**For Quick Start Installation**
see page 21

PATTON Electronics Co.

# *Model 3201 and Model 3241*
# G.SHDSL Router Modems

## *User Guide*


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

Document Number: **033211U Rev. A**
Part Number: **07M3201**
Revised: **February 7, 2003**

**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
url: www.patton.com
e-mail: support@patton.com

# Contents

# Compliance Information

## Radio and TV Interference

The Model 3201 or 3241 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. The Models 3201 and 3241 have been tested and found to comply with the limits for a Class A computing device in accordance with 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 Model 3201 or 3241 does cause interference to radio or television reception, which can be determined by disconnecting the unit, the user is encouraged to 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 Notice

The CE symbol on your Patton Electronics equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU). A Certificate of Compliance is available by contacting Technical Support.

## FCC Part 68


The Model 3201 is not intended to be connected to the public telephone network.

1. You are required to request service from the telephone company before you connect the Model 3201 or 3241 to a network. When you request service, you must provide the telephone company with the following data.

   — The required Universal Service Order code (USOC) jack: RJ-11C

   — The make, model number, Ringer Equivalence Number (REN), and FCC Registration number of the Model 3201 or 3241.

   The REN helps you determine the number of devices you can connect to your telephone line and still have all of those devices ring when your number is called. In most, but not all, areas, the sum of the RENs of all devices should not exceed five (5.0). To be certain of the number of devices you can connect to your line, you should call your local telephone company to determine the maximum REN.

   — The Facility Interface Code: **02LS2**

   — The Service Order Code(s) (SOC): **9.0F**

   — REN No.: **0.2**

2. Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. The telephone company will notify in advance of such changes to give you an opportunity to maintain uninterrupted telephone service.

3. If your Model 3201 or 3241 causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible and will be informed of your right to file a complaint with the FCC.
4. If you experience trouble with the Model 3201 or 3241, please contact Patton Electronics Company for service or repairs. Repairs should be performed only by Patton Electronics Co.
5. You are required to notify the telephone company when you disconnect the Model 3201 or 3241 from the network.

## Industry Canada Notice

**Note** 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.

## Service

All warranty and non-warranty repairs must be returned freight prepaid and insured to Patton Electronics. All returns must have a Return Materials Authorization number on the outside of the shipping container. This number may be obtained from Patton Electronics Technical Services at:

- Tel: **+1 (301) 975-1007**
- Email: **support@patton.com**
- URL: **http://www.patton.com**

**Note** Packages received without an RMA number will not be accepted.

# About this guide

This guide describes installing and configuring a Patton Electronics Model 3201 or 3241 G.SHDSL Router modem. The instructions in this guide are based on the following assumptions:

- The router modem will connect to another router modem or DSLAM
- There is a LAN connected to the Ethernet port of the router modem
- Users will be connected to remote router modems

## 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 router modem features and capabilities
- Chapter 2 contains an overview describing router modem operation
- Chapter 3 provides quick start installation procedures
- Chapter 4 describes configuring the router modem for typical applications
- Chapter 5 describes configuring the router modem for specialized applications
- Chapter 6 describes configuring security for the router modem
- Chapter 7 describes configuring for network address translation (NAT)
- Chapter 8 contains definitions for the LED status indicators
- Chapter 9 describes router modem diagnostics
- Appendix A contains specifications for the router modems
- Appendix B provides cable recommendations
- Appendix C describes the router modem's ports
- Appendix D describes how to use the command line interface (CLI)

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

## Precautions

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

**Note** Calls attention to important information.


**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.**


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


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.


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

## Factory default parameters

The **Model 3201/R** G.SHDSL router modem has the following factory default parameters.

- Ethernet IP address: 192.168.200.10/24
- WAN Connection: PPPoH Routed
- WAN IP address: 10.1.1.1
- Autonegotiate the G.SHDSL speed.

The **Models 3201/I/CP** and **3201/I/CO** bridge modems have the following factory default parameters.

- Ethernet IP Address:
  - 192.168.200.10 (for the CP version)
  - 192.168.200.11 (for the CO version)
- Autonegotiate the G.SHDSL speed.

# 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 |
|---|---|
| **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 3201/3241 G.SHDSL Router Modem overview

The Patton Models 3201 and 3241 router modems are G.SHDSL routers/bridges for delivering basic and advanced IP services from the wide-area network to a local 10/100Base-T Ethernet LAN.

G.SHDSL offers an alternative, standards based DSL transmission medium. It offers connection speeds of 2.3 Mbps (Model 3201) or 4.6 Mbps (Model 3241) in each direction over a single twisted-pair (TP). Supporting 100 or more users, the router modems are optimized for users in a small office, as an enterprise tele-working solution or for multimedia high-speed Internet access. Local and remote web-based management ensures easy setup and continuous trouble-free operation.

The following sections describe Model 3201 and 3241 features and capabilities:



## General attributes

- Compact low-cost plug-and-play router
- 10/100 Ethernet
- Comprehensive hardware diagnostics, works with any operating system, easy maintenance and effortless installation.
- Built-in web configuration.
- 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.

## G.SHDSL Characteristics (Models 3201 and 3241)

- 2.3 Mbps (Model 3201) or 4.6 Mbps (Model 3241) speed over 2 wires.
- DTE rates:
  - Model 3201: 144 kbps to 2.32 Mbps, nx64k with n=3 to 36
  - Model 3241: 144 kbps to 4.6 Mbps, nxz64k n=3 to 72.
- Distance from 24,900 feet (7,589 m) at 144kbps (192 kbps line rate) to 10,200 feet (3,109 m) at 2.3 mbps on 26 AWG (0.4 mm) wire
- CO and CP modes supported
- 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.

### 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.

### Management

- User selectable ATM, PPP, or HDLC 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)
- 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.
- DoS Detection/protection.
- Password protected system.
- Access list for 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

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


Figure 1. Model 3201

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

- Power
- WAN Link, Tx, and Rx
- Ethernet Link, 100M, Tx, and Rx

Table 3. Status LED descriptions

| | | | |
|---|---|---|---|
| **Power** | Yellow | | *ON* indicates that power is applied. *Off* indicates that no power is applied.<br>*2 Hz flash* occurs during POST<br>*1 Hz flash* occurs for non-fatal error.<br>*8 Hz flash* on **all LEDs** for fatal POST outcome or critical error. |
| **WAN (DSL)** | Link | Yellow | *Solid yellow:* connected<br>*2 Hz flash:* training<br>*8 Hz flash:* DSL error<br>*No indication:* no signal detected. |
| | TX | Yellow | *Flashing:* when transmitting data from the unit to the WAN. |
| | RX | Yellow | *Flashing:* when receiving data from the WAN to the unit. |
| **Ethernet** | Link | Yellow | *On:* Ethernet is linked. |
| | 100M | Yellow | *On:* 100 Mbps Ethernet is selected. |
| | TX | Yellow | *Flashing:* when data is transmitted from the unit to the LAN. |
| | RX | Yellow | *Flashing:* when data is received from the LAN. |

### *Rear panel connectors and switches*

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

- Power input connector
- Console Port
- Ethernet connector
- MDI-X switch
- Line connector

## Power input connector

The router modem comes with an AC or DC power supply. (see "Power and Power Supply Specifications" on page 117)

- The power connection to the router modem is a 2.5 mm barrel receptacle with the center conductor positive (see figure 2).
- 5 VDC, 1 A

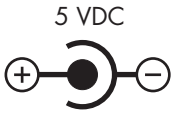



Figure 2. Power connection barrel receptacle 5 VDC diagram

### *External AC universal power supply*

For additonal specifications, see "Power and Power Supply Specifications" on page 117.

- Output from power supply: 5 VDC, 2 A
- Input to power supply: universal input 100–240 VAC 50/60 Hz 0.3A

CAUTION

An approved external power supply that incorporates a disconnect device must be used and positioned within easy reach of the operator's position.

CAUTION

Connect the equipment to a 5 VDC source that is electrically isolated from the AC source. The 5 VDC source is to be reliably connected to earth.

### *External 48 VDC power supply*

Refer to see "Power and Power Supply Specifications" on page 117 for additonal specifications.

- Input
  - Rated voltage: 36–60 VDC
  - Rated current: 0.25 A DC
  - 3-pin locking connector, 3.5 mm pitch
  - Transient over-voltage protection, 100VDC at 2 ms
- Output
  - Rated voltage: 5 VDC ± 5%, 5W
  - Rated current; 1 A DC
  - 6-inch cable terminated with 2.5 mm barrel plug, center positive

CAUTION

Connect the equipment to a 30–60 VDC source that is electrically isolated from the AC source. The 30–60 VDC source is to be reliably connected to earth.

### 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 |

### 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 3201 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 3201 modem operates as a bridge or a router and has two 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 modem

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

When configuring the 3201, questions must be answered so the 3201 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, Frame Relay, PPPoE or another?

These decisions can be made and implemented more easily if the Model 3201's fundamental architecture is understood. Also, while configuring the Model 3201 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*, *PPPoE*, *Frame Relay*, *RFC 1483* (Multiprotocol Encapsulation over ATM AAL5), *IPoA*, *PPPoH*, and *Ethernet*.

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 3201 via CLI commands through the RS-232 control port, it must be done manually.

Model 3201 modems can connect over an ATM PVC or HDLC 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.

Several ATM connections are offered to address a variety of user applications. Although they all use RFC1483 as the transport mechanism between the two 3201 modems, WAN services may use different PPP applications, such as *PPPoE routed*, *PPPoA routed*, or *PPPoA bridged*. Each one has its advantages and disadvantages.

## Applications Overview

The Model 3201 is used for bridged or routed applications.

**Note** In bridged applications the 3201 modem functions transparently on layer 2 to provide MAC level bridging for Ethernet networks. The bridging is between Ethernet and the DSL link between the two 3201 modems. The devices attached to each 3201 are on the same subnet. The number of attached devices and the size of the filter table are configurable. No IP address is necessary unless

the administrator desires management through a web browser. Then an IP address is necessary for the administrator to access the 3201 modem.

In a **typical bridged configuration**, the DSL bridge is transparent to the network. It bridges the DSL line to the Ethernet line, making both sides appear as a single subnet. However, it may still be beneficial to provide an IP address to the DSL modem for management. In the bridged configuration it is not necessary for the Ethernet port to have an IP address.

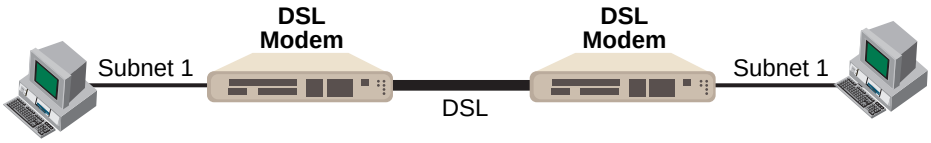



Figure 3. Bridged Application

In a **typical routed configuration**, the DSL router is treated as a separate device on the network that receives packets from the PC and DSLAM. The Ethernet and DSL networks are configured as separate IP subnets. The PC must have the DSL router set up as its default gateway.

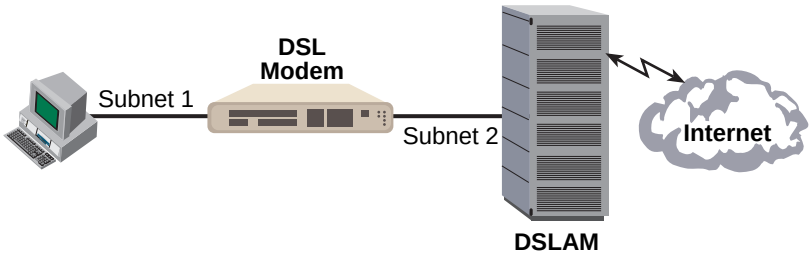



Figure 4. Routed Application

Model 3201 applications are divided as follows:

- Connecting two stand-alone Model 3201 Bridge/Routers back-to-back using *PPPoH Bridged* or *PPPoH Routed*. PPPoH Bridged can be considered as Ethernet extension since the same logical LAN exists at both ends of the 3201s and only bridging is required. PPPoH is network extension in the more general sense since a different logical network is on each end of the 3201s.
- Connecting the Model 3201 bridge/routers as a CPE device to a DSLAM. They can be configured for bridged or routed mode.
  - The bridged modes commonly used to connect to a DSLAM are RFC1483, HDLC (PPPoH), and PPPoA.
  - The routed modes are *RFC1483*, *HDLC* (PPPoH), *PPPoA*, *IPoA* and *PPPoE*.

For more information about router modem applications, refer to Chapter 4, “Basic Application Configurations” on page 27 and Chapter 5, “Specialized Configurations” on page 79.

# Chapter 3 **Quick Start Installation**

## *Chapter contents*

# Hardware installation

If you are already familiar with Model 3201/3241 Router Modem installation and configuration, this chapter will enable you to finsh 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 “Identify the connectors and attach the cables”)
- Changing the IP address from the factory default setting (see section “IP address Quick Start modification” on page 23)
- Launching a web browser in preparation for configuring the modem (see “Web Operation and Configuration” on page 24)

## What you will need

- Model 3201 or 3241 G.SHDSL Router Modem
- External power supply for Model 3201 or 3241 (included)
- Ethernet cable with RJ45 plugs on each end (included)
- DB9-RJ45 Adapter (included)
- RJ45/RJ45 straight-through cable for connecting to control port (included)
- PC computer with HyperTerminal or equivalent VT-100 emulation program, or an ASCII (“dumb”) terminal.

## Identify the connectors and attach the cables

All connectors are on the rear panel of the DiamondLink with the exception of the power connection. The Console port is Red, the Ethernet port is Green, and the Line is Yellow.

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 modem.
2. Do NOT connect the router modem 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. Power up the router modem.
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 command’s parameters may be seen by entering the command followed by a space and a question mark.

```
→ 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 192.168.200.10 (for the CP units) or 192.168.200.11 (for CO units) to your selected IP address. Follow these steps. Comments are in brackets […].

```
→ 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>
    ------------------------------------------------------------------------
```

→ `ip set interface ip1 ipaddress 10.10.10.5 255.255.255.0` [Sets the new IP address which you have selected. The IP address in this example is for illustrative purposes only.]

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

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

