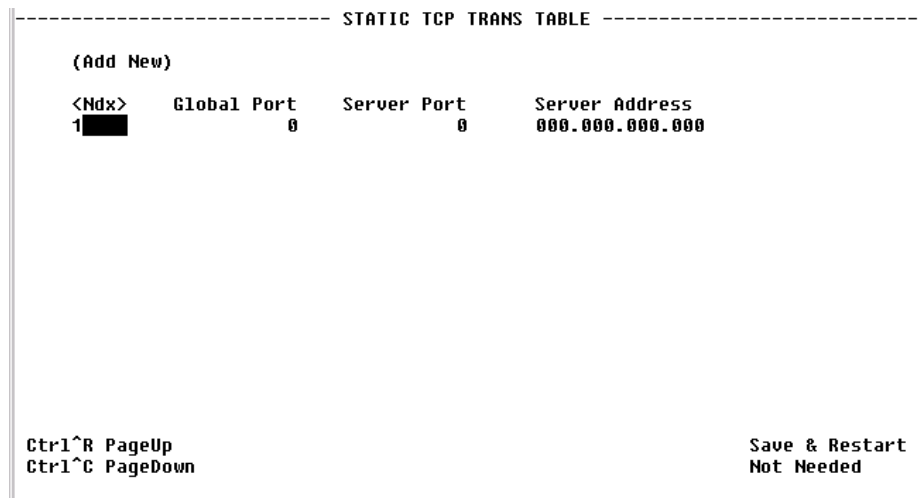
The NAT Details screen provides the following user-activated prompts:

Prompt	Function
Static TCP Translation Table	Allows static mapping of global TCP Server ports to a local host IP Address/port combination.
NAT Ports	Defines NAT global/Internet and local/corporate ports.
Static UDP Translation Table	Allows static mapping of global UDP Server ports to a local host IP Address/port combination.

### ***Static TCP Trans Table Screen***

The Static TCP Trans Table screen (Figure 4.67) allows static mapping of global TCP Server ports to a local host IP Address/port combination. The parameters described below enable access to TCP servers on the private/corporate network “behind the NAT.” The parameters may be used only when in NAPT mode.

**Figure 4.67** *Static TCP Translation Table Screen*



**Global Port** Decimal IP Port exposed to the global Internet. Default is 0.

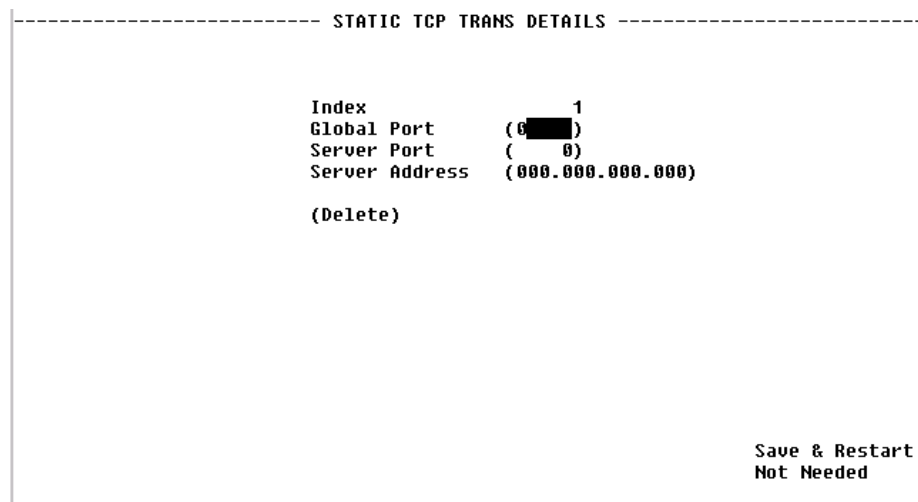
**Server Port** Decimal IP Port of the local TCP Server. This port is usually the same as the Global Port. Default is 0.

**Server Address** IP Address of the local TCP Server. Default is 0.0.0.0.

The “Add New” prompt lets the user add additional addresses.

You can configure or change the above-listed parameters on the Static TCP Trans Details screen (Figure 4.68), which is accessed by selecting the appropriate <Ndx> number on the Static TCP Trans Table screen.

**Figure 4.68** *Static TCP Translation Details Screen*



### ***NAT Ports Screen***

The parameters on the NAT Ports screen (Figure 4.69) define the NAT global/Internet and local/Corporate ports. These parameters are configured in the NAT Ports Details screen shown in Figure 4.70. Access the NAT Ports Details

screen by selecting the <Ndx> number of the desired port on the NAT Ports screen.

**Figure 4.69** NAT Ports Screen

----- NAT PORTS -----						
(Add New)						
<Ndx>	Enable	Default	Type	IP Address	Mask	Endpoint
1	Enable	Disable	Global	192.168.025.012	255.255.255.000	LAN

Ctrl^R PageUp  
Ctrl^C PageDown

Save & Restart  
Not Needed

**Enable** Enables or disables the NAT port. Default is “Enable.”

**Default Translation** Forces translation on a specific IP port regardless of the source IP Address. If Default Translation is set to “Enable,” the packet will never be discarded, but will always pass through the translation path. Therefore, any packets with a destination address different from the global/Internet network address will be processed by the IP Gateway, and may be routed to another port. If this parameter is set to “Disable,” no packet with a destination address different from the global/Internet address will be processed. Setting this parameter to “Disable” will override an “Enable” parameter set under “Filter Non Local Address” on the NAT Details menu.

**Type** Defines whether this port is local or global. Default is LAN global. All others are local.

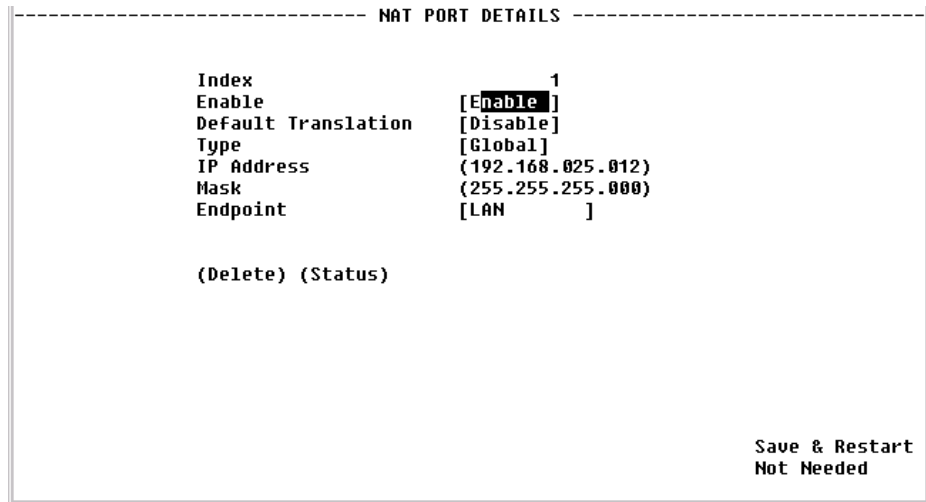
**IP Address** IP Address of this port. Default is the value defined in the IP Gateway Circuit Table.

