For Quick Start Installation
see page 27

Model 3086FR
G.SHDSL Frame Relay over ATM IAD

User Guide

Important
This is a Class A device and is intended for use in a light industrial environment. It is not intended nor approved for use in an industrial or residential environment.

Sales Office: **+1 (301) 975-1000**
Technical Support: **+1 (301) 975-1007**
E-mail: **support@patton.com**
WWW: **www.patton.com**

Part Number: **07M3086FR-UG, Rev. C**
Revised: **February 16, 2012**

Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
tel: +1 (301) 975-1000
fax: +1 (301) 869-9293
support: +1 (301) 975-1007
web: www.patton.com
e-mail: support@patton.com

Copyright © 2012, Patton Electronics Company. All rights reserved.

The information in this document is subject to change without notice. Patton Electronics assumes no liability for errors that may appear in this document.

Warranty Information

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

Patton Electronics warrants all Model 3086FR components to be free from defects, and will—at our option—repair or replace the product should it fail within one year from the first date of the shipment.

This warranty is limited to defects in workmanship or materials, and does not cover customer damage, abuse or unauthorized modification. If the product fails to perform as warranted, your sole recourse shall be repair or replacement as described above. Under no condition shall **Patton Electronics** be liable for any damages incurred by the use of this product. These damages include, but are not limited to, the following: lost profits, lost savings and incidental or consequential damages arising from the use of or inability to use this product. **Patton Electronics** specifically disclaims all other warranties, expressed or implied, and the installation or use of this product shall be deemed an acceptance of these terms by the user.

Contents

About this guide

This guide describes installing and configuring a Patton Electronics Model 3086FR Frame Relay to ATM Converter. The instructions in this guide are based on the following assumptions:

- The Frame Relay to ATM Converter may connect to a serial DTE device
- There is a LAN connected to the Ethernet port of the IAD
- Users will be connected to remote IADs

Audience

This guide is intended for the following users:

- Operators
- Installers
- Maintenance technicians

Structure

This guide contains the following chapters and appendices:

- Chapter 1 provides information about Frame Relay to ATM Converter features and capabilities
- Chapter 2 contains an overview describing Frame Relay to ATM Converter operation
- Chapter 3 provides quick start installation procedures
- Chapter 4 describes connecting the DSL and data ports
- Chapter 6 describes configure Frame Relay and ATM features
- Chapter 7 describes the Local Management Interface
- Chapter 8 describes setting up 3086FR routed and bridged ATM connections
- Chapter 9 describes configuring the Frame Relay to ATM Converter for specialized applications
- Chapter 10 describes configuring security for the IAD
- Chapter 11 describes configuring for network address translation (NAT)
- Chapter 12 contains definitions for the LED status indicators
- Chapter 13 describes Frame Relay to ATM Converter diagnostics
- Appendix B contains specifications for the IADs
- Appendix C provides cable recommendations
- Appendix D describes the IAD’s physical ports
- Appendix E describes how to use the command line interface (CLI)

For best results, read the contents of this guide *before* you install the IAD.

Precautions

Notes and cautions, which have the following meanings, are used throughout this guide to help you become aware of potential Frame Relay to ATM Converter problems. *Warnings* relate to personal injury issues, and *Cautions* refer to potential property damage.

Note Calls attention to important information.

WARNING

The shock hazard symbol and WARNING heading indicate a potential electric shock hazard. Strictly follow the warning instructions to avoid injury caused by electric shock.

WARNING

The alert symbol and WARNING heading indicate a potential safety hazard. Strictly follow the warning instructions to avoid personal injury.

CAUTION

The shock hazard symbol and CAUTION heading indicate a potential electric shock hazard. Strictly follow the instructions to avoid property damage caused by electric shock.

CAUTION

The alert symbol and CAUTION heading indicate a potential hazard. Strictly follow the instructions to avoid property damage.

Safety when working with electricity

- **This device contains no user serviceable parts. The equipment shall be returned to Patton Electronics for repairs, or repaired by qualified service personnel.**
- **Mains Voltage: Do not open the case the when the power cord is attached. Line voltages are present within the power supply when the power cords are connected. The mains outlet that is utilized to power the devise shall be within 10 feet (3 meters) of the device, shall be easily accessible, and protected by a circuit breaker.**
- **For AC powered units, ensure that the power cable used meets all applicable standards for the country in which it is to be installed, and that it is connected to a wall outlet which has earth ground.**
- **For units with an external power adapter, the adapter shall be a listed Limited Power Source.**
- **Hazardous network voltages are present in WAN ports regardless of whether power to the unit is ON or OFF. To avoid electric shock, use caution when near WAN ports. When detaching the cables, detach the end away from the device first.**
- **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

Factory default parameters

The **Model 3086FR** Frame Relay to ATM Converter has the following factory default parameters.

- Ethernet IP address: 192.168.200.10/24
- Autonegotiate the G.SHDSL speed
- Annex B
- Remote (CPE)

Typographical conventions used in this document

This section describes the typographical conventions and terms used in this guide.

General conventions

The procedures described in this manual use the following text conventions:

Table 1. General conventions

Convention	Meaning
Garamond blue type	Indicates a cross-reference hyperlink that points to a figure, graphic, table, or section heading. Clicking on the hyperlink jumps you to the reference. When you have finished reviewing the reference, click on the **Go to Previous View** button ⬅ in the Adobe® Acrobat® Reader toolbar to return to your starting point.
Futura bold type	Indicates the names of menu bar options.
Italicized Futura type	Indicates the names of options on pull-down menus.
Futura type	Indicates the names of fields or windows.
Garamond bold type	Indicates the names of command buttons that execute an action.
< >	Angle brackets indicate function and keyboard keys, such as <SHIFT>, <CTRL>, <C>, and so on.
`Are you ready?`	All system messages and prompts appear in the `Courier` font as the system would display them.
`% dir *.*`	Bold Courier font indicates where the operator must type a response or command

Mouse conventions

The following conventions are used when describing mouse actions:

Table 2. Mouse conventions

Convention	Meaning
Left mouse button	This button refers to the primary or leftmost mouse button (unless you have changed the default configuration).
Right mouse button	This button refers the secondary or rightmost mouse button (unless you have changed the default configuration).
Point	This word means to move the mouse in such a way that the tip of the pointing arrow on the screen ends up resting at the desired location.
Click	Means to quickly press and release the left or right mouse button (as instructed in the procedure). Make sure you do not move the mouse pointer while clicking a mouse button.
Double-click	Means to press and release the same mouse button two times quickly
Drag	This word means to point the arrow and then hold down the left or right mouse button (as instructed in the procedure) as you move the mouse to a new location. When you have moved the mouse pointer to the desired location, you can release the mouse button.

Chapter 1 General Information

Chapter contents

Model 3086FR Frame Relay over ATM IAD overview

The Model 3086FR is a G.SHDSL Integrated Access Device that combines high speed IP routing and access via ATM /PPP. In addition, the Model 3086FR serial port converts FR legacy traffic to ATM traffic using FRF.5 (Frame Relay/ATM PVC Network Internetworking Implementation) and FRF.8 (Frame Relay/ATM PVC Service Internetworking Implementation). The Model 3086FR offers direct connection to a 10/100Base-T Ethernet environment, a V.35 or X.21 serial direct connection to a router or FRAD. The 3086FR combines traffic from the Serial and Ethernet ports over a single pair DSL connection.

The Model 3086FR complies with ETSI/ITU standard G.991.2 and allows full duplex, up to 2.3 Mbps speed over a single twisted pair. In addition, the Model 3086FR works at up to 4.6 Mbps over 2-wire. Whereas G.991.2 specifies 4-wire for data rates from 2.3 to 4.6 Mbps, the 3086FR is able to operate up to 4.6 Mbps *over just 2 wires!* Speed setting ranges are user selectable in nx64 kbps increments from 64 kbps.

The following sections describe Model 3086FR features and capabilities:

- General attributes, see page 14
- G.SHDSL Characteristics (Model 3086FR), see page 15
- Ethernet, see page 15
- Protocol support, see page 15
- PPP support, see page 16
- ATM protocols, see page 16
- Frame Relay to ATM support, see page 16
- Management, see page 16
- TDM Interface, see page 15
- Security, see page 17
- Front panel status LEDs, switches, etc., see page 18

General attributes

- Compact, low cost IAD
- 10/100 Ethernet
- Unlimited host support.
- Comprehensive hardware diagnostics, works with any operating system, easy maintenance and effortless installation.
- Plug-and-Play operation for fast and seamless turn-up with pre-configured WAN and LAN options.
- Built-in web configuration.
- Setup allows for standard IP address and unique method for entering an IP address and mask WITHOUT use of a console connection. Default IP address of 192.168.1.1/24.
- Simple software upgrade using FTP into FLASH memory.

- Twelve front panel LEDs indicate , DSL WAN, Sync Serial, Ethernet LAN speed and status, and Test mode status.
- Convenient and standard RJ connectors for Ethernet, Line, and Console.
- Field Factory Default Option.
- Standard 1 year warranty.
- Convenient and standard RJ connectors for Ethernet, Line, and Console.

G.SHDSL Characteristics

- Full duplex 2.3 Mbps speed over 2-wire (in accordance with ETSI/ITU standard G.991.2). 2.3 Mbps to 4.6 Mbps, full duplex, over 2-wire.
- DTE rates 64 kbps to 2.3 Mbps operation (Sync serial can work in increments of 64 kbps up to a bandwidth of 2.3 Mbps, n=32).
- Distance from 24,900 feet (7,590 m) at 192 kbps to 10,200 ft (3,109 m) at 2.3 Mbps on 26 AWG (0.4 mm) wire
- Annex A (ANSI), Annex B (ETSI) PSD selection.
- CO and CP modes supported
- TC-PAM based DSL modulations.
- EOC Management channel for remote end-to-end management.

Ethernet

- Auto-sensing Full-Duplex 10Base-T/100Base-TX Ethernet.
- Standard RJ-45 connector
- Built-in MDI-X cross-over switch.
- IEEE 8021.d transparent learning bridge up to 1,024 addresses and Spanning Tree.
- 8 IP address/subnets on Ethernet interface.

TDM Interface

- V.35, X.21, or T1/E1 interface
- Available with female M/34, DB-25, DB-15, and RJ-48C connectors
- User configurable DTE/DCE for X.21

Protocol support

- Complete internetworking with IP (RFC 741), TCP (RFC 793), UDP (RFC 768), ICMP (RFC 950), ARP (RFC 826).
- IP Router with RIP (RFC 1058), RIPv2 (RFC 2453) for up to 64 static routes.
- Built-in Ping and Traceroute facilities.
- Integrated DHCP Server (RFC 2131).

- DHCP relay agent (RFC 2132/RFC 1542) with 8 individual address pools.
- DNS Relay with primary and secondary Name Server selection.
- NAT (RFC 3022) with Network Address Port Translation (NAPT), MultiNat with 1:1, Many:1, Many:Many mapping, Port/IP redirection and mapping.

PPP Support

- Point-to-Point Protocol over HDLC
- PPPoA (RFC 2364) Point-to-Point Protocol over ATM.
- PPPoE (RFC 2516) Client for autonomous network connection. Eliminates the requirement of installing client software on a local PC and allows sharing of the connection across a LAN.
- User configurable PPP PAP (RFC 1661) or CHAP (RFC 1994) authentication..

ATM Protocols

- Multiprotocol over ATM AAL5 and Multiprotocol Bridged encapsulation RFC 2684 (Formerly RFC 1483) and RFC 1577 Classical IP over ATM. Default RFC-1483 route mode. Logical Link Control (LLC)/ Subnetwork Access Protocol (SNAP) encapsulation. Default VC mux mode.
- ATM UNI 3.0, 3.1, and 4.0 signaling ATM QoS with UBR, CBR, nrt-VBR, and rt-VBR.
- Peak cell rate shaping on a per-VCC basis up to 32 active VCCs across VPI 0-255, VCI 0-65525. Single default PVC: 8/35 with PCR=5,500 cells.

Frame Relay to ATM conversion protocols

- FRF.5 (Frame Relay/ATM PVC Network Internetworking Implementation)
- FRF.8 (Frame Relay/ATM PVC Service Internetworking Implementation)

Protocol Support

- Complete internetworking with IP (RFC 741), TCP (RFC 793), UDP (RFC 768), ICMP (RFC 950), ARP (RFC 826).
- IP Router with RIP (RFC 1058), RIPv2 (RFC 2453),
- Up to 64 static routes with user selectable priority over RIP/OSPF routes.
- Built-in ping facilities.
- Integrated DHCP Server (RFC 2131). Selectable general IP leases and user specific MAC/IP parings. Selectable lease period.
- DHCP relay agent (RFC 2132/RFC 1542) with 8 individual address pools.
- DNS Relay with primary and secondary Name Server selection.
- NAT (RFC 3022) with Network Address Port Translation (NAPT) for cost-effective sharing of a single DSL connection. Integrated Application Level Gateway with support for over 80 applications.
- NAT MultiNat with 1:1 mapping.
- NAT Many:1.
- NAT Many:Many mapping.
- NAT Port/IP redirection and mapping.

- uPNP controlled device for seamless networked device interconnectivity and Windows XP integration.
- IGMPv2 Proxy support (RFC 2236).
- Frame Relay with Annex A/D/LMI, RFC 1490 MpoFR and FRF.12 Fragmentation.

Management

- User selectable ATM, PPP, or Frame Relay WAN datalink connection.
- Web-Based configuration via embedded web server
- CLI menu for configuration, management, and diagnostics.
- Local/Remote CLI (VT-100 or Telnet).
- SNMPv1 (RFC 1157) MIB II (RFC 1213)
- Quick Start Setup runs through common options to simplify circuit turn-up.
- Logging via SYSLOG, and VT-100 console. Console port set at 9600 bps 8/N/1 settings no flow control.
- EOC access for End-To-End management, configuration, and control.

Security

- Packet filtering firewall for controlled access to and from LAN/WAN. Support for 255 rules in 32 filter sets. 16 individual connection profiles.
- DoS Detection/protection. Intrusion detection, Logging of session, blocking and intrusion events and Real-Time alerts. Logging or SMTP on event.
- Password protected system management with a username/password for console and virtual terminal. Separate user selectable passwords for SNMP RO/RW strings.
- Access list determining up to 5 hosts/networks which are allowed to access management system SNMP/HTTP/TELNET.
- Logging or SMTP on events: POST, POST errors, line/DSL, PPP/DHCP, IP.

Front Panel Status LEDs, Test Mode Switches, and Console Port

The IpRocketLink routers have all status LEDs and console port on the front panel of the unit, and all other electrical connections are located on the rear panel.

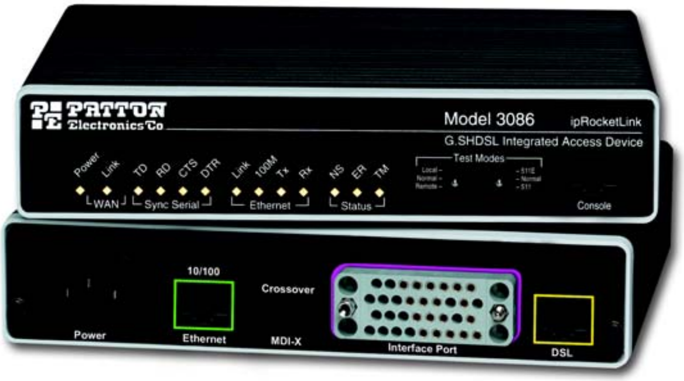


Figure 1. Model 3086FR

The status LEDs from left to right are (see table 3 for LED descriptions):

- Power
- WAN Link (DSL)
- Sync Serial (TD, RD, CTS, and DTR) or T1/E1 (Link, LOSS, TD, and RD)
- Ethernet Link, 100M, Tx, and Rx
- Status NS, ER, and TM

Table 3. Status LED descriptions

Power		Green	ON indicates that power is applied. Off indicates that no power is applied.
WAN (DSL)	Link	Green	Solid green: connected Off: disconnected
Sync Serial	TD	Green	Green: indicates a binary '0' condition *off*: indicates a binary '1'or idle condition
	RD	Green	Green: indicates a binary '0'condition off: indicates a binary '1' or idle condition
	CTS	Green	ON: indicates the CTS signal from the Frame Relay to ATM Converter is active, binary '1' off: indicates CTS is binary '0'
	DTR	Green	ON: indicates the DTR signal from the DTE device attached to the serial port is active, binary '1'
T1/E1	Link	Green	On: indicates the T1/E1 interface is connected to a live T1/E1 line
	LOS	Red	On: indicates a T1/E1 loss-of-frame condition. It also indicates that no T1/E1 signal is detected.
	TD	Green	Green: indicates a binary '0' condition *off*: indicates a binary '1'or idle condition
	RD	Green	Green: indicates a binary '0'condition off: indicates a binary '1' or idle condition
Ethernet	Link	Green	ON: indicates an active 10/100 BaseT connection
	100M	Green	ON: connected to a 100BaseT LAN Off: connected to a 10BaseT LAN
	Tx	Green	Flashing: when transmitting data from the Frame Relay to ATM Converter to the Ethernet
	Rx	Green	Flashing: when transmitting data from the Ethernet to the IAD.
Status	NS	Red	ON: incidates absence of a valid DSL connection
	ER	Red	flashes once: indicates bit errors occurring during 511/511E tests
	TM	Yellow	ON: is under one of the test modes (local loop, remote loop, or V.54 BER pattern)

The test mode switches are:

- Normal, Local, and Remote Loopbacks
- Normal, 511, and 511E pseudo-random bit patterns

Console port (outlined in red)

The unshielded RJ-45 RS-232 console DCE port (EIA-561) with the pin-out listed in the following table:

Pin No.	Signal Direction	Signal Name
1	Out	DSR
2	Out	CD
3	In	DTR
4	—	Signal Ground
5	Out	RD
6	In	TD
7	Out	CTS
8	In	RTS

Rear panel connectors and switches

On the rear panel from left to right are the following:

- Power input connector
- Ethernet connector
- MDI-X switch
- TDM port. V.35 (3086FR/RIC), X.21 (3086FR/RID), T1/E1 (3086FR/RIK)
- Line connector

Power connector

AC universal power supply.

The Model 3086FR offers internal or external AC power supply options.

- The internal power supply connects to an AC source via an IEC-320 connector (100–240 VAC, 200 mA, 50/60 Hz)
- The external power supply connects to an external source providing +5 VDC via a barrel-type connector

48 VDC power supply.

- Rated voltage and current: 36–60 VDC, 400 mA
- Fuse rating: 250 Volts, 400 mA, time delay

CAUTION

Connect the equipment to a 36–60 VDC source that is electrically isolated from the AC source. The 36–60 VDC source is to be reliably connected to earth.

Ethernet port (outlined in green)

Shielded RJ-45 10Base-T/100Base-TX Ethernet port using pins 1,2,3, & 6. See MDI-X switch for hub or transceiver configuration.The following table defines conditions that occur when the MDI-X switch is in the out position.

Pin No.	Signal Direction	Signal Name
1	Output	TX+
2	Output	TX-
3	Input	RX+
4	—	—
5	—	—
6	Input	RX-
7	—	—
8	—	—

MDI-X

The MDI-X push switch operates as follows:

- When in the default "out" position, the Ethernet circuitry takes on a straight-through MDI configuration and functions as a transceiver. It will connect directly to a hub.
- When in the "in" position, the Ethernet circuitry is configured in cross-over MDI-X mode so that a straight-through cable can connect the Model 3086FR DSL modem's Ethernet port directly to a PC's NIC card.

Line port (outlined in yellow)

The RJ-11/4 DSL line port uses pins 2 and 3 of the RJ-11 port.

Pin No.	Signal Name
1	—
2	In/Out-A
3	In/Out-B
4	—

Chapter 2 **Product Overview**

Chapter contents

Product Overview

The Model 3086FR IAD operates as a Frame Relay to ATM converter (via serial port), as a bridge or a router and has three ports for communication:

- The Ethernet port—Connects to the LAN side of the connection
- The Line port—Provides the G.SHDSL transmission connection between the CPE and CO DSL IAD
- The TDM port—Connects to local device for Frame Relay to ATM conversion and data uplink via the DSL link

The IAD provides all layers 2 and layer 3 protocols required for end-to-end-link communication.

When configuring the 3086FR, questions must be answered so the 3086FR functions as desired. For example, when a router or bridge module needs to be activated, some questions would be:

- Is a default gateway required?
- Which encapsulation technique is best for this application: PPPoA, IPoA, or another?

These decisions can be made and implemented more easily if the Model 3086FR's fundamental architecture is understood. Also, while configuring the Model 3086FR via a browser using the built-in HTTP server is very intuitive, an understanding of the architecture is essential when using the command-line interface (CLI) commands.

The fundamental building blocks comprise a router or bridge, interfaces, and transports. The router and bridge each have interfaces. A transport provides the path between an interface and an external connection. For example, the Ethernet transport attaches to an Internet Protocol (IP) interface. A transport consists of layer 2 and everything below it. Creating a transport and attaching it to a bridge or router's interface enables data to be bridged or routed. The supported transports are *PPPoA*, *RFC 1483* (Multiprotocol Encapsulation over ATM AAL5), and *IPoA*.

Configuring an interface and transport for the router or bridge requires naming the interface and transport before attaching them. When using the built-in HTTP server web browser, this is done automatically. But when configuring the Model 3086FR via CLI commands through the RS-232 control port, it must be done manually.

Model 3086FR IADs can connect over an ATM PVC transport.

The PVC requires the configuration of the virtual path identifier (VPI) and virtual circuit identifier (VCI). The VPI can be any integer between 0–4095 inclusive. The general rule for the VCI is an integer between 1–65,535 inclusive. Examples in this manual use a VCI of 600 or above. The main restriction in choosing a VCI is that VCIs below 32 are reserved for such predefined functions as ILMI. The VCI values of 600 and above used in this manual are also above the range used by many signaling implementations for SVCs.

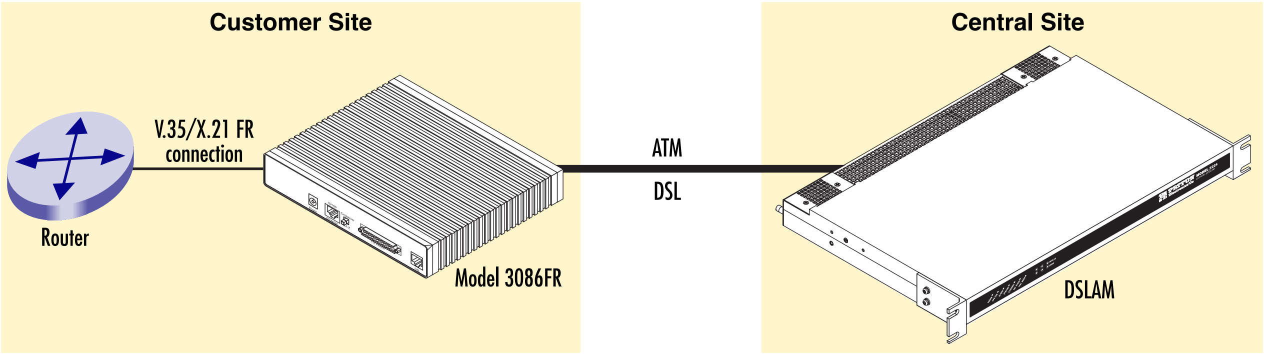
The HDLC is a packet-based transmission across the DSL Link.

Applications Overview

The Model 3086FR is used in FR over ATM applications connecting FRAD equipment to ATM based DSLAMs. In addition, the 3086FR is used in the connection of small to medium size enterprise to internet services (connection to ISP), or connection to remote branches using DSL access using PPP over ATM. In most applications, the Model 3086 works with Patton's 3096RC ForeFront System, but it will also connect to third-party G.SHDSL devices.

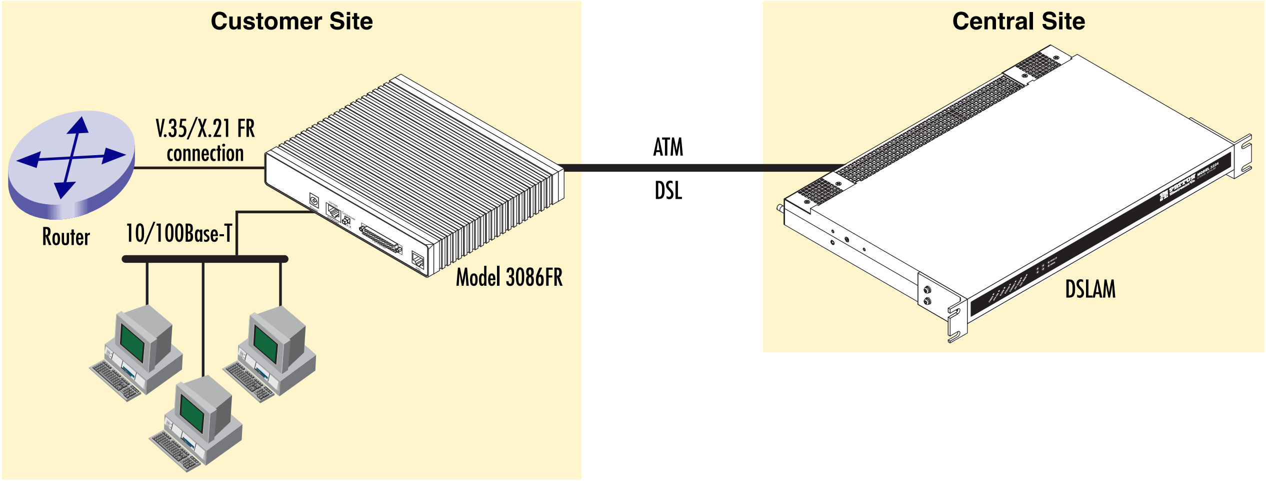
FR over ATM

The Model 3086FR primary function is the conversion of legacy ports running FR traffic to ATM. In many instances, customers have older but functioning equipment, and need to connect to newer technology offerings from service providers or telcos. Customers are not ready to make a significant investment in new and expensive equipment. The Patton model 3086FR fills that gap providing seamless and economical FR to ATM conversion, allowing customers to keep using their legacy equipment.



Integrated access

In addition to FR to ATM conversion and transport over DSL, the 3086FR is a full feature router allowing routed or bridged services between the DSL interface and the 10/100Base-T port. The 3086 can simultaneously transport traffic from the serial port and the 10/100Base-T Ethernet port over a single pair DSL link. In this case, the 3086FR operates in split mode DSL bandwidth allocating dedicated timeslots in the DSL frame for the serial port, and for the Ethernet traffic.



Chapter 3 **Quick Start Installation**

Chapter contents

Hardware installation

If you are already familiar with Model 3086FR Frame Relay to ATM Converter installation and configuration, this chapter will enable you to finish the job quickly. Installation consists of the following:

- Preparing for the installation (see section "What you will need")
- Hooking up cables, verifying that the unit will power up, and running a HyperTerminal session (see section "Connecting network cables" on page 29)
- Changing the IP address from the factory default setting (see section "IP address Quick Start modification" on page 30)
- Launching a web browser in preparation for configuring the modem (see "Web Operation and Configuration" on page 30)

What you will need

- Model 3086FR G.SHDSL IAD
- Ethernet cable with RJ45 plugs on each end (included with IAD)
- DB9-RJ45 Adapter (included with IAD)
- RJ45/RJ45 straight-through cable for connecting to control port (included with IAD)
- PC computer with HyperTerminal or equivalent VT-100 emulation program, or an ASCII ("dumb") terminal.

Installing the AC power cord

This section describes installing the power cord into the IEC-320 connector on the 3086FR. ***Do not connect the male end of the power cord to the power outlet at this time.*** Do the following:

1. Install the power cable into *Power* connector (see figure 2). The AC main socket outlet shall be within 10 feet (3 meters) of the equipment and shall be easily accessible.

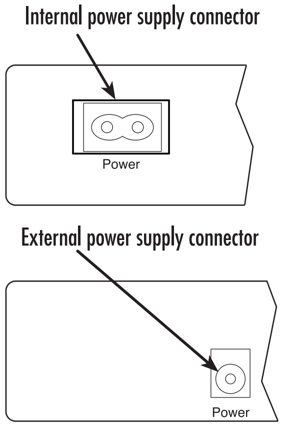

Internal power supply connector
Power
External power supply connector
Power

Figure 2. Power connector location on rear panel

WARNING

To avoid the risk of injury from electric shock, the power cord connected to the IEC-320 connectors must be a grounded power cord.

CAUTION

The 3086FR power supply automatically adjusts to accept an input voltage from 100 to 240 VAC (50/60 Hz).

Verify that the proper voltage is present before plugging the power cord into the receptacle. Failure to do so could result in equipment damage.

2. Verify that the AC power cord included with your 3086FR is compatible with local standards. If it is not, refer to Chapter 14, “Contacting Patton for assistance” on page 27 to find out how to replace it with a compatible power cord.
3. Connect the male end of the power cord to an appropriate power outlet.
4. Verify that the green *POWER* LED is lit.
5. Unplug the AC power cord from the Model 3086FR to power down the unit.

Connecting network cables

Except for the Console port, all connectors are on the rear panel of the ipRocketLink with the exception of the power connection. The Ethernet port is Green and the Line is Yellow. The Console port is the only electrical connection on the front panel.

Do the following:

1. Connect the DB9-RJ45 adapter to the DB-9 serial port on the PC or dumb terminal. Use the RJ45-RJ45 straight-through cable between the adapter and the red marked RJ45 port on the 3086FR IAD.
2. Do NOT connect the Frame Relay to ATM Converter to the Ethernet LAN now.
3. On the PC, start a HyperTerminal session at 9600 bps, 8 data bits, 1 stop bit, and no parity.
4. Plug the AC power cord into the Model 3086FR to power up the IAD.
5. Type *superuser* for Login:, and press Enter.
6. Then type *superuser* for the password, press Enter.
7. A message will display, “Login Successful.” By typing the character “?”, all the commands will be displayed. Any commands parameters may be seen by entering the command followed by a space and a question mark.

```
fi ethernet ? [The following parameters appear]
    add
    delete
    set
    show
    list
    clear
```

IP address Quick Start modification

The first parameter to change is the IP address from the default IP address of 192.168.1.1/24 (for the CP units) or 192.168.200.11 (for CO units) to your selected IP address. Follow these steps. Comments are in brackets [...].

fi `ip list interfaces  <enter>` [lists the characteristics of the different interfaces]

```
IP Interfaces:
  ID   |     Name      |   IP Address     |    DHCP     |     Transport
-------|---------------|------------------|-------------|------------------
  1    |   ip1         |   192.168.200.10 |  disabled   |   <bridge>
--------------------------------------------------------------------------
```

fi `ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0 <enter>`[Sets the new IP address which you have selected. The IP address in this example is for illustrative purposes only.]

fi `ip list interfaces <enter>` [To see if the change in IP address is correct]

fi `system config save <enter>` [To save the new IP address in flash memory.]

```
Wait for “configuration saved” message…

Saving configuration
```

fi

```
Configuration saved.
<enter>
```

fi

The IP address has now been successfully changed.

Web Operation and Configuration

Now that the IP address has been configured for your application, you can complete the configuration using any standard web browser.

PC Configuration

In order to connect the PC to the Ethernet LAN to communicate with the Model 3086FR, the PC’s IP address should be on the same subnet as the modem.

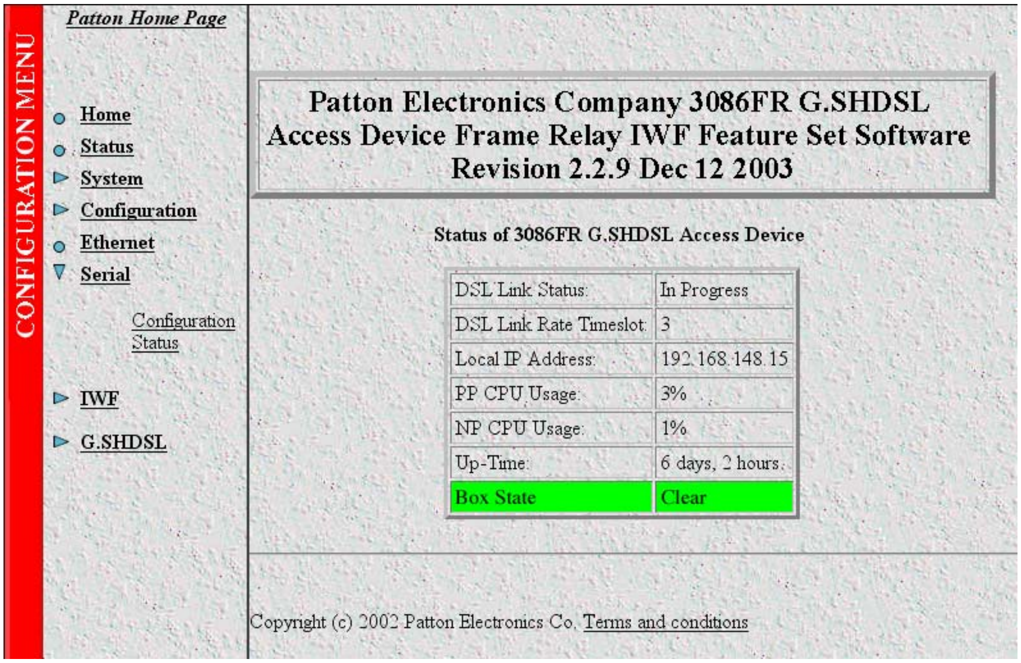
Connect a straight-through Ethernet cable between the PC’s NIC or PCMCIA Ethernet card and an Ethernet hub or switch.

Web Browser

Do the following:

1. Launch a standard web browser such as Netscape Communicator or Internet Explorer (IE).
2. Enter the 3086FR’s IP address into the URL or Address field of the browser.

The Model 3086FR home page displays (see figure 3).



Patton Electronics Company 3086FR G.SHDSL Access Device Frame Relay IWF Feature Set Software Revision 2.2.9 Dec 12 2003

Status of 3086FR G.SHDSL Access Device

DSL Link Status:	In Progress
DSL Link Rate Timeslot:	3
Local IP Address:	192.168.148.15
PP CPU Usage:	3%
NP CPU Usage:	1%
Up-Time:	6 days, 2 hours:
Box State	Clear

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

Figure 3. Model 3086FR home page

The Model 3086FR menu structure for models RIC and RID is shown in figure 4 on page 32, the menu structure for Model RIK is shown in figure 5 on page 33.