```
    Wait for  configuration saved  message

    Saving configuration
→

    Configuration saved.
    <enter>
→
```

The IP address has now been successfully changed.

### *Router/Bridge Status LEDs*

The LEDs indicate the status of power, the WAN (DSL) inter-modem link, and the Ethernet connection.

**Note** When extinguished, the LED indicators are clear; when lit, they shine a brilliant yellow.

| | | | |
|---|---|---|---|
| **Power** | Yellow | | *ON* indicates that power is applied.<br>*off* indicates that no power is applied.<br>*2 Hz flash* occurs during POST<br>*1 Hz flash* occurs for non-fatal error.<br>*8 Hz flash* on **all LEDs** for fatal POST outcome or critical error. |
| **WAN (DSL)** | Link | Yellow | *Solid yellow:* connected<br>*2 Hz flash:* training<br>*8 Hz flash:* DSL error<br>*No indication:* no signal detected. |
| | TX | Yellow | *Flashing:* when transmitting data from the unit to the WAN. |
| | RX | Yellow | *Flashing:* when receiving data from the WAN to the unit. |
| **Ethernet** | Link | Yellow | *On:* Ethernet is linked. |
| | 100M | Yellow | *On:* 100 Mbps Ethernet is selected. |
| | TX | Yellow | *Flashing:* when data is transmitted from the unit to the LAN. |
| | RX | Yellow | *Flashing:* when data is received from the LAN. |

## 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 3201, 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 3201's IP address into the URL or Address field of the browser.

The Model 3201 home page displays (see Figure 5).

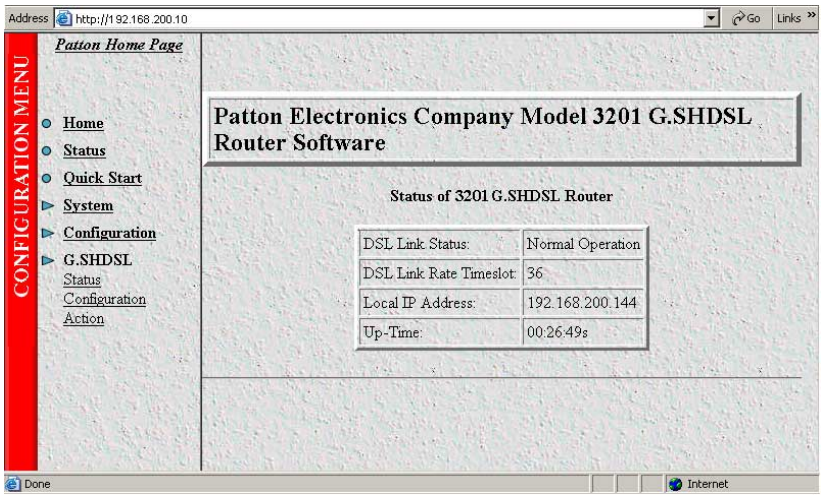



Figure 5. Model 3201 home page

The Model 3201/3241 menu structure is shown in figure 6 on page 26.

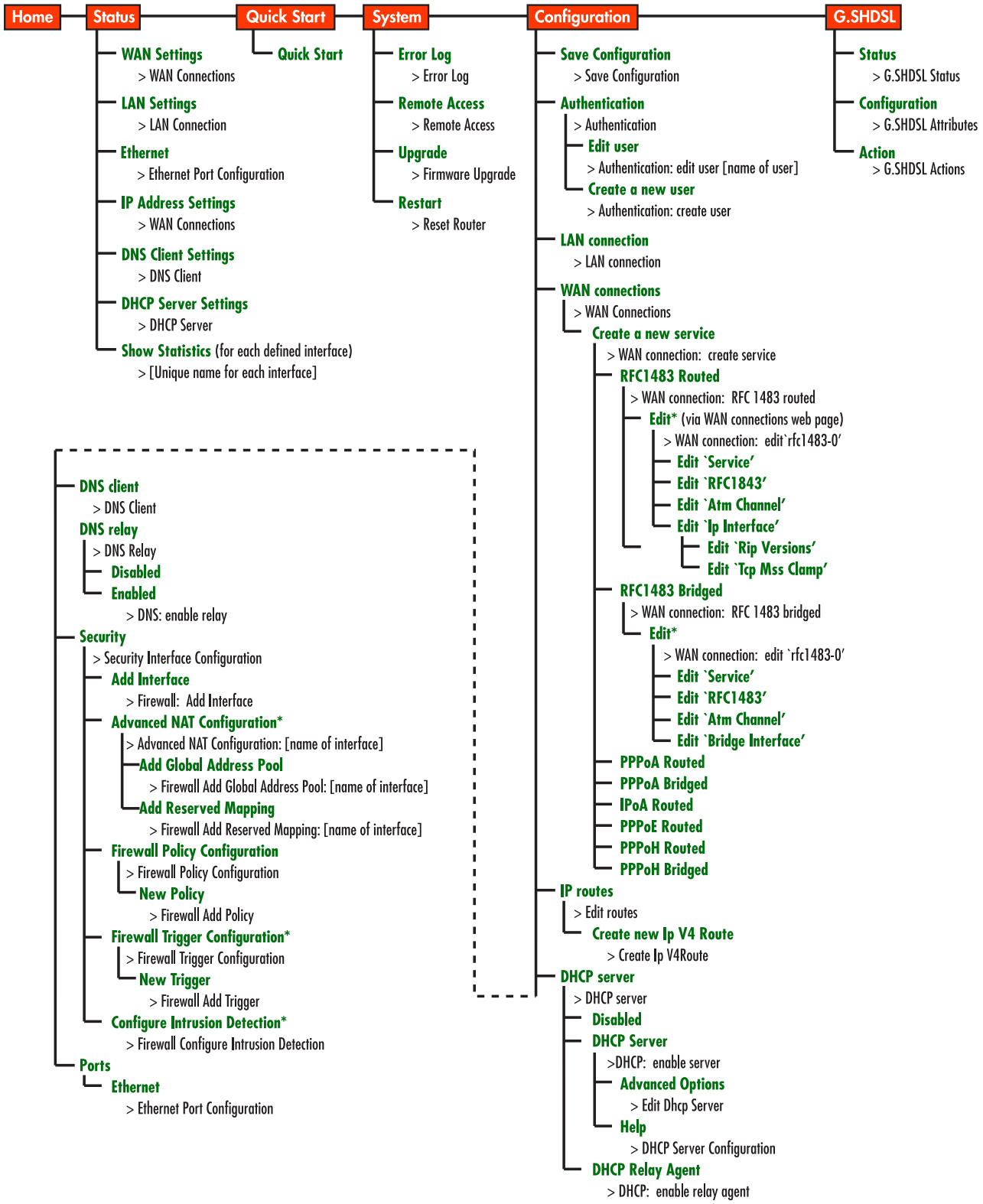



Figure 6. Model 3201/3241 Menu Structure

# Chapter 4 Basic Application Configurations

## *Chapter contents*

## Introduction

The basic applications are divided according to whether the application is bridged or routed.

The bridged applications are *RFC 1483 Bridged*, *PPPoA Bridged*, and *HDLC Bridged*.

The routed applications are *RFC 1483*, *PPPoA*, *IPoA*, *PPPoE*, and *HDLC*.

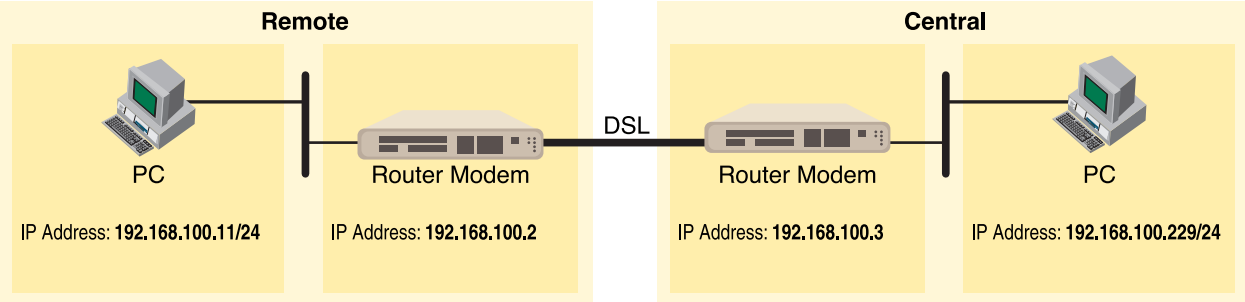
Another way of organizing the applications is according to the type of encapsulation: *PPP*, *RFC 1483*, or *Frame Relay*. PPP encapsulation is available as *PPPoA bridged* or *routed* and *PPPoE*. RFC 1483 and Frame Relay can be configured for bridged and routed connections.

The following table shows the parameters that can be configured via the HTTP server using a web browser.

| | Routed WAN Services | | | | | Bridged WAN Services | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Web Page Parameter** | **RFC 1483** | **PPPoA** | **IPoA** | **PPPoE** | **PPPoH** | **RFC 1483** | **PPPoA** | **PPPoH** | **Comments** |
| Description | X | X | X | X | X | X | X | X | |
| VPI | X | X | X | X | | X | X | | default = 0 |
| VCI | X | X | X | X | | X | X | | default = 35 |
| Encapsulation | LLC | | | VcMux | | LLC | | | LLC or VcMux |
| Use DHCP | X | | X | | X | | | | |
| WAN IP address | X | | X | | X | | | | default mask = 255.255.255.0 |
| LLC header | | | | X | | | | | |
| HDLC header | | | | | ON | | | ON | |
| No authentication | | X | | X | | | X | | |
| PAP | | X | | X | | | X | | |
| CHAP | | X | | X | | | X | | |
| User Name | | X | | X | | | X | | |
| Password | | X | | X | | | X | | |
| WAN IP address (Client modem for PPPoA) | | X (0.0.0.0) for client | | | | | | | Local IP Mask = 255.255.255.0 |
| Access Concentrator | | | | X | | | | | |
| HDLC Encapsulation | | | | | X | | | X | |

# Two stand-alone units directly connected

## *Ethernet Extension (HDLC - PPPoH Bridged)*




### *Model 3201 (Remote) Configuration Steps (PPPoH Bridged)*

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

```
→ ip list interfaces
```

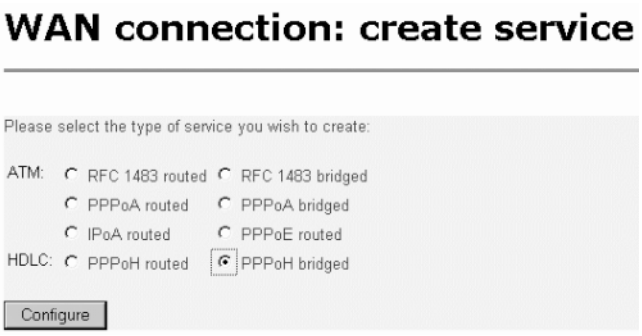
One IP interface is called *ip1* with an IP address of 192.168.1.1

Let's change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2

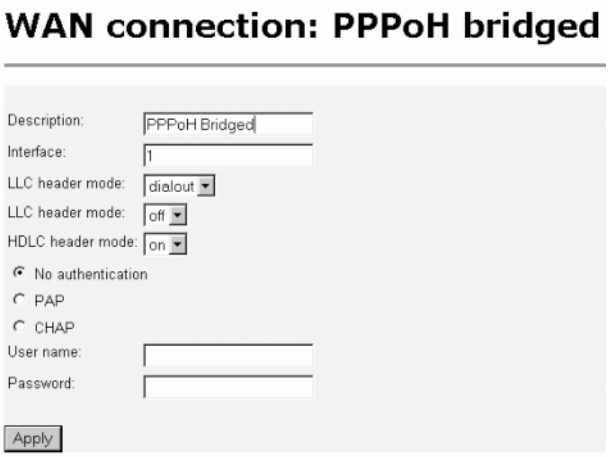
```
→ ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3201.
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 **PPPoH_Bridged** and click on the **Configure** button.




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




Verify the settings to be:

– Interface = 1

– LLC header mode = dialout

– LLC header mode = off

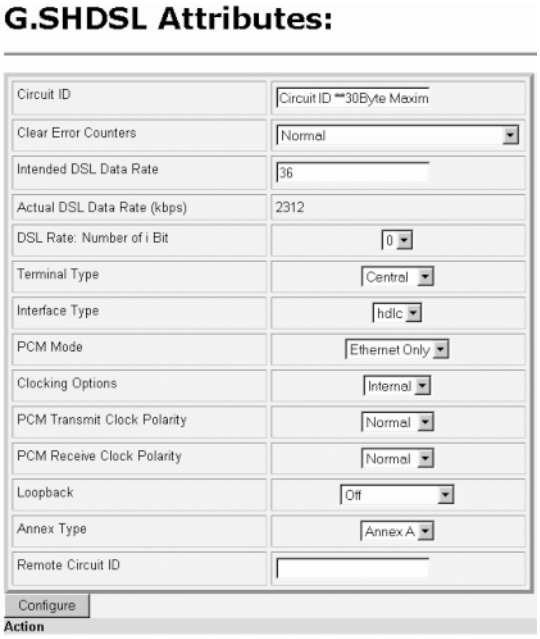
– HDLC header mode = on

– No authentication

– Leave User name and Password blank.

Click on **Apply**.

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




Change Terminal Type to *Central* and 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**.

### *Model 3201 (Central) Configuration Steps (PPPoH Bridged)*

See the Web page images for the Remote Model 3201 configuration above.

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

```
→ 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*

```
→ 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 3201.
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 **PPPoH_Bridged** and click on the **Configure** button.

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

   Verify the settings to be:

   – Interface = 1

   – LLC header mode = dialout

– LLC header mode = off

– HDLC header mode = on

– No authentication

– Leave User name and Password blank.

Click on **Apply**.

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

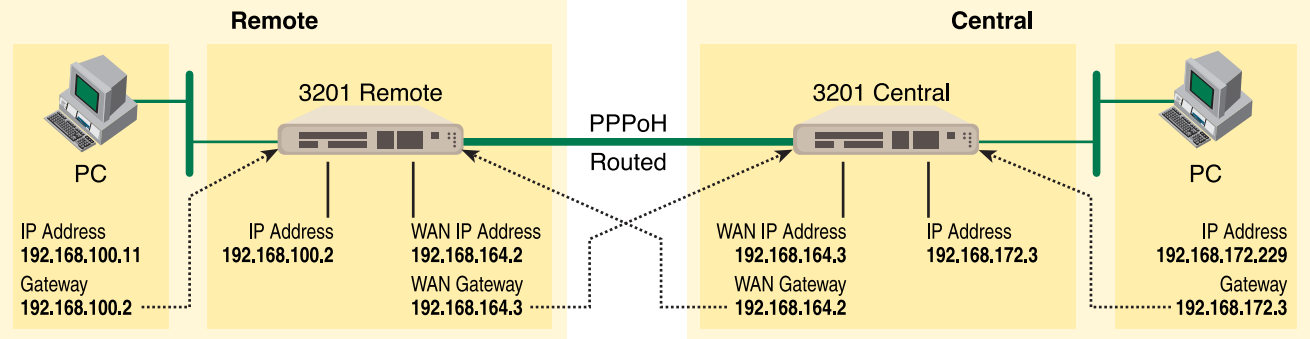
Leave Terminal Type as *Remote*.

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**.

## Network Extension (HDLC—PPPoH Routed)



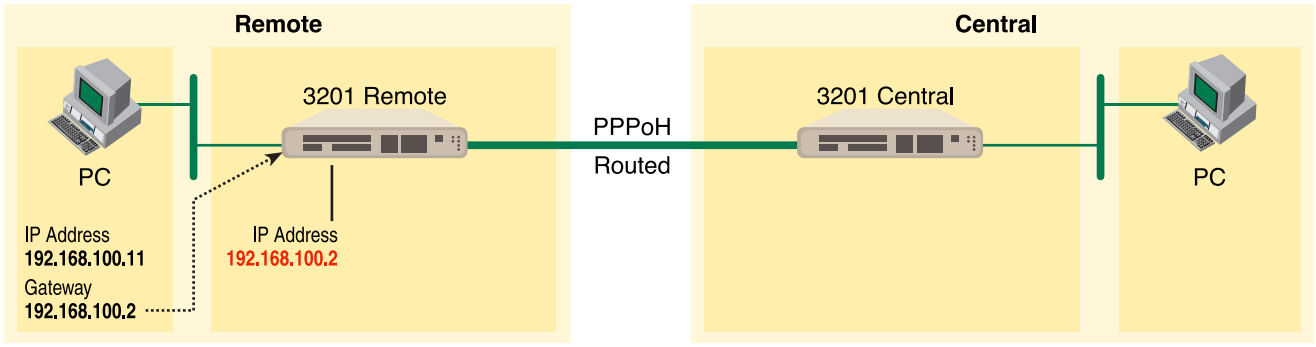

### *Model 3201 (Remote) Configuration Steps (PPPoH Routed)*

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

```
→ 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.

```
→ 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 3201.

   Click on **G.SHDSL** in the **Configuration Menu > Configuration** > verify that Terminal Type is **Central** and Interface Type is "**hdlc**." 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 **PPPoH_Routed** and click on the **Configure** button.

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

   – Description: PPPoH Routed

   – Interface: 1

   – WAN IP address: 192.168.164.2

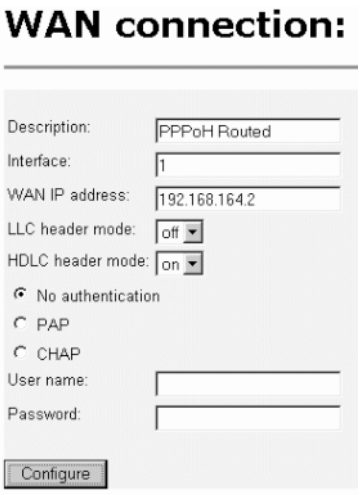
   – LLC Header Mode: off

   – HDLC Header Mode: ON

   – No authentication

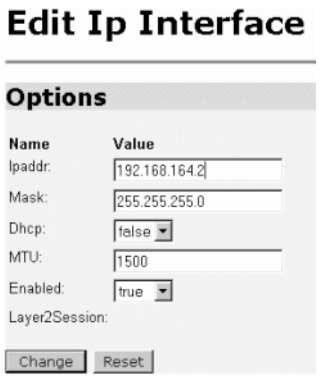
   – Username: [blank]

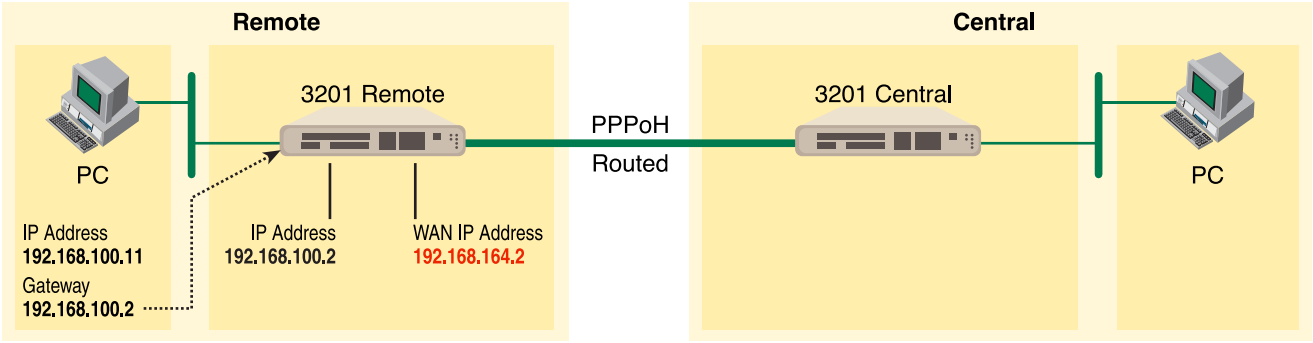
   – Password: [blank]



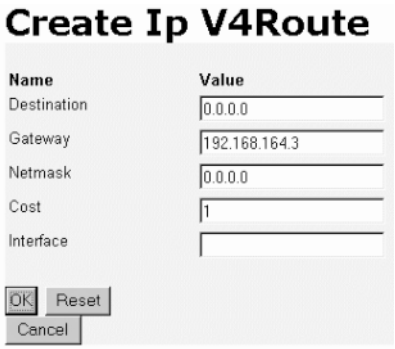

Click on **Configure**.