**Mask** Mask related to the defined IP Address. Default is the value defined in the IP Gateway Circuit Table.

**Endpoint** The Endpoint name of the circuit associated with the LAN or WAN port. Default is LAN for the first port.

The “Add New” prompt lets the user add additional ports.

**Figure 4.70 NAT Port Details Screen**

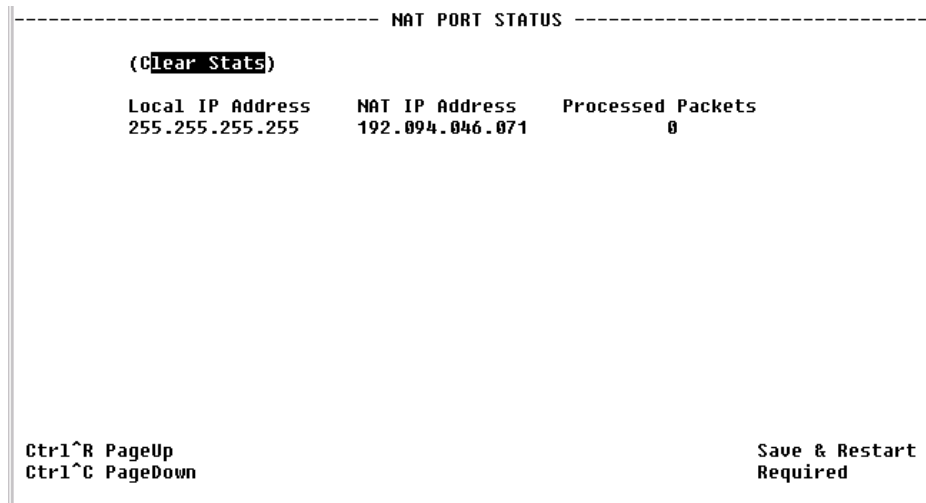


The NAT Port Details screen provides the following user-activated prompts:

Prompt	Function
Delete	Deletes the specified NAT Port.
Status	Displays the NAT Port Status screen (Figure 4.71).

The NAT Port Status screen shown below displays for each port the processed packets from specific IP Addresses.

**Figure 4.71 NAT Port Status Screen**



**IP Address** Original IP Address of the host.

**NAT IP Address** Translated IP Address of the host.

**Processed Packets** Number of packets processed by NAT for this address.

### Static UDP Trans Table Screen

The Static UDP Trans Table screen (Figure 4.72) allows static mapping of global UDP Server ports to a local host IP Address/port combination. The parameters described below enable access to UDP Servers on the private/corporate network “behind the NAT.” The parameters may be used only when in NAPT mode.

Figure 4.72 Static UDP Translation Table Screen

```
----- STATIC UDP TRANS TABLE -----
(Add New)
<Ndx>   Global Port   Server Port   Server Address
1       0             0            000.000.000.000

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Not Needed
```

- Global Port** Decimal IP Port exposed to the global Internet. Default is 0.
- Server Port** Decimal IP Port of the local UDP Server. This port is usually the same as the Global Port. Default is 0.
- Server Address** IP Address of the local UDP Server. Default is 0.0.0.0.

The “Add New” prompt lets the user add additional addresses.

You can configure or change the above-listed parameters on the Static UDP Trans Details screen (Figure 4.73), which is accessed by selecting the appropriate <Ndx> number on the Static UDP Trans Table screen.

Figure 4.73 Static UDP Translation Details Screen

```
----- STATIC UDP TRANS DETAILS -----

Index           1
Global Port     (0)
Server Port     (0)
Server Address  (000.000.000.000)

(Delete)

Save & Restart
Not Needed
```

# Bridge

A Bridge operates at the physical network layer, connecting two or more networks and forwarding packets between those networks. For example, a Bridge will connect two or more physical Ethernet cable segments and forward Ethernet packets from one segment to the other.

Bridges differ from routers in that bridges forward packets based on physical addresses rather than on the IP Addresses that routers use to forward packets. Bridges will not “blindly” forward packets from one network to others, however. Rather, it learns all local physical addresses and forwards packets based on those learned “tables.” This greatly reduces the number of broadcasted packets, thus saving valuable bandwidth.

The Bridge Details screen shown in Figure 4.74 lets you access and configure the parameters described below.

**Figure 4.74** *Bridge Details Screen*

```
----- BRIDGE DETAILS -----
Enable                               [Disable]
Group Multicast MAC Addr             (0180C2000000 )
Bridge ID                             (      0)
Hello Timer                           (     10)
Max Age Timer                          (     60)
Forward Delay                          (      5)
Filter Aging Timer                     (    300)

(Bridge Port Table)
(Bridge Lookup Table)

Save & Restart
Not Needed
```

From this screen, you may view the parameters described below.

**Enable** Enables or disables Bridging capability.  
Values: Enable, Disable  
Default: Disable

**Group Multicast MAC Address** MAC Address recognized by the Bridge as the group address for the Bridge Protocol Data Unit (BPDU) transfer between bridges.  
Values: Any valid Group Multicast MAC Address  
Default: 0180C2000000

**Bridge ID** Consists of a bridge priority and its own MAC Address.  
Values: 1–65535  
Default: 2

**Hello Timer** Specifies the BPDU broadcasting interval.  
Values: 1–65535 s  
Default: 10 s

**Max Age Timer** Specifies the length of time a bridge will consider the network topology held in memory as valid.

Values: 1–65535 s

Default: 60 s

**Forward Delay** Specifies the length of time to delay creation of a temporary loop in the network.

Values: 1–65535 s

Default: 5 s

**Filter Ageing Timer** Specifies the length of time an entry in the lookup table will be held if no traffic is received from the specified MAC Address.

Values: 1–65535 s

Default: 300 s

Selecting the Bridge Port Table prompt displays the screen shown below in Figure 4.75. Selecting a number in the “Index” column of the Bridge Port Table will bring up the Bridge Port Details screen (Figure 4.76), which displays, and, in some cases, lets you change, these parameters.

**Figure 4.75** *Bridge Port Table*

```
----- BRIDGE PORT TABLE -----
(Add New)
<Ndx> Enable  Endpoint  BPDUs  Filter  Filter  Forward
      Disabled LAN      Option Multicasts Broadcasts IP Only  State
1     Disabled LAN      Disable No          No          No      Disabled

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Not Needed
```

**Figure 4.76** *Bridge Port Details*

```

----- BRIDGE PORT DETAILS -----
Bridge Port      1          State      Disabled
Enable          [Disabled]
Endpoint        [LAN      ]
BPDU Option     [Disable ]
Filter Multicasts [No     ]
Filter Broadcasts [No     ]
Forward IP Only [No     ]
Priority        (          1)
Path Cost       (          100)
Designated Root 0000000000000000
Designated Cost 0
Designated Bridge 0000000000000000
Designated Port  1
Forward Transitions 0
Input Frame      0
Output Frames    0
Input Discards   0

(Delete Port)

Save & Restart
Not Needed

```

**Enable** Enables or disables Bridging on this port.

**Endpoint** Endpoint name.

**BPDU Option** Shows if BPDU packet will be sent and received on this port.

**Filter By Multicast Addr Dest** Filters broadcast messages received on this port, which reduces the load on the WAN connection.