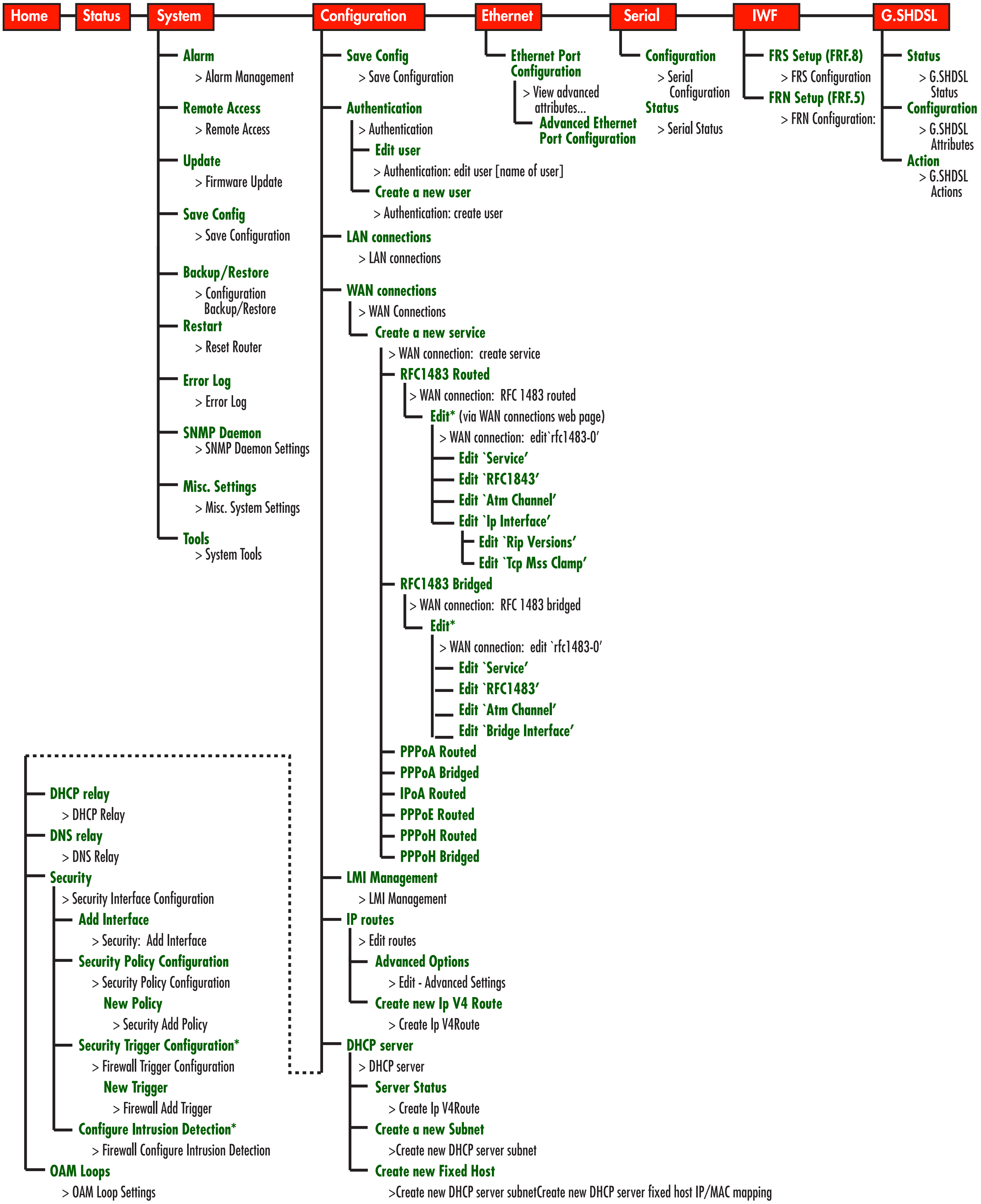


Figure 4. Model 3086FR Menu Structure (Models RIC and RID)

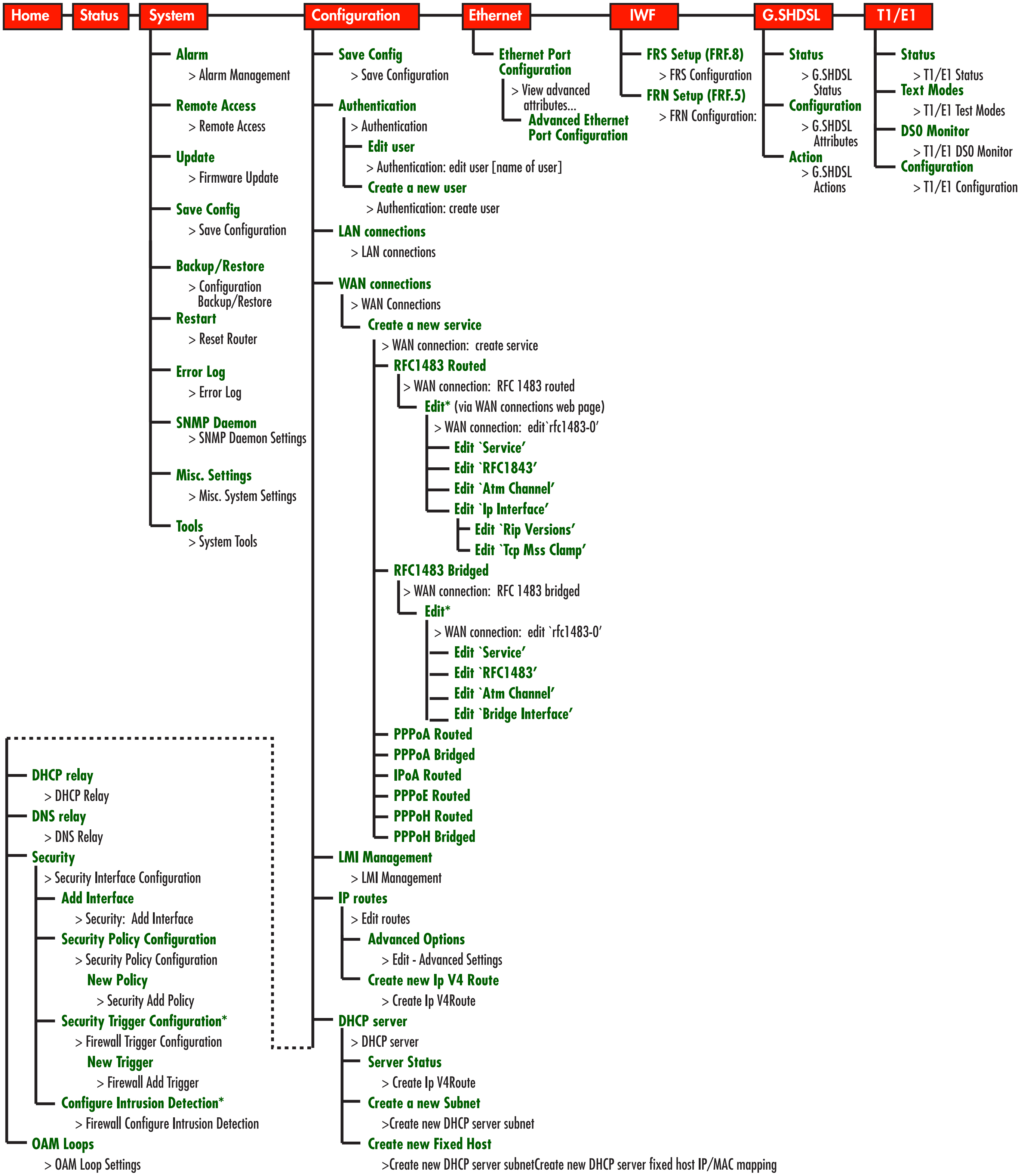


Figure 5. Model 3086FR Menu Structure (Model RIK)

Chapter 4 Connecting the DSL and data ports

Chapter contents

Introduction

The model 3086FR comes with a DSL port, 2 data ports: serial (V.35, X.21, or T1/E1), and a 10/100Base-T Ethernet port. Frame Relay data from the serial port is passed to the FR to ATM converter engine and is prepared for transmission over the DSL link – data from or to the serial port does not enter the router core of the 3086FR. Data from the Ethernet port is processed by the router or bridge core before entering the ATM encapsulation layer.

The 3086FR can be used as FR to ATM converter (ATM transport over DSL). In this case, configuration of the unit involves the following steps:

- Configure the DSL interface (assigning all bandwidth to the serial port).
- Configure the serial port
- Configure the FR to ATM conversion

When the 3086FR Ethernet port is used to route data from and to the Ethernet port, the following steps are required to configure the unit:

- Configure the DSL interface (assign bandwidth required to the serial port, the 3086FR will assign the remaining bandwidth to the Ethernet port)
- Configure the serial port
- Configure the FR to ATM conversion
- Configure the WAN link layer 2 (ATM)

DSL port

The DSL port (see figure 6) is located on the back of the unit, and is presented on an RJ-11 female jack. The interface has a nominal impedance of 135-ohms. The Model 3086FR supports DSL communication between a customer location and a central office from 192kbps to 2.3 Mbps.

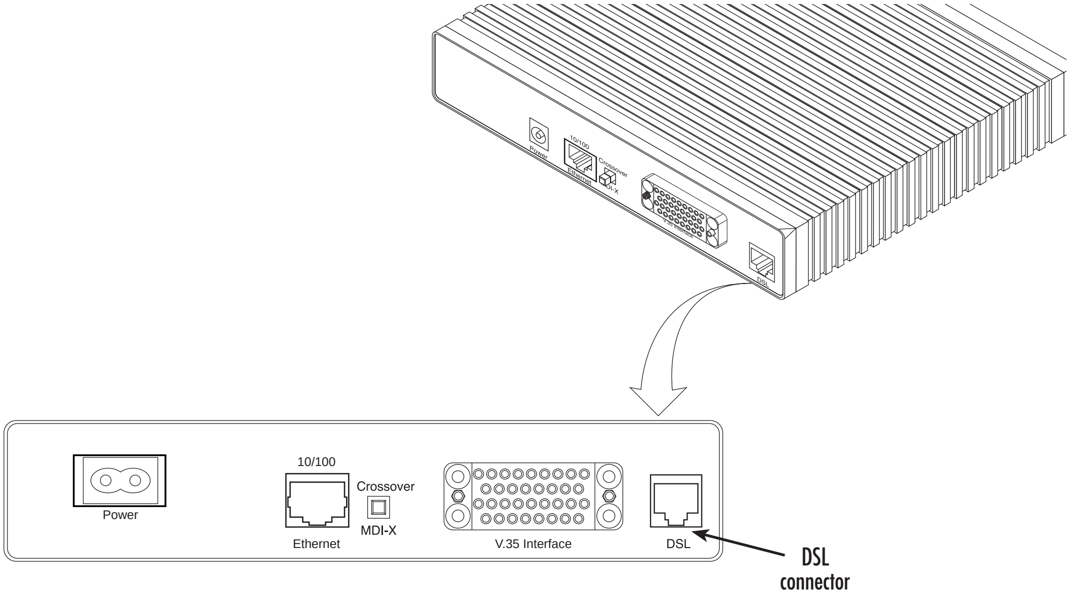


Figure 6. DSL port location

To function properly, the Model 3086FR needs one twisted pair of metallic wire. This twisted pair must be unconditioned, dry, metallic wire, between 19 (.9mm) and 26 AWG (.4mm) (the higher number gauges will limit distance). Standard dial-up telephone circuits, or leased circuits that run through signal equalization equipment, or standard, flat modular telephone type cable, are not acceptable. The female RJ-11 connector on the Model 3086FR's twisted pair interface is polarity insensitive and is wired for a two-wire interface.

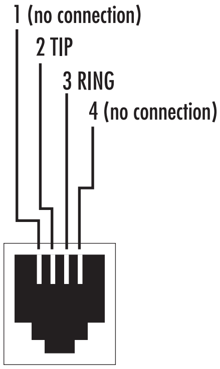


Figure 7. RJ-11 pinout

TDM Port

Model 3086FR units enable V.35, X.21, or T1/E1 interface connection to local routers, multiplexers, and other Frame Relay devices. The V.35 interface is presented either on a M/34, or DB-25 female connectors. The X.21 interface is presented on a female DB-15 connector, while the T1/E1 interface is presented on an RJ-48C jack, additionally the E1 interface is presented on dual BNC. Figure 8 on page 38 shows the different connectors offered for the serial port.

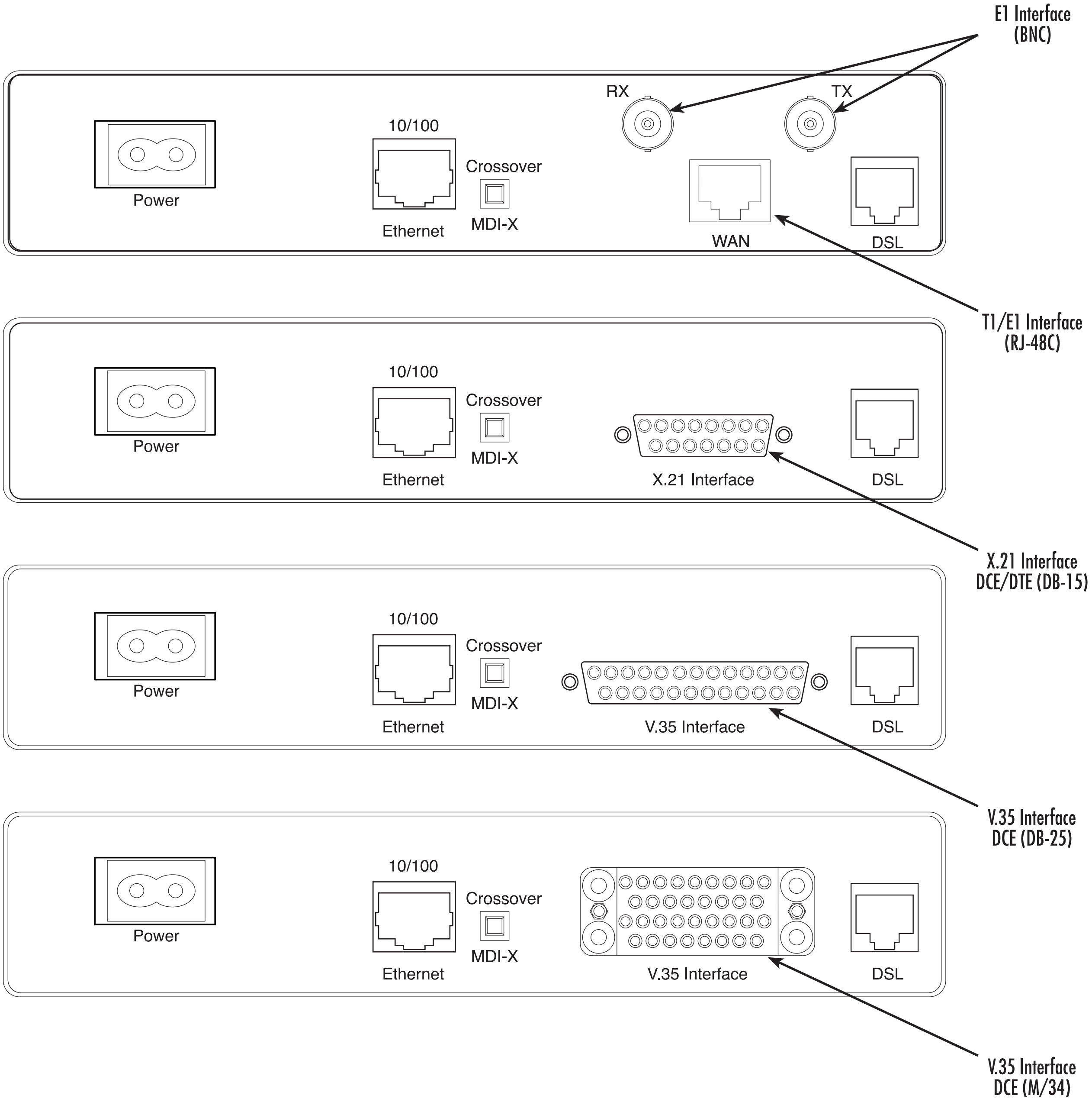


Figure 8. Rear panel power and interface connectors

V.35 and X.21 ports

The serial port in the 3086FR is simple to configure. The V.35 interface is wired as a DCE, the X.21 interface can be configured as a DCE (factory default), or as a DTE via internal configuration jumper. The following sections describe the 3086FR X.21 and V.35 port connection to DTE and DCE devices.

Connecting the 3086FR serial port to a DTE

The serial port on the Model 3086FR is configured as a DCE so it connects directly to a DTE using a standard straight through cable. The cable should present either a male M/34 or DB-25 connector on one end, for V.35 interfaces, or a male DB-15 for X.21 interface connection. The other end should be terminated with the appropriate connector (check your DTE equipment manual for pinout, gender, and DTE/DCE port configuration).

Connecting the 3086FR serial port to a DCE

V.35 interfaces.

The V.35 interface in the 3086FR is wired as a DCE, no DTE configuration is possible. If the equipment that the 3086FR is connecting to locally does not have the option for DTE configuration, a tail-circuit cable will be required (this cable is available from most datacomm supply vendors). The tail-circuit cable will cross most interface signals, so that the DCE interface of the 3086FR and the DCE interface of the third party equipment can function properly. Please be aware that some third party equipment will not be able to work properly in DCE to DCE configurations even when using a tail circuit cable (please refer to your third party equipment user manual for information on DCE-to DCE operation). The 3086FR requires a cable with a male M/34 or male DB-25 connector.

X.21 interfaces.

The Model 3086FR's X.21 interface configuration can be modified, by the user, as DCE (factory default) or DTE, via an internal jumper board. When the local third party equipment is configured as DCE, the Model 3086FR X.21 serial port can be configured as DTE, and a regular straight through cable can then be used. Do the following to configure the X.21 port as a DTE:

1. Open the 3086FR's case by inserting a screwdriver into the slots and twist the screwdriver head slightly. The top half of the case will separate from the lower half of the case (see Figure 9). Take caution not to damage any of the PC board mounted components.

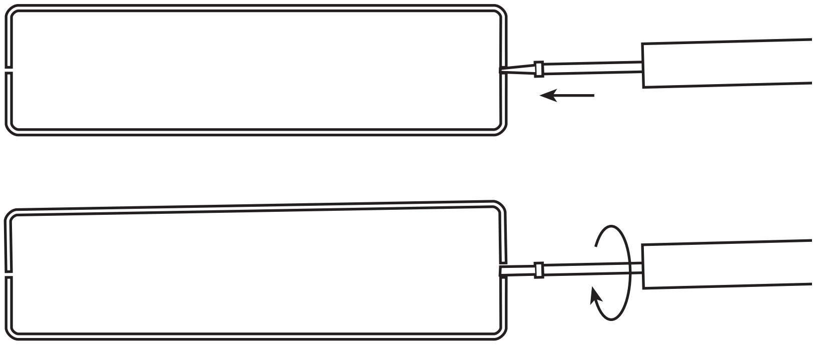
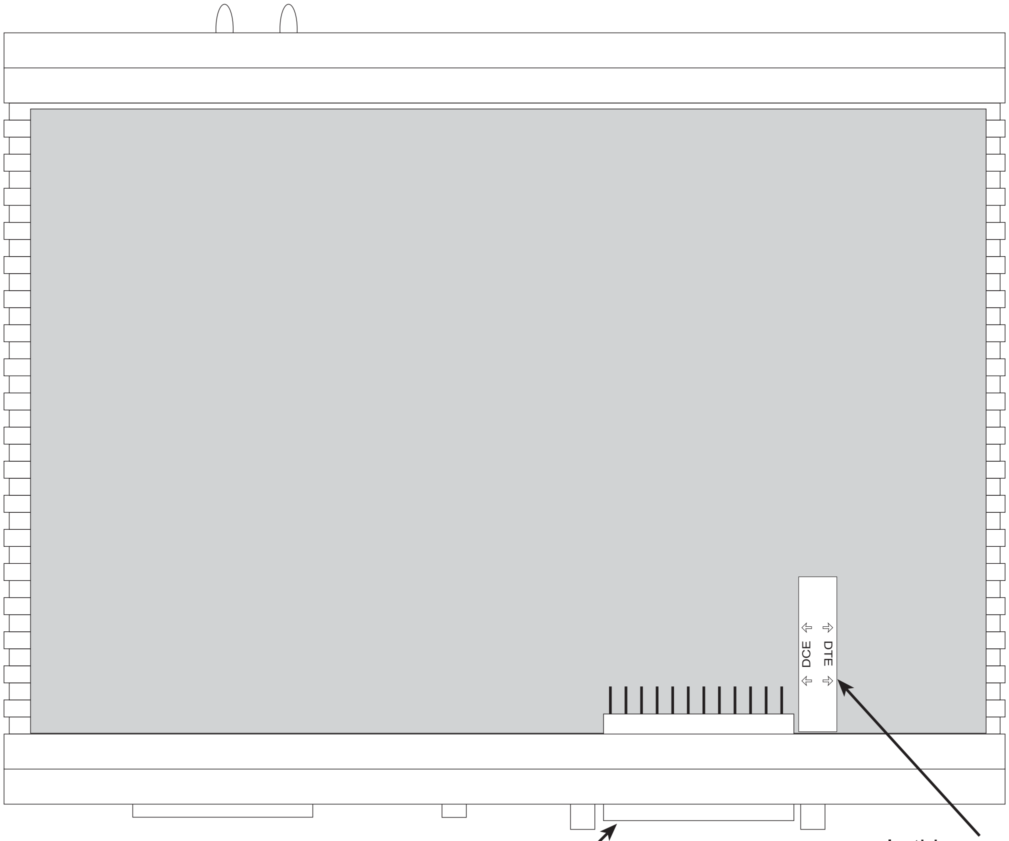


Figure 9. Case being opened with screwdriver

2. Locate the small daughter board on the 3086FR board between the DSL port (RJ-45) connector and the serial port connector (Figure 10 shows location of DTE/DCE daughter board).



X.21 connector

In this example, the DCE/DTE strap is configured for DCE because the “DCE” label on the strap is pointed toward the X.21 connector

Figure 10. Location of DCE/DTE board

3. The DTE/DCE daughter board is installed at the factory with the DCE label and arrows pointing towards the X.21 connector (DCE configuration). To change to DTE configuration, lift the daughter board from the connector, turn it around so that the DTE label an arrows point to the X.21 connector, and place it back on the connector. The X.21 port is now configured as a DTE.

Note When the X.21 port is configured as a DTE, the clocking mode for the port must be set for external clock.

T1 Interface

The 3086FR enables T1 or E1 device located at customer locations to access a carrier's network over two wire, long reach DSL links. This capability allows providers to offer T1/E1 services at customer locations that were previously outside the reach of standard T1/E1 lines.

The 3086FR/K offers a user configurable T1 or E1 interface. Selection of the interface is done via DIP switches, HTTP/SNMP, or command line interface (CLI).

The T1 interface is an eight position keyed modular jack configured as a RJ-48C for connection to 100-ohm twisted pair lines.

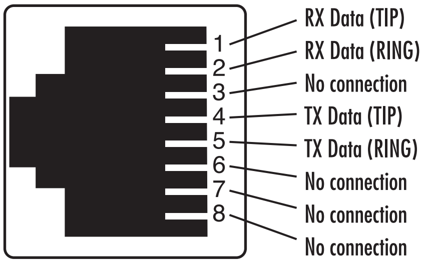


Figure 11. 3086FR T1 port pinout

T1 Interface Connection

The 3086FR will usually connect either to a local T1 device, or to a Telco terminated T1 line jack.

- To connect the 3086FR's T1 port to a local T1 device (PBX, router, mux) use a T1 'crossover' twisted pair cable. A crossover cable connects the transmit pins of the Model 3086FR's T1 port to the receive pins of the device attached to this port and vice versa. Check the third party T1 equipment documentation for pinout information and cable requirements.
- To connect the 3086FR's T1 port to a Telco terminated T1 line jack, use a straight through twisted pair patch cable. Consult with your T1 service provider for exact pinout information and cable requirements.

T1 Interface Configuration

The 3086FR T1 interface can be configured via HTTP/SNMP, or command line interface (CLI). This section discusses HTTP (web server) configuration. For CLI, see Appendix D, "Command Line Interface (CLI) Operation" on page 165.

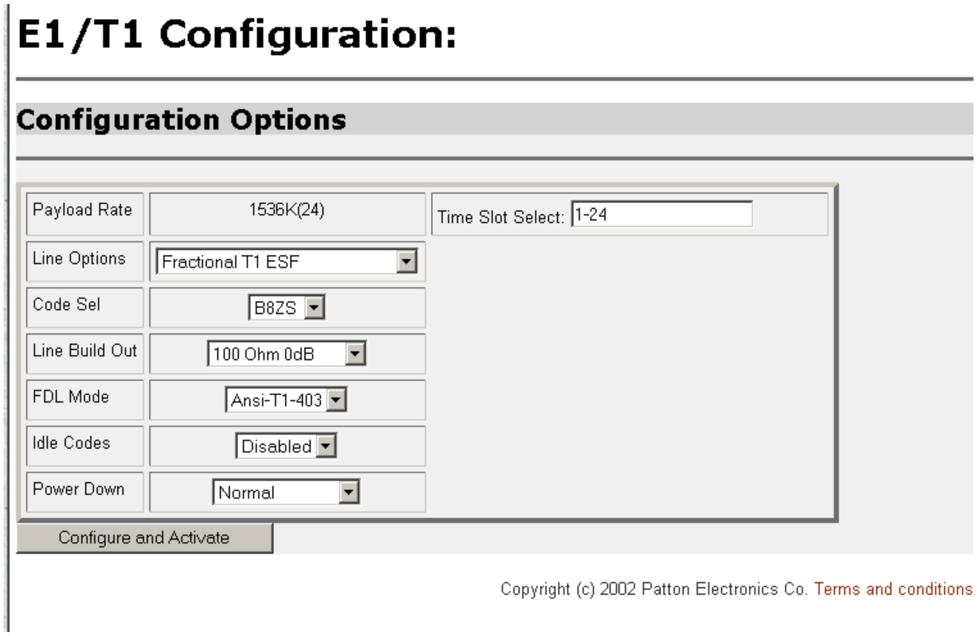
Web Interface Configuration

The T1 interface page is accesed from the Main Menu > E1/T1. This page allows configuration of T1 paraemeters as follows:

Time Slot Select. For a T1 using all 24 time slots, enter 1-24, for fractional T1 enter in any format for example: 1,2,3,5; or 1-5,10-24. Any entry for timeslots above 24 will return and invalid selection message.

Line Options: Fractional T1

Line Code: The 3086FR T1 interface uses B8ZS



E1/T1 Configuration:

Configuration Options

Payload Rate	1536K(24)	Time Slot Select: 1-24
Line Options	Fractional T1 ESF	
Code Sel	B8ZS	
Line Build Out	100 Ohm 0dB	
FDL Mode	Ansi-T1-403	
Idle Codes	Disabled	
Power Down	Normal	

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

Line Build Out: Select from 100 ohm (0dB), 100 ohm (-7.5dB), 100 ohm (-15dB), and 100 ohm (-22.5dB). For CSU/DSU application use 100 0dB option, consult your T1 service provider for more information.

FDL Mode: Options are ANSI-T1-403, ATT-54016, and Fdl-none. Consult your T1 service provider or third party equipment for FDL mode required.

Idle code: Enabled, Disabled. When enabled, the 2603 inserts idle codes on unused timeslots. Set this option to ‘Disabled’ unless instructed otherwise.

Power Down: Normal, Powered Down. When powered down, T1/E1 transceiver input and output lines will be set to high impedance to protect the device—set unit to “Normal” for regular operation.

Once all options have been selected, click on the **Configure and Activate** at the bottom of the screen. Additionally, save the configuration by going to the *Configuration* > *Save Config* menu.

E1 Interface

The 3086FR enables T1 or E1 device located at customer locations to access a carrier’s network over two wire, long reach DSL links. This capability allows providers to offer T1/E1 services at customer locations that were previously outside the reach of standard T1/E1 lines.

The 3086FR offers a user configurable T1 or E1 interface. Selection of the interface is done via HTTP/SNMP or command line interface (CLI).

The E1 interface is presented on both a modular, 8-pin RJ-48C jack for connection to 120-ohm twisted pair lines, and dual BNC female connectors for connection to 75-ohm coaxial lines.

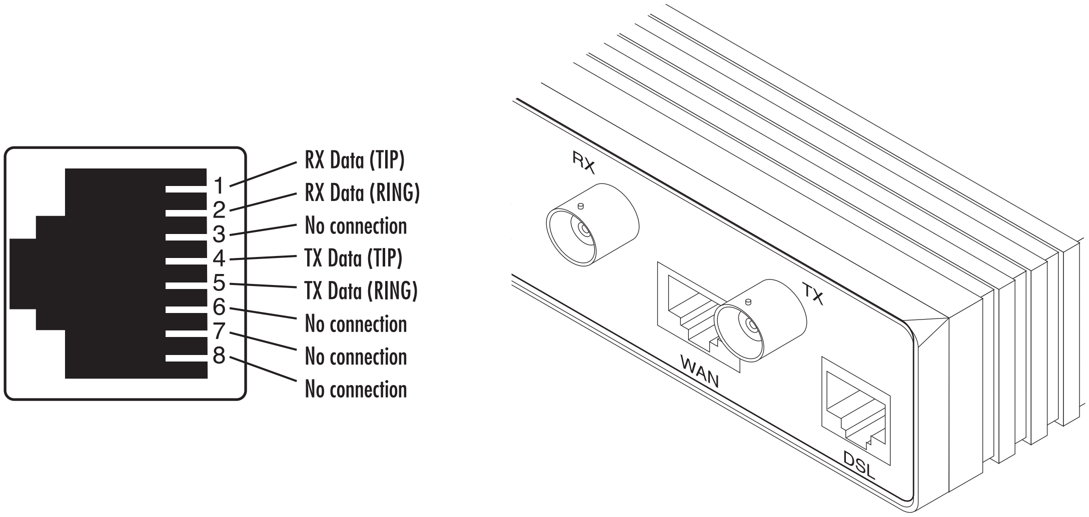


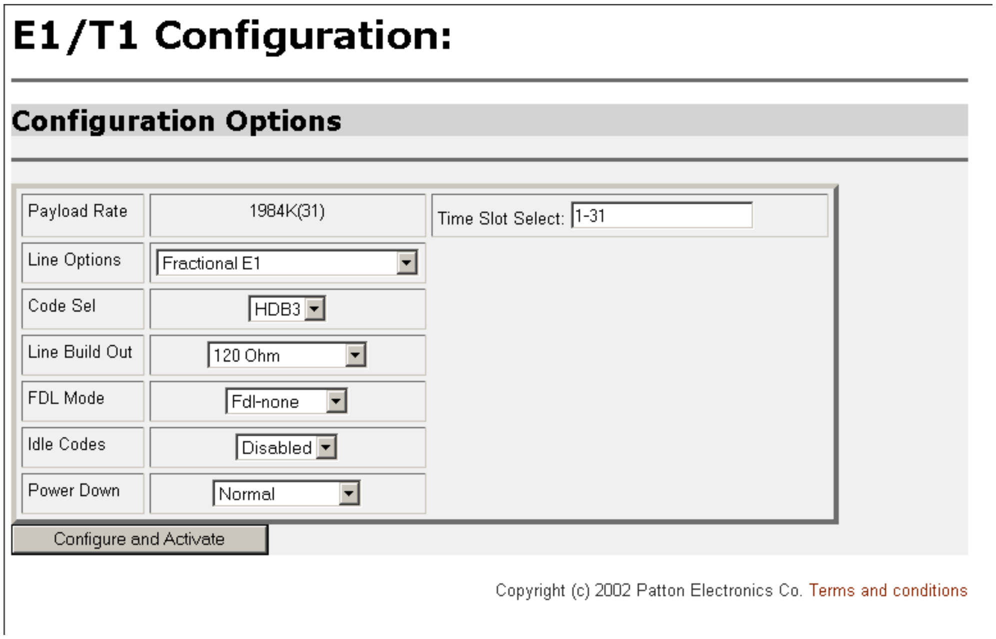
Figure 12. E1 interface with RJ-48C jack (120–ohm) and dual BNC (75-ohm) connectors

E1 Interface Connection

The 3086FR will usually connect either to a local E1 device, or to a Telco terminated E1 line jack.

- To connect to the 3086FR E1 port and a local E1 device, use an E1 crossover twisted-pair cable. A crossover cable connects the transmit pins of the Model 3086FR's E1 port to the receive pins of the device attached to this port and vice versa. Check the third party E1 equipment documentation for pinout information and cable requirements. If the E1 connection is made via the BNC connectors, connect the TX BNC of the 3086FR to Recive (RX) BNC of the local E1 device, and vice versa.
- To connect the 3086FR's E1 port to a Telco terminated E1 line jack, use a straight through twisted pair patch cable. Consult with your E1 service provider for exact pinout information and cable requirements.

The 3086FR T1/E1 port can be configured via HTTP/SNMP or command line interface (CLI). This section discusses HTTP (web server) configuration, for CLI and SNMP information see Appendix E on page 165.



E1/T1 Configuration:

Configuration Options

Payload Rate	1984K(31)	Time Slot Select: 1-31
Line Options	Fractional E1	
Code Sel	HDB3	
Line Build Out	120 Ohm	
FDL Mode	Fdl-none	
Idle Codes	Disabled	
Power Down	Normal	

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

Web Interface Configuration

Launch Internet Explorer or similar web browser, type the IP address of the 2603, enter username 'superuser' and password 'superuser'. From the main page click on the E1/T1 option > Configuration. This page allows configuration of E1 parameters as follows:

Time Slot Select. For unframed E1 service (Clear Channel) enter time slots 0-31. For a full framed E1 enter 1-31, for partially filled E1 enter the range of timeslots using the format for example: 1,2,3,5; or 1-5,10-31. Any entry for timeslots above 31 will return and invalid selection message.

Line Options: Choose from Clear Channel E1, Fractional E1, Fractional E1, Multi-Frame(CAS) E1, Multi-Frame(CAS) E1 with CRC. Consult with your service provider which option is required.

Line Code: Choose from AMI or HDB3. Most E1 applications use HDB3

Line Build Out: Select 120 ohm if the E1 connection is made via the RJ-48C connector, select 75 Ohm if the E1 connection is made via the Dual BNC connectors.

FDL Mode: FDL is a T1 application, therefore select 'Fdl- none' for E1 applications.

Idle code: Options are Enabled or Disabled. When idle code is Enabled, the 3086FR/K inserts idle codes on E1unused timeslots. Set this option to 'Disabled' unless instructed otherwise.

Power Down: Options are Normal and Powerdown. When the 3086FR is set to powered down, it will set the E1 interface pins to high impedance to protect the device – set unit to "Normal" for regular operation.

Once all options have been selected, click on the **Configure and Activate** button at the bottom of the screen. Additionally, save the configuration by going to the *Configuration* > *Save Config* menu.

Chapter 5 Configuring the DSL and serial ports

Chapter contents

Introduction

Configuration of the 3086FR can be broken down into the following steps:

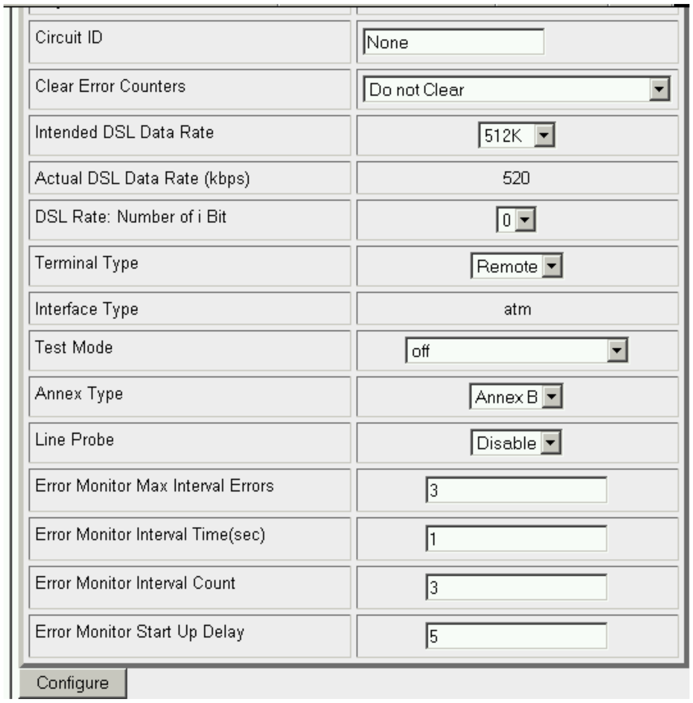
- Configuring the DSL interface (see section "Configuring the DSL interface")
- Configuring the serial interface (see section "Configuring the serial port" on page 50)
- Configuring the ATM/FR features (see chapter "Configuring FR and ATM features" on page 53)
- Configuring the LMI (local management interface) (see chapter "Configuring the DSL and serial ports" on page 45)

Configuration can be done via web browser, or via command line interface (CLI) through local terminal or Telnet.

Configuring the DSL interface

Configuring DSL interface using the web browser.

To go to the G.SHDSL attributes page, from the main menu click on the G.SHDSL option, then click on the configuration option.



Circuit ID	None
Clear Error Counters	Do not Clear
Intended DSL Data Rate	512K
Actual DSL Data Rate (kbps)	520
DSL Rate: Number of i Bit	0
Terminal Type	Remote
Interface Type	atm
Test Mode	off
Annex Type	Annex B
Line Probe	Disable
Error Monitor Max Interval Errors	3
Error Monitor Interval Time(sec)	1
Error Monitor Interval Count	3
Error Monitor Start Up Delay	5

Circuit ID

User can enter up to 30 alphanumeric characters for circuit identification

Clear Error Counters

Selecting "Clear" will reset the error counters displayed in the "Status" screen.

Intended DSL Data Rate

DSL line rate at which you wish to connect. In a CPE to DSLAM configuration, the 3086FR (CPE) will have the DSL rate dictated by the DSLAM (CO). The model 3086FR will connect at nx64kbps speeds from 192kbps to 2.3Mbps.

Actual DSL Rate

This field displays the DSL rate connection; it displays the payload rate plus 8kbps automatically assigned to a DSL management channel. For instance, if a DSL rate of 512kbps is selected in the "Intended DSL Data Rate" window, the actual DSL Data rate field will display 520kbps, this corresponds to 512kbps payload plus 8kbps management channel.

DSL Rate

Number of i Bit: The i bit increments DSL speed by 8kbps in addition to the DSL rate selected in the "Intended DSL Data Rate" window. Most applications use nx64kbps DSL speeds, leave this setting at "0", unless your application calls for a non-nx64 speed. Selections for the I bit are 0 through 7 as follows:

0 = no increment

1 = Intended DSL data rate + 8 kbps

2 = Intended DSL data rate + 16 kbps

3 = Intended DSL data rate + 24 kbps

4 = Intended DSL data rate + 32 kbps

5 = Intended DSL data rate + 40 kbps

6 = Intended DSL data rate + 48 kbps

7 = Intended DSL data rate + 56 kbps

Terminal Type

Select between Remote and Central. Use the "Remote" setting for 3086s located at customer premises and which connect to a DSLAM.

Note The unit set to "Central" will act as master and will impose DSL rate on the unit set as "Remote"

Interface Type

The 3086FR is set to ATM transport.

Test Modes

The 3086 use a series of loopbacks to test the serial, Ethernet, and DSL links, please refer to the Diagnostics section for more information.

Annex Type

Annex type refers to spectral compatibility between DSL and T1 or E1 signals. For North America and other areas where T1 lines are used, select Annex A, for areas where E1 lines are used select Annex B.

Line Probe

Line probe is a tool used to determine maximum achievable rate when initially connecting 3086 to a copper line of unknown quality. Set this feature to “Enable” on both 3086s at each end of the link.

> **Note** Once line probe measurements have been completed set this feature to “Disabled”

The bottom four fields in the G.SHDSL Attributes page correspond to error monitors. Error monitor will watch the DSL line parameters and determine whether or not the current DSL link is capable of passing error free data. The error monitor will accumulate DSL line statistics (CRC count, FIFO errors, LOSW count, etc..) and make a determination on whether or not to drop DSL link and retrain based on the thresholds setup by the user

- **Error Monitor Max Interval Errors:** Number of allowable errors per interval. Default = 3
- **Error Monitor Interval Time (sec):** Length in seconds of the current interval. Default = 1
- **Error Monitor Interval Count:** Number of intervals in error before the DSL link is restarted. Default = 3
- **Error Monitor Start Up Delay:** Amount of time to wait, after the link is up, before monitoring the DSL link. Default = 5

Once you have entered your selections or changes, click on the “Configure” button at the bottom of the screen. Additional go to the G.SHDSL > Action link on the left side of the screen, and hit “action” to start the DSL interface with the new settings.

Refer to section “Configuring the serial port” on page 50.

Configuring the DSL interface using the CLI

Access the command line interface via local terminal or Telnet. To configure the DSL interface enter the following commands.

DSL Data Rate

Set the DSL rate by entering bandwidth in number of timeslots (each timeslot (TS) equals 64kbps) for example to select a DSL bandwidth of 512kbps enter 8 timeslots as follows:

```
--> gshdsl set dslrateTS 8
```

DSL timeslot options go from 3 = 192kbps to 36= 4.6Mbps

Data Link Interface

The datalink interface for the 3086FR is ATM. Enter the command as follows:

```
--> gshdsl set interface atm
```

Annex Type

Annex type refers to spectral compatibility between DSL and T1 or E1 lines traveling in the same bundle. For North America and other areas where T1 lines are used, select Annex A, for areas where E1 lines are used select Annex B.