3. Go to **Configuration Menu > Configuration > WAN connections > Edit (for PPPoH Routed service) > Edit 'IP Interface' > Ipaddr:** [enter the WAN IP Address, in this example = 192.168.164.2] > Click on **Change**.






4. **Configuration Menu > Configuration > IP Routes >** Click on **Create new Ip V4 Route** > Create the gateway to the remote 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.3 in the Gateway field > OK




The other fields should be:

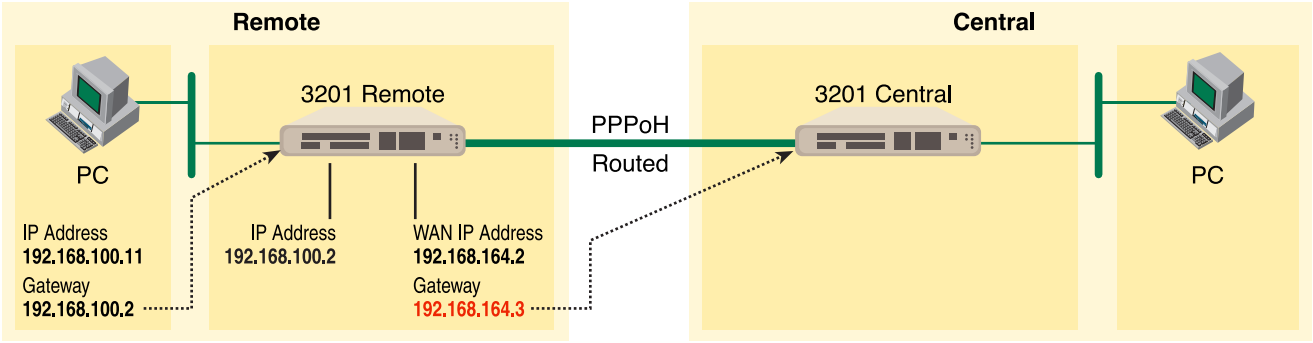
– Destination: 0.0.0.0

– Gateway: 192.168.164.3 [already configured in first part of step 4).]

– Mask: 0.0.0.0

– Cost: 1

– Interface: [blank]




5. 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 3201 (Central) Configuration Steps (PPPoH Routed)***

See the web pages for the desktop above. Some parametric values are different although the process is the same.

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

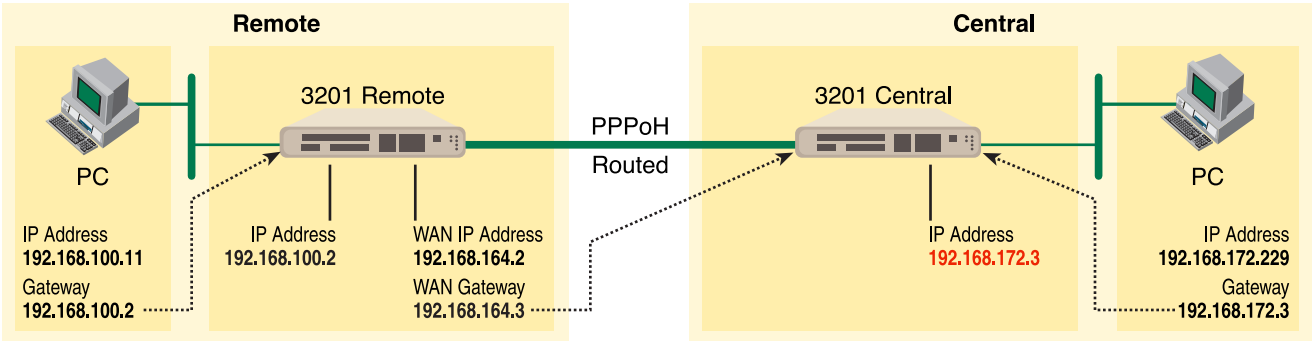
```
→ ip list interfaces
→ ip clear routes
→ pppoh clear transports

→ ethernet add transport eth1 ethernet
```

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 3201 to 192.168.172.3. The default IP mask is 255.255.255.0.

```
→ 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 3201.

Click on **G.SHDSL** in the **Configuration Menu > Configuration >** verify that Terminal Type is *remote* and Interface Type is "*hdlc*." 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 **PPPoH_Routed** and click on the **Configure** button.

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

   Description:PPPoH Routed

   – Interface:1

   – WAN IP address: 192.168.164.3

   – LLC Header Mode:off

   – HDLC Header Mode:ON

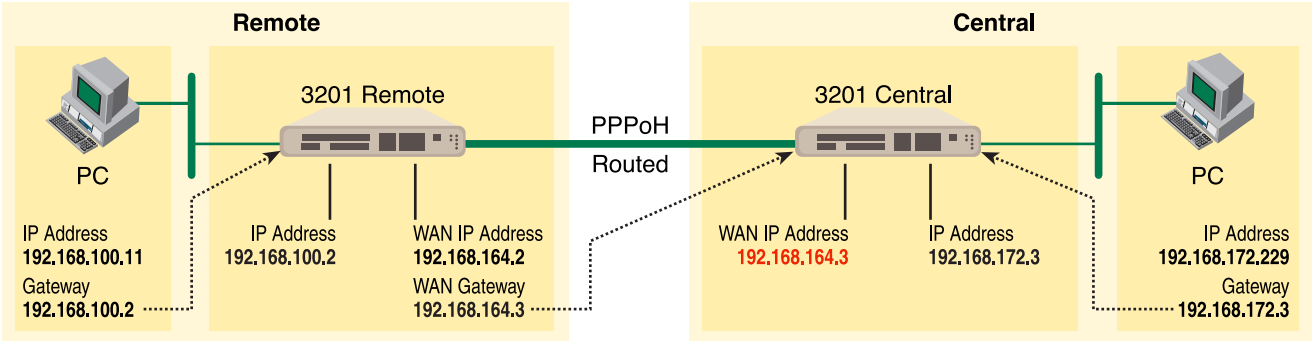
   – No authentication

   – Username:[blank]

   – Password:[blank]

   Click on **Configure**.

3. Go to **Configuration Menu > Configuration > WAN connections > Edit (for PPPoH Routed service) > Edit 'IP Interface' > Ipaddr:** [enter the WAN IP Address, in this example = 192.168.164.3] > Click on **Change**.




4. **Configuration Menu > Configuration > IP Routes** > Click on **Create new Ip V4 Route** > Create the gateway to the remote 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.2 in the Gateway field > OK

   The other fields should be:

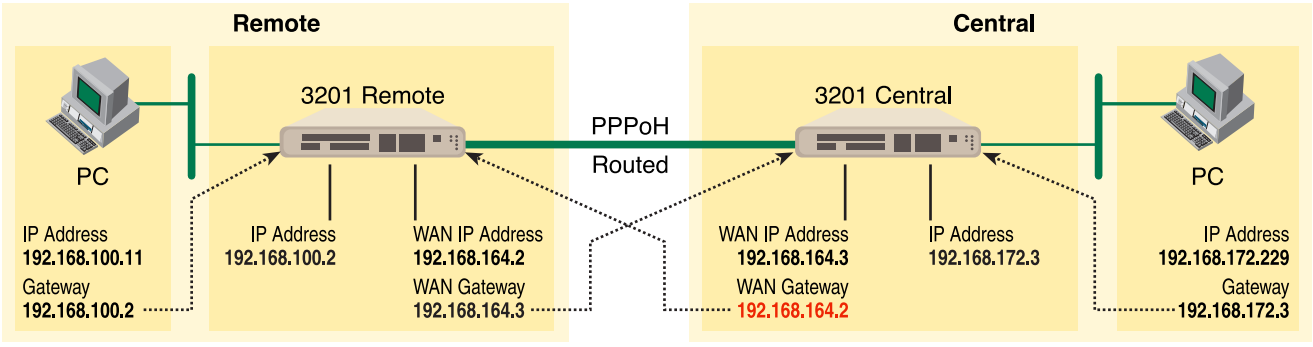
   – Destination:0.0.0.0

   – Gateway:192.168.164.2 [already changed in the first part of step 5).]

   – Mask:0.0.0.0

– Cost:1

– Interface:[blank]




5. 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**.

## DSLAM Connections with remote CPE units

### *Bridged application configurations to a DSLAM*

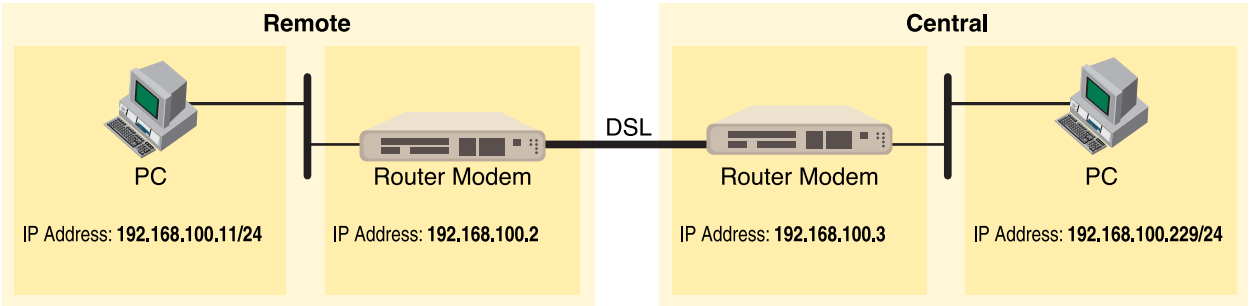
Three bridged services are offered, *RFC 1483 Bridged, PPPoA Bridged*, and *HDLC Bridged*.

The configurations show a desktop on one end and a laptop on the other. The laptop and its Model 3201 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 3201 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 3201 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.



### *Model 3201 (Remote) Configuration Steps (RFC 1483 Bridged)*

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

```
→ ip list interfaces
```

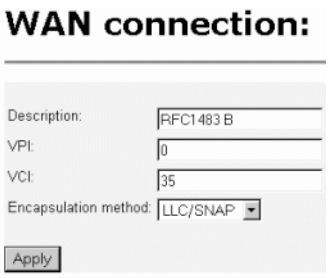
One IP interface is called ip1 with an IP address of 192.168.1.1

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

```
→ 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 3201.
2. On the Menu, go to Configuration, then to WAN Connections. Delete the factory default WAN services already defined.

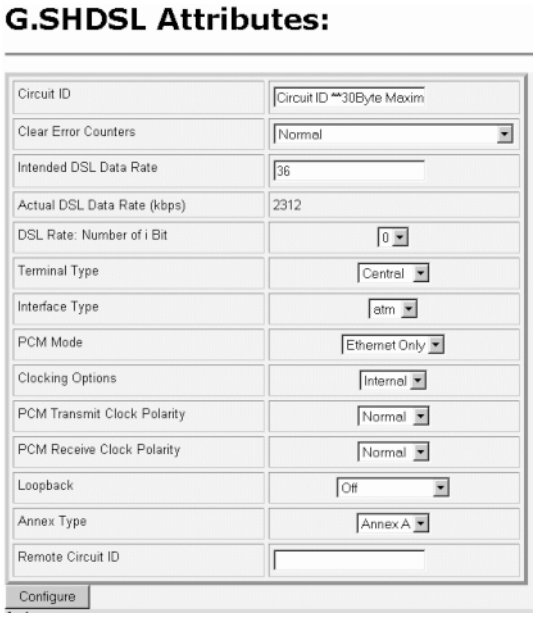
   Click on **Create a new service** in the main window, select **RFC_1483_Bridged** and click on the **Configure** button.




   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**.




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 3201 (Central) Configuration Steps (RFC 1483 Bridged)***

Although the some parametric values may vary from the desktop's Model 3201, the process is identical.

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

```
→ 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

```
→ 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 3201.
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*.

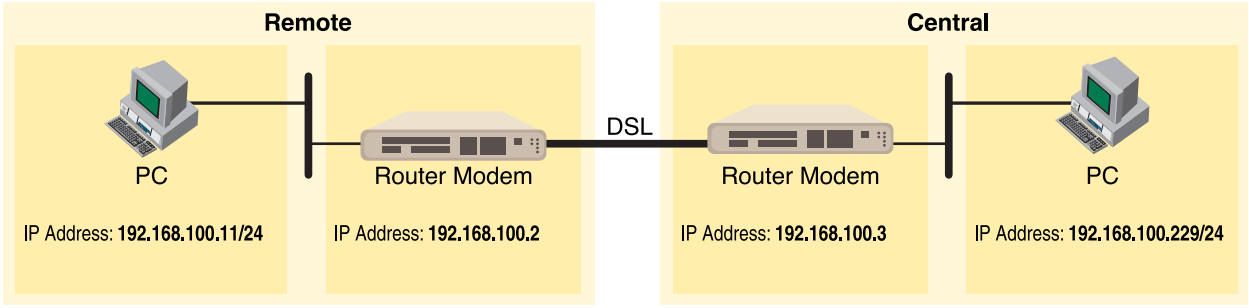
   Leave VCI as 35 and Encapsulation Method as LLC/SNAP. Then click on **Apply**.
3. Go to G.SHDSL in the Configuration Menu, then the submenu Configuration.

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


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


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

*PPPoH Bridged Configuration*




***Model 3201 (Remote) Configuration Steps (PPPoH Bridged)***

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

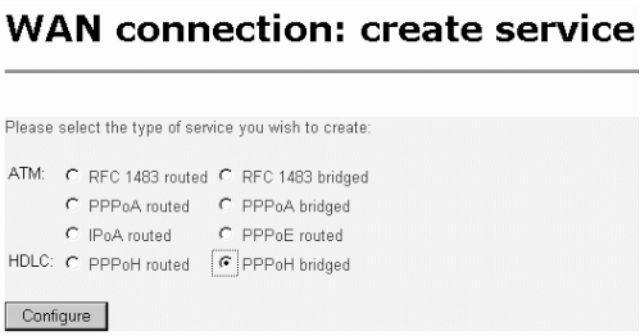
```
→ ip list interfaces
```

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 sub-net as both PCs. For example, to 192.168.100.2

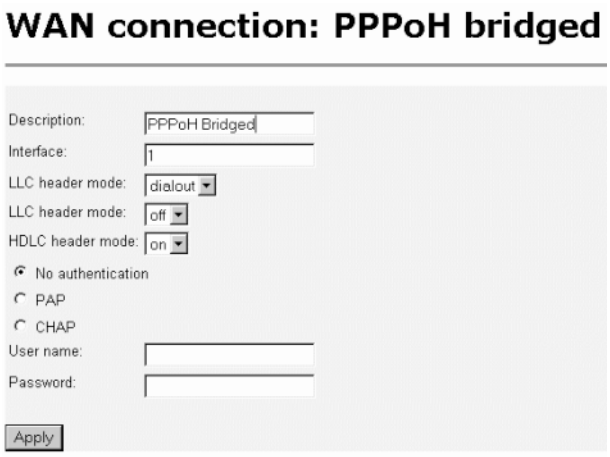
```
→ ip set interface ip1 ipaddress 192.168.100.2 255.255.255.0
```

1. Now you can bring up the web-page management system on your browser by entering the IP address of the 3201.
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 **PPPoH_Bridged** and click on the **Configure** button.




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




- Interface = 1
- LLC header mode = dialout
- LLC header mode = off
- HDLC header mode = on
- No authenticaion
- 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 *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**.

### *Model 3201 (Central) Configuration Steps (PPPoH Bridged)*

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

```
→ 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

```
→ 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 3201.
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 **PPPoH_Bridged** and click on the **Configure** button.

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

   – Interface = 1

   – LLC header mode = dialout

   – LLC header mode = off

   – HDLC header mode = on

   – No authenticaion

   – 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*.

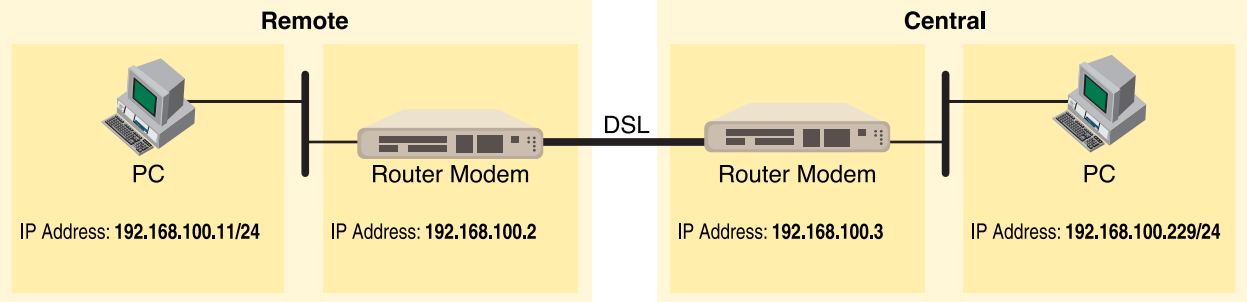
   Change Interface Type to *hdlc*. Click on the Configure button.