**Filter By Broadcast Addr Dest** Filters broadcast messages received on this port, which reduces the load on the WAN connection.

**Forward IP Frames Only** Setting this option to “Yes” specifies that only IP frames will be forwarded and all other frames will be filtered.

**Priority** Value of priority associated with this port. The lower the value, the higher the priority.

**Path Cost** Associated Path Cost to the route for this port.

**State** If Enabled, reflects the state of the port. “Blocking” means there is no data transfer between LANs. “Listening” means the frames received from this port are filtered, but do not modify the Lookup Table. “Learning” means that while the port continues to look at frames without participating in data transfer, the frames received from the port will be used to update the Lookup Table. “Forwarding” means the port participates fully in data transfer and the frames received are used to update the Lookup Table.

**Designated Root** MAC Address of the designated root of the spanning-tree topology.

**Designated Cost** Associated Path Cost of this port to the route.

**Designated Bridge** Designated Bridge MAC Address.



- Forward Transmissions** Number of times this port has changed from any other state to a “Forwarding” state.
- Input Frame** Number of frames received.
- Output Frame** Number of frames transmitted.
- Input Discards** Number of frames discarded.

## TFTP Configuration

A Trivial File Transfer Protocol (TFTP) service on a server can provide remote file access to the WANsuite 6450 to

- Update the firmware on a WANsuite unit
- Save the configuration setup of a WANsuite unit
- Restore a saved configuration setup to a WANsuite unit

To transfer a file to or from a TFTP server from a WANsuite unit, you must indicate the TFTP server’s IP address and file name, and then perform a Get operation to receive a file from the server, or a Put operation to send a file to the server. The file name and its extension determine the type of file transferred.

The table below shows the possible file operations.

Operation	File Name Extension	Action
Update Application Firmware	.CHX or .HEX	Get
Update Boot Firmware	.HEX	Get
Save Configuration Setup	.CFG	Put
Restore Configuration Setup	.CFG	Get

Note that when updating the application software using a .HEX file, the file name should have the form xxAPxxxx.HEX; the AP indicates the file is an application load. When updating the boot software, the file name should have the form xxWBxxxx.HEX; the WB indicates the file is a boot load.

**Figure 4.77** TFTP Configuration Screen

```

----- TFTP CONFIGURATION -----

TFTP Server IP Address (000.000.000.000)
File Name ( )

(TFTP Get File)
(TFTP Put File)
(TFTP Abort )

Status Idle

Save & Restart
Not Needed
  
```

**TFTP Server IP Address** IP address of the server providing TFTP access.

**File Name** Name of the file to be transferred.

**Status** Indicates the current status of the TFTP operation. Possible values include Idle, Getting File, Putting File, Aborting, Transfer Complete, Invalid File Name, and Invalid File.

The following user-selectable prompts appear on the TFTP Configuration screen.

Prompt	Function
TFTP Get File	Initiates a transfer from a server to the WANsuite unit.
TFTP Put File	Initiates a transfer from the WANsuite unit to a server.
TFTP Abort	Aborts the transfer.

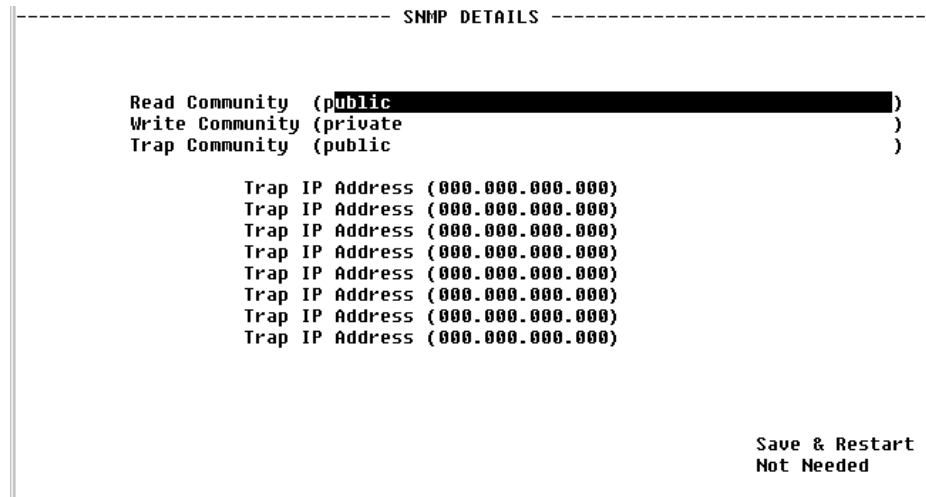


**NOTICE:** Before performing the “Get” or “Put” operation, verify that the server IP address and filename have the correct values.

## SNMP

The unit detects and reports T1 or E1 network alarms and provides several options for reporting them, one of which is SNMP traps. When a network alarm occurs, the unit sends a trap message to as many as eight destinations on your network. The unit will report each alarm by transmitting an SNMP “trap” to each non-zero Trap IP Address. The SNMP Details screen (Figure 4.78) lets you configure the SNMP parameters described below.

**Figure 4.78** *SNMP Details Screen*



- Read Community** Accepts a character string identifying the group authorized to perform read operations. The default setting is “Public.”
- Write Community** Accepts a character string identifying the group authorized to perform write operations. The default setting is “Private.”
- Trap Community** Accepts a character string, which is included in SNMP traps generated by the unit. The default setting is “Public.”
- Trap IP Address** Accepts the IP Address of a network device where alarm reporting traps are to be sent.

## Top Talkers

Selecting “Top Talkers” displays the Top Talkers screen (Figure 4.79), which is used to set parameters for and initiate the generation of a list of IP Addresses ranked in terms of the number of frames and octets they have transmitted during a specified reporting period. This report allows MIS managers to determine who is generating the most traffic on a WAN based on IP Addresses.

**Figure 4.79** *Top Talkers Screen*

```

----- TOP TALKERS -----
Duration (sec)      (0)
Requested Report Size ( 0)
Time Remaining (sec) 0
                    (Start)
Report #           0
Size              0
Start Time
System Up Time 4 days, 00:01:14

Index IP Address   Timestamp      Rx Frames Rx Octets Tx Frames Tx Octets

Ctrl^R PageUp
Ctrl^C PageDown

Save & Restart
Not Needed
    
```

To generate a Top Talkers report, enter the duration parameters and desired report size in the available fields as described below, and then press the “Enter” key or select the “Start” prompt on the screen.

**Duration (sec)** Establishes the amount of time (in seconds) for which the Top Talkers report will capture IP traffic; typically this value is 900 seconds (15 minutes).

**Requested Report Size** Establishes how many IP Addresses will be reported as the “Top Talkers.”




---

**NOTICE:** *While you may request any number, the unit is internally limited to a maximum report size of 20.*

---

As soon as you initiate generation of a report by pressing the “Enter” key or selecting the “Start” prompt, the Duration value is copied over to the Time Remaining field. When the specified Duration for the report has elapsed, the resulting report-specific information will be displayed on the left side of the screen.

**Time Remaining** The amount of time (in seconds) for which the Top Talkers report will capture IP traffic; typically this value is 900 (15 minutes). As soon as you initiate generation of the report, the Duration value is copied over to the Time Remaining field.