To enter annex B type:

```
--> gshdsl set ghsannex AnnexB
```

For Annex A type:

```
--> gshdsl set ghsannex AnnexA
```

Line Probe

This is not a required step. Line probe is a tool used to determine maximum achievable rate when initially connecting 3086 to a copper line of unknown quality. Set this feature to “Enable” on both 3086s at each end of the link. Once line probe measurements have been completed set this feature to “Disabled”

```
--> gshdsl set LineProbe
Disable
Enable
--> gshdsl set LineProbe Disable
```

Error Monitors

Error monitor will watch the DSL line parameters and determine whether or not the current DSL link is capable of passing error free data. The error monitor will accumulate DSL line statistics (CRC count, FIFO errors, LOSW count, etc..) and make a determination on whether or not to drop DSL link and retrain based on the thresholds setup by the user

Error Monitor Max Interval Errors

Number of allowable errors per interval. Default = 3

```
--> gshdsl set errMonIntervalThreshold 3
```

Error Monitor Interval Time (sec)

Length in seconds of the current interval. Default = 1

```
--> gshdsl set errMonIntervalTime 1
```

Error Monitor Interval Count

Number of intervals in error before the DSL link is restarted. Default = 3

```
--> gshdsl set errMonIntervalCnt 3
```

Error Monitor Total Intervals

TBD

Error Monitor Start Up Delay

Amount of time to wait, after the link is up, before monitoring the DSL link. Default = 5

```
--> gshdsl set errMonStartupDelay 5
```

Once you have entered the options, at the command prompt type:

```
-->system config save    to save the configuration.
```

Refer to section “Configuring the serial port” on page 50.

Configuring the serial port

This section defines the configuration options available for the serial interface on the Model 3086FR. This information could be used to configure the V.35 or X.21 interface available on the unit.

Configuration variables available

Click on *Serial* > *Configuration* to configure variables. The following variables are configurable through the CLI or web interface on the unit.

Clock Mode

Determines the source of timing for the unit.

- **Internal:** The unit will generate the appropriate clock speed defined by the speed setting of the interface.
- **External:** The unit will accept the clock from the interface and will use that clock to receive and transmit data across the interface

Clock Invert Functions: (rxClkInv – receive clock, txClkInv – transmit clock)

Setting this variable will invert the appropriate clock at the interface. This should only be used under direction of Patton Electronics technical support in order to trouble shoot system installations. Possible settings include both normal and inverted

Speed

The speed setting function will determine the clock rate that will be used by the interface. Appropriate settings include any n x 64K speed setting between 64–2048 kbps.

CLI Configuration Methods

The following section defines how to configure the serial interface using the CLI. All serial interface functions are available under the “serial” directive of the CLI.

Set configuration variable

Command: serial set <variable> <value>

The following shows the user setting the speed of the serial interface to a value of 2048MHz.

```
ﬁ serial speed 2048
```

Show current configuration settings

Command: serial show

The “serial show” command will tell the system to display the current configuration settings for the serial interface. The following shows the output of the “serial show” command.

```
ﬁ serial show
             Clock Source : internal
               Intf Speed : 2048
          Tx Sample Point : txclk
               Tx Clk Inv : normal
```

```
                    Rx Clk Inv : normal
```

Gain help about the Serial Interface

Command: serial help

This command will request that the system provide help about each of the configuration variables that are available in the serial interface. The following shows the output of the “serial help” command.

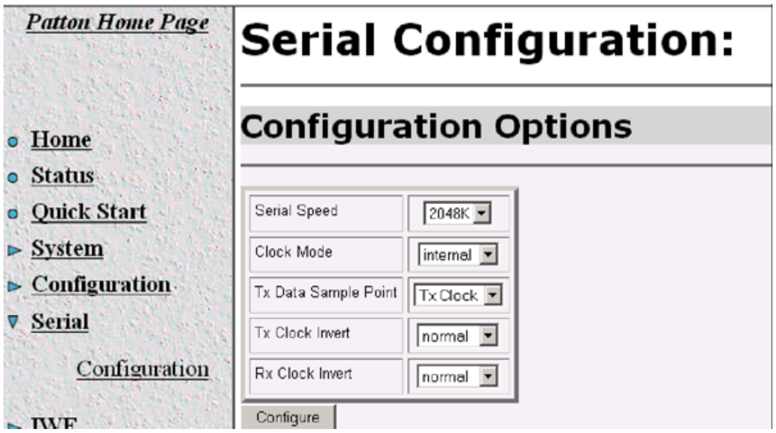
```
ﬁ serial help
```

Serial Interface Help Screen

```
>serial show:
>              Show the current configuration of the
>              serial interface
>serial help:
>              Show this help screen
>serial clock:
>              Defines the clock mode or source of timing
>              for the serial interface.
>     options: internal - internal timing
>              external - external timing
>     notes:   For X.21 devices this setting must match
>              the DTE/DCE jumper inside the unit
>serial speed:
>              Defines the clock speed for the serial interface
>     options: n x 64K speed (n= 1..32), example: "1536" or "256"
>
> serial txClkInv:
>              Allows the user to invert the clock source
>     options: normal - use normal clock
>              inverted - use the inverted version of the clock
> serial rxClkInv:
>              Allows the user to invert the clock source
>     options: normal - use normal clock
>              inverted - use the inverted version of the clock
> serial txSamplePoint:
>              Determines whether the TxData will use the External
>              Clock or the Transmit clock to sample data
>     options: txClk  - use Transmit Clock
>              extClk - use External Clock
>
```

Web Interface Configurations

The serial interface can be configured using the web interface by following the “Serial” hyperlink on the web management screen. The following screen shot shows the configuration variables as they are displayed on the web management screen.



Serial Configuration:

Configuration Options

Serial Speed	2048K
Clock Mode	internal
Tx Data Sample Point	Tx Clock
Tx Clock Invert	normal
Rx Clock Invert	normal

Chapter 6 Configuring FR and ATM features

Chapter contents

Introduction

This chapter explains the three basic Frame Relay (FR)/ATM configurations of the 3086FR IAD and how to configure them. They are:

- Frame Relay Network (FRN) interworking (FRF.5)
- Frame Relay Service (FRS) interworking (FRF.8)
- Ethernet-based Frame Relay/ATM operation

FRF.5 and FRF.8 are two agreements between the FR Forum and ATM Forum that enable FR and ATM networks to be used together; along with the Ethernet-based Frame Relay operation configuration, the three ports may be configured as Ethernet, FR/PPP and ATM with the ability to route between these three ports. Consult the specific sections for each type of application.

Frame Relay Network (FRN) Interworking (FRF.5) provides a mapping and encapsulation mechanism between FR and ATM networks so an ATM network may be used to transport FR from end-to-end. The ATM network is completely transparent to the FR network and equipment. The IWF (Interworking Function equipment) implements this function; in this case, done by the Model 3086FR.

If transport speeds higher than the typical FR network are desired or if only an ATM network is available for transport between two locations running FR, FRF.5 provides the capability for joining these two types of networks together. Obviously there are significant differences between FR and ATM networks. FR uses variable-length frames while ATM uses a fixed-length cells (53 octets). They also have different parameters and variables in their headers and trailers. Figure 13 is a typical application in which both end locations have FR equipment but uses an ATM network for transport. The IWF is equipment which implements the Interworking Function, which in this case is FRF.5. The IWF is the Model 3086FR IAD.

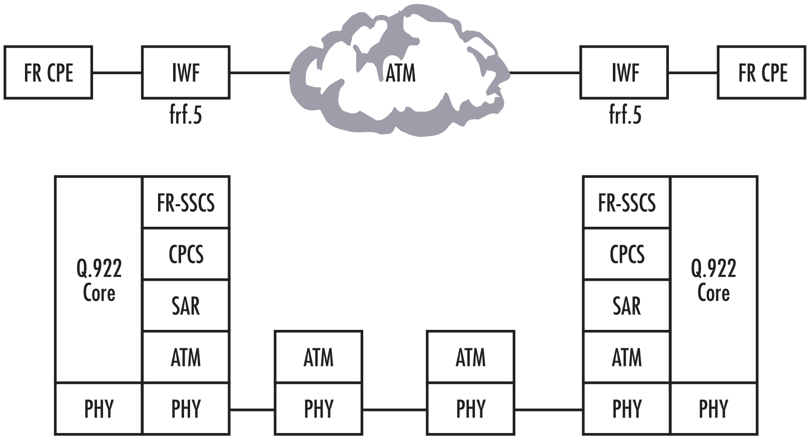


Figure 13. Application with both end locations having FR equipment but using ATM for transport

Figure 14 is a variation upon the previously described application. Here one end has FR equipment but the other location has special ATM equipment which recognizes FR. Specifically it must support the FR Service Specific Convergence Sublayer (FR-SSCS).

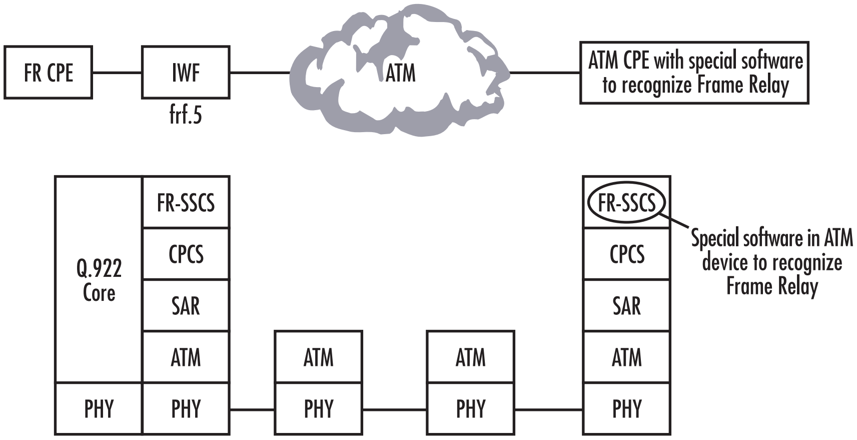

FR CPE
IWF
frf.5
ATM
ATM CPE with special software to recognize Frame Relay
Q.922 Core
FR-SSCS
CPCS
SAR
ATM
PHY
PHY
ATM
PHY
ATM
PHY
FR-SSCS
CPCS
SAR
ATM
PHY
Special software in ATM device to recognize Frame Relay

Figure 14. Application with one location having FR equipment and the other ATM equipment that recognizes FR

One advantage of using FRF.5 over FRF.8 is that one VCC (and one VCI/VPI within the VCC) in the ATM network is used to transport multiple DLCIs (PVCs) between two FR locations. For additional details, see section "Frame Relay Network (FRN) Interworking (FRF.5)" on page 57.

With Frame Relay Service (FRS) Interworking (FRF.8), ATM CPE equipment on one end may operate with FR CPE equipment on the other end. The FRS IWF occurs between the ATM and FR networks and/or equipment. FRF.8 provides a conversion mechanism so FR and ATM networks may function seamlessly. Neither network has no knowledge of the other. It is essentially a complete conversion of the parameters between Frame Relay and ATM. For additional details, see section "Frame Relay Service Interworking (FRF.8)" on page 66.

Figure 15 shows the service interworking between FR and ATM services.

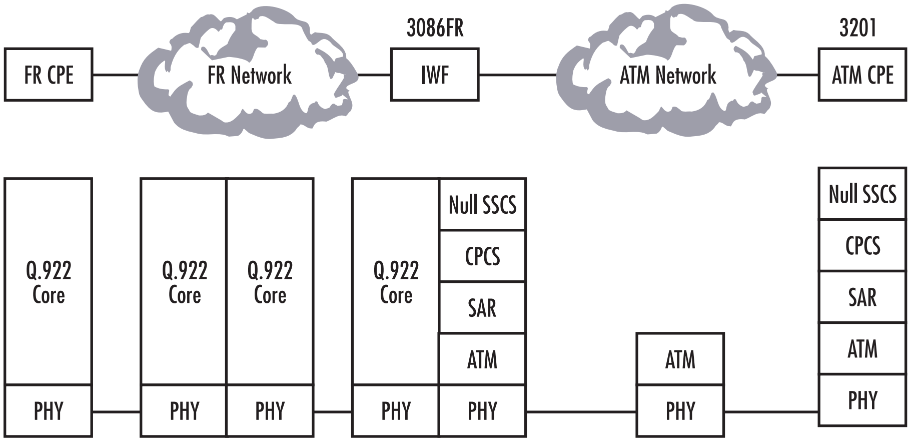


Figure 15. Service interworking between FR and ATM services

Observe from the stack that a true conversion has occurred between the FR and ATM networks. In FRF.5 the uppermost sublayer is FR-SSCS, but in the FRF.8 Interworking Agreement, it is *null SSCS*.

The third application is called Ethernet-based Frame Relay/ATM. While FRF.5 and FRF.8 has a fixed mapping of DLCI PVCs to ATM VCI/VPIs, with Ethernet-based FR/ATM there is not a fixed mapping from FR to ATM. We now have the ability to do routing between any of the three ports—Ethernet, serial (PPP or FR), and DSL (ATM) ports. Nevertheless FRF.5/FRF.8 may operate simultaneously. An example of Ethernet-based FR/ATM is a 3086FR in a company's office. All three ports are connected through the integrated router. The serial port (PPP or FR) with the WAN connection (ATM) via the DSL port. See figure 16. For additional details, see section "Frame Relay (Ethernet-based) operations" on page 74.

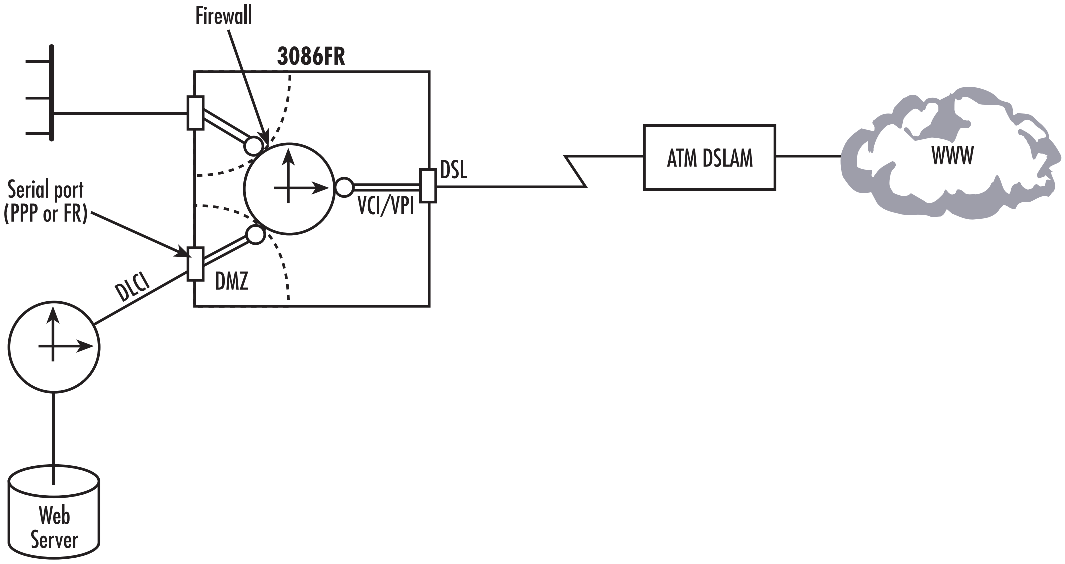


Figure 16. Example Ethernet-based FR/ATM application

The PCs on the private side of the firewall have access to the web server in the DMZ and the Internet. Outside users have access to the web server in the DMZ but cannot access the PCs on the company's private network (intranet) unless first accessed by one of the company's PCs behind the firewall.

Frame Relay Network (FRN) Interworking (FRF.5)

Frame Relay Networking (FRN) Interworking (FRF.5) is a mapping and encapsulation mechanism by which Frame Relay networks can communicate with ATM networks for transporting Frame Relay traffic. As described in the introduction to this chapter, there are two scenarios. One characteristic of FRF.5—as opposed to FRF.8—is the necesity to support the Frame Relay Service Specific Convergence Sublayer (FR-SSCS). The Model 3086FR in FRF.5 mode supports all of the required Interworking Functions (IWF) required for Frame Relay Network Interworking operation.

The Frame Relay Network Interworking functions are defined by the Frame Relay Forum specification *Frame Relay/ATM PVC Network Interworking Implementation Agreement FRF.5*.

FRN configuration options

The Frame Relay Network Interworking functions on the Patton Electronics Model 3086FR are defined by ports and channels. It is important to understand the implementation of FRF.5 in the Model 3086FR. There are 8 ATM Ports (called VCC or *channel* in FRF.5). Each port can be configured to have one channel (DLCI) or up to 8 channels (DCLIs). The Mux Mode variable controls the selection of *one-to-one* or *many-to-one* multiplexing. When the connection multiplexing is configured for one-to-one, each port can carry one channel (DLCI or PVC). However when many-to-one is selected, up to 8 channels (DLCIs) can be carried in one ATM port. Since each of the 8 ports may be configured to have 8 channels, up to 64 channels (DLCIs) can be transported over the ATM network. Figure 17 shows the organization of the ports and channels with the associated variables in the Model 3086FR.

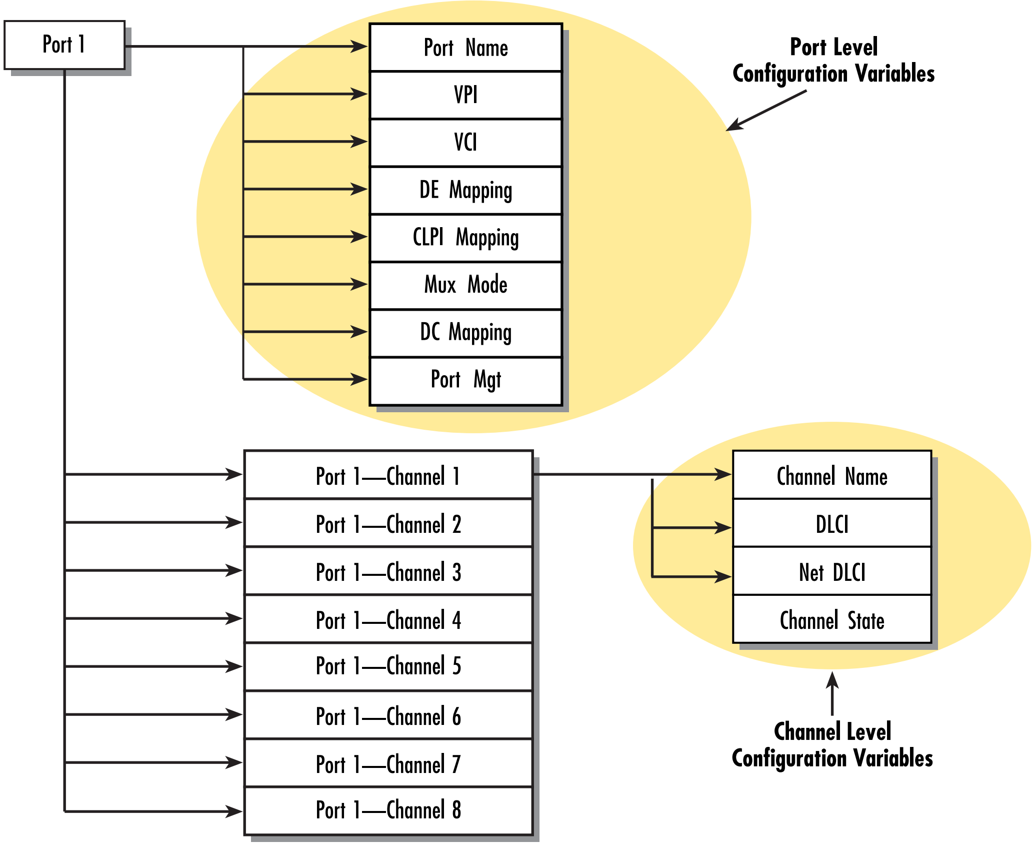


Figure 17. Organization of the Model 3086FR ports and channels with the associated variables

Web configuration methods for FRF.5 port and channel level configuration

The following information can be used to configure and manage the Frame Relay Network Interworking functions using the web interface. All FRN configuration options can be found under the IWF link.

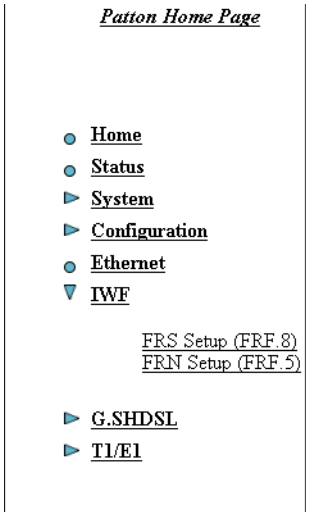
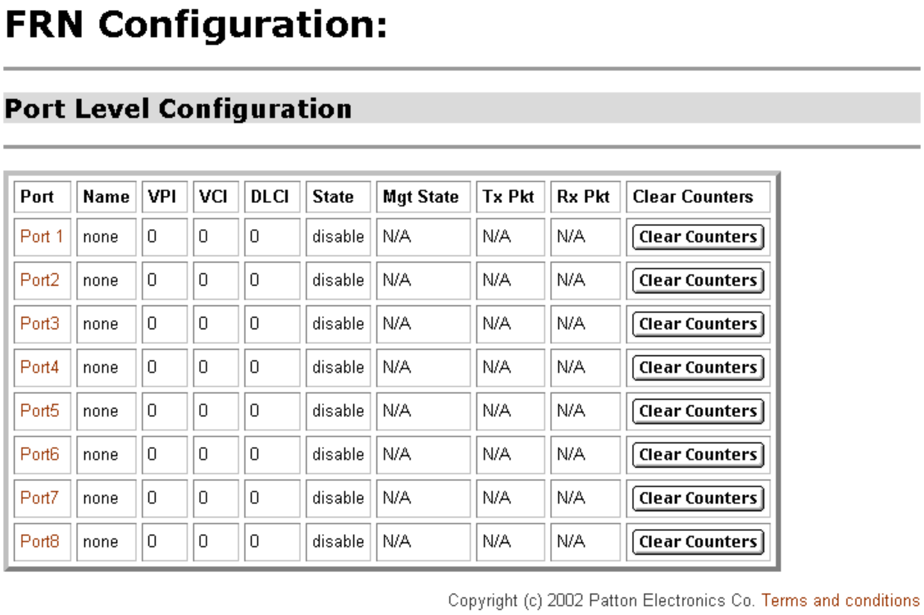


Figure 18. FRN Setup (FRF.5) link location

Once *FRN Setup (FRF.5)* is selected (see figure 18), the Port Level Configuration screen is displayed (see figure 19).



FRN Configuration:

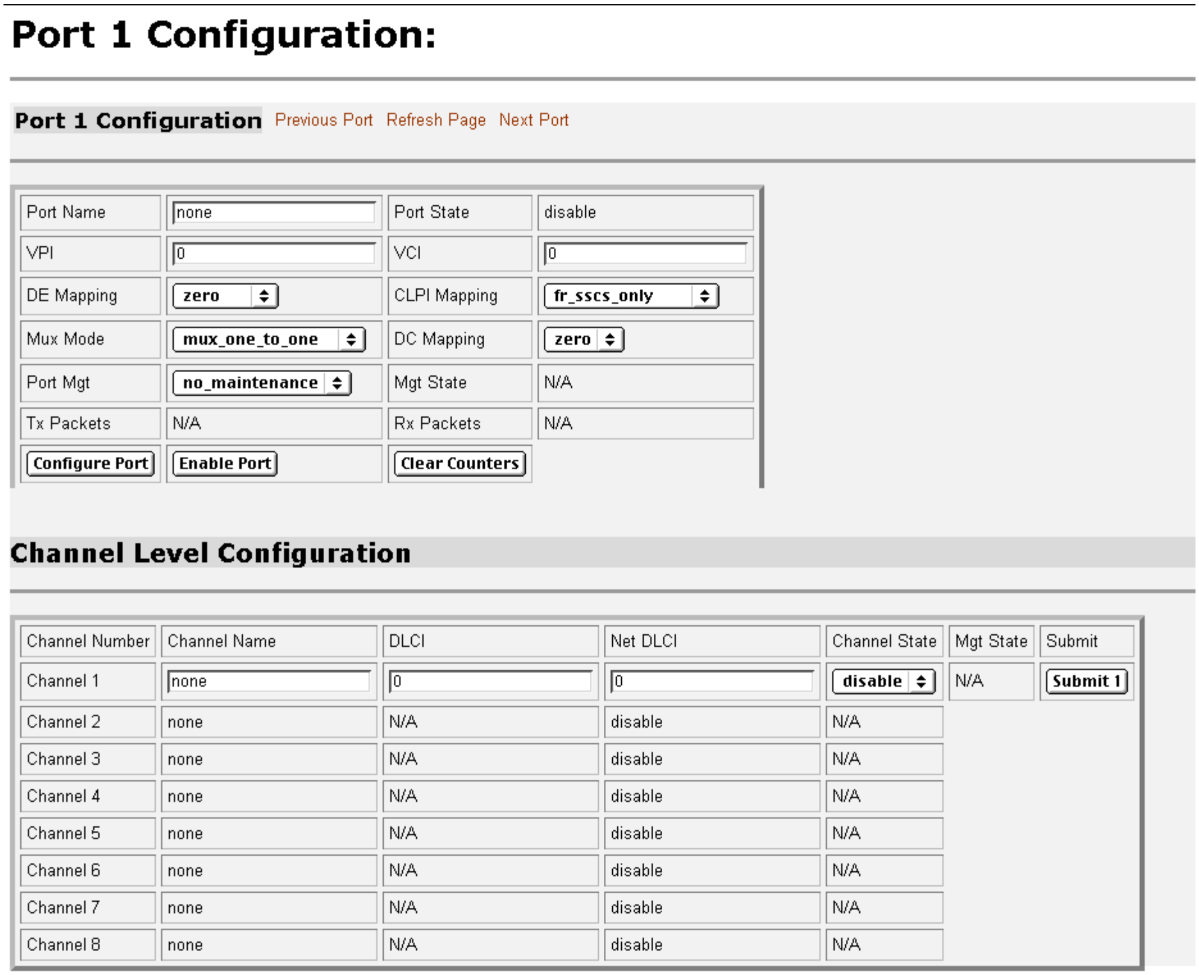
Port Level Configuration

Port	Name	VPI	VCI	DLCI	State	Mgt State	Tx Pkt	Rx Pkt	Clear Counters
Port 1	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port2	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port3	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port4	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port5	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port6	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port7	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters
Port8	none	0	0	0	disable	N/A	N/A	N/A	Clear Counters

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

Figure 19. FRN Configuration: Port Level Configuration window

The screen gives an overview of the FRN connections that are available. Each *Port Number* in the left column is a hyperlink that will display the Port X Configuration window (where *x* is the port number selected) (see figure 20), a more detailed view of the port along with the configuration of the channel level information.



Port 1 Configuration:

Port 1 Configuration Previous Port Refresh Page Next Port

Port Name	none	Port State	disable
VPI	0	VCI	0
DE Mapping	zero	CLPI Mapping	fr_sscs_only
Mux Mode	mux_one_to_one	DC Mapping	zero
Port Mgt	no_maintenance	Mgt State	N/A
Tx Packets	N/A	Rx Packets	N/A
Configure Port	Enable Port	Clear Counters	

Channel Level Configuration

Channel Number	Channel Name	DLCI	Net DLCI	Channel State	Mgt State	Submit
Channel 1	none	0	0	disable	N/A	Submit 1
Channel 2	none	N/A	disable	N/A		
Channel 3	none	N/A	disable	N/A		
Channel 4	none	N/A	disable	N/A		
Channel 5	none	N/A	disable	N/A		
Channel 6	none	N/A	disable	N/A		
Channel 7	none	N/A	disable	N/A		
Channel 8	none	N/A	disable	N/A		

Figure 20. Port X Configuration window

This screen is divided into the following sections:

Port Level Information screen

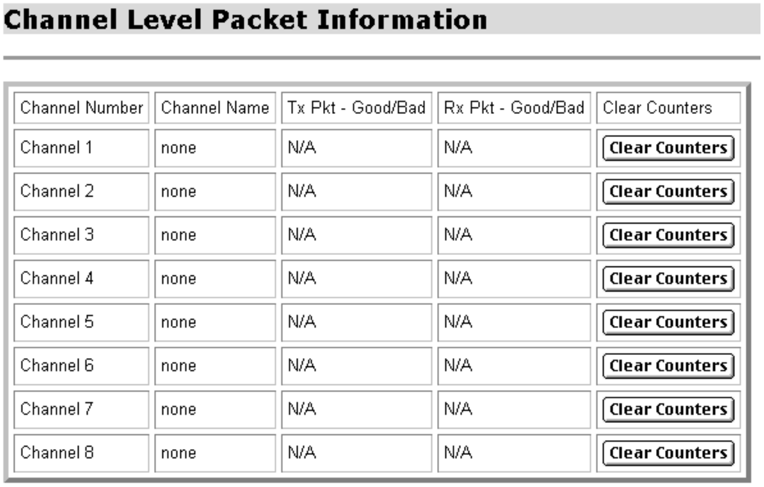
The Port Level Configuration information allows the user to configure Port Level variables (see figure 20). After configuration changes have been made, use the **Configure Port** button to set those parameters.

Channel Level Information screen

The Channel Level configuration section of the screen allows the user to setup and configure the individual channels associated with the specified port. Note that in figure 20 only a single channel is available for configuration. This is because the port is set to a MuxMode of one to one.

Packet Information screen

Figure 21 shows the packet information that is available for each channel. Note that the direction of the data is referenced to the ATM link. Thus Tx Data is data that is received on the Frame Relay link and transmitted out the ATM Link.



Channel Level Packet Information

Channel Number	Channel Name	Tx Pkt - Good/Bad	Rx Pkt - Good/Bad	Clear Counters
Channel 1	none	N/A	N/A	Clear Counters
Channel 2	none	N/A	N/A	Clear Counters
Channel 3	none	N/A	N/A	Clear Counters
Channel 4	none	N/A	N/A	Clear Counters
Channel 5	none	N/A	N/A	Clear Counters
Channel 6	none	N/A	N/A	Clear Counters
Channel 7	none	N/A	N/A	Clear Counters
Channel 8	none	N/A	N/A	Clear Counters

Figure 21. Channel Level Packet Information window

FRN configuration options

The Frame Relay Network Interworking functions on the Patton Model 3086FR are defined by CHANNELS and VPI/VCI. Ports are used to define the lower level Interworking Functions. First a port must be created that defines such items as the ATM VPI/VCI and the type of mapping that will be used to make the connection. Once the port is created, channels can be attached to the ports that will allow data channels to pass from the Frame Relay interface to the ATM interface. Channel configuration variables options include the Frame Relay DLCI that will be used to communicate with the Frame Relay Network.

Port Level Configuration Options:

Ports are used to define the lower level Interworking Functions. The port configuration defines the following variables:

- **VPI**—Virtual Path Identifier: ATM side Virtual Path Identifier for the specified connection.
- **VCI**—Virtual Channel Identifier: ATM side Virtual Channel Identifier for the specified connection
- **DE Mapping**—The DE Mapping variable is used to determine how the Frame Relay DE field (Discard Eligibility) will be mapped to the ATM CLPI (Cell Loss Priority Indication). This variable is only used in the Frame Relay to ATM mapping direction. Note that the DE bit from the core Q.922 (Frame Relay) packet will always be copied unchanged into the FR-SSCS PDU header cell. The following options define how the DE will be mapped to the ATM CLPI bit:
  - **Always_zero**: All ATM cells will have the CLPI field set to a constant value of 0.
  - **Always_one**: ATM: All ATM cells will have the CLPI field set to a constant value of 1.

- **Convert**: The system will convert the DE field received from the Frame Relay packet into the CLPI field of the outgoing ATM cell that is generated by the segmentation process.

- **CLPI Mapping**: The CLPI Mapping variable is used to determine how the ATM CLPI (Cell Loss Priority Indication) bit in the ATM cell will be mapped to the DE (Discard Eligibility) bit of the resulting Frame Relay packet. There are two options available.

  - **Fr_sscs_only**: The FR-SSCS removed from the ATM header PDU is used to set the DE bit in the out-put Frame Relay packet. The CLPI bit from the ATM cell is ignored.

  - **Fr_sscs_and_clpi**: Both the DE bit from the ATM header PDU and the CLPI bit from the received ATM cells are used to determine the output state of the resulting Frame Relay packet. The following table defines how.

CLPI received from ATM cell	DE from FR-SSCS of ATM cell	Outgoing DE bit of FR Packet
0	0	0
1	X	1
X	1	1

- **Multiplexing Mode**: The MuxMode variable allows multiple channels to be multiplexed onto a single port. A port is defined by its' VPI/VCI of the ATM rfc1483 data path. Channels are defined by their Frame Relay DLCI. Thus, the multiplexing mode will allow multiple Frame Relay channels to be transported over a single ATM VPI/VCI link. There are two options available.

  - **Mux_many_to_one**: The "many to one" option allows multiple DLCI channels to be transported over a single ATM rfc1483 connection. Note that if the MuxMode is not set to "many to one" trying to add multiple DLCI connections will result in errors.

  - **Mux_one_to_one**: The "one to one" option notifies the system that there will be a one to one mapping between a single ATM port VPI/VCI and a single Frame Relay DLCI.

- **FRN Name**: Allows the user to name the FRN port. This is helpful when viewing multiple connections to determine which VPI/VCI is associated with each port.

- **FRS state**: The state variable allows the user to enable or disable the port for operation. Note that port level configuration variables are not changeable "on the fly". If it is required that configuration changes are required, the user should disable the port, make the configuration changes, and then re-enable the port.

- **Port Level Maintenance**: Port level maintenance creates an LMI session across the ATM link. This is useful to determine the status of the link. There are three options available for Port Level Maintenance. The description of these variables is identical to that described in the beginning of this document. Note that in each case the only option available is "both". This means that the system is performing both "Network" and "User" side LMI functions.

  - **933A_both**

  - **617D_both**

  - **LMI_both**

- Port Level Mgt State: This variable defines the state of the Port Level Maintenance.

  - **Mgt_Port_DOWN**: Currently the LMI on the DTE side is DOWN

- **Mgt_Port_UP**: Currently the LMI on the DTE side is UP

Channel Level Configuration Options

The Channel Level Configuration variables are used to define the channels that are attached to the ATM port. The following variables are used to define each channel configuration.

- **DLCI**—Data Link Connection Identifier: Frame Relay side DLCI for the associated channel.
- **FRN Channel Name**: Allows the user to name the FRN channel. This is helpful when viewing multiple channel connections to determine which DLCI is associated with each channel.
- **FRN Channel State**: The state variable allows the user to enable or disable the channel for operation. Note that the port that the channel is connected to must be enabled before the channel can be enabled for operation.
- **Network DLCI**: The network DLCI allows the system to transport data over the atm link using a different DLCI than is used on the DTE side. If the network DLCI is set to "0", then the DTE side DLCI will be used. If the Network DLCI is set to any other value, that value will be used to transport data across the link using the FR-SSCS.
- **Mgt State**: The Mgt State variables defines the state of the Channel using the Port Level Management information. The following options are available
  - **N/A**: The port associated with this channel is disabled.
  - **n/a**: There is no Port Level Management function enabled for the port associated with this channel.
  - **Down**: The Port Level Management is currently in the "down" state.
  - **active-congested**: The Port Level Management is reporting that this channel is active and it has detected that the channel is congested.
  - **Active**: The Port Level Management is reporting that this channel is active
  - **Deleted**: The Port Level Management is reporting that this channel has been deleted. This could also result if the associated channel at the remote end is not configured
  - **not active**: No information has been received from the management port related to this channel

CLI Configuration Methods for Port Level Management

The following information can be used to configure the Port Level information associated with the FRN connections. The CLI uses the **frn** directive of the CLI interface for Port Level configuration.

List all ports available to the system

Command: frn list

The **frn list** command will display the current high level state of each port available in the system. More information about each specific port can be gained by the **show port** command described below. The following shows the output of the **frn list** command.

```
ﬁ  frn list
    ---------------------------------------------------------------------
    |Port  | Name      | VPI  | VCI  | DLCI | Activate | Mux Mode
    |port1 | main      | 0    | 100  | 100  | disable  | mux_one_to_one |
    |port2 | backup    | 10   | 110  | 110  | disable  | mux_one_to_one |
    |port3 | none      | 20   | 120  | 120  | disable  | mux_one_to_one |
    |port4 | none      | 30   | 130  | 130  | disable  | mux_one_to_one |
    |port5 | none      | 40   | 140  | 140  | disable  | mux_one_to_one |
    |port6 | none      | 50   | 150  | 150  | disable  | mux_one_to_one |
    |port7 | none      | 60   | 160  | 160  | disable  | mux_one_to_one |
    |port8 | none      | 70   | 170  | 170  | disable  | mux_one_to_one |
    ---------------------------------------------------------------------
```

Show detailed information about a specific port

Command: frn show port#

The **frn show port#** command will display detailed information about the port defined in the command. The following shows the actual output of the configuration of port 3. Note that the "frn show port" will also display information about the channels that are associated with that port.

```
ﬁ    frn show port1 command output

    Port Level Information: Port 1
    FRN Port Name:      none
    FRN VPI:            0
    FRN VCI:            100
    FRN DE Mapping:     zero
    FRN CLPI Mapping:   fr_sscs_only
    FRN Mux Mode:       mux_one_to_one
    FRN Header Type:    2_byte
    FRN DC Mapping:     zero
    FRN State:          enable
    FRN Core Name:      FRN0
    FRN Tx Packets:     146/1
    FRN Rx Packets:     145/0
    FRN Network Mgt:    lmi_both
    FRN Net Mgt State:  port_mgt_UP
```

```
Channel Level Information:
---------------------------------------------------------------------
|Chn1 |DLCI|Net DLCI|Activate| Tx Pkt G/B | Rx Pkt G/B |Status
|chn1 |100 |0       |enable  | 0/0        | 0/0        |active
|chn2 |101 |0       |disable | N/A        | N/A        |N/A
|chn3 |102 |0       |disable | N/A        | N/A        |N/A
|chn4 |103 |0       |disable | N/A        | N/A        |N/A
|chn5 |104 |0       |disable | N/A        | N/A        |N/A
|chn6 |105 |0       |disable | N/A        | N/A        |N/A
|chn7 |106 |0       |disable | N/A        | N/A        |N/A
|chn8 |107 |0       |disable | N/A        | N/A        |N/A
-------------------------------------------------------------------
```

Set configuration variables associated with the specified port

Command: frn set port# <variable> <value>

The **frn set port#** command allows the user to set port level specific variables to their optional values. All variables described above for the port level configurations are available from the **frn set port#** command screen. The following example shows the setting of port #5 MuxMode to mux_many_to_one.