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

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

### *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.




***Model 3201 (Remote) Configuration Steps (PPPoA Bridged)***

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

```
→ ip list interfaces
```

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

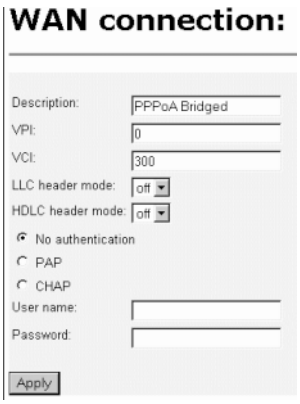
Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2

```
→ 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 3201.
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.

   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 3201 (Central)Configuration Steps (PPPoA Bridged)*

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

```
→ 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

```
→ 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 3201.
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*.

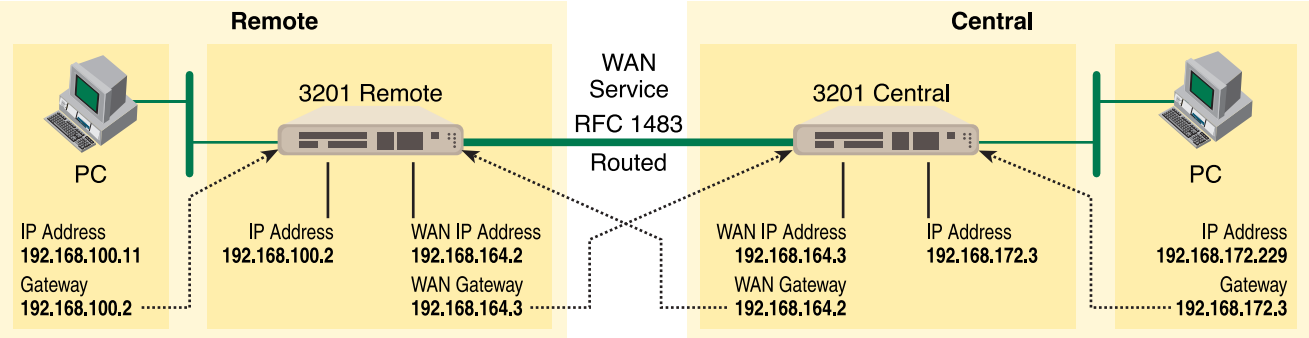
Change Interface Type to *atm*. Click on the **Configure** button.

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, PPPoH, IPoA, PPPoA,* and *PPPoE Routed*.




### *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.

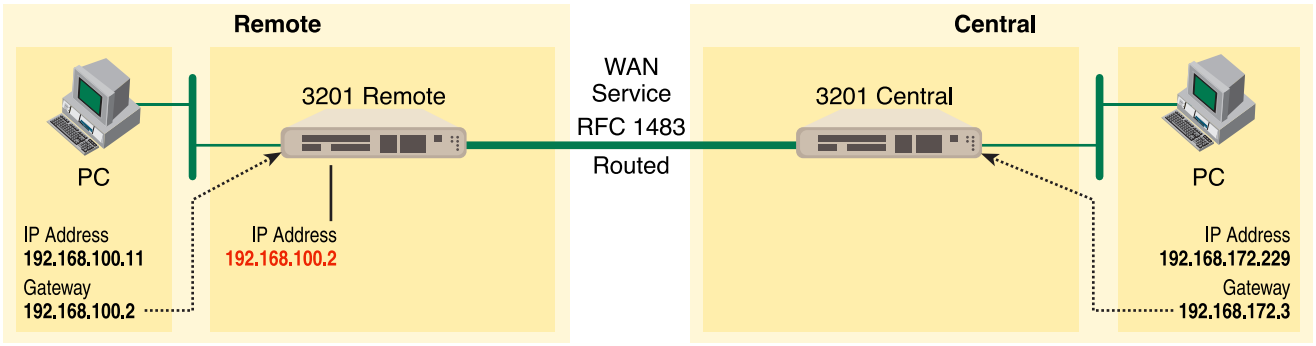
***Model 3201 (Remote) Configuration Steps (RFC 1483 Routed)***

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

```
→ 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.

```
→ 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 3201.

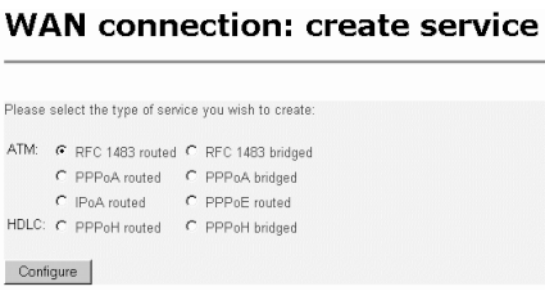
   Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Central* and Interface Type is *atm*. If changed, then click on **Configure**.


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

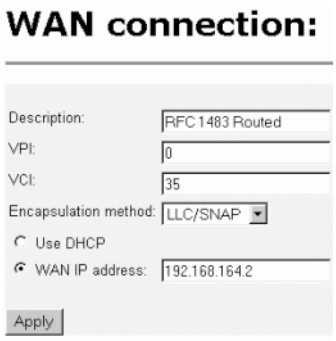
2. On the Menu, go to Configuration, then to WAN Connections.

   Delete both default WAN services already defined.

   Click on **Create a new service** in the main window, select **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*. Change the configuration parameters to match the following.




Description:RFC 1483 Routed

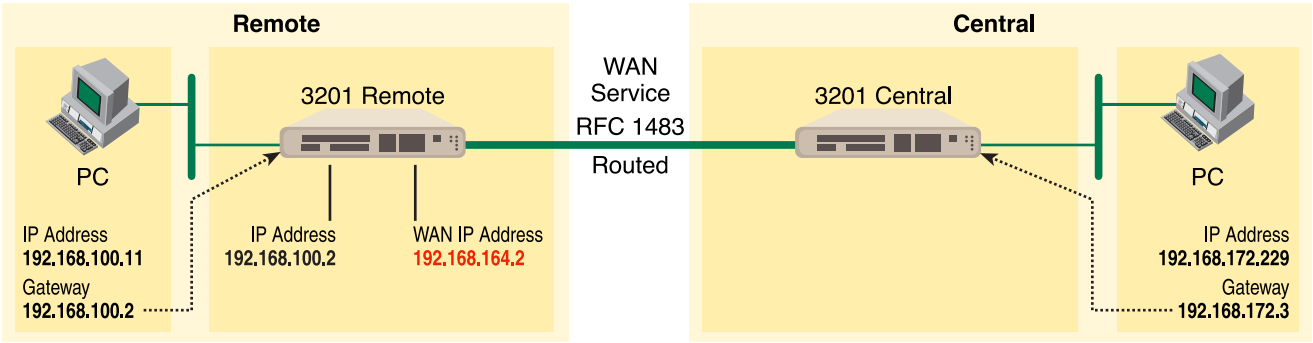
– VPI:0

– VCI:35

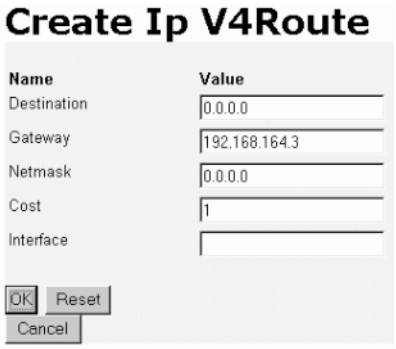
– Encapsulation Method: LLC/SNAP

– 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 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.3 in the Gateway field > OK




The other fields should be:

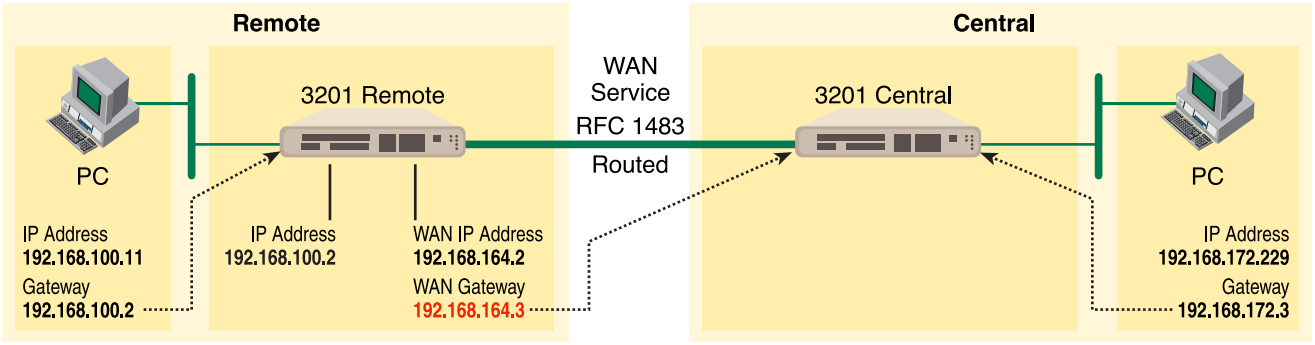
– Destination:0.0.0.0

– 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 3201 (Central) Configuration Steps (RFC 1483 Routed)*

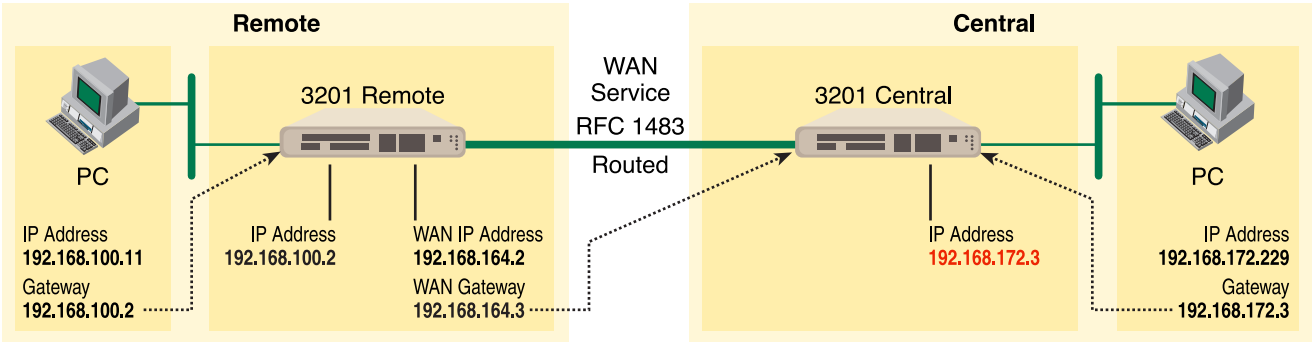
From the command line interface (CLI) via the RS-232 control port,

```
→ ip list interfaces
→ pppoh clear transports
```

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

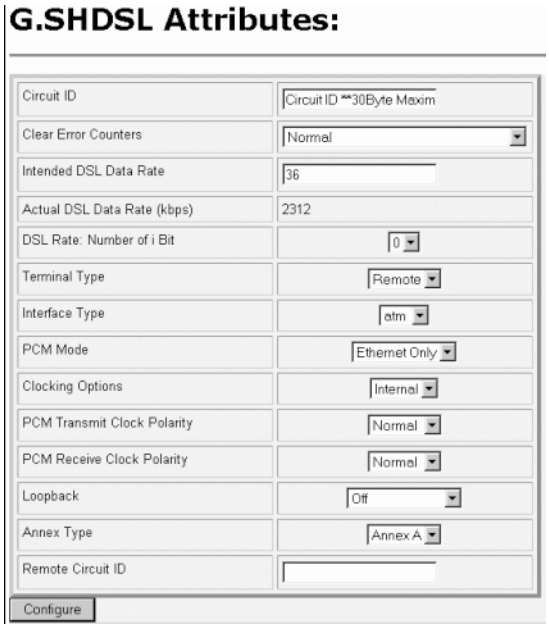
Change the IP address so it is in the same subnet as the laptop PC. The laptop's IP address is 192.168.172.229, so in this example, change the IP address of the 3201 to 192.168.172.3. The default IP mask is 255.255.255.0.

```
→ 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 3201.

   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**.



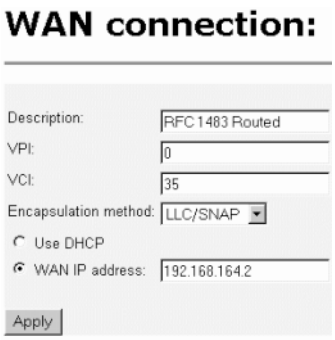
Click on Action > Select deactivate for Action > Click on the Action button.


**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.

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




Description:RFC 1483 Routed

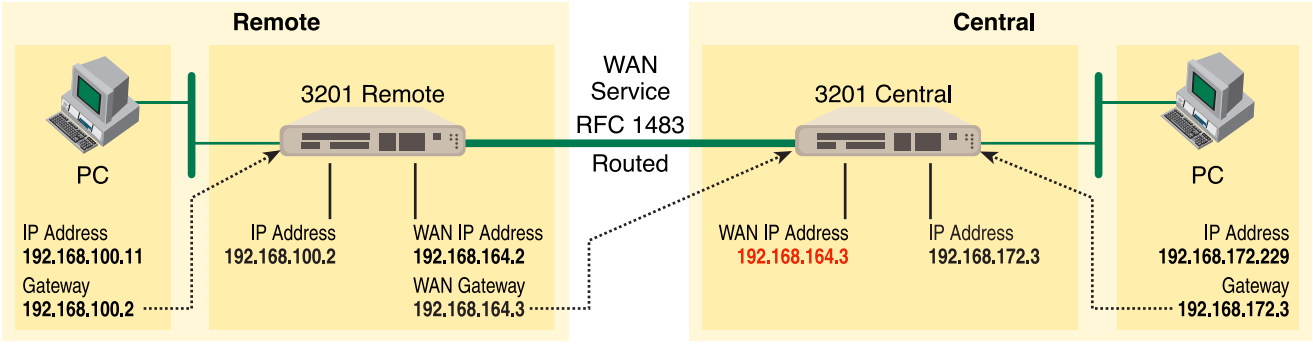
– VPI:0

– VCI:35

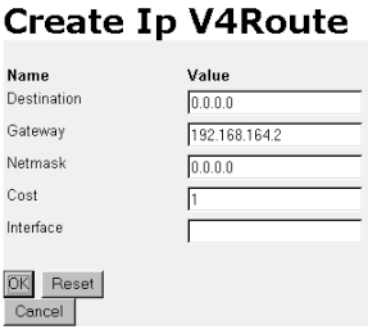
– Encapsulation Method:  LLC/SNAP

– 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 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.2 in the Gateway field > OK




The other fields should be:

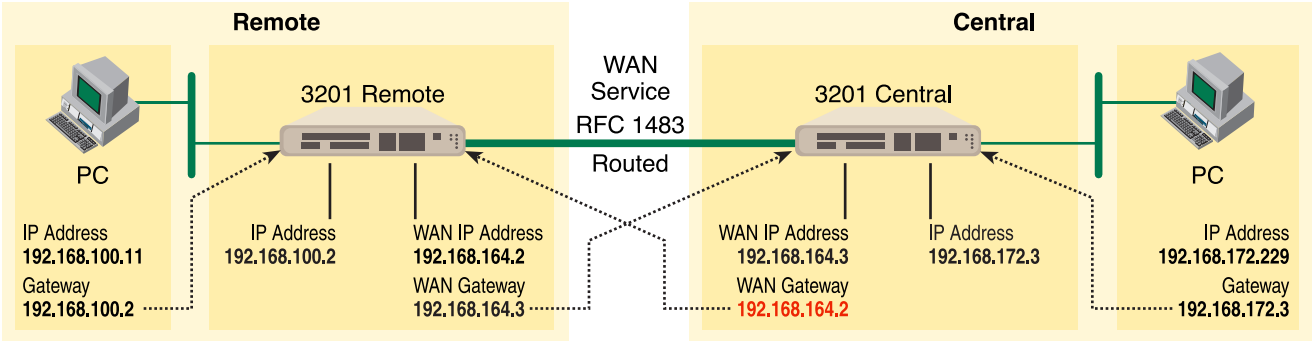
– Destination:0.0.0.0

– Gateway:192.168.164.2

– Mask:0.0.0.0

– Cost:1

– Interface:[blank]

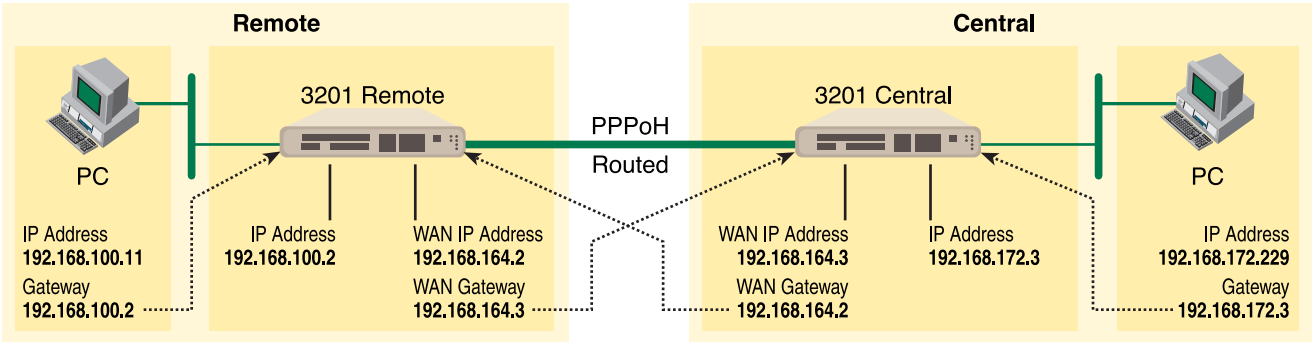



4. Go to G.SHDSL in the Configuration Menu, then the submenu Status. The Modem State should be "deactivated." (If not, go to the Action and change it to deactivate.)