**Report #** Displays a unique number used to identify the generated report. This number is generated automatically, is incremented sequentially for each report, and can be used by management stations for automatic polling (via the ipadv2.mib).

**Size** Displays the actual number of IP Addresses identified as Top Talkers in the generated report. The maximum report size is 20.

**Start Time** Displays the time at which the Top Talkers report was initiated (based on System Up Time).

**System Up Time** Displays the amount of time that the unit has been operational since it was turned on or last reset.

The Top Talkers table reports in descending order the IP Addresses that have generated the most traffic during the requested report's duration. For each IP Address listed, the report displays the number of Rx frames, Rx octets, Tx frames, and Tx octets that have been passed across it. In addition, the Timestamp field indicates the time at which a packet was examined for the specified IP Address.

## Originate Ping

The WANSuite 6450 Originate Ping (Figure 4.80) function helps telephone companies determine if a network is properly configured and also helps them maintain SLAs.

**Figure 4.80** *Originate Ping Screen*

```
----- ORIGINATE PING -----

(Start Ping)      Dest IP Address      (000.000.000.000)
(Stop Ping)       Number to Send      (  5)
(Reset Status)    Ping Size (Bytes)   ( 100)
                  Ping Reply Timeout (sec) (  1)

Ping Status:
Ping IP Address required

Save & Restart
Required
```

The parameters on the left side of the screen offer you the following choices: Start Ping, Stop Ping, or Reset the Status (clears all counts activity). Other parameters include the following:

**Dest IP Address** Destination IP Address of sent Ping request messages.

**Number to Send** Number of Ping request messages to send.

Values: 1–10,000

Default: 5

**Ping Size** Number of bytes in a Ping request message.

Values: 100–4096 bytes

Default: 100 bytes

**Ping Reply Timeout** Number of seconds to wait for a reply to a Ping request message.

Values: 1–60 s

Default: 1 s

Below these parameters is a status table that shows the number of pings returned versus the number requested, and provides minimum, average, and maximum statistics.

## Dynamic Host Configuration Protocol (DHCP)

DHCP provides a mechanism through which computers using TCP/IP can obtain protocol configuration parameters automatically through the network.

The most important configuration parameter associated with DHCP is the IP Address. A computer must initially be assigned a specific IP Address that is appropriate to the network to which the computer is attached, and that is not assigned to any other computer on that network. If a computer moves to a new network, it must be assigned a new IP Address for that new network. DHCP can be used to manage these assignments automatically.

DHCP has other important configuration parameters also, such as the subnet mask, default router, and Domain Name System (DNS) server. Using DHCP, a network administrator can avoid “hands-on” configuration of individual computers through complex and confusing setup applications. Instead, those computers can obtain all required configuration parameters automatically, without manual intervention, from a centrally managed DHCP server. DHCP is available on the 10/100 Ethernet port only.



---

**NOTICE:** *You must Save and Restart for any changes in DHCP configuration parameters to take effect.*

---



---

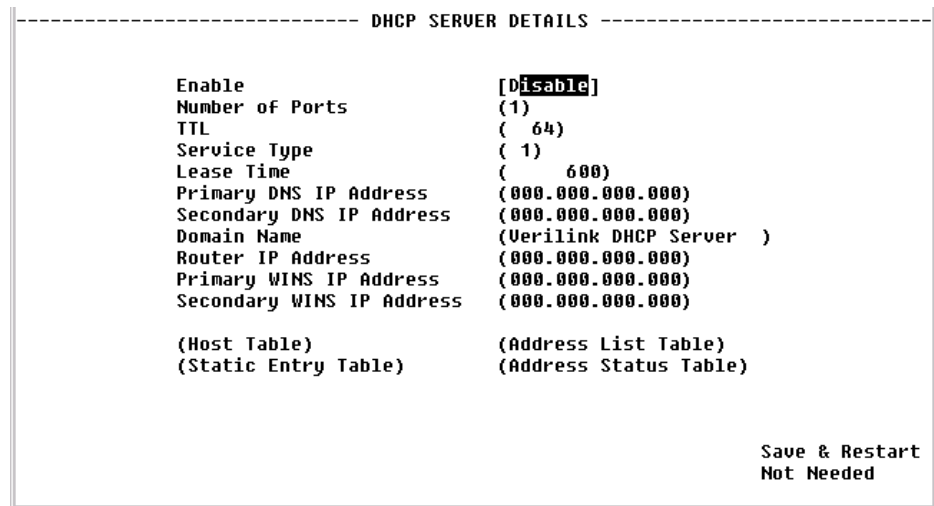
**NOTICE:** *Always verify that a DHCP server is available on the network before enabling DHCP Client. If, on power-up, a DHCP server is not found, a 60-second timeout will occur.*

---

### DHCP Server Details Screen

The DHCP Server Details screen (Figure 4.81) lets you configure the parameters described below.

**Figure 4.81** DHCP Server Details Screen



- Enable** Enables or disables the DHCP Server. Default is “Enable.”
- Number of Ports** Defines the number of DHCP ports to be used. In this version, only “1” is a valid value.
- TTL** Time to Live for any DHCP packet. Default is 64.
- Service Type** Type of Service used by the DHCP Server packet. Default is 1.
- Lease Time** Tells the DHCP client the number of seconds it can retain this IP Address. The client should make a new DHCP request within the specified amount of time to ensure the IP Address is not given to another PC. Default is 600 seconds.
- Primary DNS IP Addr** If requested by DHCP client, the client then uses this address to resolve names of IP Addresses. Default is 0.0.0.0.
- Secondary DNS IP Addr** If requested by DHCP client, the client then uses this secondary address to resolve names of IP Addresses. Default is 0.0.0.0.
- Domain Name** Domain name to be used by all DHCP clients. Default is user’s server.
- Router IP Addr** IP Address that all clients use for Gateway or Router. Default is 0.0.0.0.
- Primary WINS IP Addr** If requested by DHCP client, the client then uses this address to resolve names of IP Addresses. Default is 0.0.0.0.
- Secondary WINS IP Addr** If requested by DHCP client, the client then uses this secondary address to resolve names of IP Addresses. Default is 0.0.0.0.

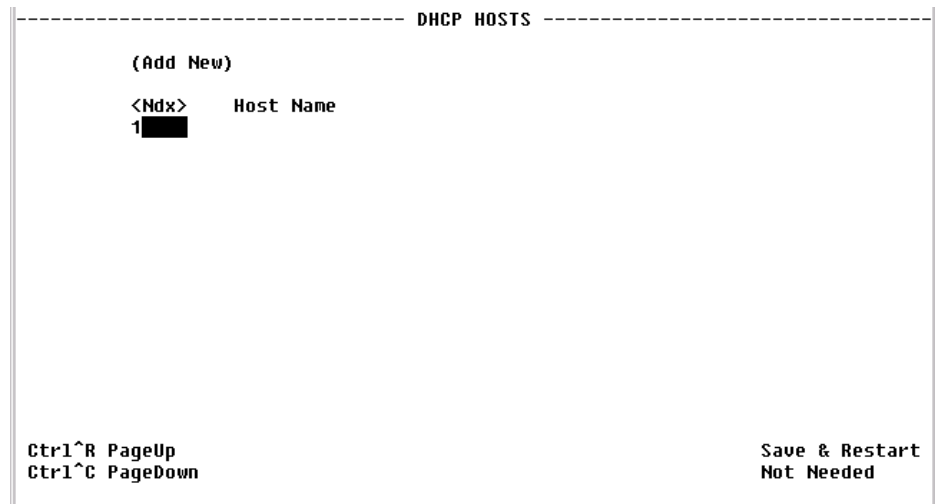
The DHCP Server Details screen provides the following user-activated prompts:

Prompt	Function
Host Table	Lists Host names (DHCP server identification).
Static Entry Table	Creates a list of static IP Addresses associated with MAC Addresses.
Address List Table	Defines the addresses available for DHCP clients.
Address Status Table	Displays DHCP Server statistics.