Note After the first line the "?" was used to determine the possible configuration options available to the user.

Note At any point during the typing of the command selecting the "?" will display the possible options available to the user.

Note After the first several letters of the command are typed pressing the Tab key will tell the system to complete the variable or command name.

```
fi  frn set port5 MuxMode
  mux_many_to_one
  mux_one_to_one
fi  frn set port5 MuxMode mux_many_to_one
```

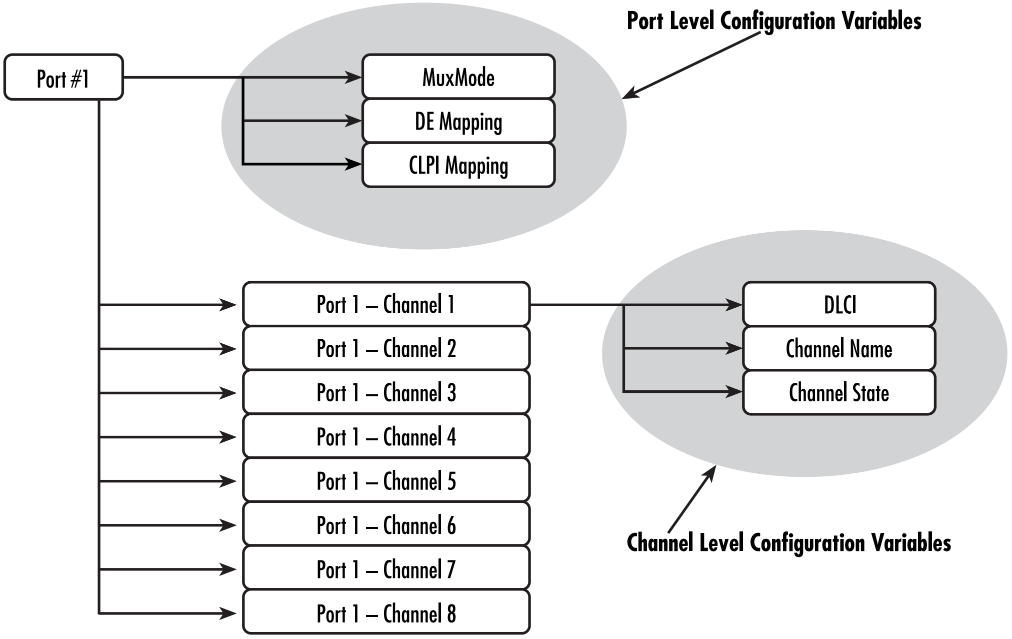
Configuration Management of the Channel Level Variables

The following information can be used to configure the Channel Level information associated with the FRN connections. The CLI uses the **frn** directive of the CLI interface for Channel Level configuration.

Note The **frn show port** and **frn list** commands already discussed at the port level are also useful to gain detailed and overview information about the channels.

Understanding the Channel Level View

The Model 3086FR supports up to 8 individual FRN ports. Each port can support up to 8 channels while set to the "many to one" multiplexing mode. To access the port level information the user must first define the port number that is being configured and then the channel number that is being configured. The following chart shows how the ports and channels are viewed by the system:



Set Configuration Variables associated with the channels
Command: frn set port# channel # <variable> <value>

The **frn set port# channel** # command allows the user to set channel level variables. Note that the port number must be specified along with the channel # as described in the above chart. The following screen capture shows the setting of the DLCI for port #5 channel #1. Note that after the channel number was input the ? key was used to request that the system displays the possible variables that the user has access to.

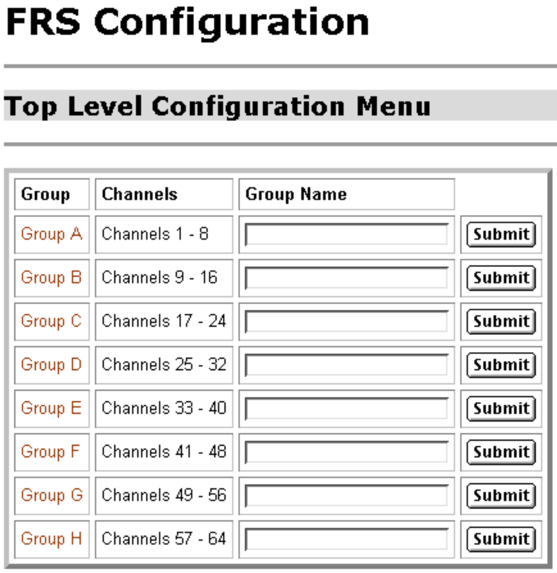
```
ﬁ frn set port5 channel 1
  ChannelName
  DLCI
  state
ﬁ frn set port5 channel 1 DLCI 180
```

Frame Relay Service Interworking (FRF.8)

FRF.8 is a conversion mechanism by which Frame Relay networks can communicate directly with ATM-based networks. Neither the ATM nor the Frame Relay networks require any understanding of the other network protocols involved. This conversion is performed within the Model 3086FR's IWF at the transport service level. Frame Relay Service Interworking functions are defined by the Frame Relay Forum specification *Frame Relay/ATM PVC Service Interworking Implementation Agreement FRF.8.1*.

FRS Configuration Options

The Model 3086FR supports 64 FRF.8 connections (divided into 8 groups of 8 channels each). The IWF are configured by group and channel. The group level configuration options are applied to eight channels that are related to that group. The following list of variables are configured at the group level.



FRS Configuration

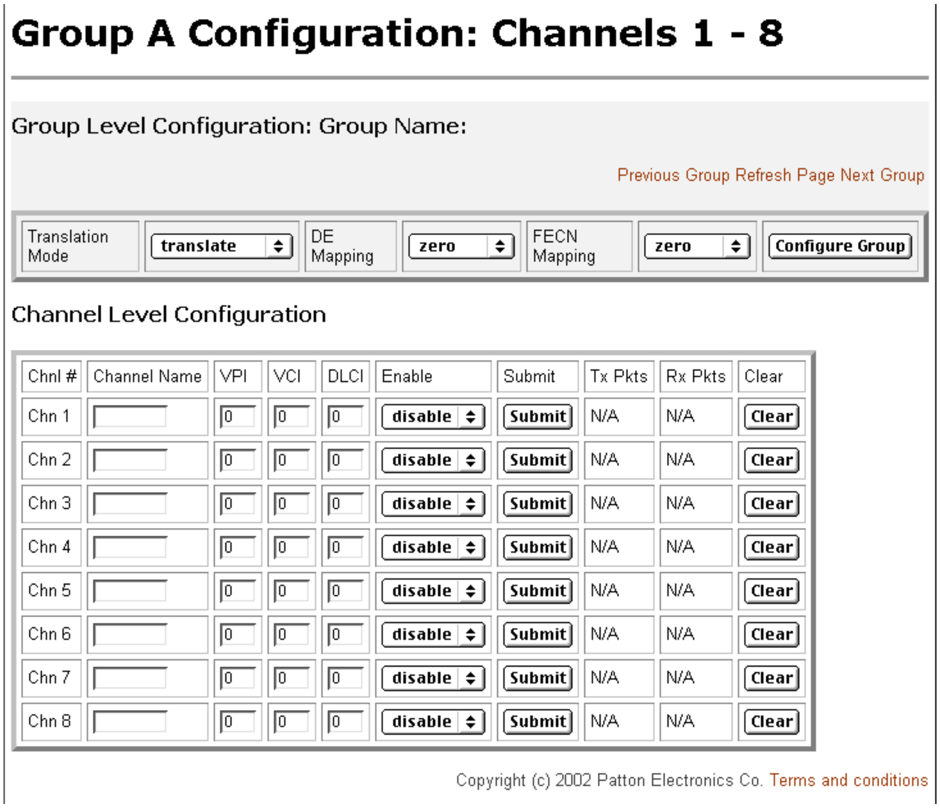
Top Level Configuration Menu

Group	Channels	Group Name	
Group A	Channels 1 - 8		Submit
Group B	Channels 9 - 16		Submit
Group C	Channels 17 - 24		Submit
Group D	Channels 25 - 32		Submit
Group E	Channels 33 - 40		Submit
Group F	Channels 41 - 48		Submit
Group G	Channels 49 - 56		Submit
Group H	Channels 57 - 64		Submit

Figure 22. FRS Configuration—Top Level Configuration Menu

Once *FRS Setup (FRF.8)* is selected (see figure 18 on page 59), the FRS Configuration—Top Level Configuration screen is displayed (see figure 22). The screen gives an overview of the FRS connections that are available.

Each *Group* in the left column is a hyperlink that will display the Group *X* Configuration window (where *x* is the group selected) (see figure 23).



Group A Configuration: Channels 1 - 8

Group Level Configuration: Group Name:

Previous Group Refresh Page Next Group

Translation Mode	translate	DE Mapping	zero	FECN Mapping	zero	Configure Group

Channel Level Configuration

Chnl #	Channel Name	VPI	VCI	DLCI	Enable	Submit	Tx Pkts	Rx Pkts	Clear
Chn 1		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 2		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 3		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 4		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 5		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 6		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 7		0	0	0	disable	Submit	N/A	N/A	Clear
Chn 8		0	0	0	disable	Submit	N/A	N/A	Clear

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

Figure 23. Groups X Configuration: Channels 1 – 8

Translation Mode

The Translation Mode variable defines the encapsulation mechanism that will be required to convert the ATM cells (encapsulated per RFC2684) to the Frame Relay packets (encapsulated per RFC1490) and back. This is required because ATM and Frame Relay encapsulate packets in different formats as defined by their respective RFC. There are two options available for the Translation Mode setting within the Model 3086FR as defined below:

- **Translate:** When the connection channel is set to translate, the IWF converts between Frame Relay encapsulated frame and the ATM encapsulated cells. This conversion is performed by inspecting each frame/cell and determining the PID (Protocol Identification) field within the packet. (Using this information, the frame/cell is routed through an encapsulation conversion utility that creates the encapsulation required for the destination network.) The Model 3086FR supports all 22 protocol types as defined by the FRF.8.1

specification. See figure 24 for the encapsulation types and includes an example where a Routed IP packet is received on both the Frame Relay and ATM sides of the connection. When the packet is received is checked against the known PID fields, and then the packet is routed to the appropriate encapsulation conversion station before being sent out the opposite interface.

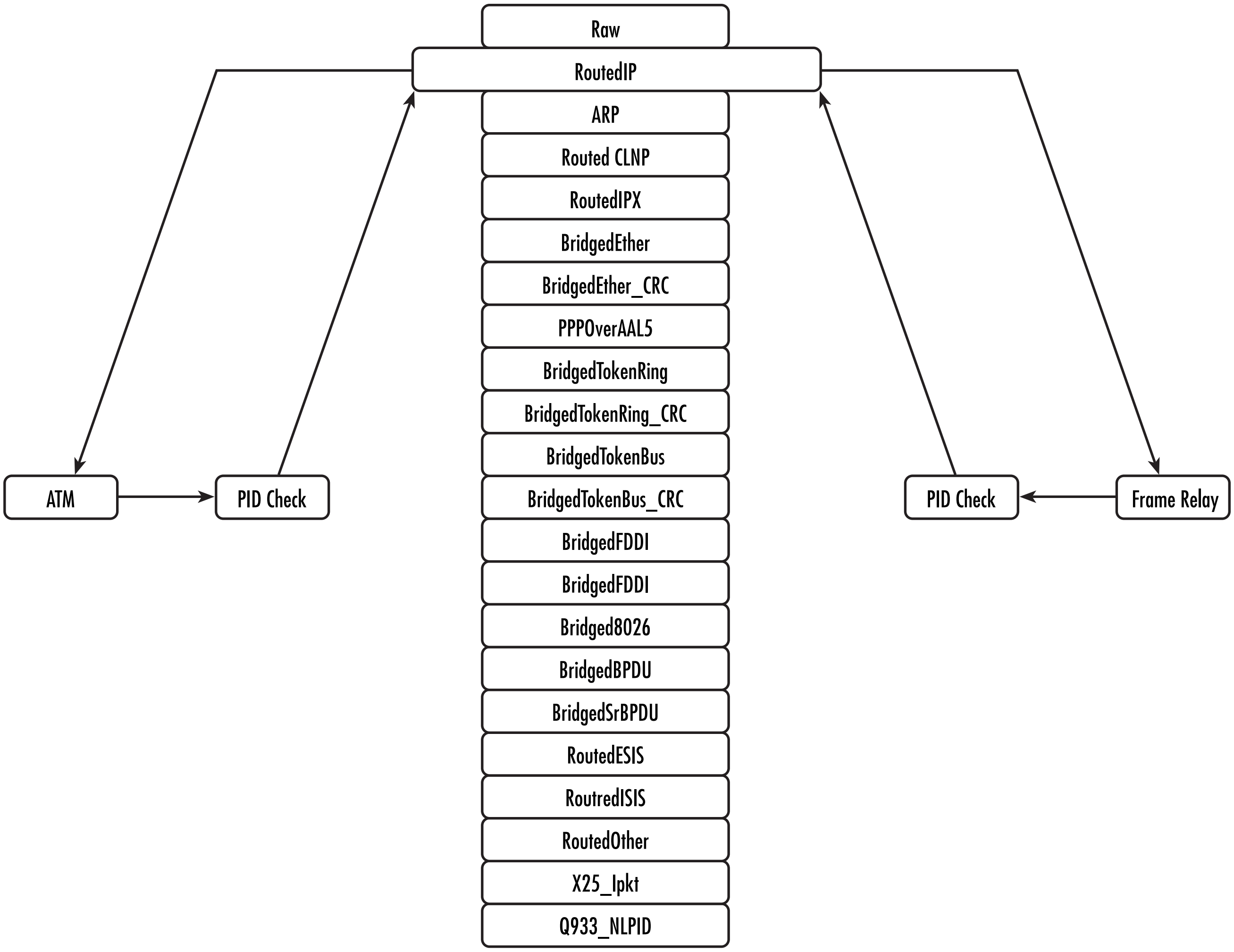


Figure 24. FRS encapsulation conversion using Translate Mode

- **Transparent**: The second translation mode option is to set the protocol value to transparent. Transparent is used when the Protocol being used is not one of the 22 predefined encapsulation types, such as is the case for voice based systems. When the translation mode is set to transparent, the packet data will be transparently passed from one network to the other without any encapsulation conversions.

DE Mapping

The DE Mapping variable is used to determine how the Frame Relay DE field (Discard Eligi-bility) will be mapped to the ATM CLPI (Cell Loss Priority Indication) and vise versa. The following options are available:

- **Always_zero**:
  - **Frame Relay**: All Frame Relay packets will have the DE field in the header set to a constant value of 0.
  - **ATM**: All ATM cells will have the CLPI field set to a constant value of 0.
- **Always_one**:
  - **Frame Relay**: All Frame Relay packets will have the DE field in the header set to a constant value of 1.
  - **ATM**: All ATM cells will have the CLPI field set to a constant value of 1.
- **Convert**:
  - **Frame Relay to ATM Direction**: The system will convert the DE field received from the Frame Relay packet into the CLPI field of the outgoing ATM cell.
  - **ATM to Frame Relay Direction**: The system will convert the CLPI bit received from the ATM cells into the DE field of the outgoing Frame Relay packet.

FECN Mapping

The FECN Mapping variable is used to determine how the Frame Relay FECN (Forward Explicit Congestion Notification) bit will be mapped to the ATM EFCI (Explicit Forward Congestion Indica-tion) bit and vise versa. The following options are available:

- **Always_zero**:
  - **Frame Relay**: All Frame Relay packets will have the FECN bit in the header set to a constant value of 0.
  - **ATM**: All ATM cells will have the EFCI bit set to a constant value of 0.
- **Always_one**:
  - **Frame Relay**: All Frame Relay packets will have the FECN bit in the header set to a constant value of 1.
  - **ATM**: All ATM cells will have the EFCI bit set to a constant value of 1.
- **Convert**:
  - **Frame Relay to ATM Direction**: The system will convert the FECN bit received from the Frame Relay packet into the EFCI bit of the outgoing ATM cell.
  - **ATM to Frame Relay Direction**: The system will convert the EFCI bit received from the ATM cells into the FECN bit of the outgoing Frame Relay packet.

FRS Name

Allows the user to name the FRS channel. This is helpful when viewing multiple connections to determine which DLCI/VPI/VCI combination is associated with each channel.

- **FRS state**: The state variable allows the user to enable or disable the channel for operation.

  The Frame Relay Service Interworking functions on the Patton Electronics Model 3086FR are also defined as sixty-four channels. Each channel creates a connection between a single DLCI on the Frame Relay network and a VPI/VCI on the ATM network. The following configuration options are available for each channel in the system.

- **VPI**—Virtual Path Identifier: ATM side Virtual Path Identifier for the specified connection.
- **VCI**—Virtual Channel Identifier: ATM side Virtual Channel Identifier for the specified connection
- **DLCI**—Data Link Connection Identifier: Frame Relay side DLCI for the specified connection

CLI Configuration Method

The following section describes how to configure FRS channel connections using the CLI interface.

The system is made up of eight groups and 64 channels. The group configuration variables apply to all eight channels within that group. Each channel is configured independently and will all run over as single LMI session or with no LMI running. The FRS (FRF.8) connections are configured using the "frs" directive in the CLI interface. The following commands are available:

Show one of the eight groups

Command: frs show group #

The **frs show group** # command shows the configuration of te group defined by the # directive. Possible options are 1–8. The following shows an example setup:

```
ﬁ frs show group 1
     Group Level Information: Group A
  Group Name:
  Group DE Mapping:   zero
  Group Trans Mode:   translate
  Group FECN Mapping: zero

  Channel Level Information: Channels 1 - 8
  --------------------------------------------------------------------
  |Chn  |VPI |VCI |DLCI| Activate | Tx Pkt G/B          | Rx Pkt G/B
  |chn1 |100 |200 |172 |enable    |0/0                  |0/0
  |chn2 |1   |101 |101 |disable   |N/A                  |N/A
  |chn3 |2   |102 |102 |disable   |N/A                  |N/A
  |chn4 |3   |103 |103 |disable   |N/A                  |N/A
  |chn5 |4   |104 |104 |disable   |N/A                  |N/A
  |chn6 |5   |105 |105 |disable   |N/A                  |N/A
  |chn7 |6   |106 |106 |disable   |N/A                  |N/A
  |chn8 |7   |107 |107 |disable   |N/A                  |N/A
```

Set variable attributes on a specified group

Command: frs set group # <variable> <value>

Note At any point during the typing of the command selecting the "?" will display the possible options available to the user.

Note After the first several letters of the command are typed pressing the Tab key will tell the system to complete the variable or command name.

The **frs set group** command allows the user to setup the configuration of the group variables. The following example could be used to set the DEMapping variable to “convert”.

Note At the end of the first line the **?** was selected and the system prompted the user with the possible options available.

```
fi  frs set group 1 DEMapping ?
   convert
   one
   zero
fi  frs set chn1 DEMapping convert
```

Set variable attributes on a specified channel

Command: frs set channel # <variable> <value>

The following example could be used to set the DLCI variable to 171.

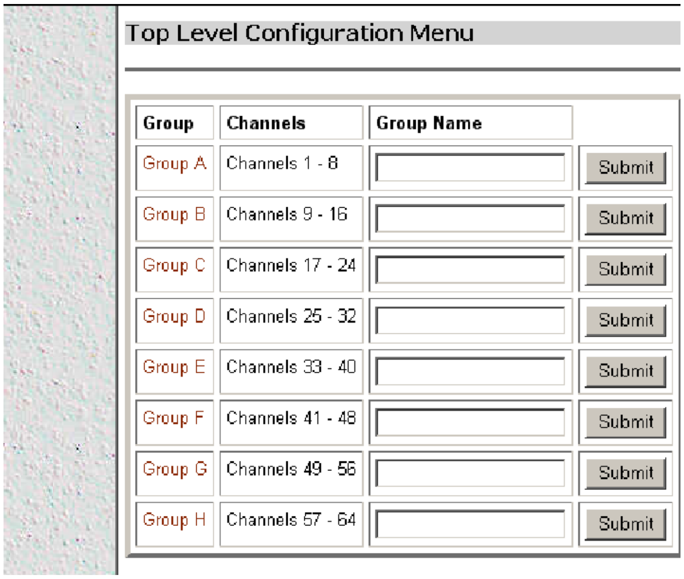
```
fi  frs set channel 1 DLCI 171
```

Web Configuration Methods

The following documentation defines how to configure the FRS channel connections using the web interface on the Model 3086FR. All web interface screens our found under the IWF link.

FRS Overview Screen

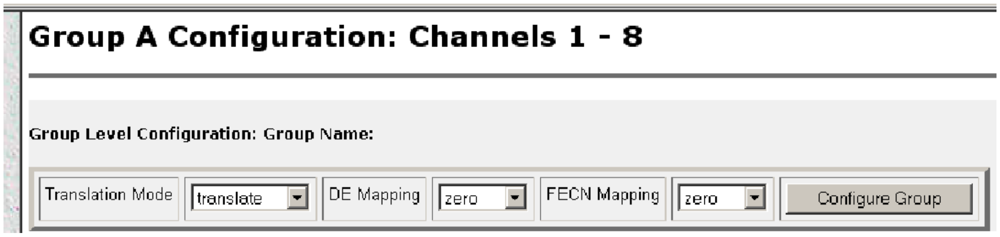
By selecting the “FRS Setup (FRF.8)” link below the IWF heading will bring up an overview of the FRS connection available within the system. This page shows a top level view of the eight groups available. The “Group #” column along the left side of the screen is a hyperlink that will bring up detailed configuration information about each group and the channels available in the group.



Top Level Configuration Menu

Group	Channels	Group Name	
Group A	Channels 1 - 8		Submit
Group B	Channels 9 - 16		Submit
Group C	Channels 17 - 24		Submit
Group D	Channels 25 - 32		Submit
Group E	Channels 33 - 40		Submit
Group F	Channels 41 - 48		Submit
Group G	Channels 49 - 56		Submit
Group H	Channels 57 - 64		Submit

Figure 25. Top Level Configuration Menu



Group A Configuration: Channels 1 - 8

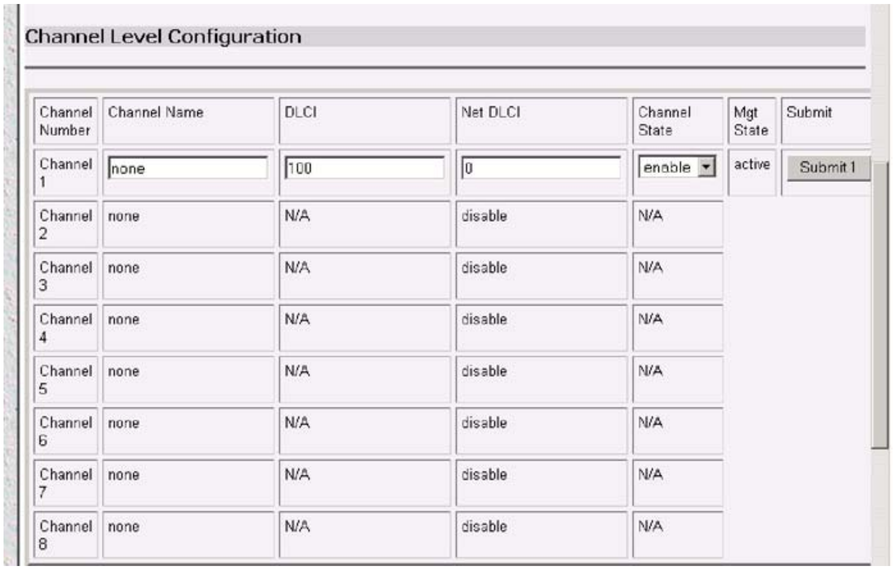
Group Level Configuration: Group Name:

Translation Mode	translate	DE Mapping	zero	FECN Mapping	zero	Configure Group

Figure 26. FRF.8 Group Level Configuration window

Group/Channel Level Configuration Screen

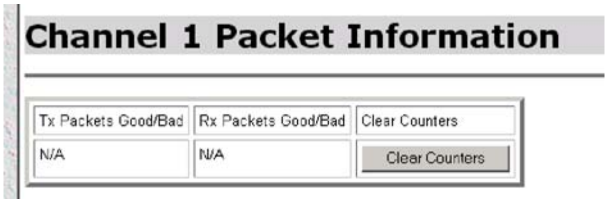
By selecting the "Group #" link in the FRS Overview screen, the detailed channel level information screen is displayed as shown below. This screen allows configuration of all variables associated with the group and channels. The screen is broken down into three sections; the first section allows configuration of the group level information, the second section allows configuration of the channels associated with the group, the last screen shows the packet counters.



Channel Level Configuration

Channel Number	Channel Name	DLCI	Net DLCI	Channel State	Mgt State	Submit
Channel 1	none	100	0	enable	active	Submit 1
Channel 2	none	N/A	disable	N/A		
Channel 3	none	N/A	disable	N/A		
Channel 4	none	N/A	disable	N/A		
Channel 5	none	N/A	disable	N/A		
Channel 6	none	N/A	disable	N/A		
Channel 7	none	N/A	disable	N/A		
Channel 8	none	N/A	disable	N/A		

Figure 27. FRF.8 Channel Level Configuration Screen



Channel 1 Packet Information

Tx Packets Good/Bad	Rx Packets Good/Bad	Clear Counters
N/A	N/A	Clear Counters

Figure 28. FRF.8 Channel Level Packet Information

Frame Relay (Ethernet-based) operations

Ethernet-based (or basic) Frame Relay is also available within the Model 3086FR. This Frame Relay service can be used in a similar fashion to other Ethernet-based transports within the system such as PPP or the Ethernet transport. Multiple Frame Relay transports, with different DLCI numbers, can be built upon the HDLC controller that is available with the 3086FR. The Frame Relay Interface is available at the serial interface for transport out of the Ethernet Interface or the ATM link.

Frame Relay Configuration Options

The Frame Relay transport is configurable from both the CLI and the web interface. The following configurable variables are available through both interfaces.

Channel Segment Size

The channel segment size is used to define fragmentation of the packets based on the Frame Relay Forum IA FRF.12. If this variable is set to 0 then FRF.12 "Frame Relay Fragmentation" will be disabled. If set to any other value it will set the fragmentation size used.

DLCI: Data Link Connection Identifier

The Frame Relay DLCI used for the specified channel. Must be set to a non-zero number as agreed upon by the Frame Relay connection.

Encapsulation Type

Defines the FRC1490 encapsulation type that will be used by the channel.

Port

Defines the port that should be used to setup the Frame Relay Connection. For routed applications the port should be set to "frf". For bridged applications the port should be set to "fr".

Rxmaxpdu

Receive side max PDU

Txmaxpdu

Transmit side max PDU

Frame Relay CLI Configuration Options

The following information describes how to configure the frame relay transport on the 3086FR through the CLI interface.

Build a new Frame Relay Transport

Command: framerelay add transport <name> <port> <dlci>

Add a new frame relay transport to the system

- **Name**: Any name can be given to the transport. This name will be used to reference the transport in later commands.
- **Port**: This variable defines the low layer port that will be used to transport data across the frame relay inter-face. For routed application the "frf" port should be used. For bridged applications the "fr" port should be used.

- **DLCI**: This variable can be set to any positive value less than 8196

Clear all Frame Relay Transports

Command: framerelay clear transport

This command can be used to clear all of the transports in the system

Delete the specified transport

Command: framerelay delete transport <name | number>

Delete a single frame relay connection using either the connection name or number

- **name:** the name used when creating the transport
- **number**: the ID number found when listing the transports

List all active Frame Relay Channels

Command: framerelay list transports

List all transports currently defined in the system

Set configuration variables for the specified frame relay transport

Command: framerelay set transport <name | number> <variable> <value>

Set a value for a specific frame relay variable

1. **name | number**: specify the connection that you would like to change
2. **variable**: any variable from the above list
3. **value**: value that you would like to set

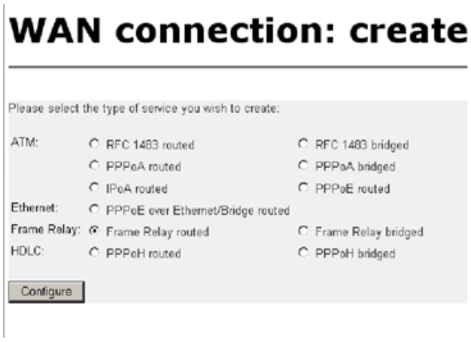
Show detailed configuration information on the specified channel

Command: framerelay show transport <name | number>

Display specific information about the frame relay connection

Web Based Configuration of the Frame Relay Channel

This section defines the configuration of the Frame Relay Service through the web interface. The Frame Relay channel is created through the Configuration->WAN link.



WAN connection: create

Please select the type of service you wish to create:

ATM:	○ RFC 1483 routed	○ RFC 1483 bridged
	○ PPPoA routed	○ PPPoA bridged
	○ IPoA routed	○ PPPoE routed
Ethernet:	○ PPPoE over Ethernet/Bridge routed	
Frame Relay:	● Frame Relay routed	○ Frame Relay bridged
HDLC:	○ PPPoH routed	○ PPPoH bridged

Chapter 7 Local Management Interface

Chapter contents

Introduction

The Frame Relay Local Management Interface (LMI) is a mechanism that enables two separate frame relay systems to communicate the status of the interface. The LMI interface supports dynamic updates on the status of the DLCI connections and the congestion state of the network. The Model 3086FR fully supports the LMI versions listed in table 4.

Table 4. LMI Implementation on the 3086FR

Protocol	Specification	Options Available
LMI	Frame Relay Forum Implementation Agreement (IA) FRF.1 superceded by FRF.1.1	• Network side • User side • Both
Annex D	ANSI T1.617	• Network side • User side • Both
Annex A	ITU Q.933 referenced in FRF.1.1	• Network side • User side • Both
Cisco	Cisco implementation of LMI	• Network • User side • Both

LMI Configuration Options

LMI is configurable via the CLI or web interface.

Note Although the Model 3086FR supports LMI implementations for *network*, *user*, and *both*, configuration options are limited to *network* for FRF.8 applications, and *both* for FRF.5 applications.

managementType: (Default Value: no_maintenance)

the managementType variable defines the LMI protocol that will be used. The following options are available.

- **no_maintenance:** No maintenance interface will be used for this frame relay connection.
- **ITU_Network:** The ITU Q.933 protocol will be used. The unit will operate as the Network side of the connection
- **ITU_User:** The ITU Q.933 protocol will be used. The unit will operate as the User side of the connection
- **ITU_Both:** The ITU Q.933 protocol will be used. The unit will operate as both the Network and User side of the connection.
- **ANSI_Network:** The ANSI T1.617 protocol will be used. The unit will operate as the Network side of the connection
- **ANSI_User:** The ANSI T1.617 protocol will be used. The unit will operate as the User side of the connection

- **ANSI_Both:** The ANSI T1.617 protocol will be used. The unit will operate as both the Network and User side of the connection.
- **Cisco_Network:** The Cisco LMI implementation will be used. The unit will operate as the Network side of the connection.
- **Cisco_User:** The Cisco LMI implementation will be used. The unit will operate as the User side of the connection
- **Cisco_Both:** The Cisco LMI implementation will be used. The unit will operate as both the Network and User side of the connection.

MgtState. Defines the current state of the DTE side LMI. Possible options are as follows:

- **Mgt_Port_DOWN:** Currently the LMI on the DTE side is DOWN
- **Mgt_Port_UP**: Currently the LMI on the DTE side is UP

mgtAutoStart: (Default Value: FALSE)

The management *Auto Start* variable allows the user to start the LMI session before any DLCI connections are created within the unit. If this variable is set to *FALSE*, the LMI session will begin when the first DLCI channel is created. If this variable is set to *TRUE* the LMI session will begin immediately.

T391_Value: (Default Value: 10)

This variable sets the T391 timers in seconds.

T392_Value: (Default Value: 16)

This variable sets the T392 timers in seconds.

fullReportCycle: (Default Value: 6)

This variable represents the N391 protocol value

netErrorWindowSize: (Default Value: 4)

Network side N393 protocol value

netMaxErrors: (Default Value: 3)

Network side N392 protocol value

userErrorWindowSize: (Default Value: 4)

User side N393 protocol value

userMaxErrors: (Default Value: 3)

Network side N392 protocol value

CLI Configuration Methods

The following describes how to configure the LMI using the CLI. All LMI commands are contained under the “lmi” directive of the CLI interface. The following options are available:

Show current configuration

Command: “lmi show”

```
ﬁ  lmi show
              FR_Mgt Type : no_maintenance
             FR_Mgt State : Mgt_Port_DOWN
        Full Report Cycle : 6
          User Max Errors : 3
           Net Max Errors : 3
   User Error Window Size : 4
    Net Error Window Size : 4
               T391_Value : 10
               T392_Value : 16
           Mgt Auto Start : false
```

Set configuration variable

Command: “lmi set <variable> <value>”

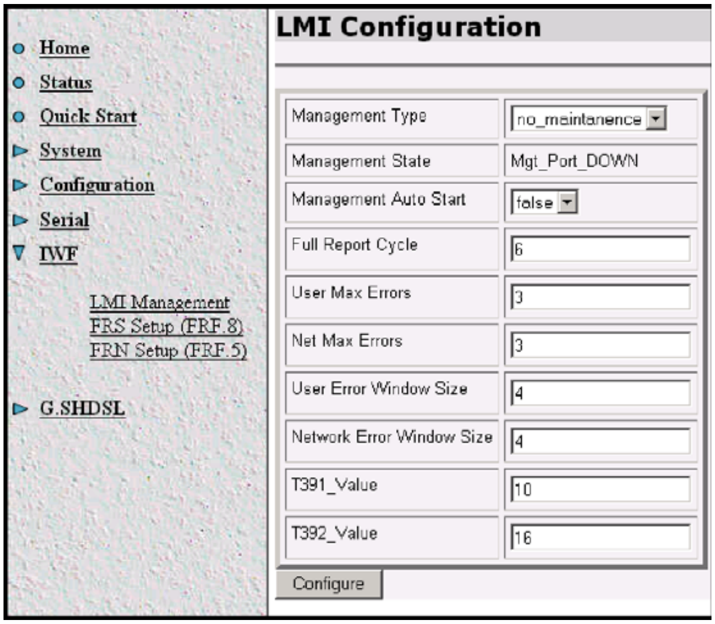
Variable: Any variable from the above list

Value: Value as defined by the variable

```
ﬁ  lmi set managementType 933A_Network
```

Web Configuration Methods

The following describes how to configure the LMI using the web interface. All LMI configuration variables are contained under the "LMI Management" window found through the IWF link. The following image shows the configuration variables available.



LMI Configuration

Management Type	no_maintanence
Management State	Mgt_Port_DOWN
Management Auto Start	false
Full Report Cycle	6
User Max Errors	3
Net Max Errors	3
User Error Window Size	4
Network Error Window Size	4
T391_Value	10
T392_Value	16

Chapter 8 3086FR routed and bridged ATM connections

Chapter contents

Introduction

In addition to FR to ATM conversion and transport over DSL, the 3086FR is a full feature ATM router, allowing routed or bridged services between the DSL interface and the 10/100Base-T. The Model 3086FR can simultaneously transport traffic from the serial port and the 10/100Base-T Ethernet port over a single-pair DSL link. In this case, the 3086FR operates in split-mode DSL bandwidth allocating dedicated timeslots in the DSL frame for the serial port, and for the Ethernet traffic.

When routing or bridging data from the 10/100Base-T port, keep in mind that data from the 3086FR serial port is converted from Frame Relay to ATM encapsulation only, this traffic does not go thru the router or bridge core in the 3086FR. When enabling the router or bridge for traffic from the 10/100Base-T, a separate PVC and dedicated DSL timeslots have to be configured for this traffic.

The main configuration steps for this scenario are as follows:

1. Configure the DSL interface. Assign DSL bandwidth to the serial port, and the remaining DSL bandwidth will be assigned to 10/100Base-T port. For instance, if you select a DSL rate of 512 kbps and 256 kbps are assigned to the serial port, the remaining 256 kbps of DSL bandwidth will be automatically assigned to 10/100Base-T traffic.
2. Configure the serial port. Assign the DSL bandwidth required for the traffic on this port.
3. Configure the FR to ATM features for the serial port.
4. Configure the LMI

If you are using the 10/100Base-T port to route or bridge data:

1. Create a bridged or routed ATM connection.
2. Configure the bridge or router, and ATM parameters (including a PVC)
3. Configure DHCP, NAT, Authentication, Security features, etc, if needed, for this routed or bridged connection.

The following ATM routed and bridged connections are available with the 3086FR:

- RFC 1483 bridged
- PPPoA (PPP over ATM) bridged
- RFC 1483 routed
- IPoA (IP over ATM) routed
- PPPoA (PPP over ATM) routed

DSLAM Connections with remote CPE units

Bridged application configurations to a DSLAM

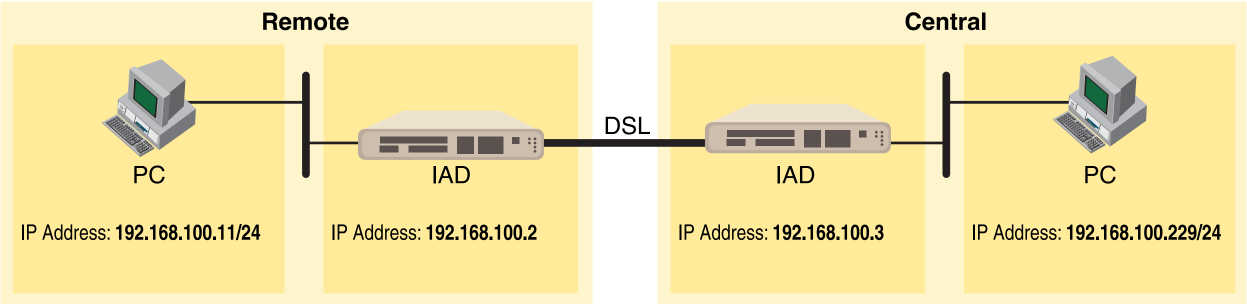
Two bridged services are offered, *RFC 1483 Bridged* and *PPPoA Bridged*.