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


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

*PPPoH Routed*



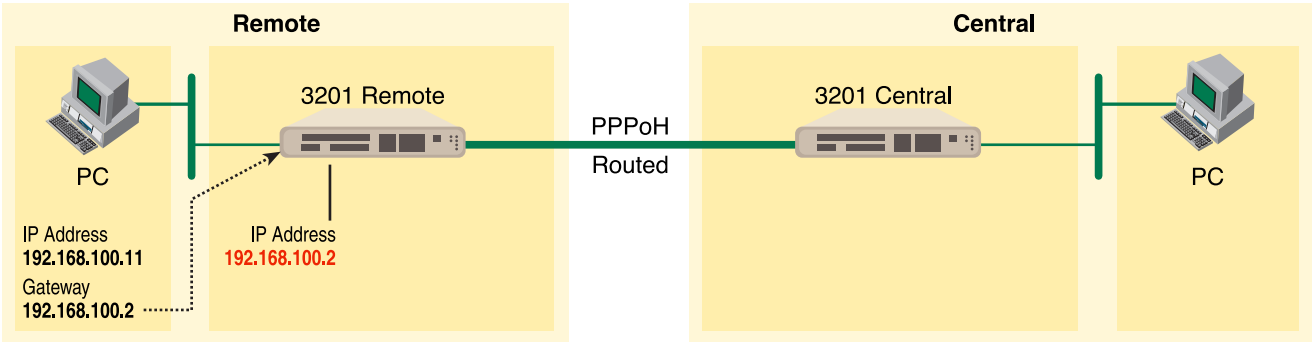

***Model 3201 (Remote) Configuration Steps (PPPoH Routed)***

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

```
→ ip list interfaces
→ ip clear routes
→ pppoh clear transports
```

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.

```
→ 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 3201.

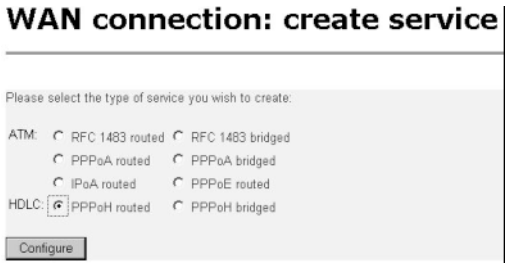
   Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Central* and Interface Type is *hdlc*. If changed, then click on **Configure**.

   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 **PPPoH_Routed** and click on the **Configure** button.




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

   – Description:PPPoH Routed

   – Interface:1

   – WAN IP address: 192.168.164.2

   – LLC Header Mode:off

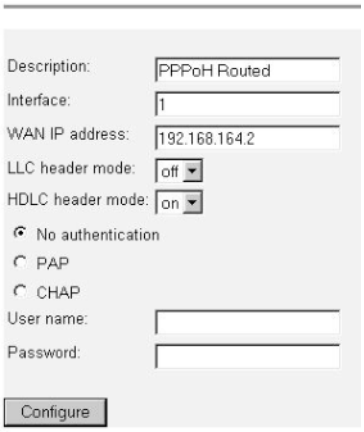
   – HDLC Header Mode:ON

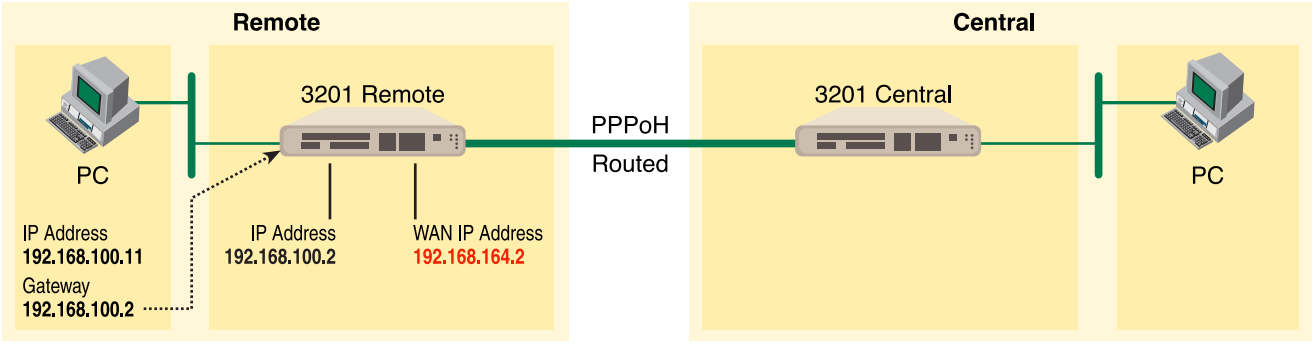
   – No authentication

– Username:[blank]

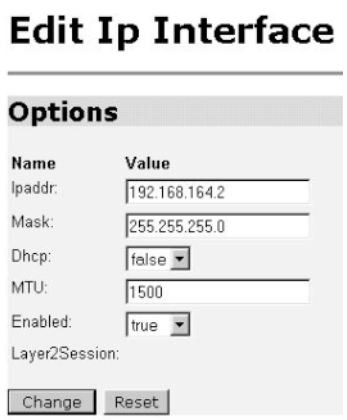
– Password:[blank]

Click on **Configure**.




**3.** Go to Configuration Menu > Configuration > WAN connections > Edit (for PPPoH Routed service) > Edit 'IP Interface' > Ipaddr: [enter the WAN IP Address, in this example = 192.168.164.2] > Click on Change.




4. Configuration Menu > Configuration > IP Routes > Click on Create new Ip V4 Route > Create the gateway to the remote 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.3 in the Gateway field > OK

   The other fields should be:

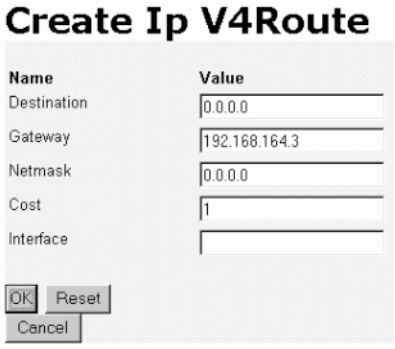
   Destination:0.0.0.0

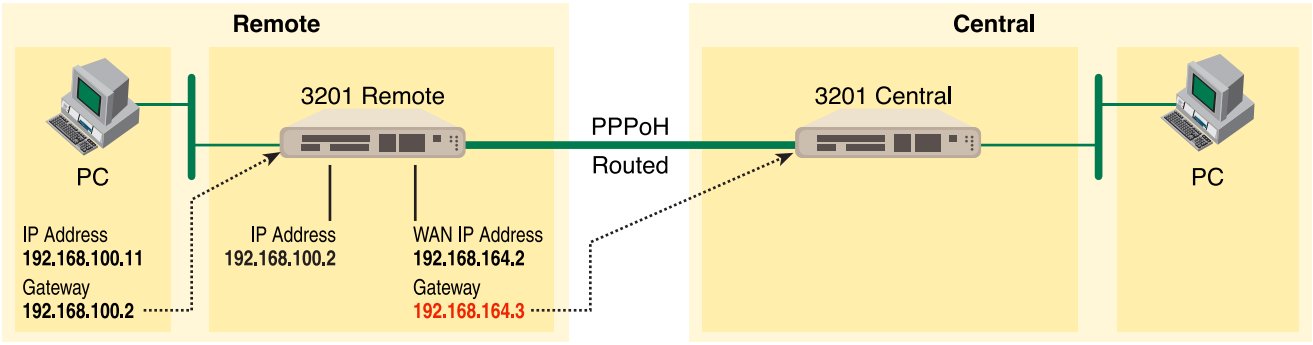
   Gateway:192.168.164.3 [already configured in first part of step 5).]

   Mask:0.0.0.0

   Cost:1

   Interface:[blank]






5. 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 3201 (Central) Configuration Steps (PPPoH Routed)*

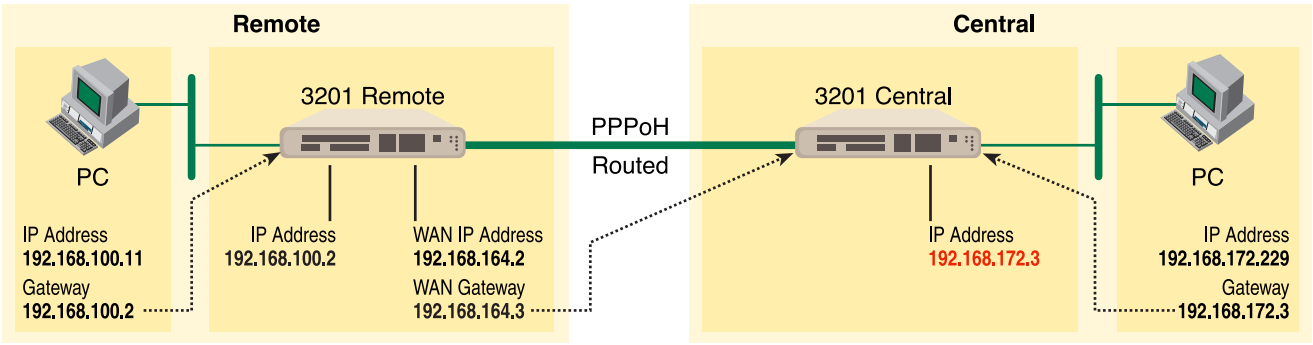
From the command line interface (CLI) via the RS-232 control port,

```
→ ip list interfaces
→ 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 3201 to 192.168.172.3. The default IP mask is 255.255.255.0.

```
→ 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 3201.

   Click on G.SHDSL in the Configuration Menu > Configuration > verify that Terminal Type is *Central* and Interface Type is *hdlc*. 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 **PPPoH_Routed** and click on the **Configure** button.

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

   – Description:PPPoH Routed

   – Interface:1

   – WAN IP address: 192.168.164.3

   – LLC Header Mode:off

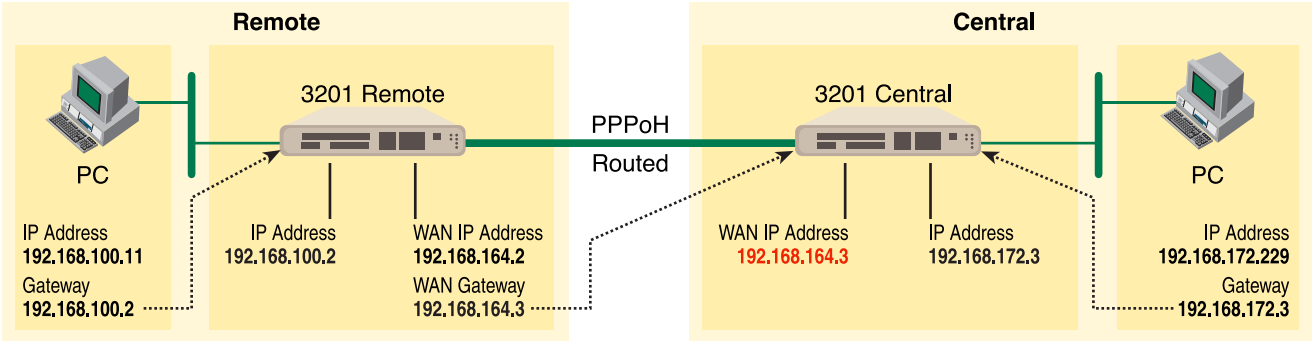
   – HDLC Header Mode:ON

   – No authentication

   – Username:[blank]

   – Password:[blank]

   Click on **Configure**.




3. Go to Configuration Menu > Configuration > WAN connections > Edit (for PPPoH Routed service) > Edit 'IP Interface' > Ipaddr: [enter the WAN IP Address, in this example = 192.168.164.3] > Click on Change.

4. Configuration Menu > Configuration > IP Routes > Click on Create new Ip V4 Route > Create the gateway to the remote 3201 by entering the WAN IP address of the remote 3201, in this example, enter 192.168.164.2 in the Gateway field > OK

   The other fields should be:

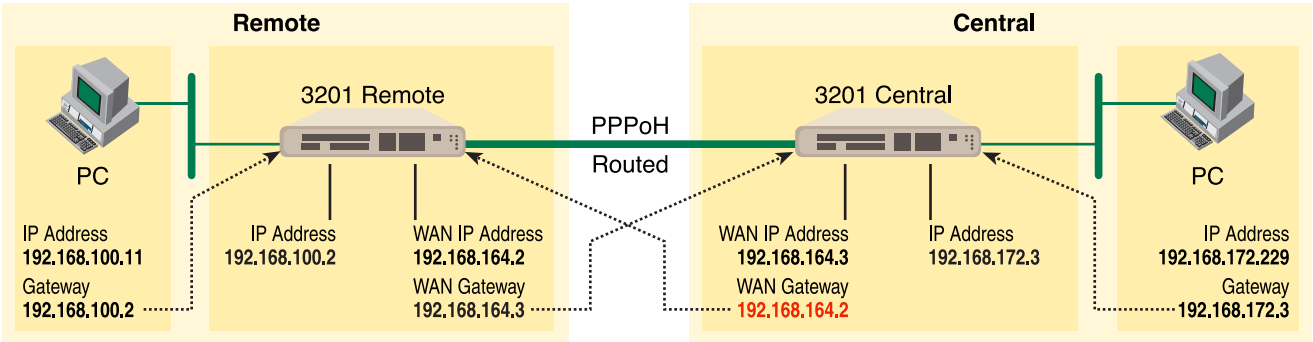
   – Destination:0.0.0.0

   – Gateway:192.168.164.2 [already changed in the first part of step 5).]

   – Mask:0.0.0.0

   – Cost:1

   – Interface:[blank]




5. 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.)

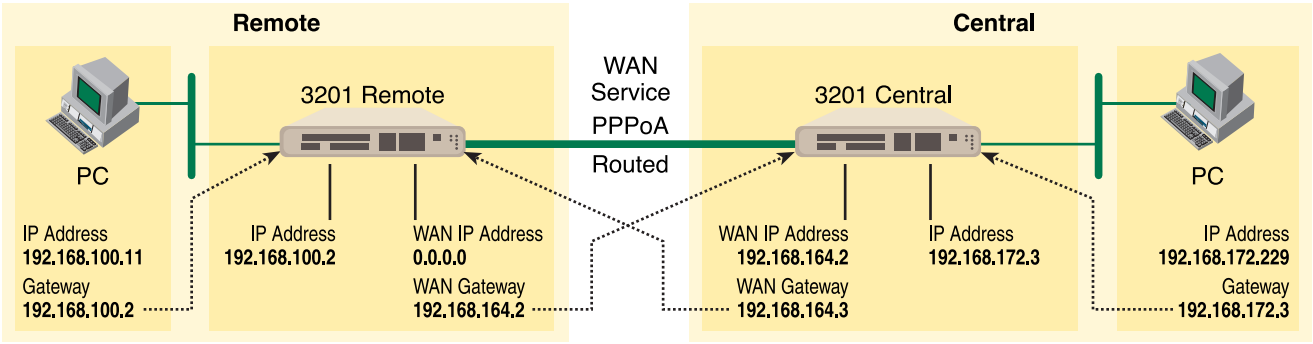
   Then in the Action submenu under G.SHDSL, change Action to Start, then click on **Action**.

### *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 3201) end functions as a local ISP which will authenticate the Remote user (Model 3201). The CPE side, with Remote and 3201-A, may represent a home PC which is connecting to a centralized PPP server (Local and 3201—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 3201 and Remote side, the Ethernet LAN on the 3201 and Central side, and lastly, the subnet of the ATM's PVC link between the two modems, 3201-A and 3201-B. The 3201-B and Local end (the Central side) may also be a DSLAM.



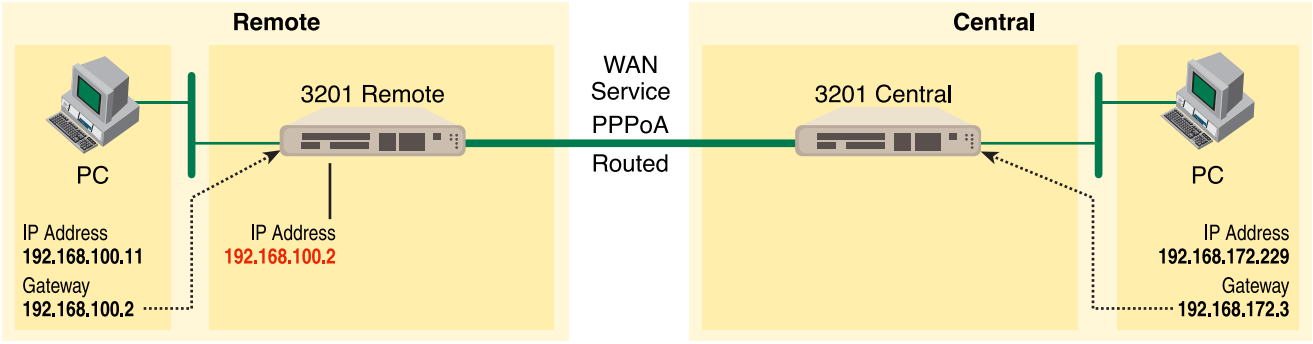

***Model 3201 (Remote—Client) Configuration Steps (PPPoA Routed)***

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