### ***DHCP Hosts Screen***

In some cases, it may be necessary to provide an IP station with a specific DHCP server name, which may be used by the IP station when making a DHCP request. That name is included on the DHCP Hosts screen (Figure 4.82), which identifies the DHCP server sending DHCP packets.

**Figure 4.82** *DHCP Hosts Screen*



**Host Name** The name of the DHCP Server. Default is none.

Select “Add New” to add a new host name.



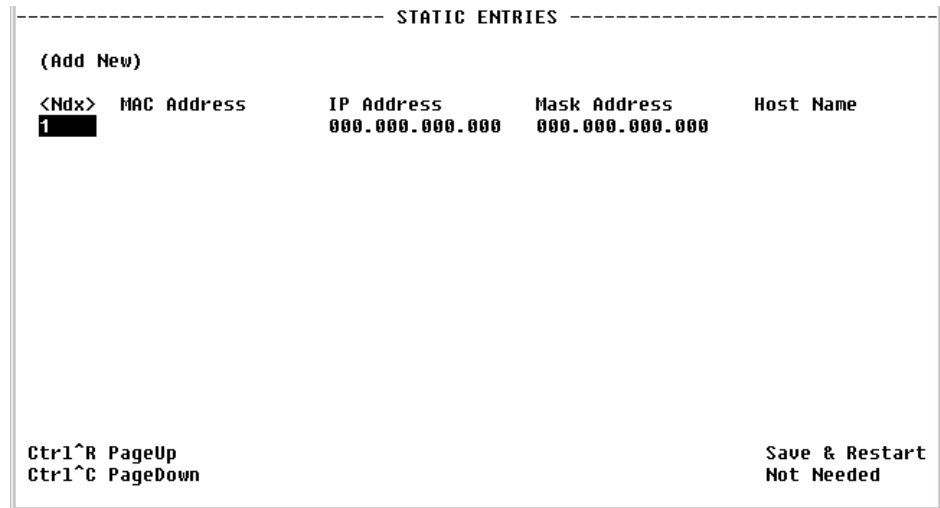
**NOTICE:** *You must Save and Restart for the new Server name to become active.*

### ***Static Entries Screen***

The Static Entries screen (Figure 4.83) lists static IP Addresses associated with MAC Addresses. This ensures that the same IP Address will always be used for a given PC provided its MAC Address is known. These parameters are configured on the Static Entries Details screen accessed by selecting a number from the “Entry Index” column.



**Figure 4.83** *Static Entries Screen*



**MAC Address** MAC Address you want to associate with an IP Address.

**IP Address** IP Address given to the DHCP client if that client has the MAC Address defined on this screen.

**Mask** Mask associated with the IP Address shown on the screen.

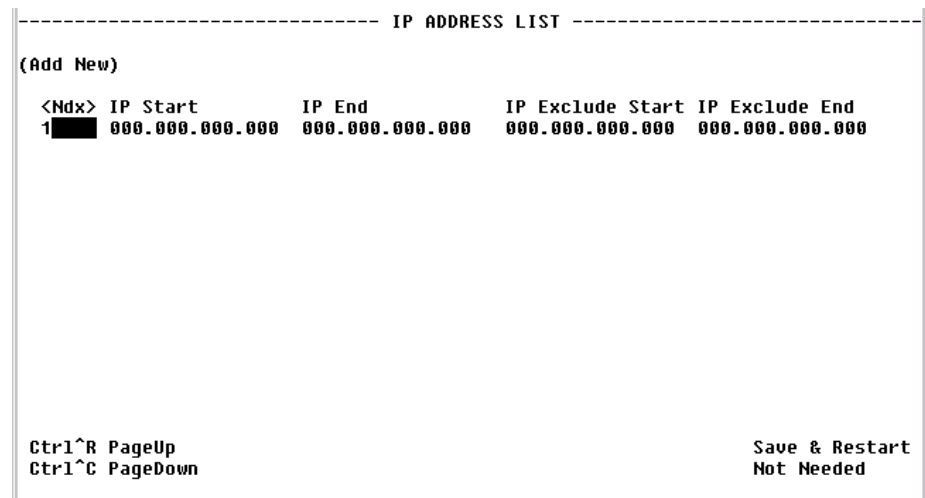
**Host Name** Name given to the DHCP client.

Select “Add New” to add a static entry.

### ***IP Address List Screen***

The IP Address List screen (Figure 4.84) displays the “pool” of addresses available for DHCP clients. These parameters are configured on the IP Address List Details screen accessed by selecting an “Index” number.

**Figure 4.84** *IP Address List*



**IP Start** Starting IP Address of the DHCP client pool.

**IP End** Ending IP Address of the DHCP client pool.

**IP Exclude Start** Beginning of “excluded” range.

**IP Exclude End** End of “excluded” range.

Select “Add New” to add an IP Address.

### ***IP Address Status Screen***

The IP Address Status screen (Figure 4.85) displays a list of all current DHCP clients.

**Figure 4.85** *IP Address Status Screen*

----- IP ADDRESS STATUS -----			
Index	MAC Address	IP Address	Status
Ctr1^R PageUp Ctr1^C PageDown			Save & Restart Not Needed

**MAC Address** MAC Address of this DHCP client.

**IP Address** IP Address given to this DHCP client if that client has the MAC Address defined on this screen.

**Status** Provides IP Address Status.

## **Simple Mail Transfer Protocol (SMTP)**

Use the SMTP Details Screen (Figure 4.86) to configure the SMTP function of the WANsuite 6450. SMTP is used to forward notification of events to a user-definable list of up to five recipients. The even notification is sent as an e-mail in the following format:

From: WANsuite@verilink.com

To: Event Receiver

Subject: Even Notification

IP Address: 192.168.60.157

System Up Time: 0 days, 01:20:02

System Name:  
System Location:  
System Contact:

Reporting the following event:  
OOFS Threshold Exceeded, ifIndex 3, Count 5

The parameters associated with the SMTP Details screen are described below.

**Figure 4.86** SMTP Details Screen

```
----- SMTP -----
Mail Server Address (000.000.000.000)
Domain Name          [                ]
Mail From            [                ]
Recipient 1          [                ]
Recipient 2          [                ]
Recipient 3          [                ]
Recipient 4          [                ]
Recipient 5          [                ]

Save & Restart
Not Needed
```

**Mail Server IP Address** IP address of the mail server to which notifications will be sent.

**Domain Name** Name of domain where the device resides (i.e., Verilink.com)

**Mail From** E-mail address of the device (WANsuite). While the device will not be able to retrieve e-mail from a service, the mail needs to have the “From” address filled in.