The configurations show a desktop on one end and a laptop on the other. The laptop and its Model 3086FR would be replaced with a DSLAM.

RFC 1483 Bridged Configuration.

No additional IP addresses are needed other than the IP address chosen earlier. In fact, if you are configuring and managing the model 3086FR only from the CLI (Command Line Interface), an IP address is not needed at all. The limitation of no IP address precludes the user from doing web management of the 3086FR since management is done via the Ethernet port.

As in the PPPoA Bridged application, both sides of the RFC 1483 bridged connection are on the same subnet.


Remote
Central
PC
IAD
DSL
IAD
PC
IP Address: 192.168.100.11/24
IP Address: 192.168.100.2
IP Address: 192.168.100.3
IP Address: 192.168.100.229/24

Model 3086FR (Remote) Configuration Steps (RFC 1483 Bridged)

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

One IP interface is called ip1 with an IP address of 192.168.1.1

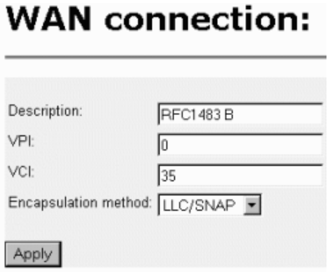
Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2

```
fi ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

   Click on **Create a new service** in the main window, select **RFC_1483_Bridged** and click on the **Configure** button.



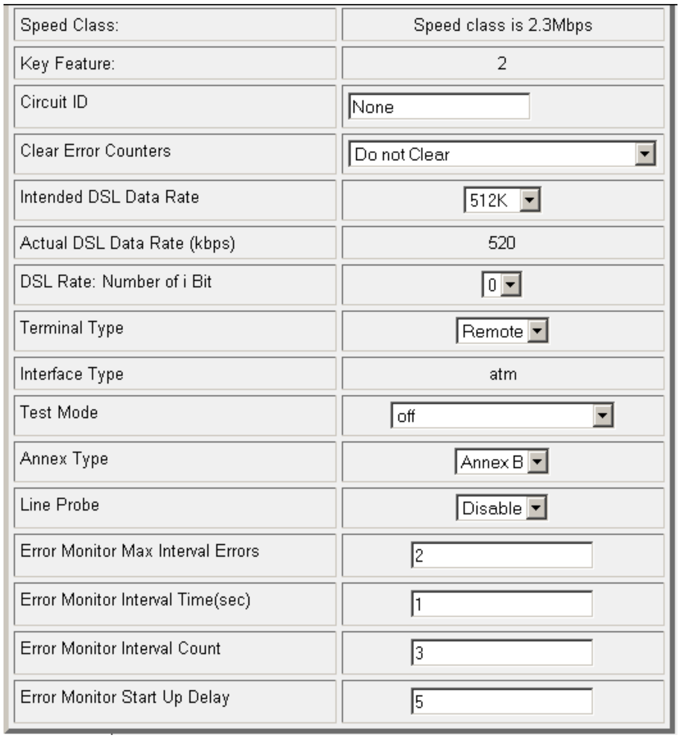
WAN connection:

Description: RFC1483 B
VPI: 0
VCI: 35
Encapsulation method: LLC/SNAP

   In the Description field, enter the description you wish. In this example, it is called *RFC 1483 B*.

   Leave VCI as 35 and Encapsulation Method as LLC/SNAP. Then click on **Apply**.

3. Go to **G.SHDSL** in the Configuration Menu, then the submenu **Configuration**.



Speed Class:	Speed class is 2.3Mbps
Key Feature:	2
Circuit ID	None
Clear Error Counters	Do not Clear
Intended DSL Data Rate	512K
Actual DSL Data Rate (kbps)	520
DSL Rate: Number of i Bit	0
Terminal Type	Remote
Interface Type	atm
Test Mode	off
Annex Type	Annex B
Line Probe	Disable
Error Monitor Max Interval Errors	2
Error Monitor Interval Time(sec)	1
Error Monitor Interval Count	3
Error Monitor Start Up Delay	5

Change Terminal Type to *Remote* and Interface Type to *atm*. Click on the **Configure** button.

In the Action submenu under G.SHDSL, change Action to **Deactivate**, then click on Action.

Return to Action, select **Start** and click on **Action**.

Model 3086FR (Central) Configuration Steps (RFC 1483 Bridged)

Although the some parametric values may vary from the desktop's Model 3086FR, the process is identical.

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

One IP interface is called ip1 with an IP address of 192.168.1.1

Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.3

```
fi ip set interface ip1 ipaddress 192.168.100.3 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.
2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

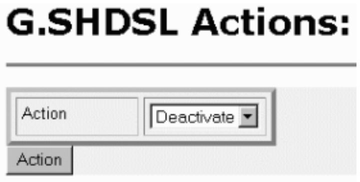
   Click on **Create a new service** in the main window, select **RFC_1483_Bridged** and click on the **Configure** button.

   In the Description field, enter the description you wish. In this example, it is called *RFC 1483 B*.

   Leave VCI as 35 and Encapsulation Method as LLC/SNAP. Then click on **Apply**.

3. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

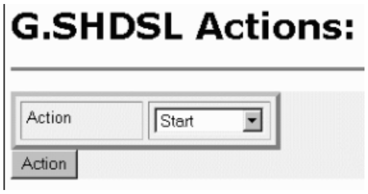
   Leave Terminal Type as *Remote*, but change Interface Type to *atm*. Click on the **Configure** button.



G.SHDSL Actions:

Action: Deactivate

In the Action submenu under G.SHDSL, change Action to **Deactivate**, then click on **Action**.



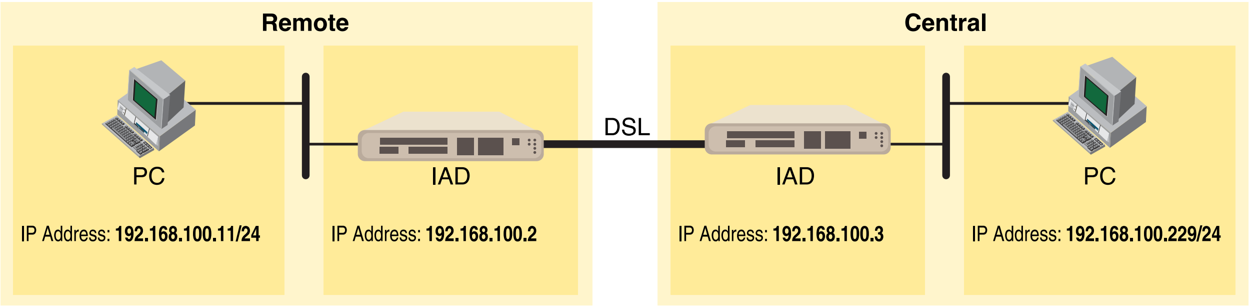
G.SHDSL Actions:

Action: Start

Return to Action, select **Start** and click on **Action**.

PPPoA Bridged (RFC 2364) Configuration

The user data for transmission is in the form of IP packets but encapsulated in a PPP packet, transmitted and received through a PPP session to the connection. The PPP packets are encapsulated according to RFC 2364 for transmission over the ATM link. The packets are de-encapsulated on the receive side so that the IP data can be delivered to the end user.


Remote
Central
PC
IAD
DSL
IAD
PC
IP Address: 192.168.100.11/24
IP Address: 192.168.100.2
IP Address: 192.168.100.3
IP Address: 192.168.100.229/24

Model 3086FR (Remote) Configuration Steps (PPPoA Bridged)

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

One IP interface is called ip1 with an IP address of 192.168.1.1

Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2

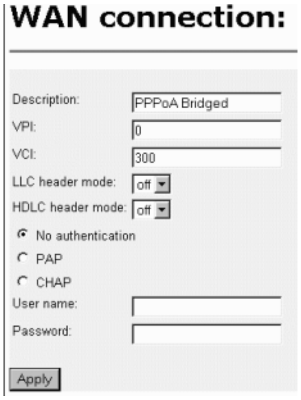
```
fi ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

   Click on **Create a new service** in the main window, select **PPPoA_Bridged** and click on the **Configure** button.

   In the Description field, enter the description you wish. In this example, it is called *PPPoA Bridged*.



WAN connection:

Description: PPPoA Bridged
VPI: 0
VCI: 300
LLC header mode: off
HDLC header mode: off
● No authentication
○ PAP
○ CHAP
User name:
Password:

   – VPI = 0

   – VCI = 300

   – LLC header mode = off

   – HDLC header mode = off

   – No authentication

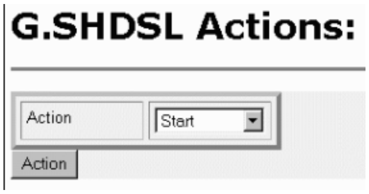
   – Leave User name and Password blank.

   Click on **Apply**.

3. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

   Change Terminal Type to *Remote* and Interface Type to *atm*. Click on the **Configure** button.

   In the Action submenu under G.SHDSL, change Action to **Deactivate**, then click on **Action**.



G.SHDSL Actions:

Action: Start

   Return to Action, select **Start** and click on **Action**.

Model 3086FR (Central)Configuration Steps (PPPoA Bridged)

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

One IP interface is called ip1 with an IP address of 192.168.1.1

Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.3

```
fi ip set interface ip1 ipaddress 192.168.100.3 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.
2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

   Click on **Create a new service** in the main window, select **PPPoA_Bridged** and click on the **Configure** button.

   In the Description field, enter the description you wish. In this example, it is called *PPPoA Bridged*.

   – VPI = 0

   – VCI = 300

   – LLC header mode = off

   – HDLC header mode = off

   – No authentication

   – Leave User name and Password blank.

   Click on **Apply**.
3. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

   Leave Terminal Type as *Central*.

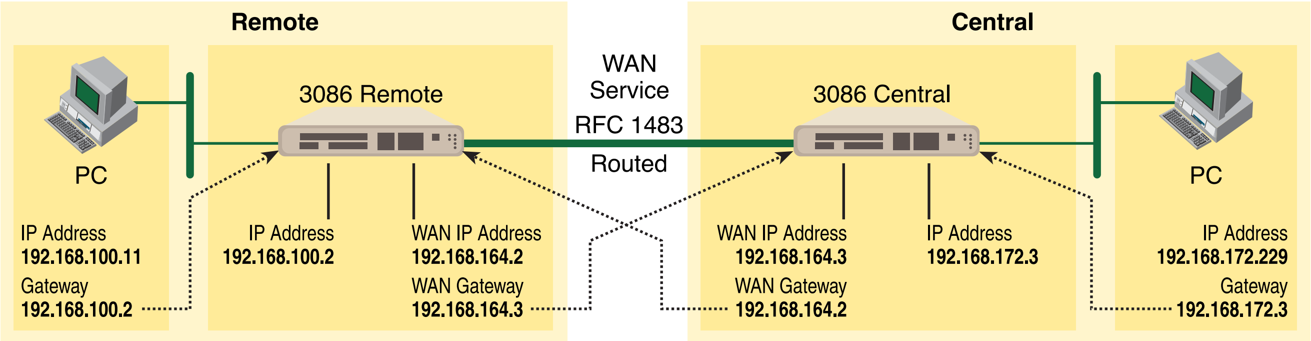
   Change Interface Type to *atm*. Click on the **Configure** button.

   In the Action submenu under G.SHDSL, change Action to Deactivate, then click on **Action**.

   Return to Action, select **Start** and click on **Action**.

Routed application configurations to a DSLAM

Five **routed** WAN services are offered, *RFC 1483, IPoA,* and *PPPoA*.



RFC 1483 Routed

RFC 1483 provides the simplest method of connecting end stations over an ATM network. User data in the form of Ethernet packets is encapsulated into AAL-5 PDUs for transport over ATM. RFC 1483 provides no authentication and configuration that would be provided by PPP.

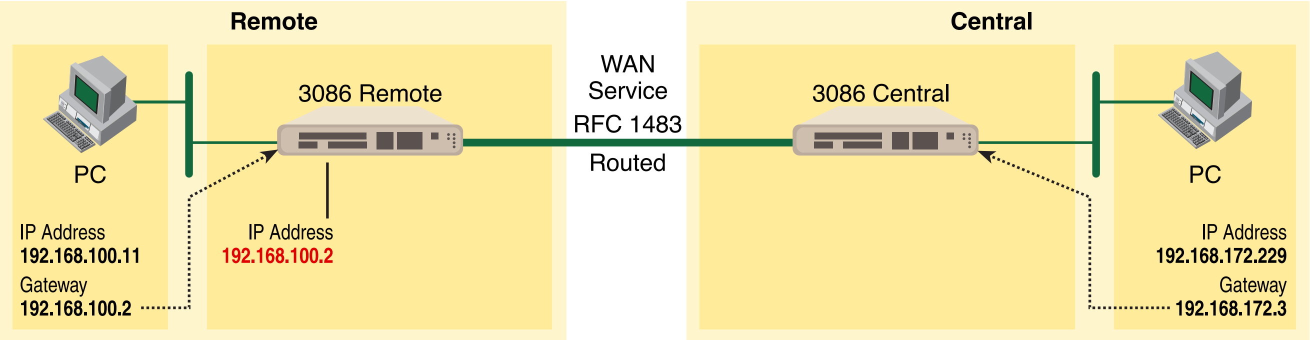
Model 3086FR (Remote) Configuration Steps (RFC 1483 Routed)

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

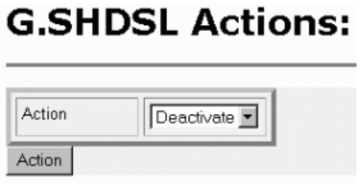
One IP interface was called ip1 with an IP address of 192.168.1.1 Change it to an IP address which is in the same subnet as the Desktop PC. For example, to 192.168.100.2.   The default IP mask is 255.255.255.0.

```
fi ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```



1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

   Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Central* and Interface Type is *atm*. If changed, then click on **Configure**.

   G.SHDSL Actions:

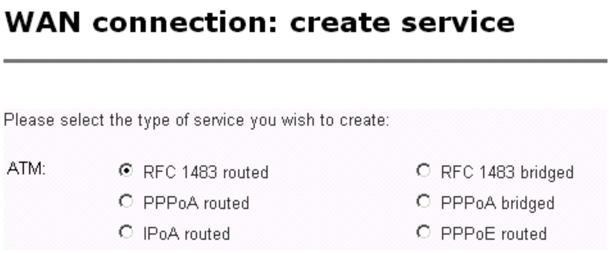
   Action: Deactivate

   Click on Action > Select deactivate for Action > Click on the Action button.

2. On the Menu, go to Configuration, then to WAN Connections.

   Delete both default WAN services already defined.

   Click on **Create a new service** in the main window, select **RFC 1483 Routed** and click on the **Configure** button.

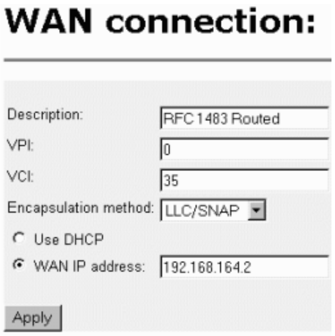


WAN connection: create service

Please select the type of service you wish to create:

ATM: ● RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ PPPoA bridged
○ IPoA routed ○ PPPoE routed

In the Description field, enter the description you wish. In this example, it is called *RFC 1483 Routed*. Change the configuration parameters to match the following.



WAN connection:

Description: RFC 1483 Routed
VPI: 0
VCI: 35
Encapsulation method: LLC/SNAP
○ Use DHCP
● WAN IP address: 192.168.164.2

Description:RFC 1483 Routed

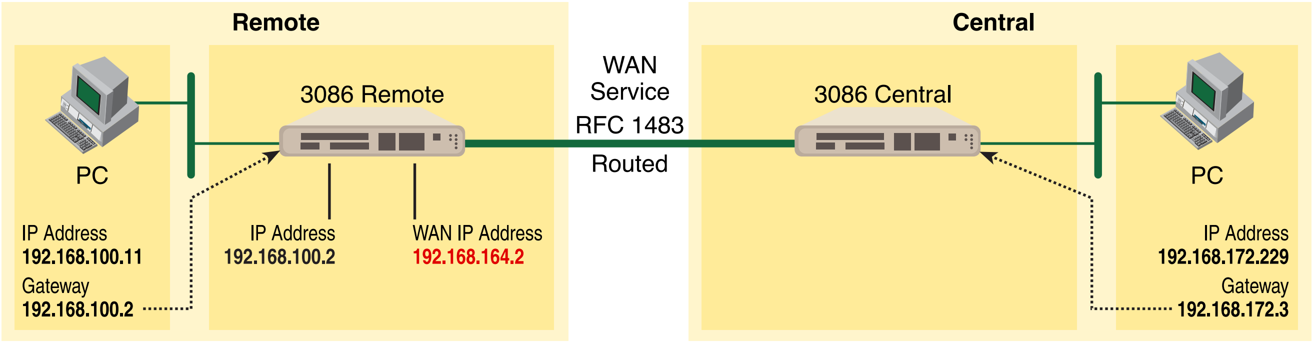
– VPI:0

– VCI:35

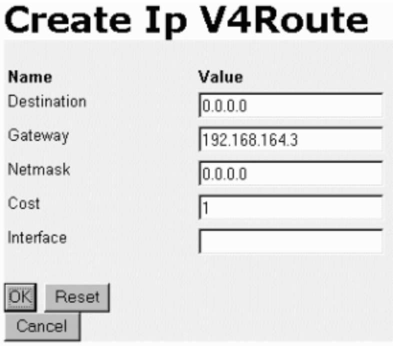
– Encapsulation Method: LLC/SNAP

– WAN IP Address:192.168.164.2

Click on **Configure**.



3. Configuration Menu > Configuration > IP Routes > Click on Create new Ip V4 Route > Create the gateway to the remote 3086FR by entering the WAN IP address of the remote 3086FR, in this example, enter 192.168.164.3 in the Gateway field > OK



Create Ip V4Route

Name	Value
Destination	0.0.0.0
Gateway	192.168.164.3
Netmask	0.0.0.0
Cost	1
Interface	

The other fields should be:

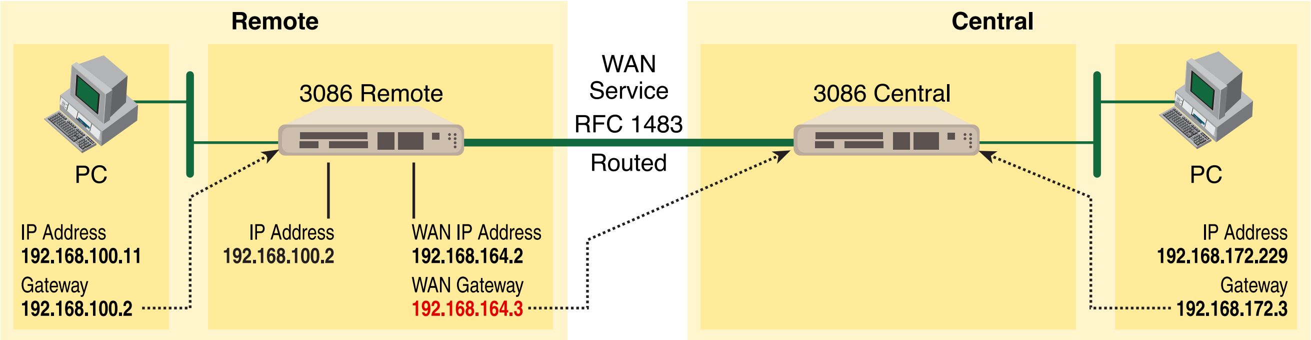
– Destination:0.0.0.0

– Gateway:192.168.164.3

– Mask:0.0.0.0

– Cost:1

– Interface:[blank]



4. Go to G.SHDSL in the Configuration Menu, then the submenu Status. The Modem State should be “deactivated.” (If not, go to the Action and change it to deactivate.)

   Then in the Action submenu under G.SHDSL, change Action to **Start**, then click on **Action**.

Model 3086FR (Central) Configuration Steps (RFC 1483 Routed)

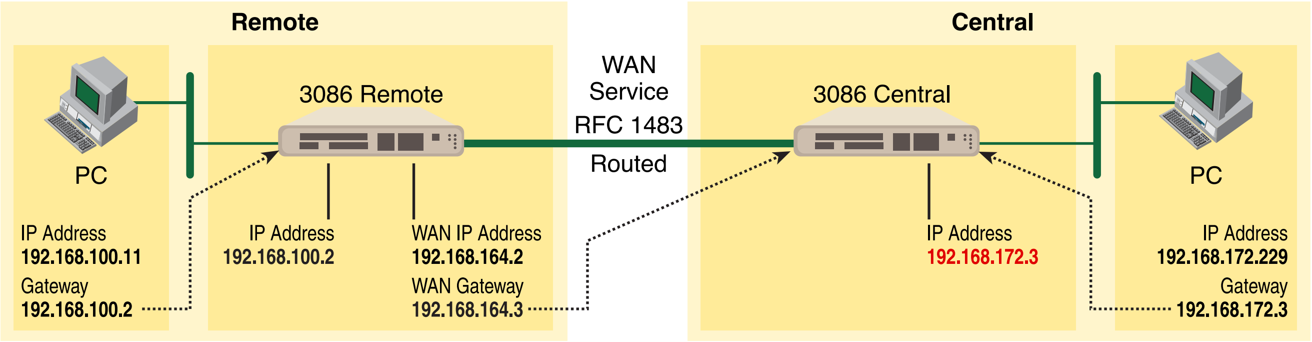
From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
fi pppoh clear transports
```

One IP interface was called ip1 with an IP address of 192.168.1.1

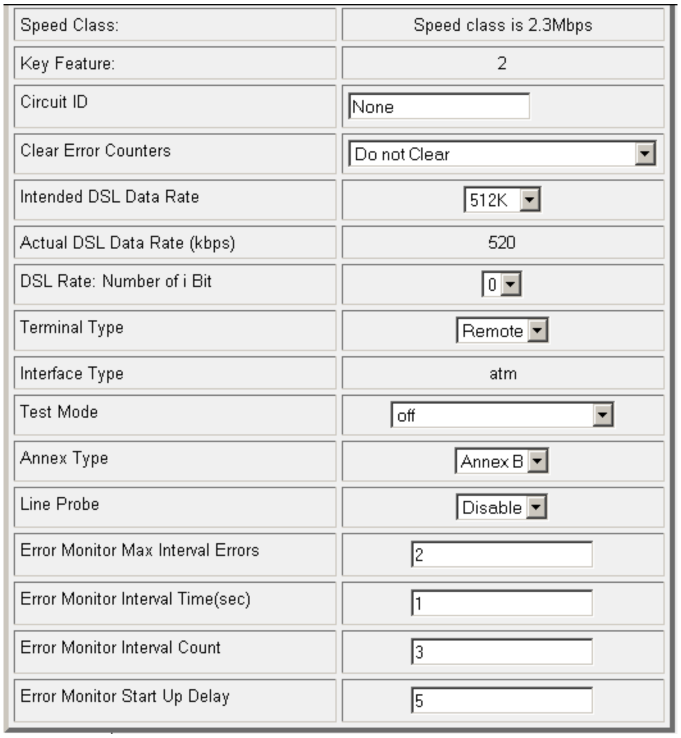
Change the IP address so it is in the same subnet as the laptop PC. The laptop's IP address is 192.168.172.229, so in this example, change the IP address of the 3086FR to 192.168.172.3. The default IP mask is 255.255.255.0.

```
fi  ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```



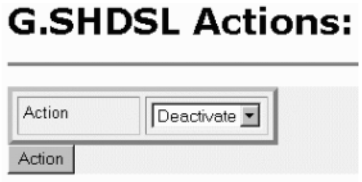
1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

   Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Remote* and Interface Type is *atm*. If changed, then click on **Configure**.



Speed Class:	Speed class is 2.3Mbps
Key Feature:	2
Circuit ID	None
Clear Error Counters	Do not Clear
Intended DSL Data Rate	512K
Actual DSL Data Rate (kbps)	520
DSL Rate: Number of i Bit	0
Terminal Type	Remote
Interface Type	atm
Test Mode	off
Annex Type	Annex B
Line Probe	Disable
Error Monitor Max Interval Errors	2
Error Monitor Interval Time(sec)	1
Error Monitor Interval Count	3
Error Monitor Start Up Delay	5

Click on Action > Select deactivate for Action > Click on the Action button.



G.SHDSL Actions:

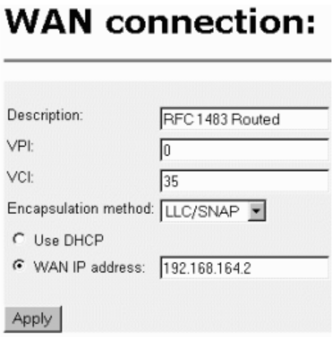
Action: Deactivate

2. On the Menu, go to Configuration, then to WAN Connections.

   Delete both default WAN services already defined.

   Click on **Create a new service** in the main window, select **RFC 1483 Routed** and click on the **Configure** button.

   In the Description field, enter the description you wish. In this example, it is called *RFC 1483 Routed*.



WAN connection:

Description: RFC 1483 Routed
VPI: 0
VCI: 35
Encapsulation method: LLC/SNAP
○ Use DHCP
● WAN IP address: 192.168.164.2

Description:RFC 1483 Routed

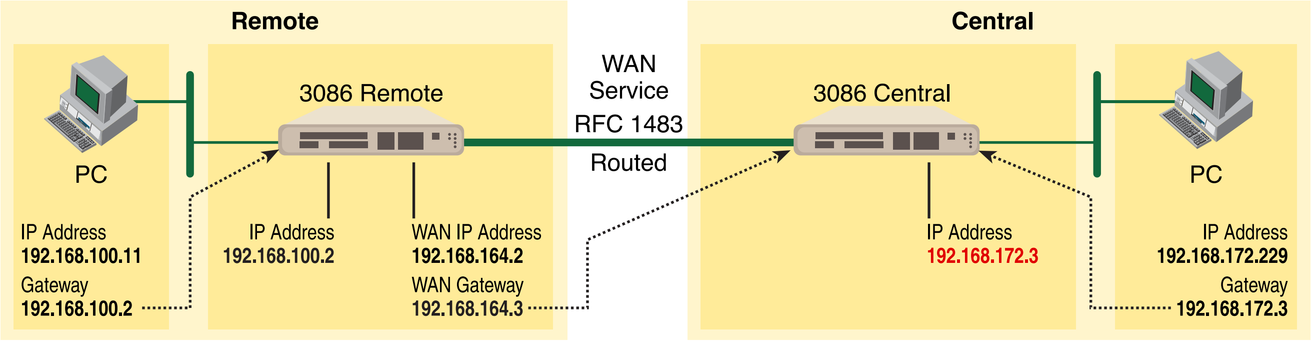
– VPI:0

– VCI:35

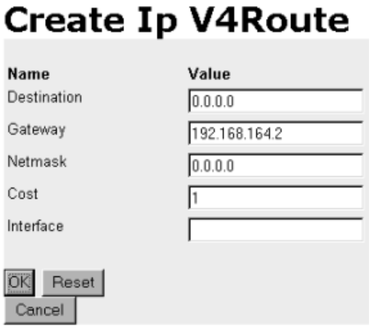
– Encapsulation Method: LLC/SNAP

– WAN IP Address:192.168.164.3

Click on **Configure**.



3. Configuration Menu > Configuration > IP Routes > Click on Create new Ip V4 Route > Create the gateway to the remote 3086FR by entering the WAN IP address of the remote 3086FR, in this example, enter 192.168.164.2 in the Gateway field > OK



Create Ip V4Route

Name	Value
Destination	0.0.0.0
Gateway	192.168.164.2
Netmask	0.0.0.0
Cost	1
Interface	

The other fields should be:

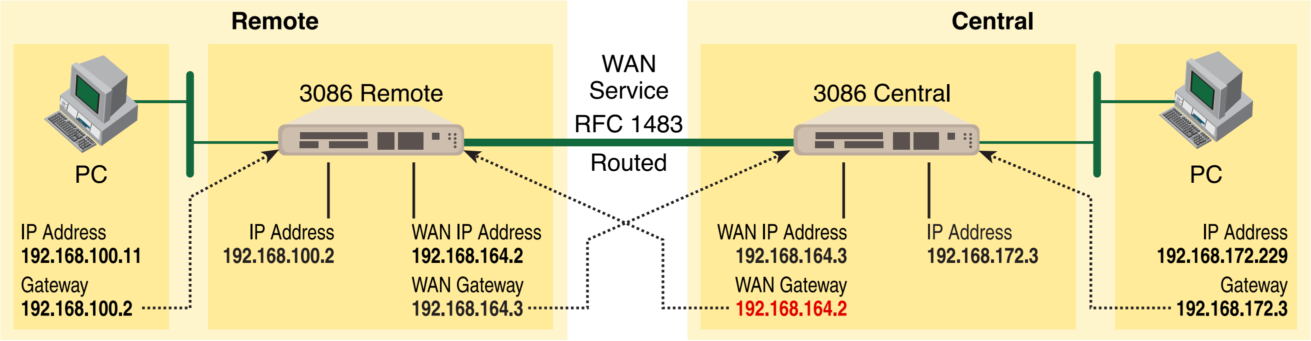
– Destination:0.0.0.0

– Gateway:192.168.164.2

– Mask:0.0.0.0

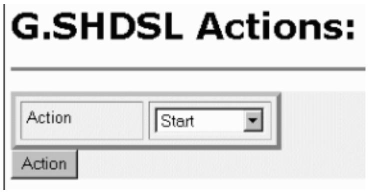
– Cost:1

– Interface:[blank]



4. Go to G.SHDSL in the Configuration Menu, then the submenu Status. The Modem State should be "deactivated." (If not, go to the Action and change it to deactivate.)

   Then in the Action submenu under G.SHDSL, change Action to Start, then click on Action.



G.SHDSL Actions:

Action: Start

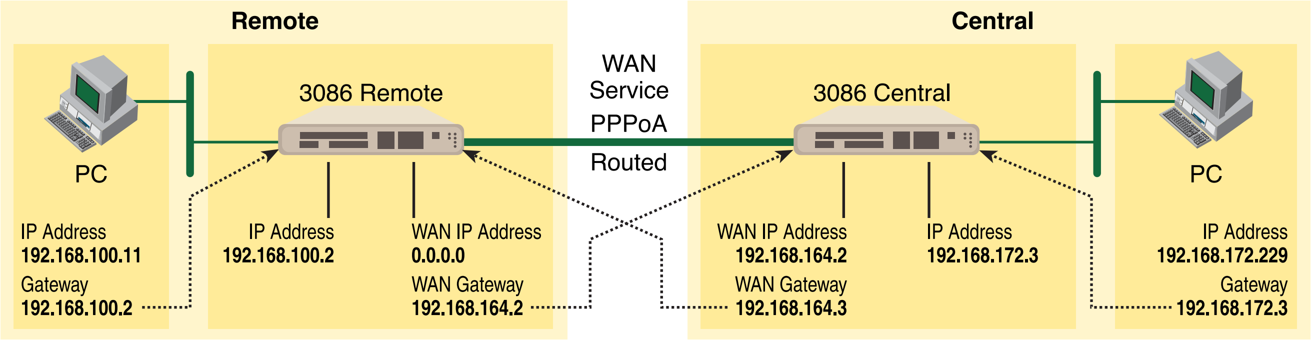
   The modems should link up within 30 seconds or so and the link is ready for communication.

PPPoA Routed (RFC 2364)

This routed application is very similar to the PPPoA Bridged application. The user data for transmission is in the form of IP packets but encapsulated in a PPP packet, transmitted and received through a PPP session to the connection. The PPP packets are encapsulated according to RFC 2364 for transmission over the ATM link. The packets are de-encapsulated on the receive side so that the IP data can be delivered to the end user.

The Central (Model 3086FR) end functions as a local ISP which will authenticate the Remote user (Model 3086FR). The CPE side, with Remote and 3086FR-A, may represent a home PC which is connecting to a centralized PPP server (Local and 3086FR—B).

Since this is a routed application, there are differences to be noted. Referring to the application diagram, three unique subnets exist. The Ethernet LAN on the 3086FR and Remote side, the Ethernet LAN on the 3086FR and Central side, and lastly, the subnet of the ATM's PVC link between the two modems, 3086FR-A and 3086FR-B. The 3086FR-B and Local end (the Central side) may also be a DSLAM.



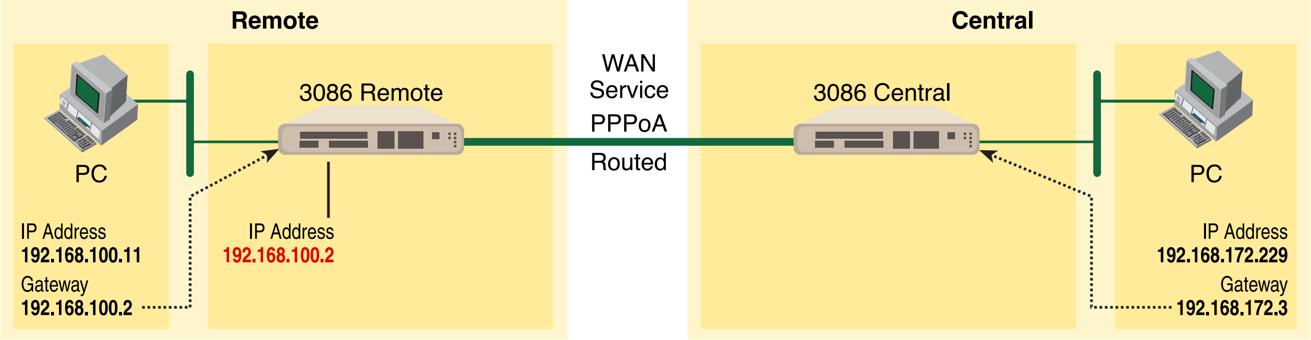
Model 3086FR (Remote—Client) Configuration Steps (PPPoA Routed)

1. From the command line interface (CLI) via the RS-232 control port,

```
ﬁ ip list interfaces
```

One IP interface was called ip1 with an IP address of 192.168.1.1 Change it to an IP address which is in the same subnet as the Desktop PC. For example, to 192.168.100.2. The default IP mask is 255.255.255.0.

```
ﬁ ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```



Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Central* and Interface Type is *atm*. If changed, then click on **Configure**.

Click on Action > Select deactivate for Action > Click on the **Action** button.

2. On the Menu, go to Configuration, then to WAN Connections

Delete both default WAN services already defined.

Click on **Create a new service** in the main window, select **PPPoA Routed** and click on the **Configure** button.

In the Description field, enter the description you wish. In this example, it is called *PPPoA Routed*. Change the configuration parameters to match the following.

– Description:PPPoA Routed

– VPI:0

– VCI:800

– WAN IP Address:0.0.0.0

– LLC Header Mode:off

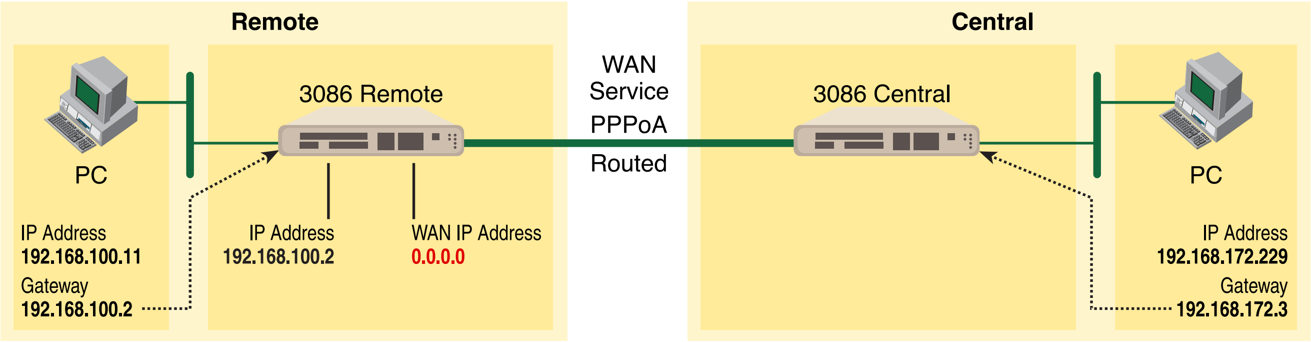
– HDLC Header Mode:off

– CHAP

– User Name:fred

– Passwood:fredspass

Click on **Configure**.



3. In the Configuration Menu, click on Configuration then > WAN Connections > Edit (for the WAN Service ppp1) > Edit 'PPP' and verify or change the following parameters on the Edit PPP webpage.