```
→ 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.

```
→ 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 3201.

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

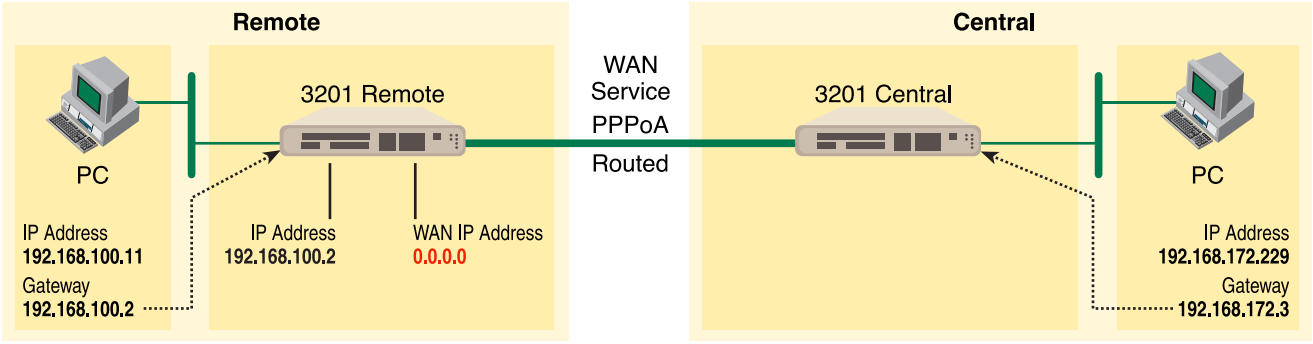
– HDLC Header Mode:off

– CHAP

– User Name:fred

– Passwood:fredspass

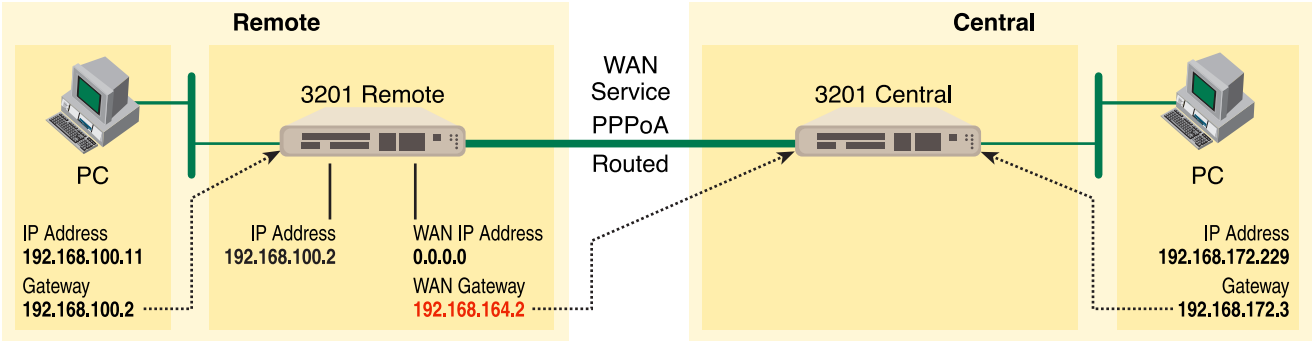
Click on **Configure**.




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 3201 (Central—Server) Configuration Steps (PPPoA Routed)***

Configuration via the web-pages has a bug which will be fixed. However the 3201 as servers functions properly via CLI configuration.

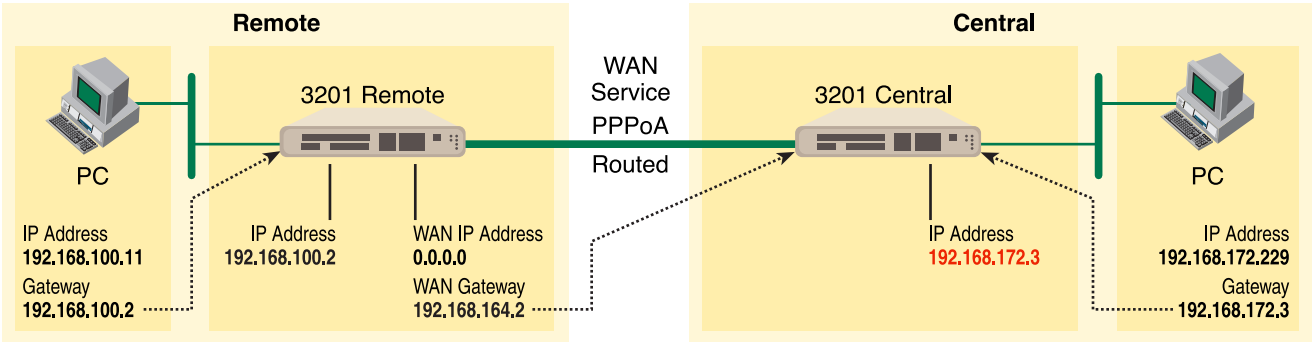
The following configuration is via the browser (web-pages). At the moment, do not use this method of configuration.

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

   ```
   → ip list interfaces
   ```

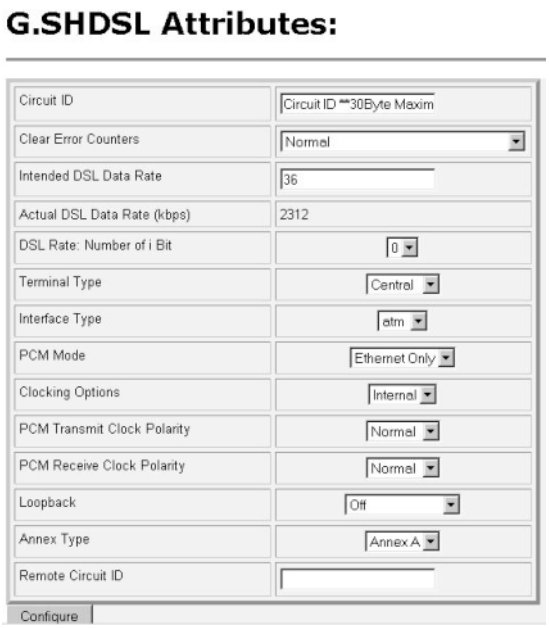
   One IP interface was called ip1 with an IP address of 192.168.1.1 Change it to an IP address which is in the same subnet as the Desktop PC. For example, to 192.168.172.3. The default IP mask is 255.255.255.0.

   ```
   → 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 3201.

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**.

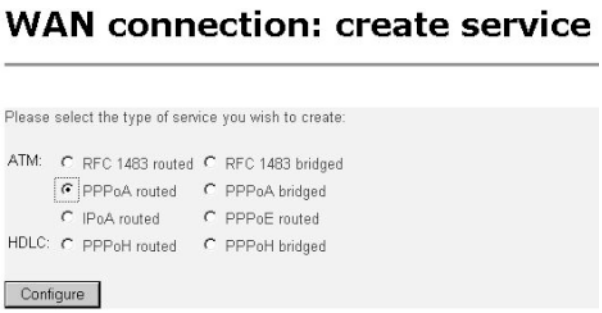



Click on Action > Select deactivate for Action > Click on the **Action** button.

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.



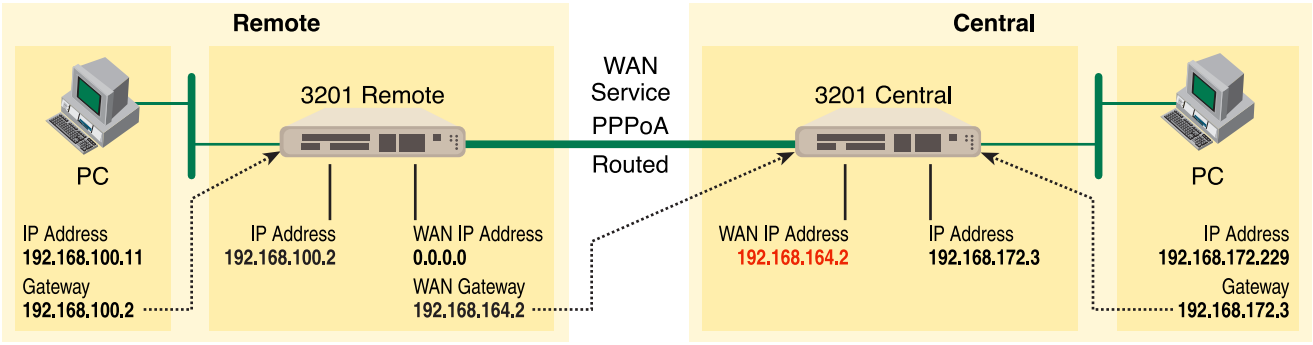

In the Description field, enter the description you wish. In this example, it is called *PPPoA Routed*. Change the configuration parameters to match the following.

– Description:PPPoA Routed
– VPI:0
– VCI:800
– WAN IP Address: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]

Click on **Configure**.

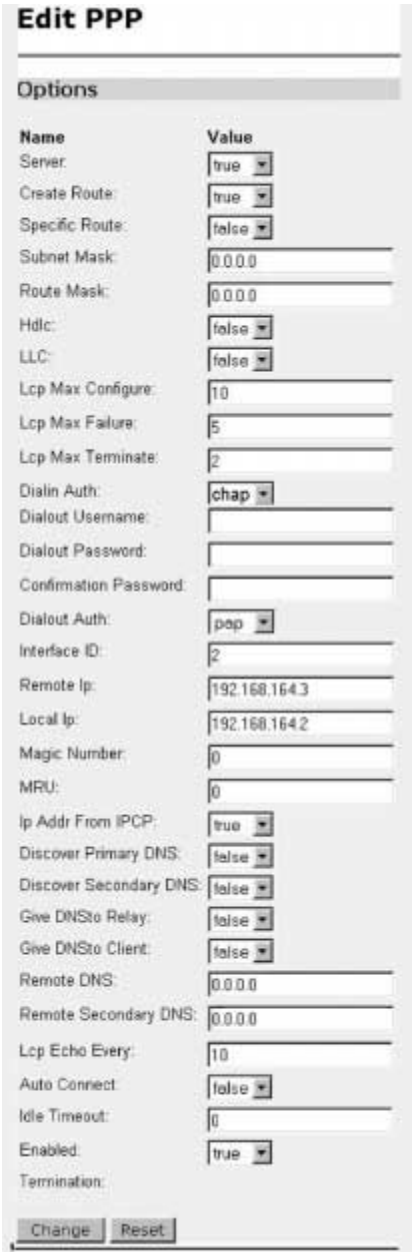



3. In the Configuration Menu, click on Configuration then > WAN Connections > Edit (for the WAN Service ppp1) > Edit 'PPP' and verify or change the following parameters on the Edit PPP webpage.

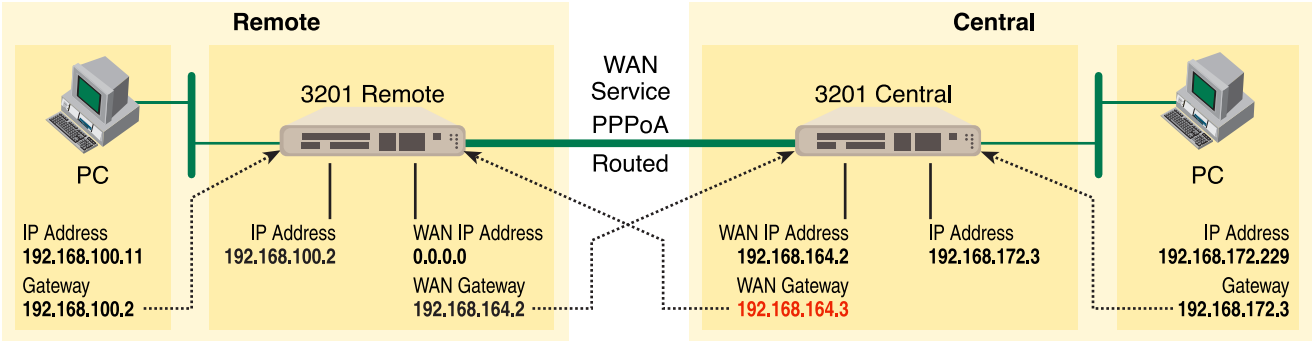
   Parameters in *red italics* are those requiring changes from the default configuration.

   – 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



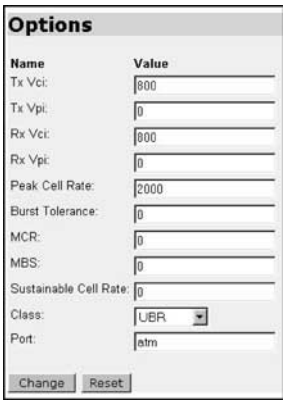

Click on **Change** button.




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.'

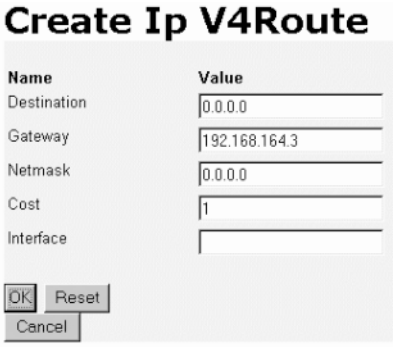
   Verify or change if necessary the following Options parameters.

   – Ipaddr:192.168.164.2
   – Mask:255.255.255.0
   – Dhcp:false
   – MTU:1500
   – Enabled:true


   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 3201 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]



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.]

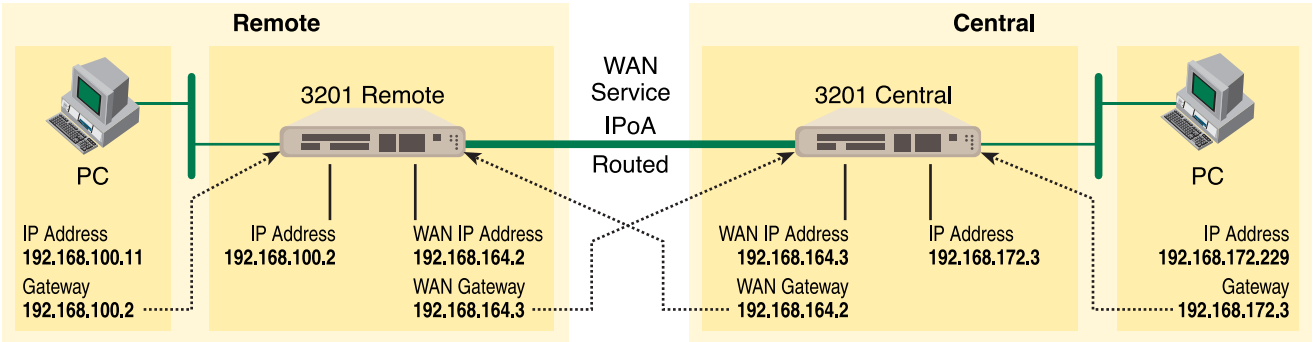
   Click on the **Create** button.

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.