---

**NOTICE:** *There can be no blank space(s) in the “Mail From” address.*

---

**Recipient 1...5** E-mail addresses of recipients of event notifications (i.e., sales@verilink.com or support@verilink.com).





## SPECIFICATIONS

### Network Interface – SHDSL Port

Line Rate:	200 kbps to 2.320 Mbps
Line Framing:	ATM Transport (G.991.2 E9)
Line Code:	Trellis Coded Pulse Amplitude Modulation
Connection:	RJ11C, 8-pin modular jack at 135 $\Omega$
Network Protocol:	ATM
Adaptation Layers:	AAL1 and AAL5
AAL5 Encapsulation:	RFC1483 – LLC MUX
AAL5 Encapsulation Mode:	Routed IP
Number of AAL5 PVCs:	Up to 20

### CBR Interface

Timing Source:	Network, AAL1 Adaptive
AAL1 Encapsulation:	Per af-vtoa-0078.000
Partial Cell Fill	3-46 bytes
Selectable Receive Cell Delay (CDV)	100 (1 ms) default

### E1

Line Rate:	2.048 Mbps ( $\pm 50$ bps)
Line Framing:	CAS, CCS, or 2 Mbits unframed
Line Code:	AMI or HDB3
Input Signal:	30 dB of cable loss
Connection:	RJ-48 jack at 120 $\Omega$ ( $\pm 10$ %)
Output Signal:	3.0 V ( $\pm 10$ %) base-peak into 120 $\Omega$
Mode:	Short- or long-haul
Jitter Control:	per G.823 Sections 2.1 and 3.0
Number of DS0s Selectable:	From 1 to full E1 (noncontiguous)

## T1

Line Rate:	1.544 Mbps ( $\pm 50$ bps)
Line Framing:	SF, ESF, or 1.544 Mbits unframed
Line Code:	AMI or B8ZS
Receiver Sensitivity:	30 dB of cable loss
Connection:	RJ-48 jack at 100 $\Omega$ ( $\pm 10$ %)
Output Signal:	3.0 V ( $\pm 10$ %) base-peak into 100 $\Omega$
Mode:	Short- or long-haul
Jitter Control:	per Bellcore Document TA-TSY-000170
Number of DS0s Selectable:	From 1 to full T1 (noncontiguous)

## Serial Interface

Connection:	DB-25 female
DTE Ports:	Selectable V.35, V.36, X.21, RS-232, RS-449, or EIA-530
DTE/DCE:	Selectable (matching cable required)
Data Rate:	Synchronous, $n \times 64$ kbps (where $n = 1-36$ )
Clocking:	Internal, External
Supports RFC 1483, Synchronous PPP, CES via AAL 1	

## IP Gateway

### 10/100 Ethernet (IP Gateway or Management)

Protocols:	RIP1, RIP2, OSPF
Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T

## Management Interfaces

### Embedded Operations Channel

Embedded messaging to enable management of the SHDSL-related parameters.

### 10/100 Ethernet

Connection:	8-pin modular
Network Protocol:	TCP/IP based networks
Data Rate:	10/100 Mbps
Compatibility:	10/100Base-T

### Supervisory Port

Connection:	DB-9 female
-------------	-------------

Data Rates: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps  
(default: 19200, 8, N, 1)

## Diagnostics

Performance: 15-minute, 24-hour, and 30-day monitoring (sampled every second)

Network Loop: SHDSL, network loopback

## Alarms

Activation: Programmable thresholds on all interfaces

Reporting: SNMP traps

## Power

Voltage: 100–240 VAC

Frequency: 50–60 Hz

Dissipation: 10 W maximum (27.4 BTU/hr)

## Mechanical

Mounting: Standalone

Dimensions: Width 11.75 inches (29.845 cm)

Height 1.86 inches (4.724 cm)

Depth 8.75 inches (22.225 cm)

Weight: 2.13 pounds (0.97 kg)

## Environmental

Operating Temp: 32 to 122 °F (0 to 50 °C)

Storage Temp: –4 to 149 °F (–20 to 65 °C)

Humidity: 95 % maximum (non-condensing)

## Industry Listings

FCC Compliance: Part 15 Class A, Subpart B; T1.TRQ.6-2001

Safety: EN 60950; 1992  
UL60950; 3rd Edition

## Standards

ETS1:	TBR 12
ETS1:	TBR 13
G.701:	1993
G.703:	1991
G.705:	1995
G.823:	1993
G.991.2	2001
G.994.1	2001
Ethernet:	ISO/IEC 8802-3
Internet:	RFC1907
	RFC1573
	RFC2863
	RFC2493
	RFC2115
	RFC2495
	RFC2011
	RFC2012
	RFC2013
	RFC2096
	RFC2571
	RFC1490
ATM	RFC1483
	RFC2364
	<i>ATM UNI Draft Spec, ver.4.0</i> , ATM Forum, April 1996
	<i>ATM UNI Spec, ver. 3.0</i> , ATM Forum, September 1993
	<i>ATM UNI Spec, ver. 3.1</i> , ATM Forum, September 1994
	<i>Recommendation I.432, B-ISDN User-Network Interface – Physical Layer Specification</i> , ITU-T, August 1996
ATM Management	RFC2514
	RFC2515
	ipadatm.mib
Frame Relay-to-ATM Networking:	FRF.5
	FRF.8

## Ordering Information

### Standard Equipment

Each WANsuite 6450 unit ships with the following standard equipment:

Description
Network Cable
Serial (SUPV) Cable (DB-9M–DB-9F)
Power Cord for Power Supply
Verilink Documentation CD



## Optional Equipment

The following optional equipment is available for the WANsuite 6450:

Description
Serial (DCE) Cable (DB-25–Cisco DB-60), 10 ft
Serial (DCE) Cable (DB–25-DB-25) M/M, pin/pin (EIA530/RS232), 6 ft
Serial (DCE) Cable (DB-25–Winchester 34-pin) M/M, pin/pin (V.35), 5 ft
Serial (DCE) Cable (DB-25–Winchester 34-pin) M/M, pin/pin (V.35), 10 ft
Serial (DCE) Cable (DB-25–V.35), M/F, pin/pin, 5 ft
X.21 Cable (DB-25/DB-15–X.21), M/M, 2 ft
RS449/V.36 Cable (DB-25– 7-pin), M/F, 5, 10, or 20 ft

## Connector Pin Assignments

### Serial Interface Pin Assignments, DTE Mode (Packet Use Only)

The Serial interface on the WANsuite 6450 is a standard DB-25 jack.