– Server:false

– Create Route:true

– Specific Route:false

– Subnet Mask:0.0.0.0

– Route Mask:0.0.0.0

– Hdlc:false

– LLC:false

– Lcp Max Configure:10

– Lcp Max Failure:5

– Lcp Max Terminate:2

– Dialin Auth:none

– Dialout Username:fred

– Dialout Password:fredspass

– Confirmation Password:fredspass

– Dialout Auth:chap

– Interface ID:1

– Remote IP:192.168.164.2

– Local IP:0.0.0.0

– Magic Number:0

– MRU:0

– IP Addr from IPCP:true

– Discover Primary DNS:true

– Discover Secondary DNS:true

– Give DNS to Relay:true

– Give DNS to Client:true

– Remote DNS:0.0.0.0

– Remote Secondary:0.0.0.0

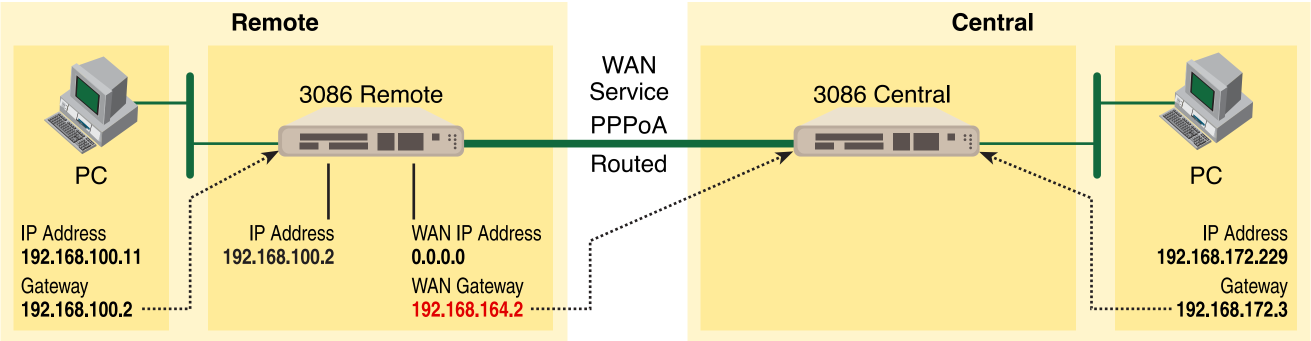
– LCP Echo Every:10

– Auto Connect:false

– Idle Timeout:0

– Termination:true

Click on **Change** button.



4. Click on Edit ‘ATM Channel.’

   Verify the Options to match the following. (Change if necessary.)

   - Tx Vci:800
   - Tx Vpi:0
   - Rx Vci:800
   - Rx Vpi:0
   - Peak Cell Rate:2000
   - Burst Tolerance:0
   - MCR:0
   - MBS:0
   - Sustainable Cell Rate:0
   - Class:UBR
   - Port:atm

   Click on the **Change** button if changes were made.

5. Click on Edit ‘IP Interface.’

   Verify or change if necessary the following Options parameters.

   - Ipaddr:0.0.0.0
   - Mask:0.0.0.0
   - Dhcp:false
   - MTU:1500
   - Enabled:true

   Click on the **Change** button if changes were made.

6. There is no gateway created in the IP routes submenu. Upon connecting, the server will provide this information while setting up the PPP connection.

7. Go to G.SHDSL in the Configuration Menu, then the submenu Status. The Modem State should be “deactivated.” (If not, go to the Action and change it to deactivate.)

   Then in the Action submenu under G.SHDSL, change Action to Start, then click on **Action**.

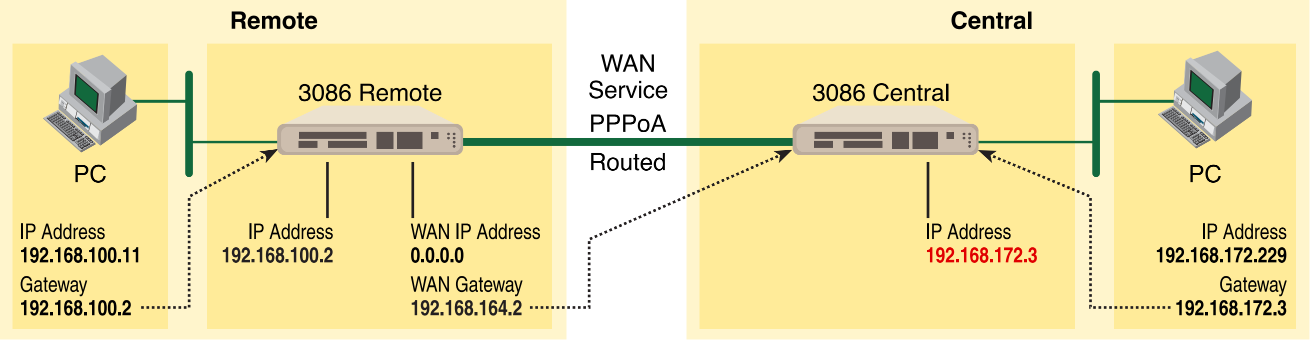
Model 3086FR (Central—Server) Configuration Steps (PPPoA Routed)

1. From the command line interface (CLI) via the RS-232 control port,

```
ﬁ ip list interfaces
```

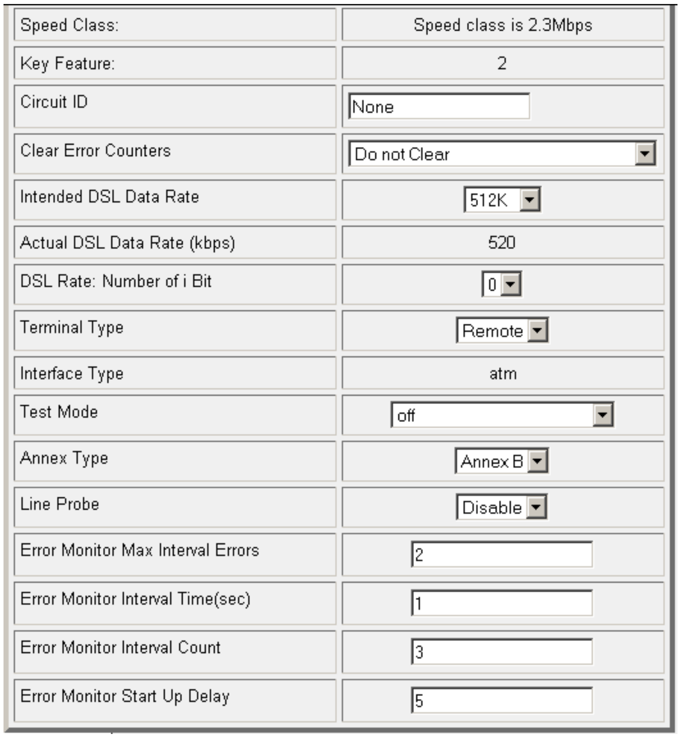
One IP interface was called ip1 with an IP address of 192.168.1.1 Change it to an IP address which is in the same subnet as the Desktop PC. For example, to 192.168.172.3. The default IP mask is 255.255.255.0.

```
fi  ip set interface ip1 ipaddress 192.168.172.3 255.255.255.0
```



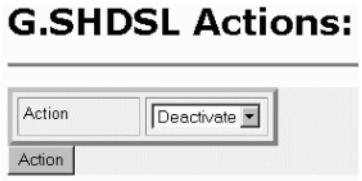
Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.

Click on G.SHDSL in the Configuration Menu> Configuration > verify that Terminal Type is *Central* and Interface Type is *atm*. If changed, then click on **Configure**.



Speed Class:	Speed class is 2.3Mbps
Key Feature:	2
Circuit ID	None
Clear Error Counters	Do not Clear
Intended DSL Data Rate	512K
Actual DSL Data Rate (kbps)	520
DSL Rate: Number of i Bit	0
Terminal Type	Remote
Interface Type	atm
Test Mode	off
Annex Type	Annex B
Line Probe	Disable
Error Monitor Max Interval Errors	2
Error Monitor Interval Time(sec)	1
Error Monitor Interval Count	3
Error Monitor Start Up Delay	5

Click on Action > Select deactivate for Action > Click on the **Action** button.



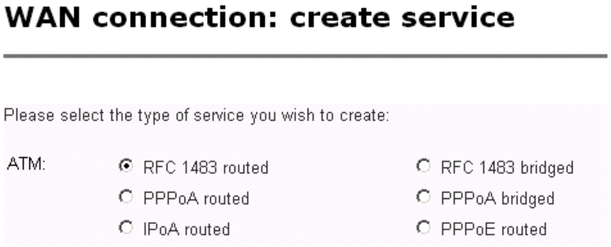
G.SHDSL Actions:

Action: Deactivate

2. On the Menu, go to Configuration, then to WAN Connections

Delete both default WAN services already defined.

Click on **Create a new service** in the main window, select **PPPoA Routed** and click on the **Configure** button.



WAN connection: create service

Please select the type of service you wish to create:

ATM:

- ● RFC 1483 routed
- ○ RFC 1483 bridged
- ○ PPPoA routed
- ○ PPPoA bridged
- ○ IPoA routed
- ○ PPPoE routed

In the Description field, enter the description you wish. In this example, it is called *PPPoA Routed*. Change the configuration parameters to match the following.

– Description:PPPoA Routed

– VPI:0

– VCI:800

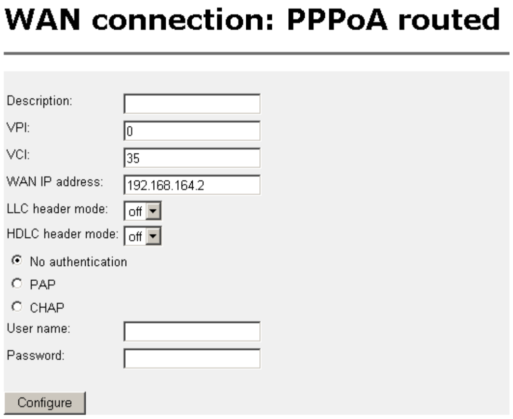
– WAN IP Address:192.168.164.2

– LLC Header Mode:off

– HDLC Header Mode:off

Note The following items are for dial-out service only, for when a remote is establishing a connection with a server.

- CHAP
- User Name: [leave blank]
- Passwood: [leave blank]



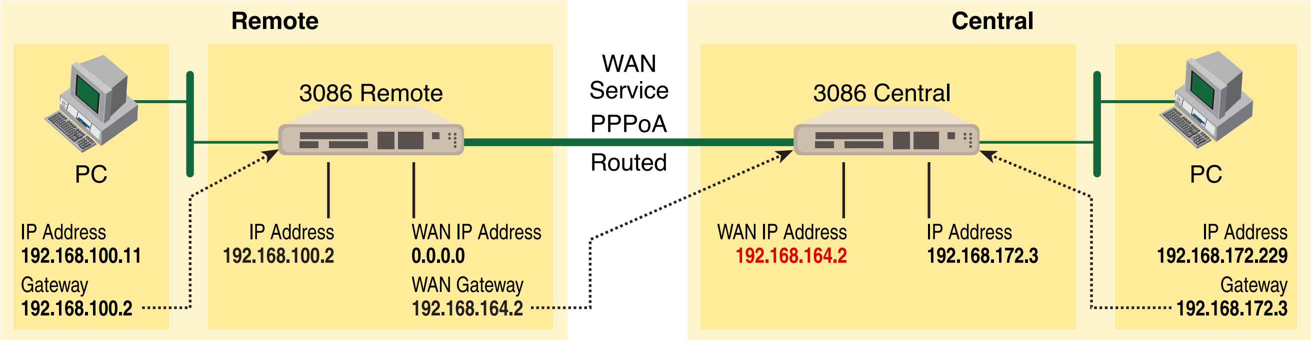
WAN connection: PPPoA routed

Description:	
VPI:	0
VCI:	35
WAN IP address:	192.168.164.2
LLC header mode:	off
HDLC header mode:	off

● No authentication
○ PAP
○ CHAP

User name:	
Password:	

Click on **Configure**.



3. In the Configuration Menu, click on Configuration then > WAN Connections > Edit (for the WAN Service ppp1) > Edit 'PPP' and verify or change the following parameters on the Edit PPP webpage.

   Parameters in *red italics* are those requiring changes from the default configuration.

   - Server: *true*
   - Create Route: true
   - Specific Route: false
   - Subnet Mask: 0.0.0.0
   - Route Mask: 0.0.0.0
   - Hdlc: false
   - LLC: false
   - Lcp Max Configure: 10
   - Lcp Max Failure: 5
   - Lcp Max Terminate: 2

– Dialin Auth: *pap*

– Dialout Username: [blank]

– Dialout Password: [blank]

– Confirmation Password: [blank]

– Dialout Auth: none

– Interface ID: 2

– Remote IP: *192.168.164.3*

– Local IP: 192.168.164.2

– Magic Number: 0

– MRU: 0

– IP Addr from IPCP: true

– Discover Primary DNS: *false*

– Discover Secondary DNS: *false*

– Give DNS to Relay: false

– Give DNS to Client: false

– Remote DNS: 0.0.0.0

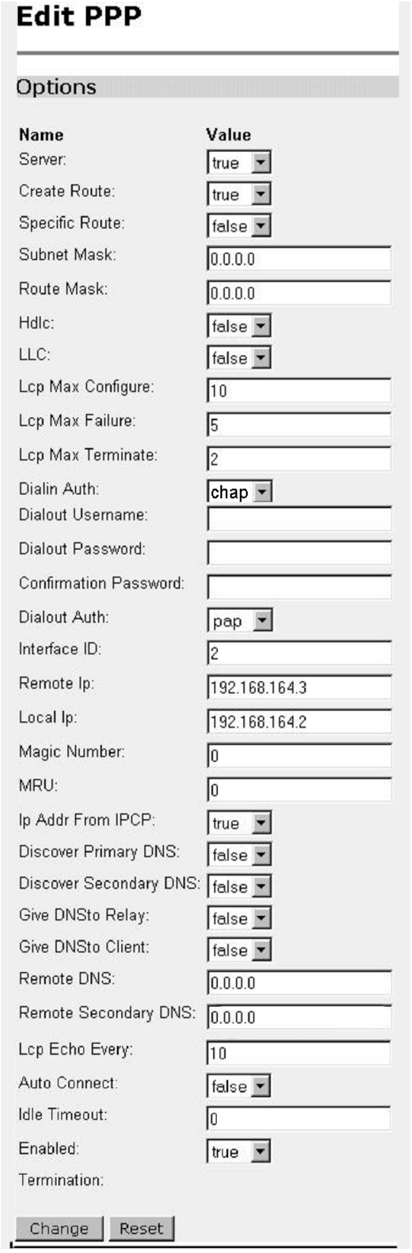
– Remote Secondary: 0.0.0.0

– LCP Echo Every: 10

– Auto Connect: false

– Idle Timeout: 0

– Termination: true

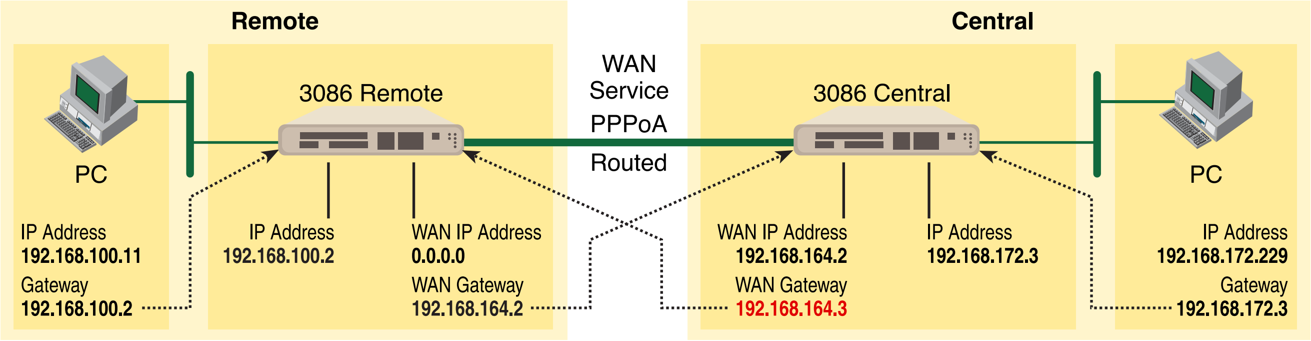


Edit PPP

Options

Name	Value
Server:	true
Create Route:	true
Specific Route:	false
Subnet Mask:	0.0.0.0
Route Mask:	0.0.0.0
Hdlc:	false
LLC:	false
Lcp Max Configure:	10
Lcp Max Failure:	5
Lcp Max Terminate:	2
Dialin Auth:	chap
Dialout Username:	
Dialout Password:	
Confirmation Password:	
Dialout Auth:	pap
Interface ID:	2
Remote Ip:	192.168.164.3
Local Ip:	192.168.164.2
Magic Number:	0
MRU:	0
Ip Addr From IPCP:	true
Discover Primary DNS:	false
Discover Secondary DNS:	false
Give DNSto Relay:	false
Give DNSto Client:	false
Remote DNS:	0.0.0.0
Remote Secondary DNS:	0.0.0.0
Lcp Echo Every:	10
Auto Connect:	false
Idle Timeout:	0
Enabled:	true
Termination:	

Click on **Change** button.



4. Click on Edit 'ATM Channel.'

Verify the Options to match the following. (Change if necessary.)

– Tx Vci:800

– Tx Vpi:0

– Rx Vci:800

– Rx Vpi:0

– Peak Cell Rate:2000

– Burst Tolerance:0

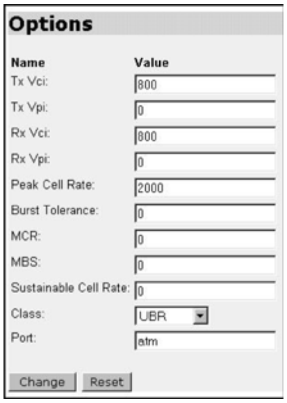
– MCR:0

– MBS:0

– Sustainable Cell Rate:0

– Class:UBR

– Port:atm



Options

Name	Value
Tx Vci:	800
Tx Vpi:	0
Rx Vci:	800
Rx Vpi:	0
Peak Cell Rate:	2000
Burst Tolerance:	0
MCR:	0
MBS:	0
Sustainable Cell Rate:	0
Class:	UBR
Port:	atm

Click on the Change button if changes were made.

5. Click on Edit ‘IP Interface.’

Verify or change if necessary the following Options parameters.

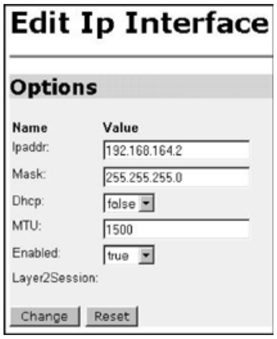
– Ipaddr:192.168.164.2

– Mask:255.255.255.0

– Dhcp:false

– MTU:1500

– Enabled:true



Edit Ip Interface

Options

Name	Value
Ipaddr:	192.168.164.2
Mask:	255.255.255.0
Dhcp:	false
MTU:	1500
Enabled:	true
Layer2Session:	

Click on the Change button if changes were made.

6. Again, **Configuration Menu > Configuration > IP Routes > Click on Create new Ip V4 Route > Create** the gateway to the remote 3086FR by changing or verifying the following parameters in the webpage Edit—Advanced Settings.

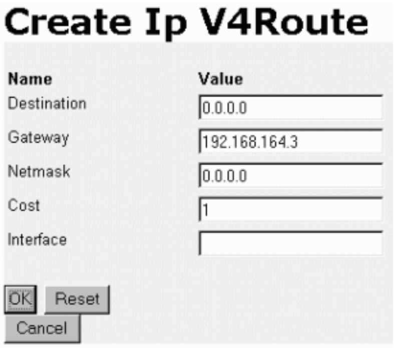
– Destination:0.0.0.0

– Gateway:192.168.164.3

– Mask:0.0.0.0

– Cost:1

– Interface:[blank]



Create Ip V4Route

Name	Value
Destination	0.0.0.0
Gateway	192.168.164.3
Netmask	0.0.0.0
Cost	1
Interface	

7. From the Configuration Menu, click on Configuration > Authentication > Create a new user > enter the information for the following parameters in the webpage Details for the new user. One of these authentication records is created for each remote end user connecting to the Server.

   – Username:fred

   – Password:fredspass

   – May dialin:true

   – Comments: [may leave blank or enter any comments for this user.]

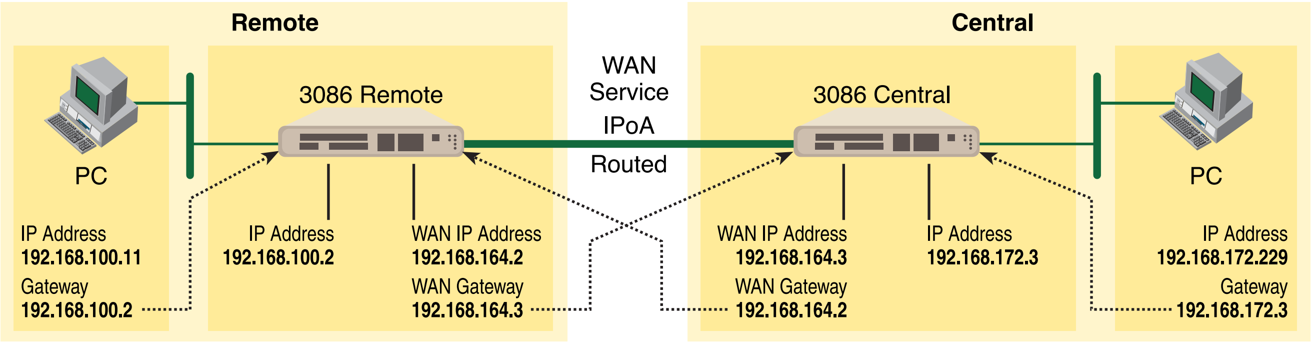
   Click on the **Create** button.

8. Go to G.SHDSL in the Configuration Menu, then the submenu Status. The Modem State should be "deactivated." (If not, go to the Action and change it to deactivate.)

   Then in the Action submenu under G.SHDSL, change Action to Start, then click on **Action**.

IPoA Routed (RFC 1577)

User data in the form of IP packets is encapsulated into AAL-5 PDUs for transport over ATM. The fact that the user data is routed at an IP layer instead of bridged at a MAC layer allows the source and destination to be on different subnets. A notable drawback of IPoA is the lack of authentication and configuration that would be provided by PPP.



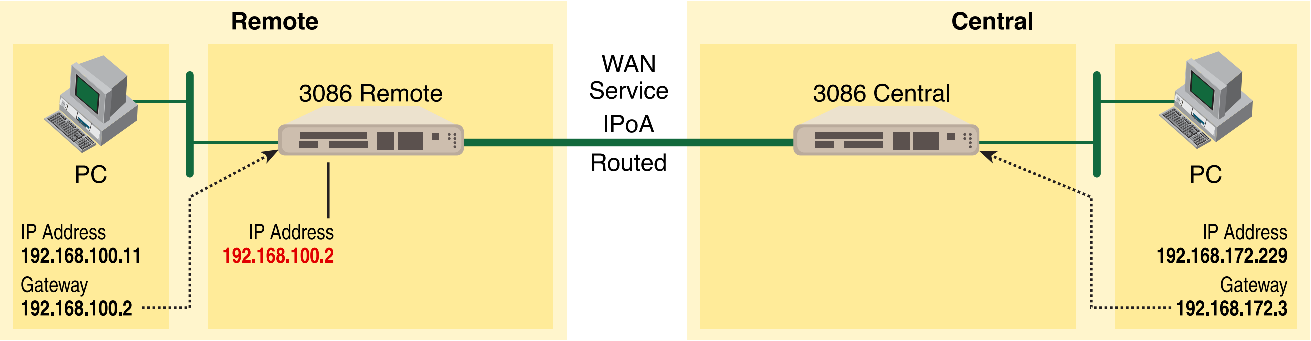
Model 3086FR (Remote) Configuration Steps (IPoA Routed)

From the command line interface (CLI) via the RS-232 control port,

```
fi ip list interfaces
```

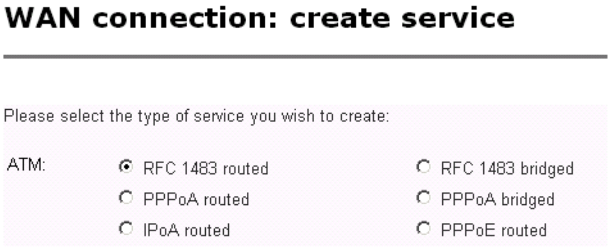
One IP interface was called ip1 with an IP address of 192.168.1.1 Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2. The default IP mask is 255.255.255.0.

```
fi ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```



1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.
2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

   Click on **Create a new service** in the main window, select **IPoA_Routed** and click on the **Configure** button.



WAN connection: create service

Please select the type of service you wish to create:

ATM:

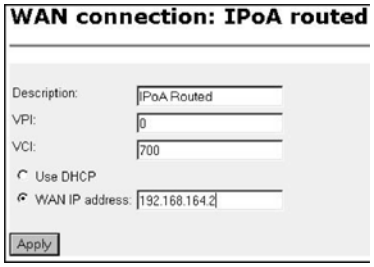
● RFC 1483 routed ○ RFC 1483 bridged
○ PPPoA routed ○ PPPoA bridged
○ IPoA routed ○ PPPoE routed

In the Description field, enter the description you wish. In this example, it is called *IPoA Routed*.

– VPI:0

– VCI:700

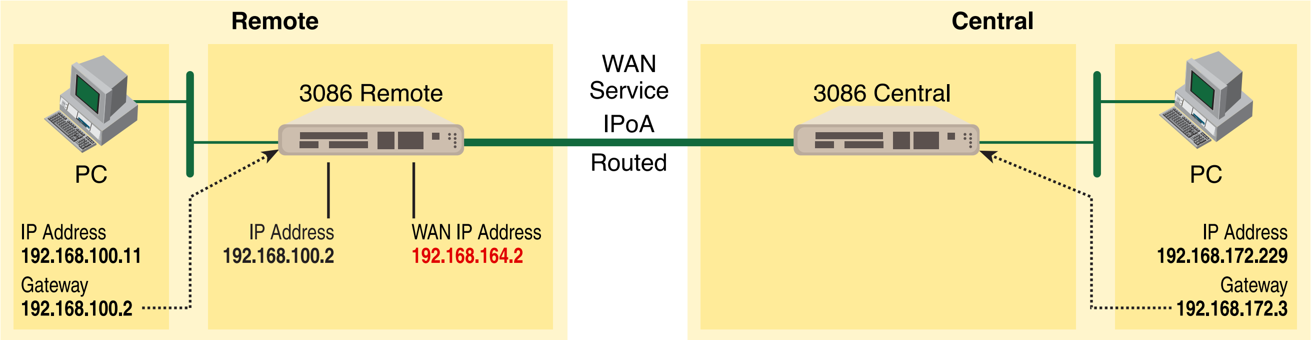
– WAN IP address: 192.168.164.2



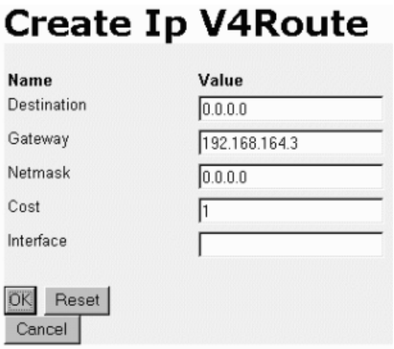
WAN connection: IPoA routed

Description: IPoA Routed
VPI: 0
VCI: 700
○ Use DHCP
● WAN IP address: 192.168.164.2

Click on **Apply**.



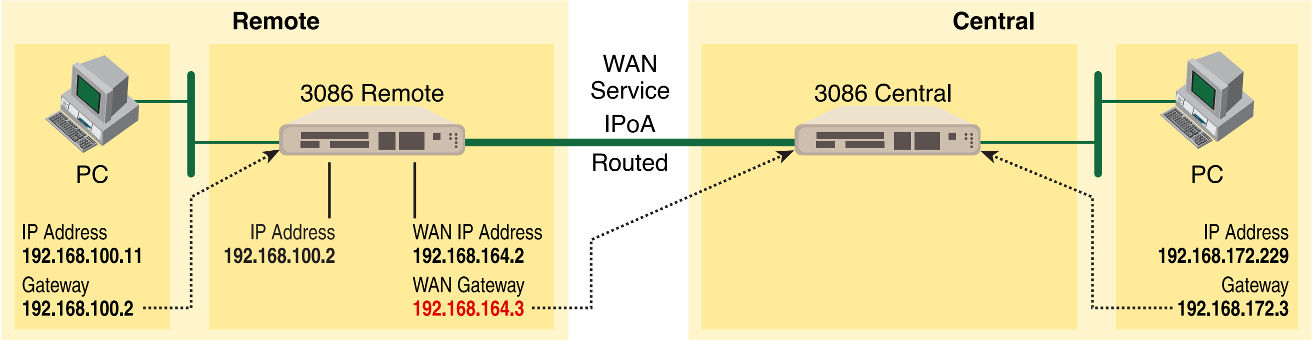
3. Returning to the 3086FR Configuration Menu, click on Configuration, then IP Routes.
   - Click on “Create new Ip V4 Route.”
   - Destination:0.0.0.0
   - Gateway:192.168.164.3
   - Mask:0.0.0.0
   - Cost:1
   - Interface:[leave blank]



Create Ip V4Route

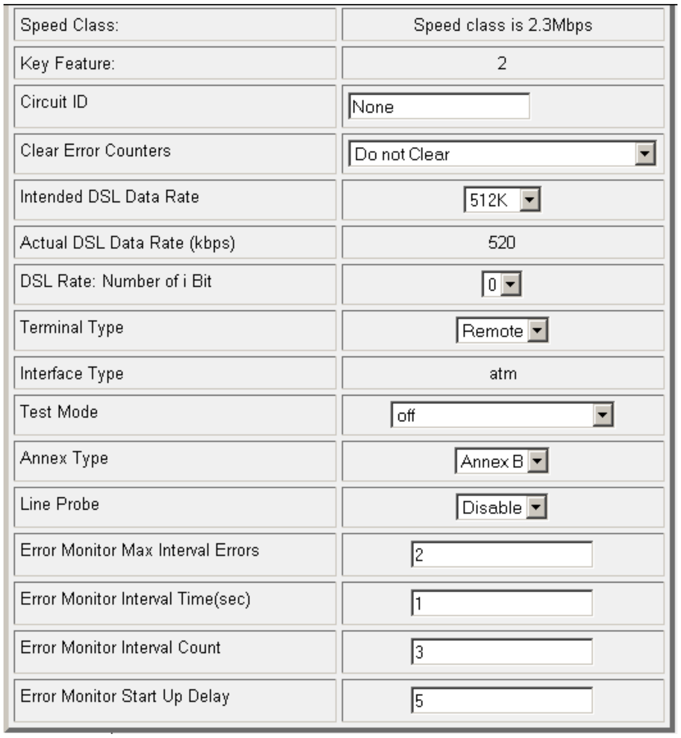
Name	Value
Destination	0.0.0.0
Gateway	192.168.164.3
Netmask	0.0.0.0
Cost	1
Interface	

Click on **OK**.



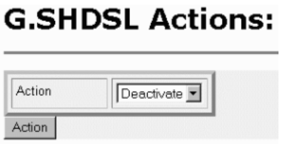
4. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

Change Terminal Type to **Central** and Interface Type to **atm**. Click on the Configure button.



Speed Class:	Speed class is 2.3Mbps
Key Feature:	2
Circuit ID	None
Clear Error Counters	Do not Clear
Intended DSL Data Rate	512K
Actual DSL Data Rate (kbps)	520
DSL Rate: Number of i Bit	0
Terminal Type	Remote
Interface Type	atm
Test Mode	off
Annex Type	Annex B
Line Probe	Disable
Error Monitor Max Interval Errors	2
Error Monitor Interval Time(sec)	1
Error Monitor Interval Count	3
Error Monitor Start Up Delay	5

In the Action submenu under G.SHDSL, change Action to Deactivate, then click on **Action**.



G.SHDSL Actions:

Action: Deactivate

Return to Action, select Start and click on **Action**.

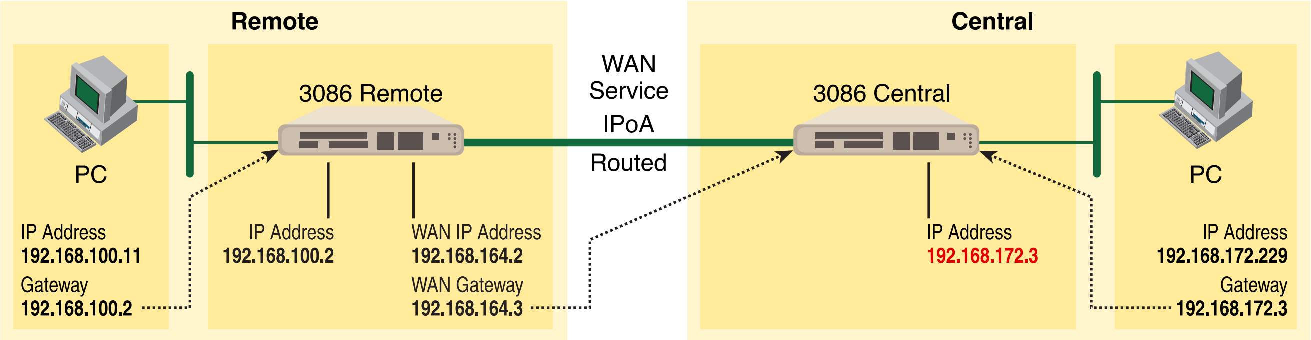
Model 3086FR (Central) Configuration Steps (IPoA Routed)

From the command line interface (CLI) via the RS-232 control port:

```
fi  ip list interfaces
```

One IP interface was called ip1 with an IP address of 192.168.1.1 Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.172.3. The default IP mask is 255.255.255.0.