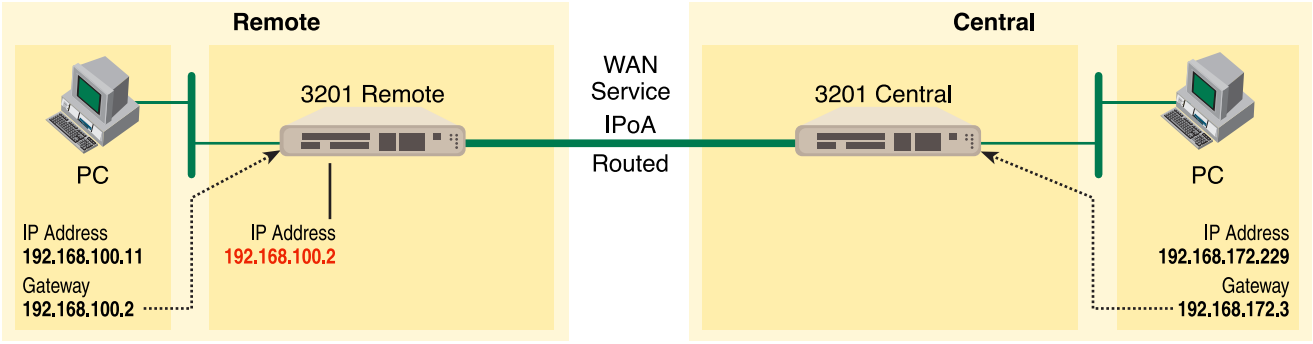

***Model 3201 (Remote) Configuration Steps (IPoA Routed)***

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

```
→ ip list interfaces
```

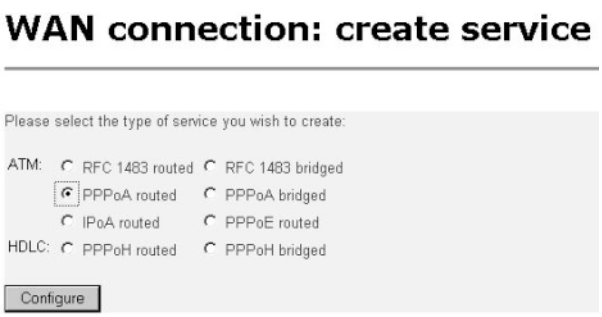
One IP interface was called ip1 with an IP address of 192.168.1.1 Change the IP address so it is in the same subnet as both PCs. For example, to 192.168.100.2. The default IP mask is 255.255.255.0.

```
→ 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 3201.
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.

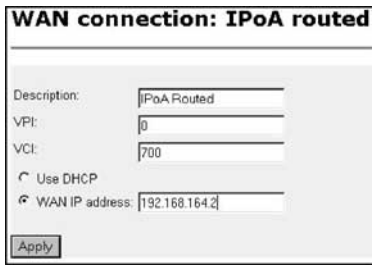



   In the Description field, enter the description you wish. In this example, it is called *IPoA Routed*.

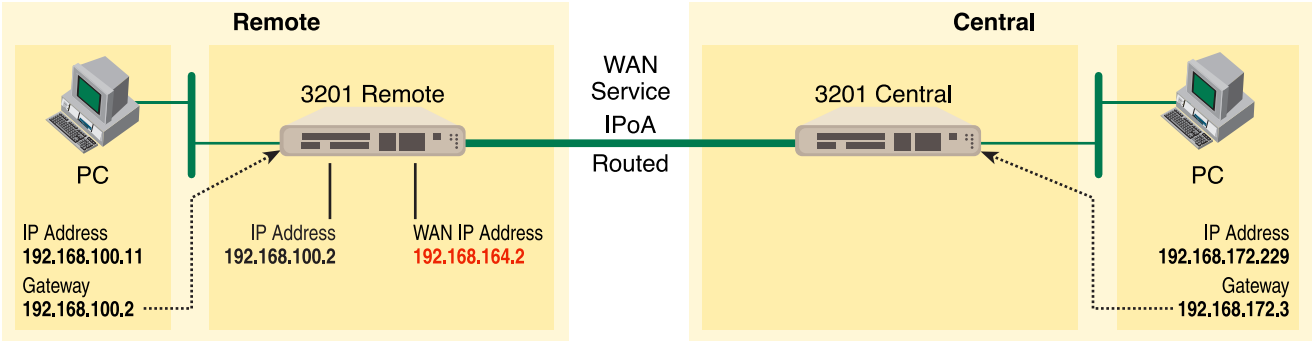
   – VPI:0

   – VCI:700

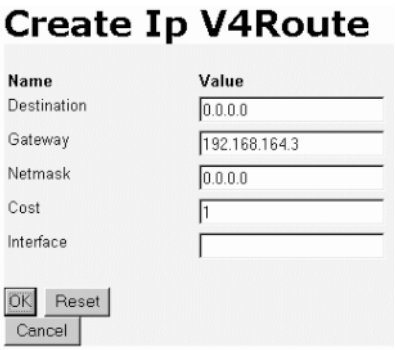
   – WAN IP address: 192.168.164.2



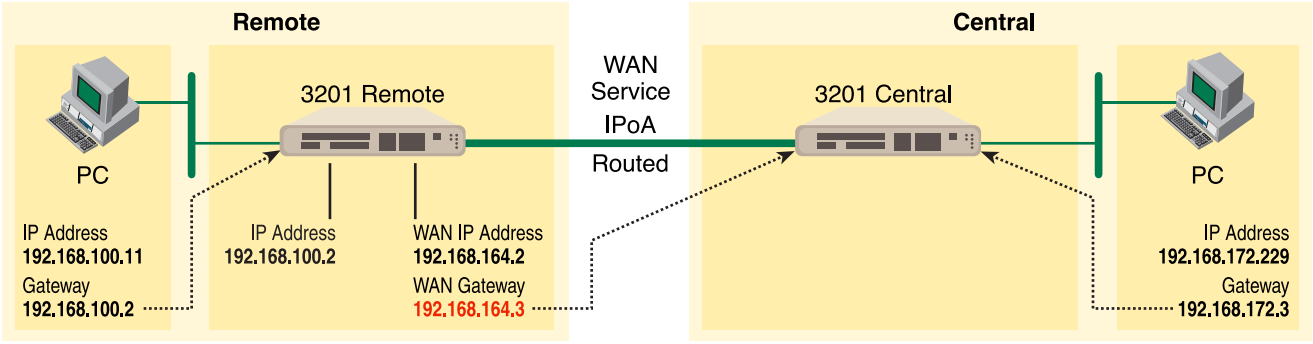

   Click on **Apply**.




3. Returning to the 3201 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]

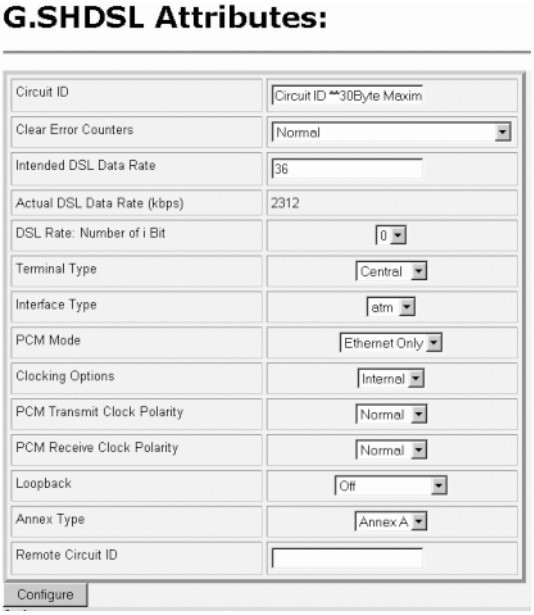



Click on **OK**.




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.




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


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

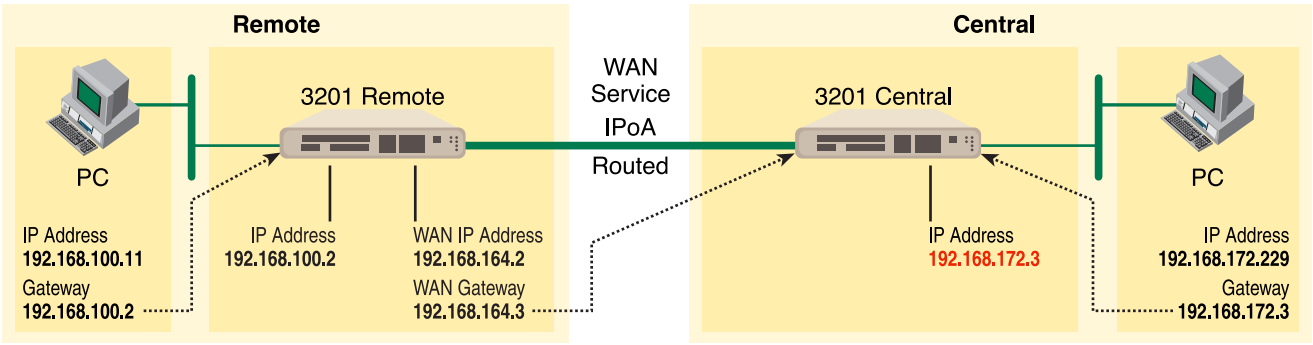
### *Model 3201 (Central) Configuration Steps (IPoA Routed)*

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

```
→ 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.

```
→ 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 3201.
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.

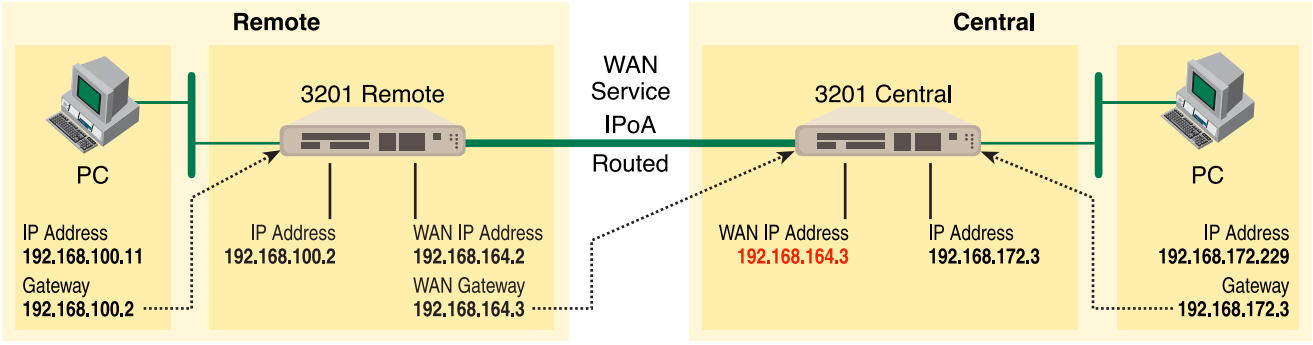
   In the Description field, enter the description you wish. In this example, it is called *IPoA Routed*.

   – VPI:0

   – VCI:700

   – WAN IP address: 192.168.164.3

   Click on **Apply**.




3. Returning to the 3201 Configuration Menu, click on Configuration, then IP Routes.

   Click on "Create new Ip V4 Route."

   – Destination:0.0.0.0

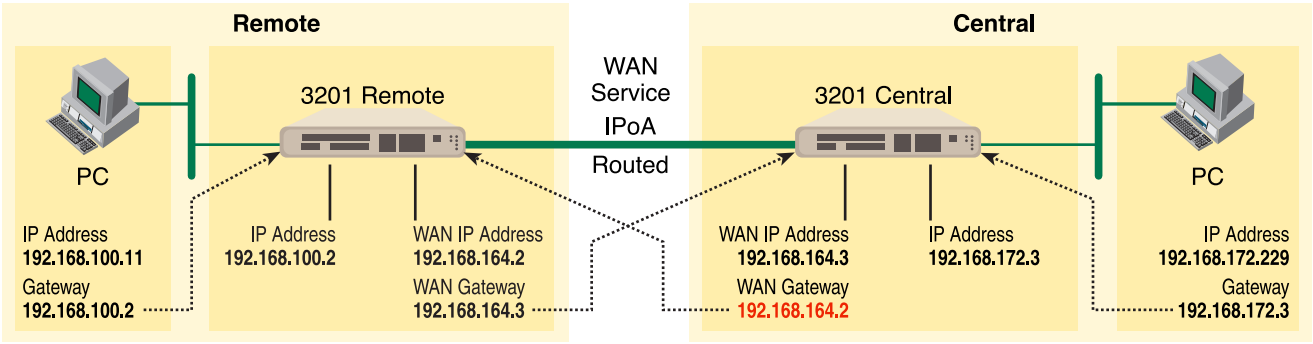
   – Gateway:192.168.164.2

   – 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 5 Specialized Configurations

## *Chapter contents*

# IP Configurations

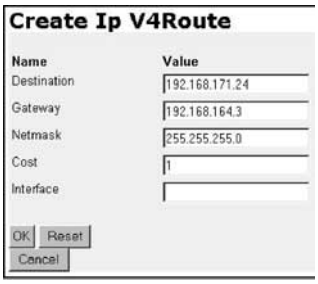
The router can be configured to use the RIP routing protocol, version 1 or 2, for accepting and sending RIP packets.

## Router

### *RIP and RIPv2*


### *Static Route*

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**.



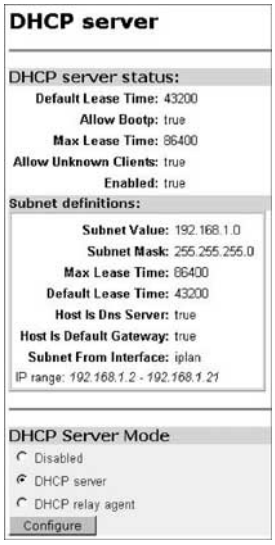

3. Enter the destination IP address in the Value field of "Destination."
4. Enter the IP address of the gateway which is the WAN IP address of the device on the other end of the DSL link in the Value field of "Gateway."
5. Enter the appropriate netmask in the Value field of "Netmask."
6. Leave Cost as "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.

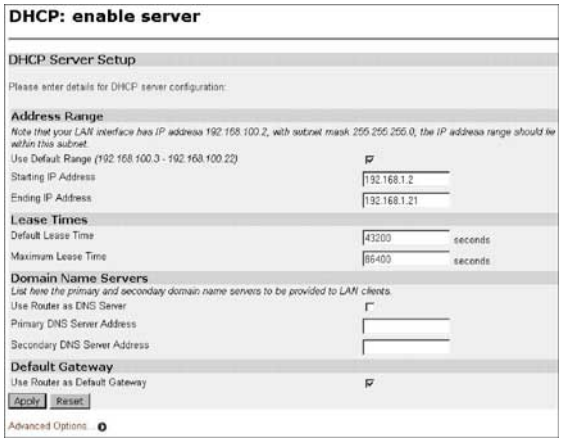
1. Go to > Configuration Menu > Configuration > DHCP Server and the DHCP Server page is displayed.

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

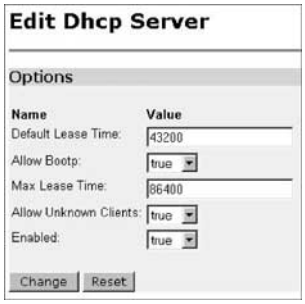



2. Click on **Configure** on the DHCP Server web page to change the configuration for any of the DHCP parameters.

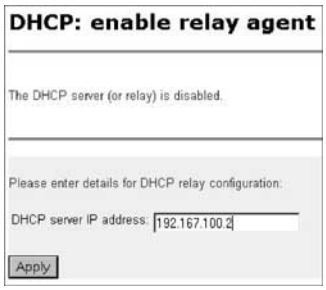
   The three categories of configuration parameters on this web page are the Address Range of the DHCP Server, the Lease Times in seconds, the selection of Domain Name Servers (if desired), and whether to use the router as the default gateway.



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




4. The router modem 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.




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 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.

# Chapter 6 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 7, “NAT (Network Address Translation)” on page 95.

## Configuring the router

The configuration of security assumes that the 3201/Router modem 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 3201/Router modems will be IPoA.

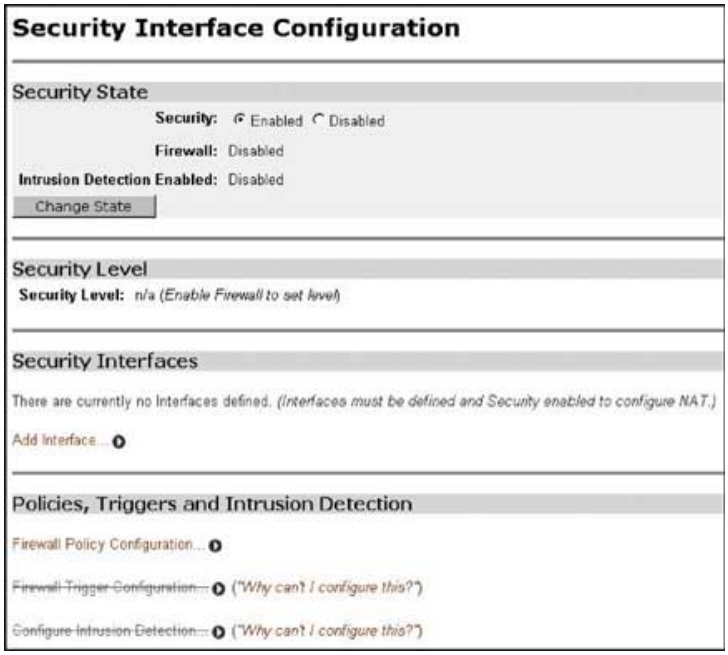
1. Click on **`WAN Connections`** under Configuration on the 3201’s Menu.
2. Click on **`Create a New Service`**.
3. Select **`IPoA Routed`** and click on the **`Configure`** button.
4. For this example, enter **`IPoA Security Firewall`** in the Description field.
5. VPI remains at *0*. Change VCI to 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 router is adding the default gateway route. Since the WAN IP address of the 3201 modem at the CO site is 192.168.101.2, this will be the gateway for the 3201 modem at the CPE site, the modem we are currently configuring.

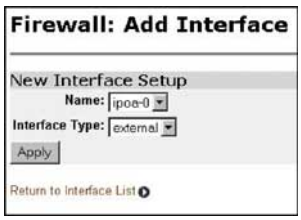
1. Click on **IP Routes** under Configuration on the 3201 modem's Menu.
2. Click on **Create a New IP Route**.
3. Enter *192.168.101.2* in the box adjacent to Gateway.
4. Leave Destination and Netmask both as *0.0.0.0* because this is the gateway default route.
5. Click on **Create** and the route will be entered.
6. The default gateway can be verified by clicking on **IP Routes** under Status in the menu.

## Configuring the security interfaces

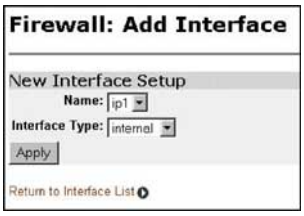
The interfaces and routes have been configured on the 3201 Router modem which will function as the firewall. The Ethernet side of the 3201 will be configured to be an internal security interface whereas the WAN side is configured as an external security interface since it is on "public" side of the modem connection.




1. Click on **Security** under Configuration on the 3201 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**.

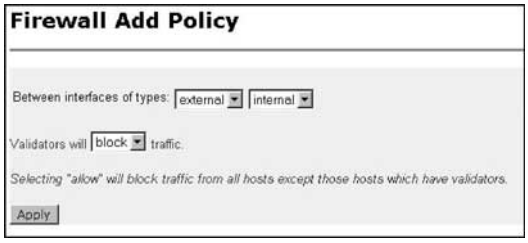



4. Add one more security interface by repeating step 2.
5. Select Name of the LAN port (*ip1*) and Interface Type to be *internal*. Click on **Apply**.




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**.




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.