Function	Abbrev.	Direction	Pin #			
			DB-25*	RS-232	V.35	X.21
Frame Ground	FG	n/a	1	1	A	1
Transmit Data	TD	Output	3	2	P	2
Receive Data	RD	Input	2	3	R	3
Request to Send	RTS	Output	5	4	C	4
Clear to Send	CTS	Input	4	5	D	5
Data Set Ready	DSR	Input	20	6	E	6
Signal Ground	SG	n/a	7	7	B	7
Data Carrier Detect	DCD	Input	8	8	F	8
Balanced Receiver Clock	(B)RC	Input	12		X	9
Balanced Data Carrier Detect	(B)DCD	Input	10			10
Balanced External Transmitter Clock	(B)ETC					
Balanced Transmitter Clock	(B)TC	Input	11		AA	12
Balanced Clear to Send	(B)CTS	Input	19			13
Balanced Transmit Data	(B)TD	Output	16		S	14
Transmitter Clock	TC	Input	24	15	Y	15
Balanced Receive Data	(B)RD	Input	14		T	16
Receiver Clock	RC	Input	15	17	V	17
Local Loopback	Loop 3	Output	18	18	J	18
Balanced Request to Send	(B)RTS	Output	13			19
Data Terminal Ready	DTR	Output	6	20	H	20
(not used)		n/a	21	21		21
Balanced Data Set Ready	(B)DSR	Input	23			22
Balanced Data Terminal Ready	(B)DTR	Output	22			23
External Transmitter Clock	ETC					
(not used)		n/a	25	25		25

\*This refers to the DB-25 Serial interface connector on the back of the unit.

## Serial Interface Pin Assignments, DCE Mode

Function	Abbrev.	Direction	Pin #				
			DB-25*	RS-232	V.35	X.21	RS449/ V.36
Frame Ground	FG	n/a	1	1	A	1	1
Transmit Data	TD	Input	2	2	P	2	4
Receive Data	RD	Output	3	3	R	3	6
Request to Send	RTS	Input	4	4	C	4	7
Clear to Send	CTS	Output	5	5	D	5	9
Data Set Ready	DSR	Output	6	6	E	6	11
Signal Ground	SG	n/a	7	7	B	7	19
Data Carrier Detect	DCD	Output	8	8	F	8	13
Balanced Receiver Clock	(B)RC	Output	9		X	9	26
Balanced Data Carrier Detect	(B)DCD	Output	10			10	31
Balanced External Transmitter Clock	(B)ETC	Input	11		W	11	35
Balanced Transmitter Clock	(B)TC	Output	12		AA	12	23
Balanced Clear to Send	(B)CTS	Output	13			13	27
Balanced Transmit Data	(B)TD	Input	14		S	14	22
Transmitter Clock	TC	Output	15	15	Y	15	5
Balanced Receive Data	(B)RD	Output	16		T	16	24
Receiver Clock	RC	Output	17	17	V	17	8
Local Loopback	Loop 3	Input	18	18	J	18	
Balanced Request to Send	(B)RTS	Input	19			19	25
Data Terminal Ready	DTR	Input	20	20	H	20	12
(not used)		n/a	21	21		21	
Balanced Data Set Ready	(B)DSR	Output	22			22	29
Balanced Data Terminal Ready	(B)DTR	Input	23			23	30
External Transmitter Clock	ETC	Input	24	24	U	24	17
(not used)		n/a	25	25		25	

*\*This refers to the DB-25 Serial interface connector on the back of the unit.*

## Ethernet Connection Pin Assignments

The **10/100 ETHERNET** interface on the WANsuite 6450 is an eight-pin modular jack that complies with standard twisted-pair, 10/100Base-T requirements. The table below displays the Ethernet Connection pin assignments.

Pin	Ethernet Interface
1	Data Out (+)
2	Data Out (-)
3	Data In (+)
6	Data In (-)

## Network Interface Pin Assignments

The **NETWORK** physical interface is a standard RJ11C, eight-pin modular jack. The table below displays the pinout assignments.

Pin	NET Interface
1	Not Used
2	Not Used
3, 6	Not Used
4	Data
5	Data
7, 8	Not Used

## CBR Interface Pin Assignments

The **CBR** physical interface is a standard RJ11C, eight-pin modular jack. The table below displays the pinout assignments.

Pin	CBR Interface
1	Data Out
2	Data Out
3, 6	Not used
4	Data In
5	Data In
7, 8	Chassis Ground

## Supervisory Port Pin Assignments

The **SUPERVISORY PORT** interface is a standard DB-9, nine-pin modular jack. The table below displays the pinout assignments.

Pin	DCE Mode	DTE Mode
1	DCD out	LL out
2	Rx Data out	Tx Data out
3	Tx Data in	Rx Data in
4	DTR in	DSR in
5	Signal Ground	Signal Ground
6	DSR out	DTR out
7	RTS in	CTS in
8	CTS out	RTS out
9	No connect	No connect



# B

## SNMP AGENT

### Introduction

---

This chapter provides specific information for configuring and using the SNMP agent within the WANSuite 6450.

The WANSuite 6450 incorporates an Ethernet card that provides connectivity for LAN-based management stations. The embedded TCP/IP Protocol Stack allows remote access from both private networks and the Internet.

### SNMP Configuration Parameters

---

To access the SNMP agent, you must have an SNMP management application, such as HP's OpenView<sup>®</sup> or Sun's NetManager<sup>™</sup>. Access to the agent is controlled by three community strings, read-access, write-access, and trap-access (the community string sent with an SNMP trap). Configuration of these community strings within the WANSuite 6450 is accomplished via the HTTP (web browser) interface (Chapter 3, *Web Server Interface*).

The defaults for these strings are "public" for read-access, "private" for write-access, and "public" for trap-access. Ensure that your SNMP management application is configured for whatever access strings you use.

### SNMP MIBs

---

The WANSuite 6450 supports the following industry-standard MIB (management information base) files:

- rfc1573.mib – defines the IANAifType textual convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable
- rfc1907.mib – SNMPv2 entities (initial revision published as RFC 1450)
- rfc2011.mib – for managing IP and ICMP implementations, but excluding their management of IP routes
- rfc2012.mib – for managing TCP implementations

- `rfc2013.mib` – for managing UDP implementations
- `rfc2096.mib` – for the display of CIDR multipath IP routes
- `rfc2493.mib` – provides textual conventions to be used by systems supporting 15-minute based performance history counts
- `rfc2514.mib` – ATM Management MIB
- `rfc2515.mib` – ATM Management MIB
- `rfc2571.mib` – the SNMP Management Architecture MIB
- `rfc2863.mib` – describes generic objects for network interface sub-layers (This MIB is an updated version of MIB-II's `ifTable`, and incorporates the extensions defined in RFC 1229.)
- `rfc3276.mib` – MIB module for SHDSL

The WANsuite 6450 supports the following Enterprise-specific MIBs:

- `ds8200tc.mib` – textual conventions used by DS8200 MIB
- `ds8200v2.mib` – provides T1 configuration and statistics information
- `ipadatm.mib` – proprietary extensions to ATM Management MIBs
- `ipadv2.mib` – provides Frame Relay, PPP, and Service Aware configuration and statistics
- `ipstart.mib` – MIB module for synchronous PPP
- `router.mib` – provides configuration of OSPF router

These MIB files may be found on the Verilink Documentation CD included with the unit.

## SNMP Trap Configuration

---

The WANsuite 6450 supports up to eight IP destinations for SNMP traps. These may be configured either through the Web interface or through an SNMP management application. For configuration of these destinations through an SNMP management application, use a MIB browser to access the table `trapdest` within `ipadv2.mib` and set the IP Addresses of the host computer running the management application(s). Entering an IP Address of 0.0.0.0 will disable the entry.