```
fi  ip set interface ip1 ipaddress 192.168.172.3 255.255.255.0
```



1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3086FR.
2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

   Click on **Create a new service** in the main window, select **IPoA_Routed** and click on the **Configure** button.

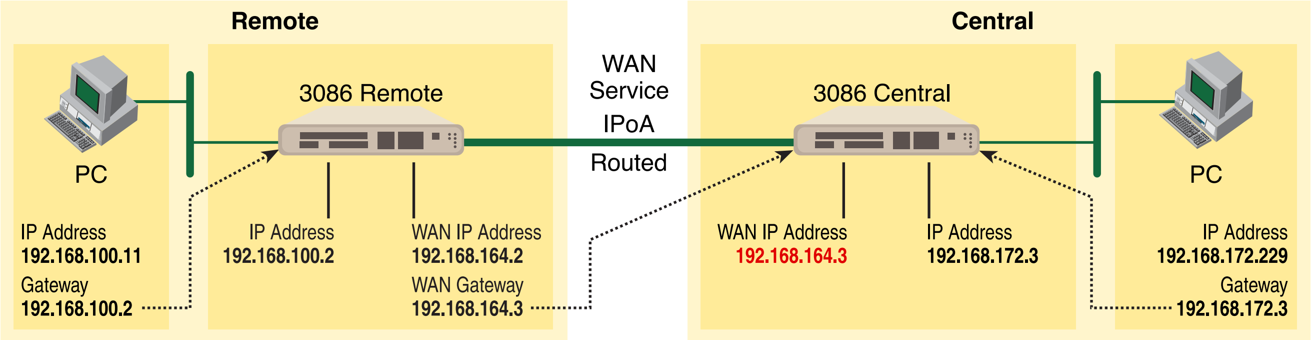
   In the Description field, enter the description you wish. In this example, it is called *IPoA Routed*.

   – VPI:0

   – VCI:700

   – WAN IP address: 192.168.164.3

   Click on **Apply**.



3. Returning to the 3086FR Configuration Menu, click on Configuration, then IP Routes.

Click on “Create new Ip V4 Route.”

– Destination:0.0.0.0

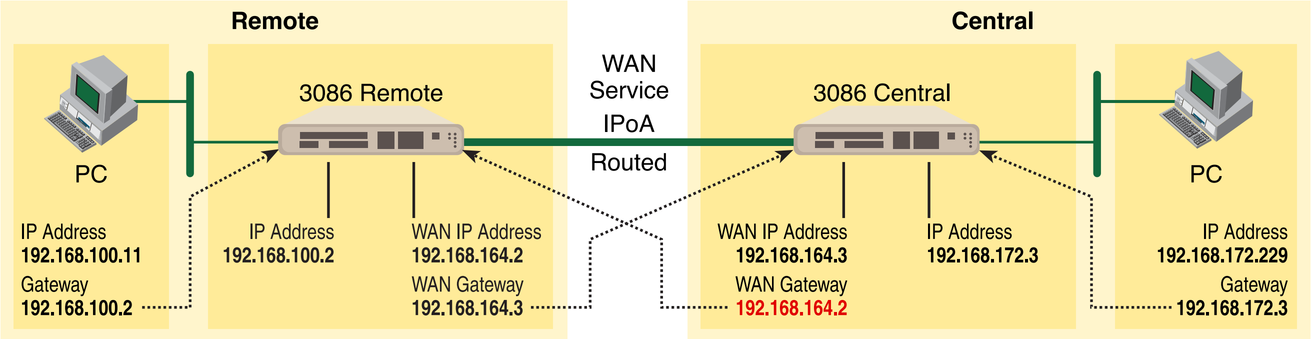
– Gateway:192.168.164.2

– Mask:0.0.0.0

– Cost:1

– Interface:[leave blank]

Click on **OK**.



4. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

Leave Terminal Type as *Remote*.

Change Interface Type to *hdlc*. Click on the **Configure** button.

In the Action submenu under G.SHDSL, change Action to Deactivate, then click on **Action**.

Return to Action, select Start and click on **Action**.

Chapter 9 **IP Configurations**

Chapter contents

IP Configurations

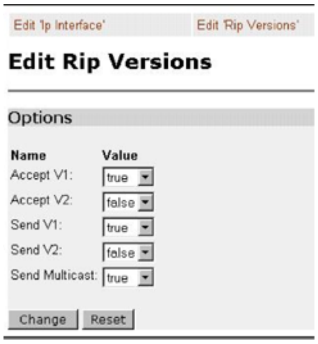
This chapter describes how to use the web page management pages to configure the router's RIP versions, create a static Ip V4Route, and configure the DHCP Server or Relay.

Router

This section describes how to edit RIP versions and create a static Ip V4Route.

RIP and RIPv2

The Routing Information Protocol (RIP) is a distance-vector protocol that enables routers to exchange information about destinations for computing routes throughout the network. You should use this routing protocol primarily in homogeneous networks of moderate size. Distance-vector algorithms cause each router to periodically broadcast its routing tables to its neighbors. Thus a router, knowing its neighbors' tables, can decide which destination neighbor to use for routing a packet.



Edit Rip Versions

Options

Name	Value
Accept V1:	true
Accept V2:	false
Send V1:	true
Send V2:	false
Send Multicast:	true

The Edit Rip Version window is where you can configure the router to accept RIPv1, RIPv2, or both. Follow these guidelines in choosing a routing configuration:

- Choose RIPv1 if you want routing advertisements to be aggregated on the network class boundary. Otherwise, choose RIPv2.
- Configure all the router interfaces on the same physical IP network to run either RIPv1 or RIPv2, but not both.
- Configure the router to run both RIPv1 and RIPv2 if there are routers on the same physical network that must use RIPv1 and others that must use RIPv2.

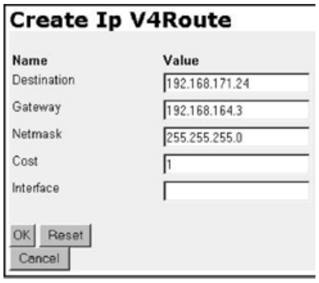
The following options are available:

- **Accept V1**—Select *True* if you want the router to accept RIPv1, otherwise select *False*.
- **Accept V2**—Select *True* if you want the router to accept RIPv2, otherwise select *False*.
- **Send V1**—Select *True* if you want the router to send RIPv1, otherwise select *False*.
- **Send V2**—Select *True* if you want the router to send RIPv2, otherwise select *False*.
- **Send Multicast**—If you want to send multicast route updates to other RIP routers, select *True*, otherwise select *False*.

Static Route

In addition to configuring the gateway, additional static routes can be entered as described below:

1. Click on > Configuration, then > IP Routes on the Configuration Menu.
2. On the main web page entitled “Edit Routes,” click on **Create new Ip V4 Route**.



Create Ip V4Route

Name	Value
Destination	192.168.171.24
Gateway	192.168.164.3
Netmask	255.255.255.0
Cost	1
Interface	

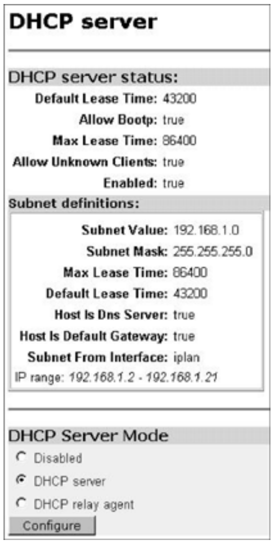
3. Enter the destination IP address in the Value field of “Destination.”
4. Enter the IP address of the gateway which is the WAN IP address of the device on the other end of the DSL link in the Value field of “Gateway.”
5. Enter the appropriate netmask in the Value field of “Netmask.”
6. Leave Cost as “1.”
7. “Interface” is an ASCII field which you may leave blank or fill in for your identification.
8. Click **OK**.
9. Add additional static routes using the same procedure.

DHCP Server and Relay

The DHCP Server or Relay are simply configured via the web page management pages.

1. Go to > Configuration Menu > Configuration > DHCP Server and the DHCP Server page is displayed.

   At the bottom of the web page are three options for the DHCP Server Mode: Disabled, DHCP server (default), and DHCP Relay Agent.



DHCP server

DHCP server status:

Default Lease Time: 43200
Allow Bootp: true
Max Lease Time: 86400
Allow Unknown Clients: true
Enabled: true

Subnet definitions:

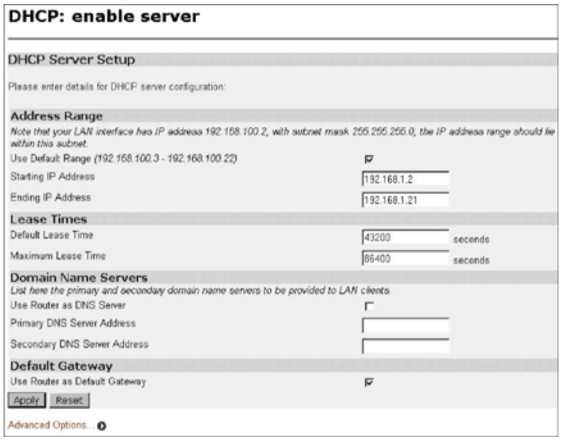
Subnet Value: 192.168.1.0
Subnet Mask: 255.255.255.0
Max Lease Time: 86400
Default Lease Time: 43200
Host Is Dns Server: true
Host Is Default Gateway: true
Subnet From Interface: iplan
IP range: *192.168.1.2 - 192.168.1.21*

DHCP Server Mode

○ Disabled
● DHCP server
○ DHCP relay agent

2. Click on **Configure** on the DHCP Server web page to change the configuration for any of the DHCP parameters.

   The three categories of configuration parameters on this web page are the Address Range of the DHCP Server, the Lease Times in seconds, the selection of Domain Name Servers (if desired), and whether to use the router as the default gateway.



DHCP: enable server

DHCP Server Setup

Please enter details for DHCP server configuration:

Address Range

Note that your LAN interface has IP address 192.168.100.2, with subnet mask 255.255.255.0; the IP address range should lie within this subnet.

Use Default Range *(192.168.100.3 - 192.168.100.22)* ☑
Starting IP Address 192.168.1.2
Ending IP Address 192.168.1.21

Lease Times

Default Lease Time 43200 seconds
Maximum Lease Time 86400 seconds

Domain Name Servers

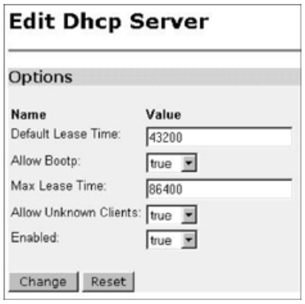
List here the primary and seconday domain name servers to be provided to LAN clients.

Use Router as DNS Server □
Primary DNS Server Address
Secondary DNS Server Address

Default Gateway

Use Router as Default Gateway ☑

3. Clicking on **Advanced Options** offers additional options for configuration. They are displayed in the following figure.

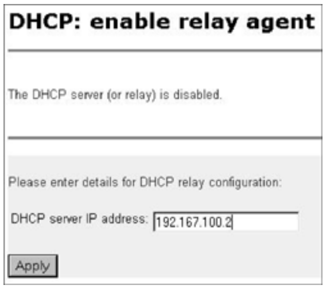


Edit Dhcp Server

Options

Name	Value
Default Lease Time:	43200
Allow Bootp:	true
Max Lease Time:	86400
Allow Unknown Clients:	true
Enabled:	true

4. The Frame Relay to ATM Converter may be used as a DHCP Relay Agent if desired. Go to > Configuration Menu > Configuration > DHCP Server. Select DHCP Relay Agent at the bottom of the web page and click on Configure. The DHCP Relay agent page is displayed.



DHCP: enable relay agent

The DHCP server (or relay) is disabled.

Please enter details for DHCP relay configuration:

DHCP server IP address: 192.167.100.2

5. Enter the DHCP server's IP address and click on **Apply**.

The router is now ready to operate as a DHCP Relay agent.

DNS Client

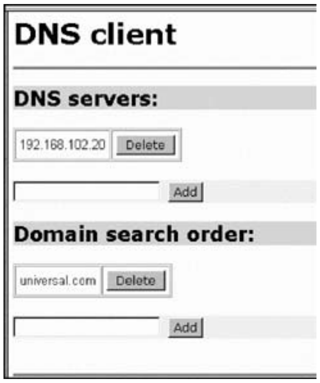
The DNS client provides a method for retrieving a list of IP addresses for a host name as well as acquiring the host name for a given IP address. The DNS client will cache any results from the name server which reduces network traffic.

1. Enter the DNS Servers by entering the IP address in the field next to the Add button.
2. Click on **Add**.

More than one DNS Server may be added.

An alternative is to create a domain search list. The DNS Client uses this list when a user asks for the IP address list for an incomplete domain name. There may be up to a maximum of 6 incomplete domain names in the search list.

Enter the domain name and click on **Add** to add it to the list.


DNS client

DNS servers:

192.168.102.20

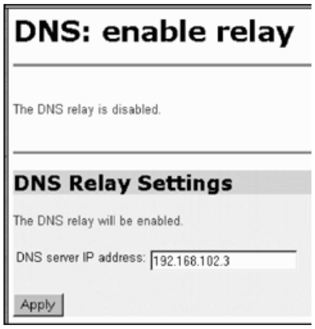
Domain search order:

universal.com

DNS Relay Mode

In the DNS Relay web page, up to 10 DNS server addresses may be added to utilize the DNS servers already being used by the network.

1. Select **Enabled**.
2. Click on **Configure**.
3. Enter the DNS server address in the field following DNS server IP address:
4. Click on **Apply**.
5. Repeat to add more DNS server addresses, not to exceed the maximum of 10.


DNS: enable relay

The DNS relay is disabled.

DNS Relay Settings

The DNS relay will be enabled.

DNS server IP address: 192.168.102.3

Chapter 10 Security

Chapter contents

Introduction

Security provides the ability to setup and enforce security policies. The policies define the types of traffic permitted to pass through a gateway, either inbound, outbound, or both, and from which origins the traffic may be allowed to enter.

Within the security configuration is a stateful firewall. A stateful firewall utilizes a security mechanism to maintain information concerning the packets it receives. This information is used for deciding dynamically whether or not a packet may pass through.

Port filters are rules that determine how a packet should be handled. The rules define the protocol type, the range of source and destination port numbers and an indication whether the packet is allowed or not.

Security triggers are used with applications that require and create separate sessions. The most common example is FTP. An FTP client establishes a connection to a server using port 21, but data transfers are done on a separate connection or port. The port number, and who makes the connection, can vary depending on the FTP client. To allow FTP to work without triggers, you would need to set up port filters allowing the correct port numbers through. This is a significant security risk.

This risk can be avoided by using security triggers. Triggers tell the security mechanism to expect these secondary sessions and how to handle them. Rather than allowing a range of port numbers, triggers handle the situation dynamically, opening the secondary sessions only when appropriate. The triggers work without needing to understand the application protocol or reading the payload of the packet, although this does happen when using NAT.

Triggering allows you to set up a trigger for different application protocols that use multiple sessions. The timeout between sessions and whether or not session chaining are allowed are configurable. Session chaining is not needed for FTP but is for NetMeeting.

See Chapter 11, “NAT (Network Address Translation)” on page 131.

Configuring the IAD

The configuration of security assumes that the 3086FR/Frame Relay to ATM Converter already has a valid IP address for the Ethernet port so that the user may access the modem via the web page. If the IP address is still the factory default, go to the section in Chapter 3 entitled IP Address Quick Start Modification.

In this example the WAN transport between the two 3086FR/IADs will be IPoA.

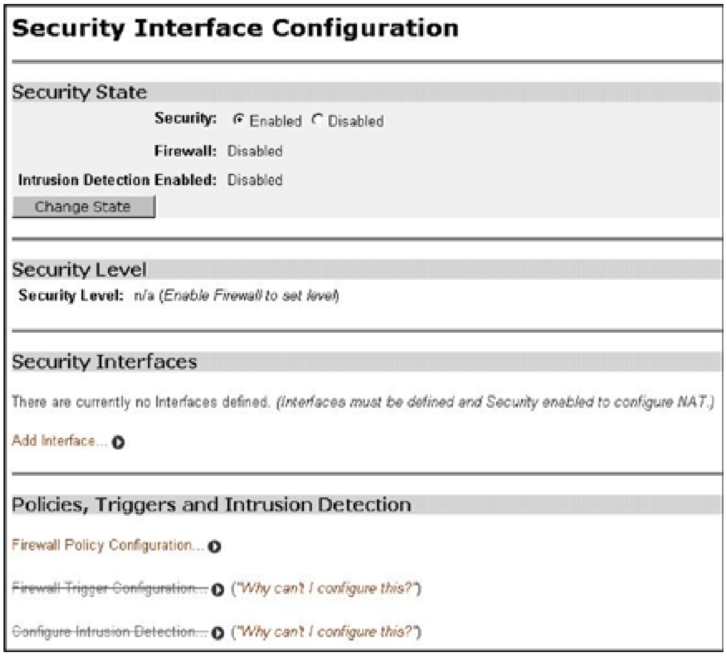
1. Click on **WAN Connections** under Configuration on the 3086FR’s Menu.
2. Click on **Create a New Service**.
3. Select **IPoA Routed** and click on the **Configure** button.
4. For this example, enter **IPoA Security Firewall** in the Description field.
5. VPI remains at *0*. Change VCI to be *100*.
6. Click on **WAN IP address** and enter *192.168.101.1* in the adjacent box. The default IP mask is 255.255.255.0.
7. Click on **Apply**.

The next step in configuring the Frame Relay to ATM Converter is adding the default gateway route. Since the WAN IP address of the 3086FR modem at the CO site is 192.168.101.2, this will be the gateway for the 3086FR modem at the CPE site, the modem we are currently configuring.

1. Click on **`IP Routes`** under Configuration on the 3086FR modem's Menu.
2. Click on **`Create a New IP Route`**.
3. Enter *192.168.101.2* in the box adjacent to Gateway.
4. Leave Destination and Netmask both as *0.0.0.0* because this is the gateway default route.
5. Click on **`Create`** and the route will be entered.
6. The default gateway can be verified by clicking on **`IP Routes`** under Status in the menu.

Configuring the security interfaces

The interfaces and routes have been configured on the 3086FR Frame Relay to ATM Converter which will function as the firewall. The Ethernet side of the 3086FR will be configured to be an internal security interface whereas the WAN side is configured as an external security interface since it is on "public" side of the modem connection.



Security Interface Configuration

Security State

Security: ● Enabled ○ Disabled

Firewall: Disabled

Intrusion Detection Enabled: Disabled

Security Level

Security Level: n/a *(Enable Firewall to set level)*

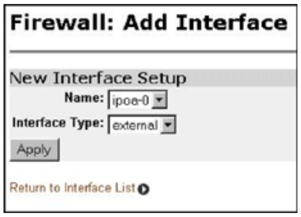
Security Interfaces

There are currently no Interfaces defined. *(Interfaces must be defined and Security enabled to configure NAT.)*

Policies, Triggers and Intrusion Detection

Firewall Policy Configuration...
~~Firewall Trigger Configuration...~~ ("Why can't I configure this?")
~~Configure Intrusion Detection...~~ ("Why can't I configure this?")

1. Click on **`Security`** under Configuration on the 3086FR modem's menu.
2. Under Security Interfaces, click on **`Add Interface`**.
3. Select Name of the WAN port (*ipoa-0*) and Interface Type to be *external*. Click on **`Apply`**.

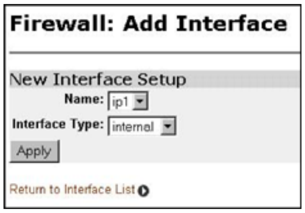


Name: ipoa-0

Interface Type: external

4. Add one more security interface by repeating step 2.

5. Select Name of the LAN port (*ip1*) and Interface Type to be *internal*. Click on **`Apply`**.



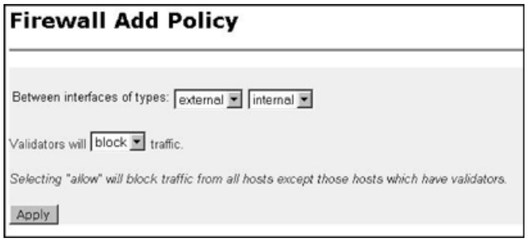
Name: ip1

Interface Type: internal

Now the Firewall policies will be added between the security interfaces. Only one Firewall policy, called *etoi*, is added between the external and internal interfaces.

1. Under Policies, Triggers and Intrusion Devices on the Security page, click on **`Firewall Policy Configuration`**.

2. In the Current Firewall Policies page, click on **`New Policy`**.



Between interfaces of types: external internal

Validators will block traffic.

Selecting "allow" will block traffic from all hosts except those hosts which have validators.

3. Select the parameters so the policy applies **`between interface of types: external internal`**.
   Also **`Validators will block traffic`**. This blocks all hosts.

4. Click on **`Apply`**.

Deleting a Firewall Policy

To delete a Firewall Policy, follow these Command Line Interface (CLI) commands via the Console port.

```
fi firewall list policies
```

Firewall Policies:

```
     ID |    Name    |   Type 1   |   Type 2   | Validator Allow Only
   ---------------------------------------------------------------------
      1 | item0      | external   | internal   | false
   ---------------------------------------------------------------------


    ﬁ firewall delete policy item0
```

The firewall policy named *item0* is now deleted.

Enabling the Firewall

At this point, both security and the firewall can be enabled and the network is secure. All the interfaces which have been defined are protected: all traffic blocked between the internal and external interfaces.

1. Return to the Security page.
2. Under Security State select **`Enabled for Security`** and click on **`Change State`**.
3. Then select **`Enabled for the Firewall`** and click on **`Change State`**.

The network is now secure. All the interfaces which have been defined are protected and all traffic is blocked between different the different interface types. That is, all traffic is blocked between the external and internal interfaces.

The next section describes how to configure the Firewall for allowing certain types of data transfer to occur between the PC's on different networks.

Firewall Portfilters

Next, we configure the Firewall to permit certain types of data transfer between the PCs on the different networks. This is done by the implementation of Firewall portfilters. Portfilters are individual rules that determine what kind of traffic can pass between two interface types.

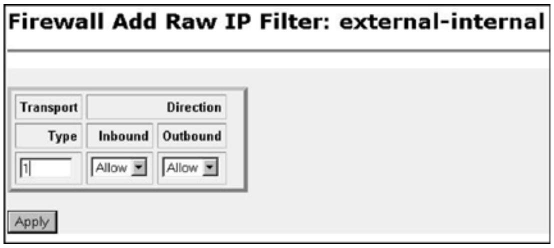
For the Transport Type below, the different types are:

Transport Type	Abbreviation
1	ICMP
2	IGMP
3	GGP
4	IP
6	TCP
8	EGP
9	IGP
17	UDP
46	RSVP
47	GRE
89	OSPFIGP
92	MTP

Transport Type	Abbreviation
94	IPIP

To allow pings between the two PCs:

1. From the Configuration Menu, > Configuration > Security > Firewall Policy Configuration > Port Filters > Add Raw IP Filter
2. Enter *1* (for ICMP) in Transport Type.
3. Both Inbound and Outbound should be allowed.
4. Click on **`Apply`**.



Firewall Add Raw IP Filter: external-internal

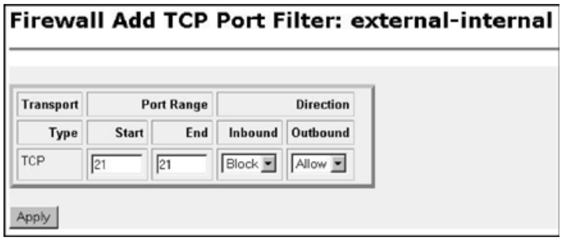
Transport	Direction	
Type	Inbound	Outbound
1	Allow	Allow

You can now ping between the two networks

Security Triggers

Security triggers are used to allow an application to open a secondary port in order to transport data. The most common example is FTP. This procedure is to set up a trigger on the Firewall to have an FTP session from PC A to PC B, but not the reverse.

1. First, create an outbound-only portfilter for FTP and add it to the item0 policy.
2. Following the path given in step 1 for the ping portfilter, click on **`Add TCP Filter`**.
3. The Port Range is entered as *21* for both Start and End.
4. Set Inbound as **`Block`**, but Outbound as **`Allow`**.
5. Click on **`Apply`**.



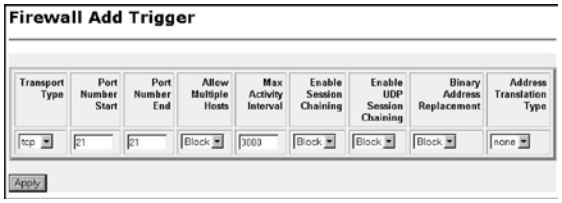
Firewall Add TCP Port Filter: external-internal

Transport	Port Range		Direction	
Type	Start	End	Inbound	Outbound
TCP	21	21	Block	Allow

After configuring the FTP portfilter, you can open an ftp session from Remote to Local, however you can issue ftp commands (e.g., login, cd, etc.) but transfer data (e.g., ls, dir, get, put commands). The portfilter allows an ftp control channel but does not allow the use of a secondary data channel for passing data by ftp.

To enable the ftp data channel, add a trigger which will open a secondary channel only when data is being passed. This prevents the need to open too many ports which offer a security risk.

1. From the Configuration Menu, > Configuration > Security > Firewall Trigger Configuration > New Trigger.
2. Set the parameters as follows:
   - Transport Type = tcp
   - Port Number Start = 21
   - Port Number End = 21
   - Allow Multiple Hosts = Block
   - Max Activity Interval = 3000
   - Enable Session Chaining = Block
   - Enable UDP Session Chaining = Block
   - Binary Address Replacement = Block
   - Address Translation Type = none
3. Click on **`Apply`**.



Firewall Add Trigger

Transport Type	Port Number Start	Port Number End	Allow Multiple Hosts	Max Activity Interval	Enable Session Chaining	Enable UDP Session Chaining	Binary Address Replacement	Address Translation Type
tcp	21	21	Block	3000	Block	Block	Block	none

You should now be able to use ftp commands to pass data between Remote and Local.

Intrusion Detection System (IDS)

The security feature in the 3086FR Frame Relay to ATM Converter provides protection from a number of attacks. Some attacks cause a host to be blacklisted (i.e., no traffic from that host is accepted under any circumstances) for a period of time. Other attacks are simply logged. The subsequent table is a summary of the attacks detected.

Attack Name	Protocol	Attacking Host Blacklisted?
Ascend Kill	UDP	yes
Echo/Chargen	UDP	no
Echo Scan	UDP	yes
WinNuke	TCP	yes
Xmas Tree Scan	TCP	yes
IMAP SYN/FIN Scan	TCP	yes
Smurf	ICMP	If victim protection set
SYN/FIN/RST Flood	TCP	If scanning threshold exceeded
Net Bus Scan	TCP	yes
Back Orifice Scan	UDP	yes

1. To enable IDS, click on Enabled for “Intrusion Detection Enabled” on the “Security Interface Configuration” page. Then click on **`Change State(s)`**.
2. Click on **`Configure Intrusion Detection.`**
3. You may choose which of the parameters to configure and for which value.

   – Use Blacklist:Default = 10 minutes when enabled.

   If IDS has detected an intrusion an external host, access to the network is denied for ten minutes.

   – Use Victim Protection:Default = Disabled.

   Enables Victim Protection. Victim Protection protects the victim from an attempted spoofing attack. Web spoofing allows an attacker to create a ‘shadow’ copy of the world wide web (WWW). All access to the shadow Web goes through the attacker’s machine, so the attacker can monitor all of the victim’s activities and send false data to or from the victim’s machine. When enabled, packets destined for the victim host of a spooking style attack are blocked.

   – DOS Attack Block Duration:Default = 1800 seconds (30 minutes).

   A Denial of Service (DOS) attack is an attempt by an attacker to prevent legitimate users from using a service. If a DOS attack is detected, all suspicious hosts are blocked by the firewall for a set time limit

   – Scan Attack Block Duration:Default = 86400 seconds

Sets the duration for blocking all suspicious hosts. The firewall detects when the system is being scanned by a suspicious host attempting to identify any open ports.

– Victim Protection Block Duration:Default = 600 seconds (10 minutes).

  Sets the duration of the block in seconds.

– Maximum TCP Open Handshaking Count:Default = 100

  Sets the maximum number of unfinished TCP handshaking sessions per second that are allowed by a firewall before a SYN Flood is detected. SYN Flood is a DOS attack. When establishing normal TCP connections, three packets are exchanged: (1) A SYN (synchronize) packet is sent from the host to the network server. (2) A SYN/ACK packet is sent from the network server to the host. (3) An Ack (acknowledge) packet is sent from the host to the network server. If the host sends unreachable source addresses in the SYN packet, the server sends the SYN/ACK packets to the unreachable addresses and keeps resending them. This creates a backlog queue of unacknowledged SYN/ACK packets. Once the queue is full, the system will ignore all incoming SYN request and no legitimate TCP connections can be established.

– Once the maximum number of unfinished TCP handshaking sessions is reached, an attempted DOS attack is detected. The firewall blocks the suspected attacker for the time limit specified in the DOS Attack Block Duration parameter.

– Maximum Ping Count:Default = 15

  Sets the maximum number of pings per second that are allowed by the firewall before an Echo Storm is detected. Echo Storm is a DOS attack. An attacker sends oversized ICMP datagrams to the system using the 'ping' command. This can cause the system to crash, freeze, or reboot, resulting in denial of service to legitimate users.

– Maximum ICMP Count:Default = 100

  Sets the maximum number of ICMP packets per second that are allowed by the firewall before an ICMP Flood is detected. An ICMP Flood is a DOS attack. The attacker tries to flood the network with ICMP packets in order to prevent transmission of legitimate network traffic.

4. After selecting the chosen parameters, click on **`Apply`**.

Chapter 11 NAT (Network Address Translation)

Chapter contents

Introduction

The basic steps for configuring NAT are:

1. Enable NAT between the internal and external interfaces of the firewall.
2. Create global addresses which will be added to the global pool of IP addresses on the WAN interface.
3. Create a reserved mapping between a global IP address and the IP address of an internal PC.

A Global Address Pool is a pool of addresses seen from the outside network. Each external interface creates a Global Address Pool with a single address—the address assigned to that interface. For outbound sessions, an address is picked from a pool by hashing the source IP address for a pool index and then hashing again for an address index. For inbound sessions, it is necessary to create a reserved mapping.

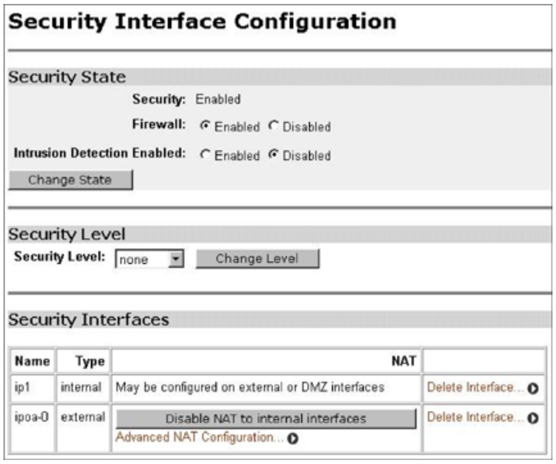
A reserved mapping is used so that NAT knows where to route packets on inbound sessions. The reserved mapping will map a specific global address and port to an inside address and port. Reserved mappings can also be used so that different inside hosts can share a global address by mapping different ports to different hosts. For example, Host A is an FTP server and Host B is a web server. By mapping the FTP port to Host A and the HTTP port to Host B, both insides hosts can share the same global address. Setting the protocol number to 255 (0xFF) means that the mapping will apply to all protocols. *Setting the port number to 65535 (0xFFFF) for TCP or UDP protocols means that the mapping will apply to all port numbers for that protocol.*

Some applications embed address and/or port information in the payload of the packet. The most notorious of these is FTP. For most applications, it is sufficient to create a trigger with address replacement enabled. However there are three applications for which a specific ALF is provided: FTP, NetBIOS, and DNS.

Enabling NAT

The configuration of NAT in this example follows on the preceding configuration completed in the chapter, “Security.”

1. Go to the “Security Interface Configuration” page by clicking on **`Security`** under Configuration in the menu.
2. Click on **`Enable NAT to internal interfaces`** in the table, Security Interfaces. NAT is now enabled between the internal (LAN) and the external (WAN) interfaces of the firewall.



Security Interface Configuration

Security State

Security: Enabled

Firewall: ● Enabled ○ Disabled

Intrusion Detection Enabled: ○ Enabled ● Disabled

Security Level

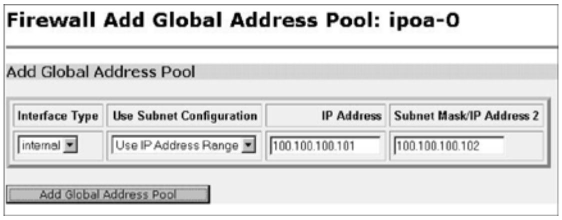
Security Level: none ▾

Security Interfaces

Name	Type	NAT	
ip1	internal	May be configured on external or DMZ interfaces	Delete Interface...
ipoa-0	external	Disable NAT to internal interfaces Advanced NAT Configuration...	Delete Interface...

Global address pool and reserved map

1. Click on **Advanced NAT Configuration...** on the web page, "Security Interface Configuration."



Firewall Add Global Address Pool: ipoa-0

Add Global Address Pool

Interface Type	Use Subnet Configuration	IP Address	Subnet Mask/IP Address 2
internal ▾	Use IP Address Range ▾	100.100.100.101	100.100.100.102

2. Click on the hyperlink **Add Global Address Pool**. The global IP addresses need to be created and put into the Global Address Pool.

3. Set the parameters to the following values:

   – Interface Type:internal

   – Use Subnet Configuration:Use IP Address Range

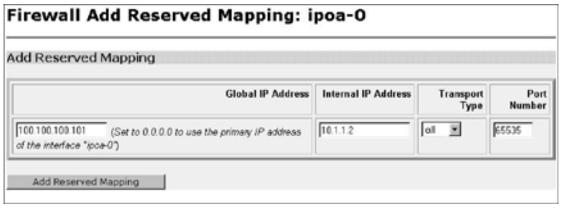
   – IP Address:100.100.100.101

   – Subnet Mask/IP Address 2:100.100.100.102

   Click on **Add Global Address Pool**.

4. Next, create a reserved mapping between a global IP address from the global pool and an internal PC's IP address (in this example, 10.1.1.2)

5. Click on **Add Reserved Mapping...**



Firewall Add Reserved Mapping: ipoa-0

Add Reserved Mapping

Global IP Address	Internal IP Address	Transport Type	Port Number
100.100.100.101 *(Set to 0.0.0.0 to use the primary IP address of the interface "ipoa-0")*	10.1.1.2	all	65535

6. Set the parameters to the following values:

   – Global IP Address:100.100.100.101

   – Internal IP address:10.1.1.2

   – Transport Type:all

   – Port Number:65535(This port number means all port numbers for TCP or UDP protocols will be mapped.)

7. Click on **`Add Reserved Mapping`**.

Chapter 12 Monitoring Status

Chapter contents

Status LEDs

The LEDs indicate the status of the Power, the WAN (DSL) inter-modem link, Sync Serial or T1/E1 port, the Ethernet connection, and Status.

All LED indicators will present the same looking profile (e.g., clear) when unlit due to being single color, water clear, high efficiency LEDs.

Table 5. Status LED descriptions

Power		Green	ON indicates that power is applied. Off indicates that no power is applied.
WAN (DSL)	Link	Green	Solid green: connected Off: disconnected
Sync Serial	TD	Green	Green: indicates a binary ‘0’ condition *off*: indicates a binary ‘1’or idle condition
	RD	Green	Green: indicates a binary ‘0’condition off: indicates a binary ‘1’ or idle condition
	CTS	Green	ON: indicates the CTS signal from the Frame Relay to ATM Converter is active, binary ‘1’ off: indicates CTS is binary ‘0’
	DTR	Green	ON: indicates the DTR signal from the DTE device attached to the serial port is active, binary ‘1’
T1/E1	Link	Green	On: indicates the T1/E1 interface is connected to a live T1/E1 line
	LOS	Red	On: indicates the T1/E1 interface is not connected to an active T1/E1 line
	TD	Green	Green: indicates a binary ‘0’ condition *off*: indicates a binary ‘1’or idle condition
	RD	Green	Green: indicates a binary ‘0’condition off: indicates a binary ‘1’ or idle condition
Ethernet	Link	Green	ON: indicates an active 10/100 BaseT connection
	100M	Green	ON: connected to a 100BaseT LAN Off: connected to a 10BaseT LAN
	Tx	Green	Flashing: when transmitting data from the Frame Relay to ATM Converter to the Ethernet
	Rx	Green	Flashing: when transmitting data from the Ethernet to the IAD.
Status	NS	Red	ON: incidates absence of a valid DSL connection
	ER	Red	flashes once: indicates bit errors occurring during 511/511E tests
	TM	Yellow	ON: is under one of the test modes (local loop, remote loop, or V.54 BER pattern)

Chapter 13 Diagnostics

Chapter contents

Introduction

The Model 3086FR offers three sets of diagnostics: Local Analog Loopback (serial port loop), Remote Digital Loopback (DSL loop), and T1/E1 Loops for the Model 3086FR/K. Some tests can be activated physically from the front panel, or via the CLI/Web management menus

Ping

The ping command is executed from the Command Line Interface (CLI). Ping in the 3086FR is executed from the “ip” command. Here is the ping format followed by a valid response.

```
ip ping 192.168.100.11
ping: PING 192.168.100.11: 32 data bytes
ping: 40 bytes from 192.168.100.11: seq=0, ttl=128, rtt<10ms
```

ﬁ

Software Upgrades

Software upgrades are required in two scenarios. First, for new features. Second, for standard software upgrades (at an additional cost).

For standard software upgrades, which are at no charge, contact **upgrades.patton.com** for the location of the new firmware and follow these instructions.

1. Get the firmware image from Patton and save on your PC. It is a .tar file and MUST NOT be unzipped!
2. Login to the 3086FR’s web page on the browser.
3. Click on > System, then > Upgrade
4. Locate the firmware image on this web page.
5. Click on Upgrade.
6. Wait until the upgrading is complete, and then restart the 3086FR.
7. It is now ready to use with the new firmware.

If you encounter problems with the firmware upgrade, do the following to upload software image into the Patton 3086FR via TFTP. .

Note The Patton 3086FR products have a TFTP server built-in, a TFTP client will be require on the user side to connect to the TFTP server

Configuration

The Patton products are configured as a TFTP server with the default IP address 192.168.200.10.

Procedure

1. Go to Upgrade.patton.com and download the software upload package. The package contains the following files:
   – Tftplock.key
   – Tftpupdt.beg
   – Image

- Npimage
- Key
- Initbun
- Im.conf
- Tftpupdt.rbt
- Tftpupdt.end
- Script.bat

2. Connect the control (console) port of the unit to a PC.
3. Connect the Ethernet port to the appropriate device where the upload package will be stored.
4. On a Window 2000 or WinXP machine, open a Command Prompt and run the script. (The script will connect to the default 192.168.200.10 IP address). If using Win9x, a TFTP client will be needed.
5. The TFTP process takes about 90 seconds, the unit will reboot automatically when done.

Operating Local Analog Loopback (LAL)—Serial Port Loop

The Local Line Loopback (LAL) applies to serial port data traffic, it does not affect traffic from the Ethernet port. The local Loop test checks the operation of the local Model 3086FR, and is performed separately on each unit. Any data sent to the local Model 3086FR in this test mode will be echoed (returned) to the user device (i.e, characters typed on the key-board of a terminal will appear on the terminal screen).

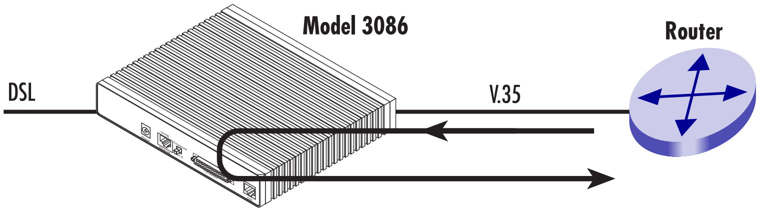


Figure 29. Local Line Loop

To perform a Local Analog Loopback test, follow these steps:

1. Move the front panel toggle switch UP to *Local*.
2. Verify that the data terminal equipment is operating properly and can be used for a test.
3. Perform a V.52 BER (bit error rate) test as described in secton “BIT Error Rate (V.52) Diagnostics” If the BER test equipment indicates no faults, but the data terminal indicates a fault, follow the manufacturer’s checkout procedure for the data terminal. Also check the interface cable between the terminal and the Model 3086FR.

Operating Remote Digital Loopback (RDL)—DSL Loop

The Remote Digital Loopback (RDL) test checks the performance of both the local and remote Model 3086FRs, as well as the communication link between them. Any characters originating at the serial port and sent to the remote Model 3086FR in the test mode will be returned to the originating device (i.e, characters typed on the keyboard of the local terminal will appear on the local terminal screen after having been passed to the remote Model 3086FR and looped back). See Figure 30.

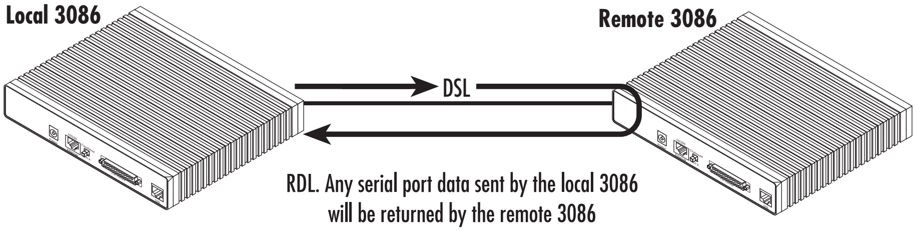

Local 3086
Remote 3086
DSL
RDL. Any serial port data sent by the local 3086
will be returned by the remote 3086

Figure 30. Remote Digital Loop

To perform an RDL test, follow these steps:

1. Activate the RDL by moving the front panel toggle switch DOWN to remote.
2. Perform a bit error test (BERT) using the internal V.52 generator (as described in section "BIT Error Rate (V.52) Diagnostics" on page 144), or using a seperate BER Tester. If the BER test indicates a fault, and the Local Line Loopback test was successful for both Model 3086FRs, you may have a problem with the twisted pair line between the modems. You should then check the twisted pair line for proper connections and continuity.

T1/E1 Diagnostics

The 3086FR/K offers two diagnostics loops for the T1/E1 interface: Network (line) loopback, and local loop, These tests can be activated via the CLI/Web management menus

Network Loop

The Network (line) Loopback applies to the T1/E1 interface data traffic; it does not affect traffic from the Ethernet port. The network Loop test verifies the operation of the T1/E1interface of the local unit and the T1/E1 line. Any data received by the 3086FR T1/E1 interface in this test mode will be echoed (returned) to the originating device. This test is useful when the device connected to the 3086FR's T1/E1 interface is unable to send loop codes to the local 3086FR's T1/E1 CSU/DSU interface.

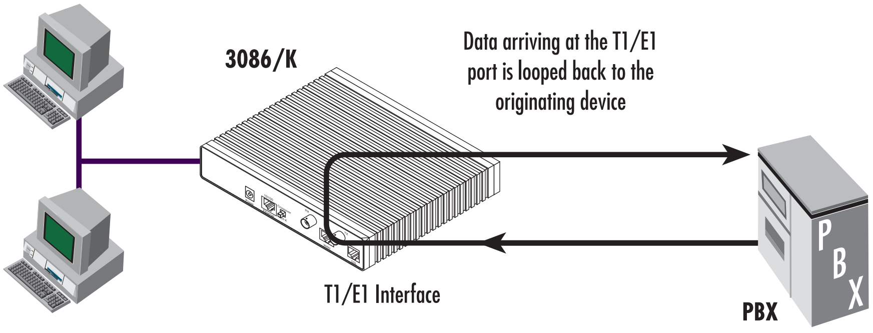
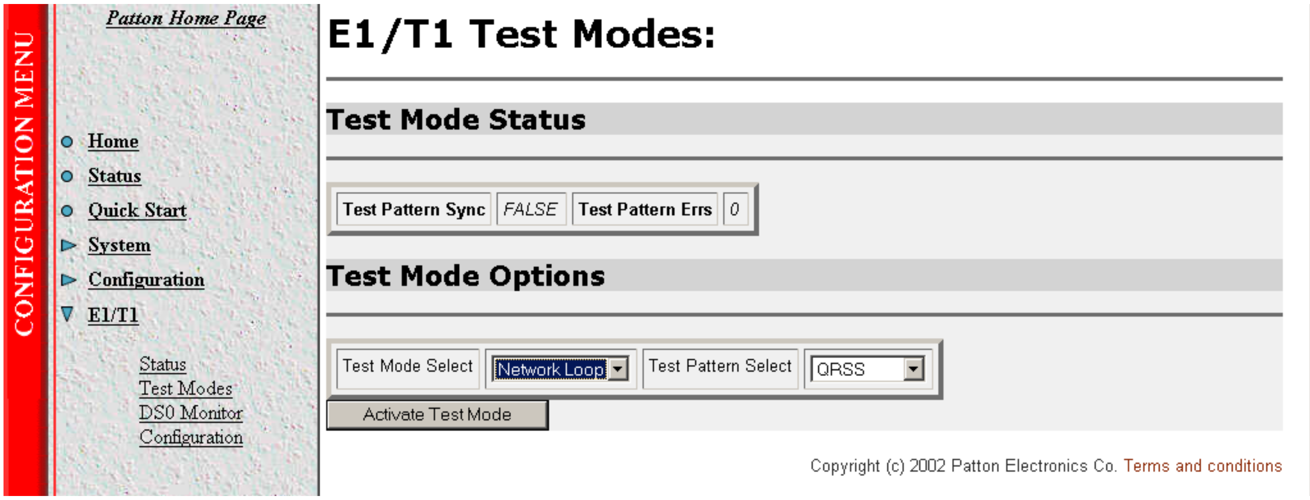


Figure 31. 3086FR Line Loop

To set the 3086FR T1/E1 port in Network Loopback test, do the following:

1. Go to the 3086FR Main page, select *E1/T1*. Next, click on *Test Modes*, select *network Loop* using the drop down menu, click on the **Activate Test Mode** button.
2. Perform a BER (bit error rate) test. Replace the Local T1/E1 equipment (PBX) with a T1/E1 tester, and initiate a BER test to verify integrity of the cable and operation of the 3086FR's T1 interface.



E1/T1 Test Modes:

Test Mode Status

Test Pattern Sync	FALSE	Test Pattern Errs	0

Test Mode Options

Test Mode Select	Network Loop	Test Pattern Select	QRSS

Copyright (c) 2002 Patton Electronics Co. Terms and conditions

T1/E1 Local Loop

When set to local loop, the 3086FR/K loops DSL timeslots assigned to carry T1/E1 data to far end 3086FR or 3096RC T-DACS.

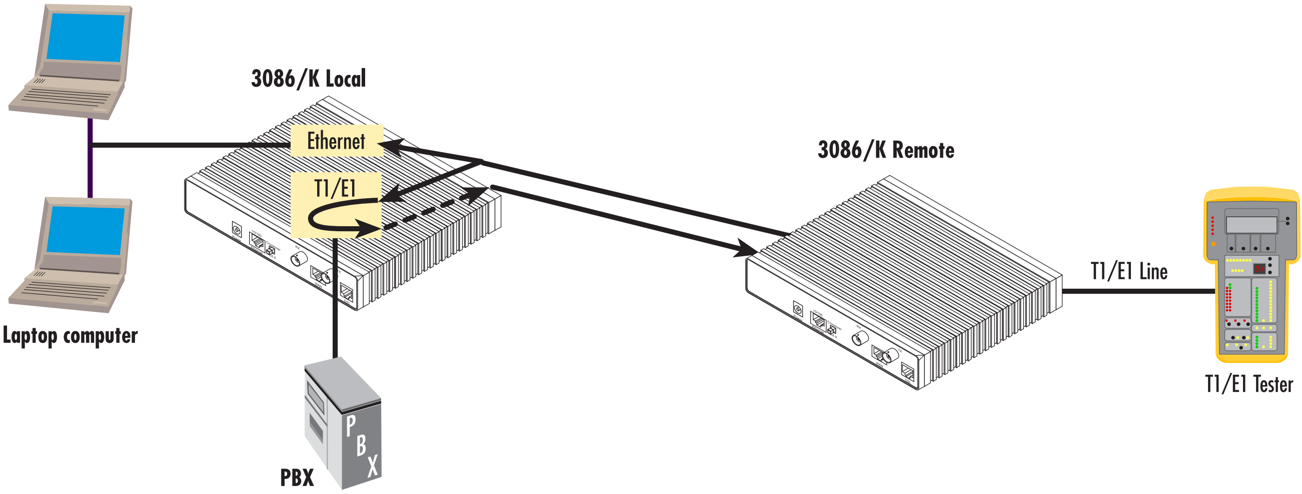


Figure 32. 3086FR/K T1/E1 local loop

To set the 3086FR in T1/E1 local loop test, follow these steps:

1. Go to the 3086FR Main page, select *E1/T1*. Next, click on *Test Modes*, select local Loop using the drop down menu, click on the **Activate Test Mode** button.
2. Perform a BER (bit error rate) test. This test can be initiated from the far end using a T1/E1 BER tester to verify the T1/E1 path over the DSL line and 3086FRs involved.

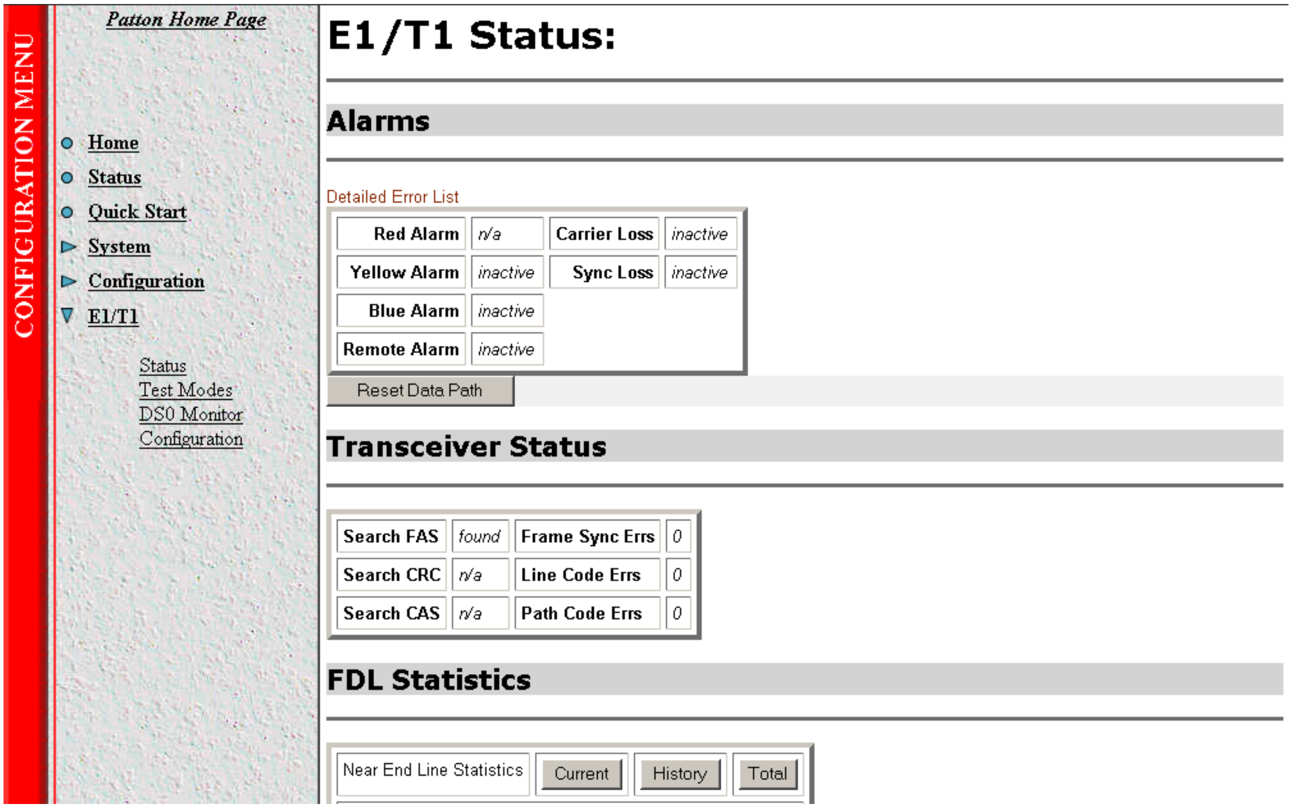
QRSS—BIT Error Rate Diagnostics

The 3086FR/K offers a Bit Error Rate (BER) QRSS test pattern. This test pattern may to be used to test the communication link and the T1/E1 interface of the device attached to the 3086FR. When a QRSS test is invoked, the 3086FR generates a pseudo-random pattern using a mathematical polynomial. The pattern is sent over the T1/E1 interface to the far end device and looped to the 3086FR (originator), the far end device i.e. PBX or routers's T1/E1 port must be set to line loop. The local 3086FR decodes the received bits using the same polynomial. If the received bits match the agreed upon pseudo-random pattern, then the 3086FR and the communication link are functioning properly. The 3086FR can also initiate a built-in QRSS pattern with errors. This test pattern generator injects intentional errors approximately once per second in the transmitted stream.

To perform a BER test, follow these steps:

1. From the Main page T1/E1 option, select the QRSS or QRSS Errs option, and then click on the Activate Test Mode button. This will start the internal test pattern generator for data sent and looped at the far end device.
2. Monitor the BER test results. The Test Mode Status window will display the number of bit errors, if any, detected in the received stream.

Note The above BER tests will not work if the 3086FR's T1/E1 interface has been placed in Network loop.



E1/T1 Status:

Alarms

Detailed Error List

Red Alarm	n/a	Carrier Loss	inactive
Yellow Alarm	inactive	Sync Loss	inactive
Blue Alarm	inactive		
Remote Alarm	inactive		

Transceiver Status

Search FAS	found	Frame Sync Errs	0
Search CRC	n/a	Line Code Errs	0
Search CAS	n/a	Path Code Errs	0

FDL Statistics

Near End Line Statistics

T1/E1 connection Status

The 3086FR E1/T1 status page displays a number of alarms conditions, Transceiver status, and statistics. The information displayed in this page is of use for monitoring and troubleshooting network problems when the 3086FR T1/E1 interface is connected directly to a Telco network

Alarms

The status page shows condition and alarm for the following:

Red Alarm, Yellow alarm, Blue Alarm, Remote Alarm, carrier loss, and Sync Loss.

Transceiver Status.

This section displays status for the following:

Search FAS, Search CRC, Search CAS, Frame Sync errors, Line Code errors, and Path Code errors

FDL statistics (T1 only)

The FDL section provides statistics on T1 link performance, this include Current and historical near end line statistics.

E1/T1 DS0 Monitor

The DS0 monitor page allows monitoring of a particular timeslot in the E1/T1 stream. To enable this feature, click on the *DSO Monitor* link under the E1/T1 menu, and select the desired receive and transmit timeslot.

BIT Error Rate (V.52) Diagnostics

The Model 3086FR offers a V.52 Bit Error Rate (BER) 511 test pattern. This test pattern may be invoked along with the LAL and RDL tests to evaluate the unit(s) and the DSL communication links. When a 511 test is invoked, the 3086FR generates a pseudo-random pattern of 511 bits using a mathematical polynomial. The receiving Model 3086FR then decodes the received bits using the same polynomial.

If the received bits match the agreed upon pseudo-random pattern, then the 3086FR(s) and the communication link(s) are functioning properly. 511 Initiates a built-in 511 bit pseudo-random pattern generator and detector. 511 with Errors Initiates a built-in 511 bit pseudo-random pattern generator and detector. The test pattern generator also injects intentional errors approximately once per second, causing the Error LED to blink.

To perform a V.52 BER test, follow these steps:

1. Locate the toggle switch group on the right side on the front panel and place it in the middle where it is marked “Normal”. This activates the V.52 transmission and reception of the selected test pattern. If there are errors in the received pattern, the error LED will blink accordingly.
2. If the above test indicates no errors are present, move the toggle switch UP to 511/E, activating the BER test with intentional errors. If the test light is working properly, the local modem’s red error LED will blink approximately once per second.

Note The above V.52 BER tests can be used independently of the Remote Digital Loopback tests.

Chapter 14 Contacting Patton for assistance

Chapter contents

Introduction

This chapter contains the following information:

- “Contact information”—describes how to contact PATTON technical support for assistance.
- “Warranty Service and Returned Merchandise Authorizations (RMAs)”—contains information about the RAS warranty and obtaining a return merchandise authorization (RMA).

Contact information

Patton Electronics offers a wide array of free technical services. If you have questions about any of our other products we recommend you begin your search for answers by using our technical knowledge base. Here, we have gathered together many of the more commonly asked questions and compiled them into a searchable database to help you quickly solve your problems.

- Online support—available at **www.patton.com**.
- E-mail support—e-mail sent to **support@patton.com** will be answered within 1 business day
- Telephone support—standard telephone support is available five days a week—from **8:00 am** to **5:00 pm EST** (**1300** to **2200 UTC**)—by calling **+1 (301) 975-1007**

Warranty Service and Returned Merchandise Authorizations (RMAs)

Patton Electronics is an ISO-9001 certified manufacturer and our products are carefully tested before shipment. All of our products are backed by a comprehensive warranty program.

Note If you purchased your equipment from a Patton Electronics reseller, ask your reseller how you should proceed with warranty service. It is often more convenient for you to work with your local reseller to obtain a replacement. Patton services our products no matter how you acquired them.

Warranty coverage

Our products are under warranty to be free from defects, and we will, at our option, repair or replace the product should it fail within one year from the first date of shipment. Our warranty is limited to defects in workmanship or materials, and does not cover customer damage, lightning or power surge damage, abuse, or unauthorized modification.

Out-of-warranty service

Patton services what we sell, no matter how you acquired it, including malfunctioning products that are no longer under warranty. Our products have a flat fee for repairs. Units damaged by lightning or other catastrophes may require replacement.

Returns for credit

Customer satisfaction is important to us, therefore any product may be returned with authorization within 30 days from the shipment date for a full credit of the purchase price. If you have ordered the wrong equipment or you are dissatisfied in any way, please contact us to request an RMA number to accept your return. Patton is not responsible for equipment returned without a Return Authorization.

Return for credit policy

- Less than 30 days: No Charge. Your credit will be issued upon receipt and inspection of the equipment.
- 30 to 60 days: We will add a 20% restocking charge (crediting your account with 80% of the purchase price).
- Over 60 days: Products will be accepted for repairs only.

RMA numbers

RMA numbers are required for all product returns. You can obtain an RMA by doing one of the following:

- Completing a request on the RMA Request page in the *Support* section at **www.patton.com**
- By calling **+1 (301) 975-1000** and speaking to a Technical Support Engineer
- By sending an e-mail to **returns@patton.com**

All returned units must have the RMA number clearly visible on the outside of the shipping container. Please use the original packing material that the device came in or pack the unit securely to avoid damage during shipping.

Shipping instructions

The RMA number should be clearly visible on the address label. Our shipping address is as follows:

Patton Electronics Company
RMA#: xxxx
7622 Rickenbacker Dr.
Gaithersburg, MD 20879-4773 USA

Patton will ship the equipment back to you in the same manner you ship it to us. Patton will pay the return shipping costs.

Appendix A **Compliance information**

Chapter contents

Compliance

EMC

- FCC Part 15, Class A
- EN55022, Class A
- EN55024

Safety

- UL60950-1/CSA C22.2 No. 60950-1
- IEC/EN 60950-1
- AS/NZS 60950-1

PSTN Regulatory

- FCC Part 68
- CS-03
- AS/ACIF S043

Radio and TV Interference (FCC Part 15)

This equipment generates and uses radio frequency energy, and if not installed and used properly—that is, in strict accordance with the manufacturer's instructions—may cause interference to radio and television reception. This equipment has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection from such interference in a commercial installation. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by disconnecting the cables, try to correct the interference by one or more of the following measures: moving the computing equipment away from the receiver, re-orienting the receiving antenna, and/or plugging the receiving equipment into a different AC outlet (such that the computing equipment and receiver are on different branches).

CE Declaration of Conformity

We certify that the apparatus identified in this document conforms to the requirements of Council Directive 1999/5/EC on the approximation of the laws of the member states relating to Radio and Telecommunication Terminal Equipment and the mutual recognition of their conformity.

The safety advice in the documentation accompanying this product shall be obeyed. The conformity to the above directive is indicated by the CE sign on the device.

Authorized European Representative

D R M Green

European Compliance Services Limited.

Avalon House, Marcham Road

Abingdon,

Oxon OX14 1UD, UK

FCC Part 68 (ACTA) Statement

This equipment complies with Part 68 of FCC rules and the requirements adopted by ACTA. On the bottom side of this equipment is a label that contains—among other information—a product identifier in the format ***US: AAAEQ##TXXXX***. If requested, this number must be provided to the telephone company.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA.

This equipment uses a Universal Service Order Code (USOC) jack: RJ-11C.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

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 in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact our company. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Industry Canada Notice

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

This Declaration of Conformity means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction. Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations. Repairs to some certified equipment should be made by an authorized maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the ground connections of the power utility, telephone lines and internal metallic water pipe system, are connected together. This protection may be particularly important in rural areas.

Appendix B Specifications

Chapter contents

General Characteristics

- Compact low-cost plug and play IAD
- 10/100 Ethernet
- Unlimited host support.
- Comprehensive hardware diagnostics, works with any operating system, easy maintenance and effortless installation.
- Plug-and-Play operation for fast and seamless turn-up with pre-configured WAN and LAN options.
- Built-in web configuration.
- Setup allows for standard IP address and unique method for entering an IP address and mask WITHOUT use of a console connection. Default IP address of 192.168.1.1/24.
- Simple software upgrade using FTP into FLASH memory.
- Eight front panel LEDs indicate Power, DSL WAN, Ethernet LAN speed and status.
- Convenient and standard RJ connectors for Ethernet, Line, and Console.
- Field Factory Default Option.
- Standard 1 year warranty.

G.SHDSL Characteristics

- Full duplex 2.3 Mbps speed over 2-wire (in accordance with ETSI/ITU standard G.991.2). 2.3 Mbps to 4.6 Mbps, full duplex, over 2-wire.
- DTE Rates 64 kbps to 2.32 Mbps operation. With nx64 with n=1 support.
- Distance from 24,900 feet (7,590 meters) at 192 kbps to 10,200 feet (3,109 meters) at 2.3 Mbps on 26 AWG (0.4 mm) wire
- Annex A (ANSI), Annex B (ETSI) PSD selection.
- 2 wire or 4 wire support (4-wire support to be keyed) for multiple line codes per ITU G.991.2 and ETSI TS 101524 with G.994.1 Handshake.
- CO and CP modes are supported
- TC-PAM based DSL modulations.
- EOC Management channel for remote end-to-end management.

Ethernet

- Auto-sensing Full-Duplex 10Base-T/100Base-TX Ethernet.
- Standard RJ-45 and built-in MDI-X cross-over switch.
- IEEE 8021.d transparent learning bridge up to 1,024 addresses and Spanning Tree.
- 8 IP address/subnets on Ethernet interface.

Sync Serial Interface

- ITU X.21 or V.35 interface
- Available with Female M34, DB-25, and DB-15 connectors
- User configurable DTE/DCE for X.21

T1/E1 Interface (3086FR/RIK and RIT models only)

- Line Rate 1.544 Mbps (T1), and 2.048 Mbps (E1)
- RJ-48C connector (with optional Dual BNC for RIK version)
- DSX-1 levels for connection to local T1/E1 device (PBX).
- Nx56/64 kbps with full DS0 mapping
- AMI/B8ZS (T1), AMI/HDB3 (E1)
- D4/ESF coding and framing (T1)

64K/G.703 Port (3086FR/RIF Model)

- Line rate 256 kbps
- Data rate 64 kbps
- RJ-48C connector
- AMI Line Coding

Protocol Support

- Complete internetworking with IP (RFC 741), TCP (RFC 793), UDP (RFC 768), ICMP (RFC 950), ARP (RFC 826).
- IP Router with RIP (RFC 1058), RIPv2 (RFC 2453),
- Up to 64 static routes with user selectable priority over RIP/OSPF routes.
- Built-in ping facilities.
- Integrated DHCP Server (RFC 2131). Selectable general IP leases and user specific MAC/IP parings. Selectable lease period.
- DHCP relay agent (RFC 2132/RFC 1542) with 8 individual address pools.
- DNS Relay with primary and secondary Name Server selection.
- NAT (RFC 3022) with Network Address Port Translation (NAPT) for cost-effective sharing of a single DSL connection. Integrated Application Level Gateway with support for over 80 applications.
- NAT MultiNat with 1:1 mapping.
- NAT Many:1.
- NAT Many:Many mapping.
- NAT Port/IP redirection and mapping.

- uPNP controlled device for seamless networked device interconnectivity and Windows XP integration.
- IGMPv2 Proxy support (RFC 2236).
- Frame Relay with Annex A/D/LMI, RFC 1490 MpoFR and FRF.12 Fragmentation.

PPP Support

- Point-to-Point Protocol over HDLC
- PPPoA (RFC 2364) Point-to-Point Protocol over ATM.
- PPPoE (RFC 2516) Client for autonomous network connection. Eliminates the requirement of installing client software on a local PC and allows sharing of the connection across a LAN.
- User configurable PPP PAP (RFC 1661) or CHAP (RFC 1994) authentication.
- PPP BCP (RFC 1638) support for bridged networking support.

ATM Protocols

- Multiprotocol over ATM AAL5 and Multiprotocol Bridged encapsulation RFC 2684 (Formerly RFC 1483) and RFC 1577 Classical IP over ATM. Default RFC-1483 route mode. Logical Link Control (LLC)/ Subnetwork Access Protocol (SNAP) encapsulation. Default VC mux mode.
- ATM UNI 3.0, 3.1, and 4.0 signaling ATM QoS with UBR, CBR, nrt-VBR, and rt-VBR and per-VC queuing and shaping. IISP V.1.0 Q.2931 UNI L3 and Q.2971 UNI L3 support.
- LAN Emulation Client (LEC) V.1 with LEC via PVC or ILMI connection.
- Peak cell rate shaping on a per-VCC basis up to 32 active VCCs across VPI 0-255, VCI 0-65525. Single default PVC: 8/35 with PCR=5,500 cells.
- I.610 OAM network management including AIS/RDI, loop-back and performance monitoring.
- Enhanced ILMI 4.0 for auto-configuration of ATM PVCs.

Management

- User selectable ATM, PPP, or Frame Relay WAN datalink connection.
- Web-Based configuration via embedded web server
- CLI menu for configuration, management, and diagnostics.
- Local/Remote CLI (VT-100 or Telnet).
- SNMPv1 (RFC 1157) MIB II (RFC 1213)
- Quick Start Setup runs through common options to simplify circuit turn-up.
- Logging via SYSLOG, and VT-100 console. Console port set at 9600 bps 8/N/1 settings no flow control.
- EOC access for End-To-End management, configuration, and control.

Security

- Packet filtering firewall for controlled access to and from LAN/WAN. Support for 255 rules in 32 filter sets. 16 individual connection profiles.
- DoS Detection/protection. Intrusion detection, Logging of session, blocking and intrusion events and Real-Time alerts. Logging or SMTP on event.
- Password protected system management with a username/password for console and virtual terminal. Separate user selectable passwords for SNMP RO/RW strings.
- Access list determining up to 5 hosts/networks which are allowed to access management system SNMP/ HTTP/TELNET.
- Logging or SMTP on events: POST, POST errors, line/DSL, PPP/DHCP, IP.

Compliance Standard Requirements

- FCC part 15 Class A (US EMC)
- CE per RTTE 99/5/EC (EMC & LVD)
- FCC Part 68 (– US Permission to connect)
- CTR 12 & CTR 13
- IC-CS03 (Canadian Permission to connect)
- Safety – EN60950

Australia Specific

- TS016 (E1 Telecom)
- AZ/NZS 3260 Safety)
- AZ/NZS 35-48 EMC

Dimensions

1.58H x 4.16W x 3.75D in. (10.6H x 4.1W x 8.8D cm)

Power and Power Supply Specifications

The 3086FR may come with either an AC or DC power supply.

AC universal power supply

The Model 3086FR offers internal or external AC power supply options.

- The internal power supply connects to an AC source via an IEC-320 connector (100–240 VAC, 200 mA, 50/60 Hz)
- The external power supply connects to an external source providing +5 VDC via a barrel-type connector

48 VDC power supply

- Rated voltage and current: 36–60 VDC, 400 mA

- Fuse rating: 250 Volts, 400 mA, time delay

CAUTION

Connect the equipment to a 36–60 VDC source that is electrically isolated from the AC source. The 36–60 VDC source is to be reliably connected to earth.

Appendix C **Cable Recommendations**

Chapter contents

DSL Cable

10 foot (3 m), RJ-11/RJ-11 (refer to "RJ-11 non-shielded port" on page 162)

Ethernet Cable

Ethernet cable (P/N 10-2500) (refer to "RJ-45 shielded 10/100 Ethernet port" on page 162)

Adapter

EIA-561 to DB-9 (P/N 16F-561) (refer to "RJ-45 non-shielded RS-232 console port (EIA-561)" on page 162)

Appendix D **Physical Connectors**

Chapter contents

RJ-45 shielded 10/100 Ethernet port

Assuming the MDI-X switch is in the out position.

Pin No.	Signal Direction	Signal Name
1	Output	TX+
2	Output	TX-
3	Input	RX+
4		
5		
6	Input	RX-
7		
8		

RJ-11 non-shielded port

Single twisted-pair (TP) for full-duplex transmission. The signals are not polarity sensitive.

Pin No.	Signal Direction	Signal Name
1		
2	In/Out	Tip
3	In/Out	Ring
4		

RJ-45 non-shielded RS-232 console port (EIA-561)

Pin No.	Signal Direction	Signal Name
1	Out	DSR
2	Out	CD
3	In	DTR
4	–	Signal Ground
5	Out	RD
6	In	TD
7	Out	CTS
8	In	RTS

Serial port

V.35 (M/34 Connector)

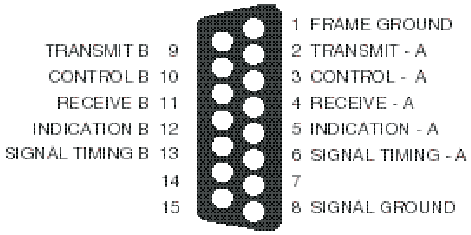
Pin #	Signal
A	GND (Earth Ground/Shield)
B	SGND (Signal Ground)
D	CTS (DCE Source)
E	DSR (DCE Source, Always On)
F	CD (DCE Source)
L	LL (Local Loop, DTE Source)
M	TM (Test Mode Indicator, DCE Source)
N	RL (Remote Loop, DTE Source)
P	TD (Transmit Data +, DTE Source)
R	RD (Receive Data +, DCE Source)
S	TD/ (Transmit Data -, DTE Source)
T	RD/ (Receive Data -, DCE Source)
U	XTC (Transmit Clock +, DTE Source)
V	RC (Receiver Clock +, DCE Source)
W	XTC/ (Transmit Clock -, DCE Source)
X	RC/ (Receiver Clock -, DCE Source)
Y	TC (Transmitter Clock +, DTE Source)
AA	TC/ (Transmitter Clock -, DTE Source)
KK	Aux. Power Input (+5VDC @ 300mA)

V.35 (DB-25 Female Connector)

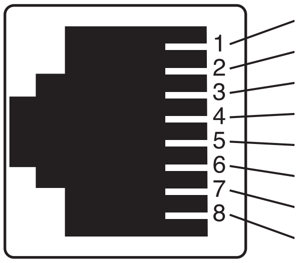
Pin #	Signal
1	FG (FrameGround)
2	TD (Transmit Data-A, DTE Source)
3	RD (Receive Data-A, DCE Source)
4	RTS (Request to Send-A, DTE Source)
5	CTS (Clear to Send-A, DCE Source)
6	DSR (Data Set Ready-A, DCE Source)
7	SGND (Signal Ground)
8	CD (Carrier Detect-A, DCE Source)
9	RC/ (Receiver Clock-B, DCE Source)
10	CD/ (Carrier Detect-B, DCE Source)
11	XTC/(External Transmitter Clock-B, DTE Source)
12	TC/(Transmitter Clock-B, DTE Source)
13	CTS/(Clear to Send-B, DCE Source)

Pin #	Signal
14	TD/(Transmit Data-A, DTE Source)
15	TC(Transmitter Clock-B, DCE Source)
16	RD (Receive Data-A, DCE Source)
17	RC (Receiver Clock-A, DCE Source)
18	LL (Local LIne Loop)
19	RTS/(Request to Send-B, DTE Source)
20	DTR (Data Terminal Ready-A, DTE Source)
21	RL (Remote Loopback)
22	DSR/ (Data Set Ready-B, DCE Source)
23	DTR/(Data Terminal Ready-B, DTE Source)
24	XTC (External Transmitter Clock-A, DTE Source)
25	TM (Test Mode)

X.21 (DB-15 Connector)



E1/T1 (RJ-48C Connector)



Power input

IEC 320 connector (two prong).

Appendix E Command Line Interface (CLI) Operation

Chapter contents

Introduction

The modem configuration and status can also be view and modified through the console, which is accessible through the RS-232 serial port or through a Telnet session over Ethernet.

CLI Terminology

In order to use the CLI commands, you need to understand the following CLI terms:

- Transport: A transport is a layer 2 session and everything below it. You can create a transport and attach it to a bridge or router so that data can be bridged or routed via the attached transport. The CLI supports the following transports:
- PPPoA: Point-to-Point Protocol over ATM
- PPPoE: Point-to-Point Protocol over Ethernet
- Frame Relay
- RFC1483
- IPoA: IP over ATM
- PPPoH: Point-to-Point over HDLC
- Ethernet
- Interface: bridges and routers both have interfaces. A single transport is attached to a bridge or router via an interface.
- Object: an object is anything that you can create and manipulate as a single entity, for example, interfaces, transports, static routes and NAT rules.
- List: Objects are numbered entries in a list. For example, if you have created more than one ethernet transport, the following command:

  ethernet list transports

produces a list of numbered transport objects:

```
ID Name Port

1 eth2 ethernet

2 eth1 ethernet
```

Local (VT-100 emulation)

A connection is made with the DB9-RJ45 adapter and an RJ45-RJ45 straight-through cable. Set the data rate to 9,600 baud, 8 data bits, one stop bits, and no parity. You may use a dumb terminal or a VT-100 emulation such as HyperTerminal.

Remote (Telnet)

Establishing a Telnet session displays the same CLI configuration and status parameters on the display.

Using the Console

The console commands needed for the various modes of operation are described in later sections. In this subsection are the most basic commands needed for console operation.

By entering “?” all the high level commands (the keywords) are seen.

By entering a keyword followed by a space and “?” the options available will print immediately without pressing enter. The previously entered commands are reprinted on the next lines. For example:

```
Æ  ethernet ?[After typing the “?” you will not see the “?”]
    add
    delete
    set
    show
    list
    clear
Æ  ethernet
```

Then you may enter one of the keywords on the displayed list followed by a space and “?”

To continue our example:

```
Æ  ethernet list ?
    ports
    transports
Æ  ethernet list
```

Then

```
Æ  ethernet list transports ?
Æ  ethernet list transports   <enter>

    Ethernet transports:
     ID  |    Name    |    Port
    -----|------------|------------
       1 | eth1       | ethernet
    -------------------------------
Æ
```

Another example shows when the user must provide a parameter.

```
Æ  ip ?
    list
    clear
    add
    delete
    set
    attach
    attachbridge
    detach
    show
    interface
    ping
Æ  ip interface ?
    <name>
```

The <name> of the interface. In this instance the interface name is ip1. It is important that you do the “?” inquiry to determine whether additional parameters follow.

```
Æ  ip interface ip1 ?
    add
    delete
```

```
          clear
          list
      Æ  ip interface ip1 list ?
          secondaryipaddresses
      Æ  ip interface ip1 list secondaryipaddresses ?
     ip interface ip1 list secondaryipaddresses   <enter>

     Secondary IP addresses for interface: ip1
      ID  |    IP Address
     -----|-----------------
     -----------------------
```

In this example there was not a secondary IP address. Now save the entire configuration in nonvolatile FLASH memory with the following command.

```
      Æ  system config save
```

Wait for the message that says “Configuration Saved”, then reboot the modem with this command.

```
      Æ  system restart
```

Administering user accounts

As admin user you can administer user accounts. This section summarizes the CLI commands which can be used to administer user accounts.

Adding new users

To add a new user username, use the command: *system add user < username >* `<“Comment”>`

```
system add login user < username > <“Comment”>
```

The first command creates a user who can access the system via a dialin connection using PPP for example. The second command creates a user who can login to the system.

For example, the commands:

```
system add user fred “user with dialin access”

system add login joe “user with login access”
```

creates two new users called fred and joe. The accounts are created with no passwords. To view details about the new users, enter:

```
system list users
```

The following information is returned:

```
Users:
May May Access
  ID | Name   | Conf.    | Dialin   | Level     | Comment
-----|--------|----------|----------|-----------|------------------------
   1 | fred   | disabled | ENABLED  | default   | user with dialin access
   2 | joe    | ENABLED  | disabled | default   | user with login access
   3 | admin  | ENABLED  | disabled | superuser | Default admin user
------------------------------------------------------------------------
```

Setting user passwords

To change the password for the user you are currently logged in as, use the command:

```
user password
```

Enter the new password twice as prompted:

```
Enter new password: ***
Again to verify: ***
fi
```

Note No check is made for any current password which may have been set for the user.

If you wish to change the password for another user, enter the command:

```
user change <username>
```

This command logs you into the system as another user. You can then use the user password command to change the password for this user.

Note Changing to another user means that you lose all superuser privileges.

Note Only superusers can use the user change command.

Changing user settings

To change any of the default settings for a user, use the following commands. For example, to change the settings for user fred:

```
system set user fred access {default|engineer|superuser}
system set user fred maydialin {enabled|disabled}
system set user fred mayconfigure {enabled|disabled}
```

For example, to change the security level for fred, enter:

```
system set user fred access engineer
```

Note Only superusers can use the user change command.

Controlling login access

To set user login access for user username, use the command (all on one line):

```
system set login < username > access {default|engineer|superuser}
```

Controlling user access

To set user access for user username, use the command (all on one line):

```
system set user < username > access {default|engineer|superuser}
```

G.SHDSL Commands:

Command format: ‘gshdsl Action Attribute Value’

- Action – Two types of actions are available: ‘set’ or ‘show’
- Set – set attributes with a value.
- Show – get information from the box
- Attribute – The name of the attributes to access.
- Value – The new value for the attribute (Set command only)

Example: To read the attribute 'Version': `gshdsl show Version`

To set data rate to 256K (4 * 64K): `gshdsl set DSLRateTS`

To set terminal type to CPE mode: `gshdsl set terminal remote`

To show the current terminal type: `gshdsl show terminal`

Attribute	Type	Value	Description
Version	RO	-	The version number of the DSL driver
Platform	RO	-	The platform name of the unit e.g. 3086FR or 3086FR
ModemState	RO	Idle Deactivated Norm Oper In-Progress	Show the state of the handshaking process: Idle – The DSL chip is in idle state Deactivated – The DSL chip is deactivated Normal Operation – The DSL chip is in operating (Link established) In-Progress – Handshaking in process
DSLRateTS	RW	3-36	Data rate N number N=3-36. e.g. 256K data rate is N=4. The composite data rate is the chosen number N times 64 kbps. E.g., 32 x 64 kbps = 2.048 Mbps.
DataRateI	RW	0-7	This attribute controls the size of the overhead channel. Valid input is 0-7. Default value is 0. (!!Keep it as 0)
terminal	RW	Central Remote	Central – CO unit Remote – CPE unit
Interface	RW	Hdlc	Utopia – Data will be packaged in ATM cell format and send through the UTOPIA interface of the processor Hdlc – Data will be packaged in HDLC frame and send through the PCM Bus
Action	WO	Start Deactivate	Start – Command the box to configure the DSL chip and start the handshaking process Deactivate – Command the box to disconnect and deactivate the DSL link.

To establish the DSL link

1. One unit needs to be set to CO (central) and the other unit as CP (remote)

2. The Data rate of the 2 units have to be the same (DatarateN)

3. The interface type needs to be the same to pass data (Interface)

4. Issue the 'Action' command to start the handshaking process (Action Start)

Example: To set up the units to run at 2.048Mbps using ATM interface.

For CO (central) unit

fi `gshdsl set terminal central`

fi `gshdsl set interface utopia`

fi `gshdsl set dataRateN 32`

fi `gshdsl set dataRateI 0`

fi `gshdsl set Action Start`

For CPE (remote) unit

fi `gshdsl set terminal remote`

fi `gshdsl set interface utopia`

fi `gshdsl set dataRateN 32`

fi `gshdsl set dataRateI 0`

fi `gshdsl set Action Start`

Default Setting of the unit

Terminal:	Remote
Interface:	Hdlc
DataRateN:	24
DataRateI:	0