## Generic MIB Loading Instructions

---

The MIBs were written using the standard ASN.1 notation. Any standard SNMP manager should be able to compile the MIBs. Although the exact procedure for loading MIBs may vary from one platform to another, the following basic steps are the same.

- 1 The SNMP manager has a directory for MIBs. Copy the files `ds8200tc.mib`, `ds8200v2.mib`, `ipadv2.mib`, `ipstart.mib`, `router.mib`, and `ipadatm.mib` into this directory. The MIBs use a DOS format; therefore, a DOS2UNIX command may have to be used for UNIX workstations (typical directories are `snmp_mibs` for HP's



OpenView<sup>®</sup>, bin for Sun's NetManager<sup>™</sup>, and mibfiles for Castle Rock Computing's SNMPc<sup>™</sup>).

- 2** Start the SNMP manager if it is not already running. Select one of the menu selections (or selection subheadings) that contains the SNMP MIB operations (this is Options subheading for HP OpenView and Config subheading for SNMPc).
- 3** Choose the option for LOADING or COMPILING MIBs. You must specify which MIBs to load.
- 4** Once the manager has successfully loaded the MIBs, you are ready to manage the Verilink product. If you have any questions please call Verilink Product Support.





## Five-Year Hardware Limited Warranty

- I. **Limited Warranty.** Subject to the limitations and disclaimers set forth in this Hardware Limited Warranty, Verilink warrants to the original purchaser ("Buyer") that the Verilink equipment and component parts ("Goods") purchased by Buyer shall be free from defects in material and workmanship under normal use and service for a period of five years from the date of shipment of the Goods to Buyer ("Limited Warranty"). Verilink's sole obligation and Buyer's sole remedy under this Limited Warranty shall be to repair or replace any Verilink Goods that Verilink determines to be so defective. Any claim by Buyer under this Limited Warranty must be presented to Verilink in writing within five years and fifteen (15) days of the date of shipment of the Goods to Buyer, as evidenced by Verilink's packing slip or similar shipment documentation from a Verilink authorized reseller. Any replacement Goods may be new or reconditioned. Verilink reserves the right to substitute equivalent Goods for defective Goods, in its sole discretion. As long as Verilink either so repairs or replaces the Goods, this Limited Warranty will not be found to have failed its essential purpose. If the defect has been caused by accident, misuse or abnormal operating conditions (including lightning damage) occurring after delivery to Buyer, repairs and/or replacement will be made at Buyer's expense. In such event, an estimate of cost will be submitted to Buyer before repair work is started. The Limited Warranty will continue to apply to replaced or repaired Goods for whichever is longer: the 90-day period after the shipment of such Goods to Buyer or the remainder of the original Limited Warranty period.
- II. **EXCLUSION OF IMPLIED WARRANTIES OR OTHER REPRESENTATION.** THE GOODS ARE SOLD BY VERILINK "AS IS" WITHOUT ANY WARRANTY OR GUARANTEE OF ANY KIND OTHER THAN THE LIMITED WARRANTY SET FORTH ABOVE, WHICH IS MADE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AND VERILINK HEREBY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, AND ALL OTHER IMPLIED WARRANTIES ON THE PART OF VERILINK. VERILINK DOES NOT WARRANT THAT THE BUYER'S USE OF THE GOODS WILL BE UNINTERRUPTED, SECURE, OR ERROR-FREE. Buyer agrees that no oral or written representation, advice, advertisement or other statement by Verilink, its reseller, agent, employee, or representative constitutes any warranty, guarantee or modification of the foregoing disclaimer and Limited Warranty, and Buyer acknowledges that no person, including resellers, agents, employees, or representatives of Verilink, is authorized to assume for Verilink any other liability on its behalf except as set forth in this paragraph.
- III. **LIMITATION ON LIABILITY.** IN NO EVENT SHALL VERILINK, ITS OFFICERS, DIRECTORS, EMPLOYEES, OR SUPPLIERS BE LIABLE FOR SPECIAL, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, OR PUNITIVE DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, DATA LOSS, DAMAGE TO EQUIPMENT, OR THE LIKE), REGARDLESS OF WHETHER THE CLAIM IS BASED ON BREACH OF WARRANTY, BREACH OF CONTRACT, STRICT LIABILITY, OR OTHER LEGAL THEORY, EVEN IF VERILINK OR ITS AGENT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL VERILINK'S LIABILITY TO BUYER OR ANY SUCCESSOR TO BUYER EXCEED THE PRICE PAID FOR THE APPLICABLE GOODS.
- IV. **LIMITED WARRANTY CONDITIONS.** The Limited Warranty shall be void (i) with respect to any Goods that have been repaired or altered outside Verilink's factory, unless Verilink specifically authorized such repairs or alterations; (ii) in the event parts not made or recommended by Verilink are used by Buyer in the Goods; or (iii) if the Goods are used by Buyer other than in the manner intended by Verilink or other than in conformance with operating instructions and specifications provided by Verilink.
- V. **MODIFICATIONS BY VERILINK.** Minor deviations from specifications that do not materially affect performance of the Goods covered hereby, as mutually agreed upon by Verilink and Buyer, shall not be deemed to constitute a breach of the Limited Warranty. Verilink also reserves the right to discontinue Goods and change specifications for Goods without notice, provided such changes do not adversely affect the performance of the Goods manufactured by Verilink or do not reduce performance below any applicable contract specifications between Verilink and the Buyer. Verilink also reserves the right to make product improvements without incurring any obligations or liability to make the same changes in Goods previously manufactured or purchased. Non-payment of any invoice rendered within the stated payment terms automatically suspends the application of, but not the running of, the Limited Warranty for the duration of the non-payment.
- VI. **AMENDMENT OF WARRANTY TERMS.** These terms and conditions of this Hardware Limited Warranty may be revised by Verilink from time to time in its sole discretion. The terms and conditions in effect at the time of purchase will apply to such Goods.
- VII. **RETURN OF GOODS.** If for any reason the Buyer must return a Verilink product, it must be returned to the factory, shipping prepaid, and packaged to the best commercial standard for electronic equipment. Verilink will pay shipping charges for delivery on return. The Buyer is responsible for mode and cost of shipment to Verilink. The Buyer must have a Return Material Authorization (RMA) number marked on the shipping package. Products sent to Verilink without RMA numbers will be returned to the sender, unopened, at the sender's expense. A product sent directly to Verilink for repair must first be assigned an RMA number. The Buyer may obtain an RMA number by calling the Verilink Customer Service Center at 1.800.926.0085, extension 2282 or 2322. When calling Verilink for an RMA, the Buyer should have the following information available:
  - Model number and serial number for each unit
  - Reason for return and symptoms of problem
  - Purchase order number to cover charges for out-of-warranty items
  - Name and phone number of person to contact if Verilink has questions about the unit(s).A return address will be provided at the time the RMA number is issued. The standard delivery method for return shipments is Standard Ground for domestic returns and International Economy for international returns (unless otherwise specified).
- VIII. **GOVERNING LAW.** This Agreement is governed by the laws of the State of Alabama, U.S.A., without reference to its conflicts of law provisions. The provisions of the UN Convention on Contracts for the International Sale of Goods shall not apply.