```
→ firewall list policies
```

Firewall Policies:

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

→ 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.

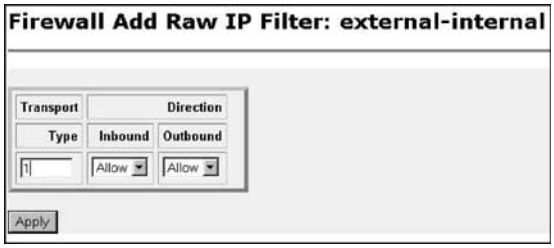
For the Transport Type below, the different types are:

| 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**.

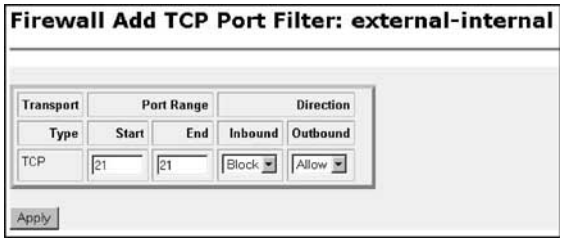



You can now ping between the two networks

## 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.

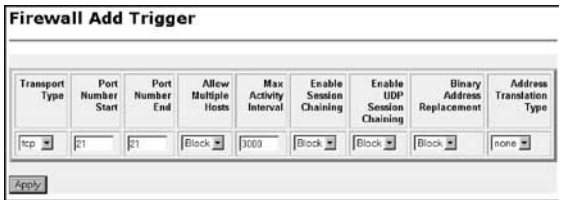
1. First, create an outbound-only portfilter for FTP and add it to the item0 policy.
2. Following the path given in step 1 for the ping portfilter, click on **Add TCP Filter**.
3. The Port Range is entered as *21* for both Start and End.
4. Set Inbound as **Block**, but Outbound as **Allow**.
5. Click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



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**.




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 3201 Router modem 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.

Table 4:

| Attack Name | Protocol | Attacking Host Blacklisted? |
|---|---|---|
| Ascend Kill | UDP | yes |
| Echo/Chargen | UDP | no |
| Echo Scan | UDP | yes |

Table 4:

| Attack Name | Protocol | Attacking Host Blacklisted? |
|---|---|---|
| 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 7 NAT (Network Address Translation)

## Chapter contents

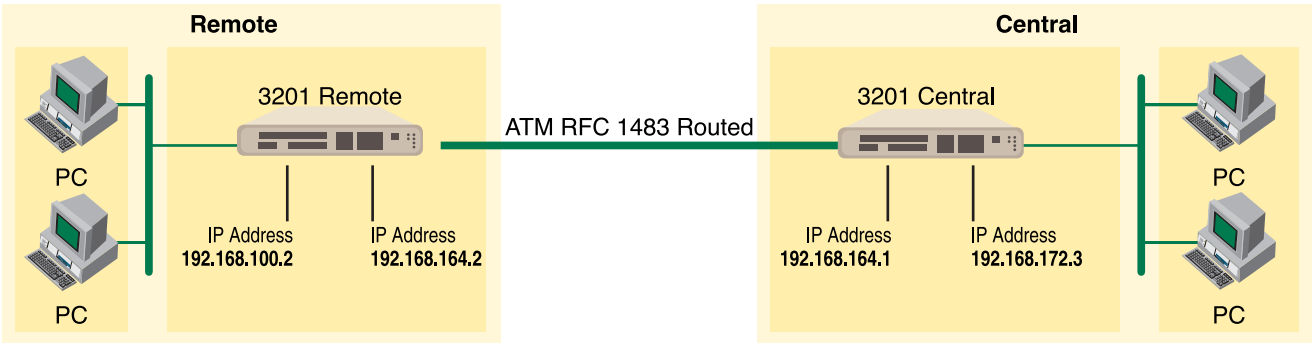
## Introduction

Network Address Translation (NAT) provides unlimited local host addresses, enabling users to connect to the Internet without having to provide a new address for each and every host. An encryption capability helps keep actual addresses confidential. This chapter describes how to configure for NAT.

## Creating an Ethernet Transport

1. From Console on the Remote unit configure the following:

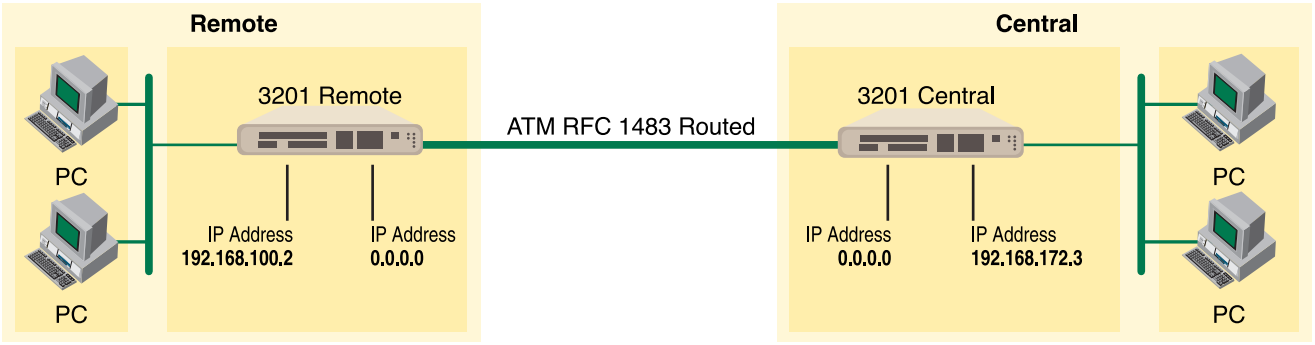
```
→ ip set interface ip1 ipaddress 192.168.100.11 255.255.255.0
→ system config save
```




2. From Console on the Central unit configure the following:

```
→ ip set interface ip1 ipaddress 209.49.110.130 255.255.255.0
→ system config save
```

Now you should be able to reach the unit through the Ethernet port from the local side using Telnet or the WWW interface. This instructions in this procedure are intended for the WWW interface.




## Creating a DSL Link

You will need the following to create a DSL link:

- One Model 3201 unit configured as *Remote*
- One Model 3201 unit configured as *Central*

- DSL data rates should be the same for Remote and Central units

### Central Side Configuration

From the WWW interface, do the following:

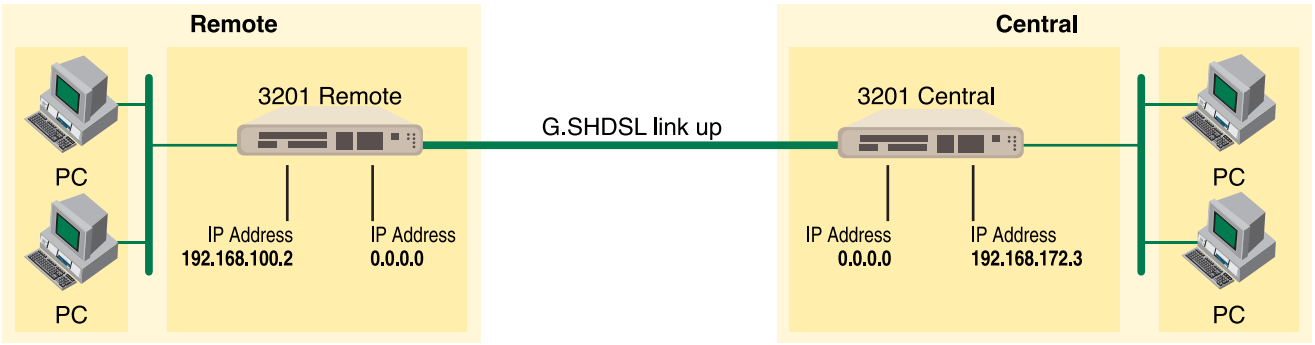
1. Click on **GSHDSL.**
2. Click on **Configuration.**
3. Change the intended DSL Data Rate to the maximum rate desired.
4. Change *Terminal Type* to **Central**.
5. Scroll to the bottom of the page and click on **Configure**.
6. Click on **(GSHDSL) Action.**
7. Set to start and click on **Action**.
8. Save the configuration.

### Remote Side Configuration

From the WWW interface, do the following:

1. Click on **GSHDSL.**
2. Click on **Configuration**.
3. Change the intended DSL Data Rate to the maximum rate desired.
4. Scroll to the bottom of the page and click on **Configure**.
5. Save the configuration.

Confirm that the DSL link is working properly by verifying that the DSL WAN LED is lit.



## Creating an ATM Routable Link

Now that you have a DSL link, do the following to configure a WAN service.

### *Remote side configuration*

From the WWW interface:

1. Click **Configuration.**
2. Click **Create a new service.**
3. Enable **RFC 1483 routed.**
4. Click **Configure.**
5. Type a description of the DSL Link.
6. Type in the IP address *192.168.164.2*.
7. Click **Apply**.
8. Save the configuration.

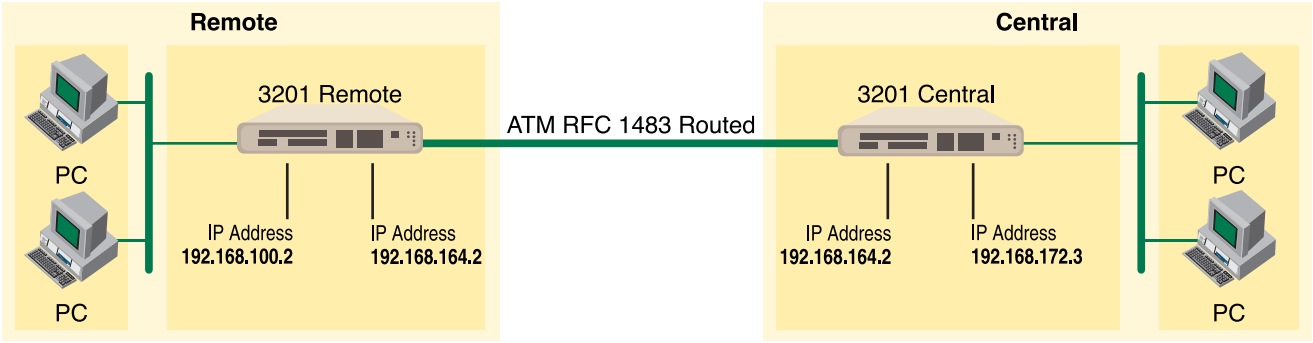
### *Central side configuration*

From the WWW interface:

1. Click **Configuration.**
2. Click **Create a new service.**
3. Enable **RFC 1483 routed.**
4. Click **Configure.**
5. Type a description of the DSL Link.
6. Type in the IP address *192.168.164.1*.
7. Click **Apply**.
8. Click **G.SHDSL**.

9. Click **Action.**

10. Save the configuration.




Do the following to confirm that the ATM link is working properly:

- Verify that the DSL WAN LED is lit.
- Ping the Remote unit from the Central Console
  `→ip ping 192.168.164.2`
- Ping the Central unit from the Remote Console
  `→ip ping 192.168.164.1`

## Creating a route for Remote and Central PCs

Do the following to create a route for the Remote and Central PCs:

### *Remote side configuration*

From the WWW interface:

1. Click **Configuration**.
2. Click **IP routes**.
3. Create new IP V4 Route.
4. Add Gateway *192.168.164.1*.
5. Click **OK**.

### *Central side configuration*

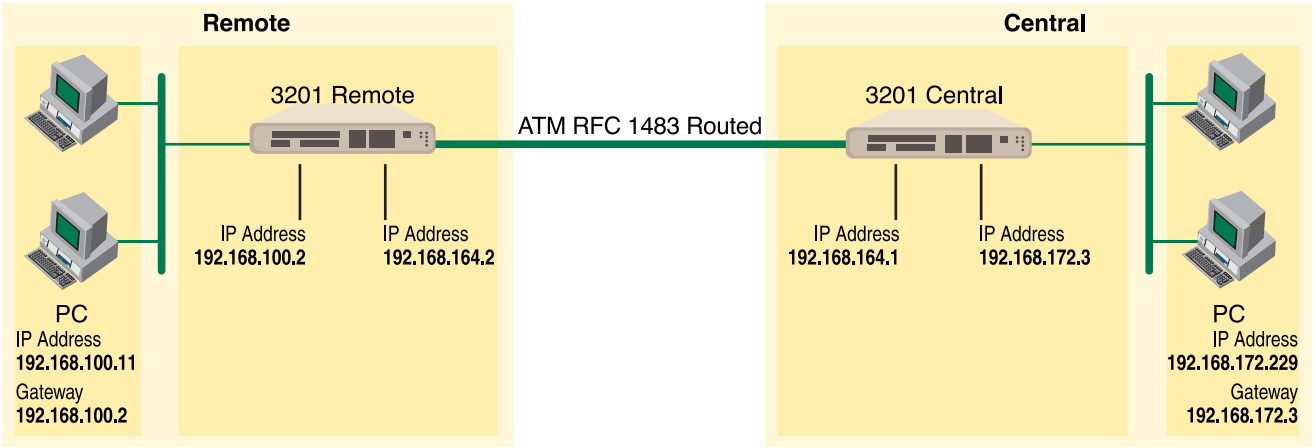
From the WWW interface:

1. Click **Configuration**.
2. Click **IP routes**.
3. Create new IP V4 Route.
4. Add Gateway *192.168.164.2*.

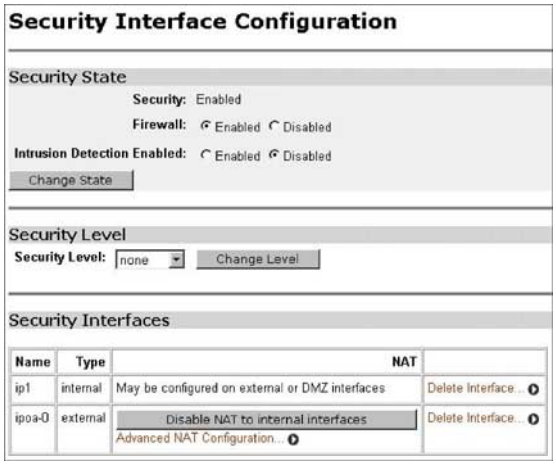
5. Click **OK**.

Do the following to confirm that the new route is working properly:

- Verify that the DSL WAN LED is lit.
- Ping the Remote unit from the Central Console
  `→ip ping 192.168.100.11`
- Ping the Central unit from the Remote Console
  `→ip ping 192.168.172.229`




**Note** It is important to understand that for PCs to be able to send IP traffic to different networks there must be routes in place. For example, the Remote PC has a gateway of 192.168.164.30 and it will successfully send out IP traffic over the DSL link to the CENTRAL Network side. Central Computer has 209.49.110.130 gateway address and it will successfully send out all IP traffic over DSL link to the REMOTE Network side. In this case all traffic that is not local to the network will be sent out the gateway interface.




## NAT Configuration

From the WWW interface:

1. Click **Security.**
2. Enable Security, then click the Web browser's refresh button to display the change.
3. Under Security interfaces, add your internal and external interfaces based on where you want NAT to be applied. For example, NAT could be applied to the public routable address 192.168.172.3 (the address of the Ethernet interface on the Central 3201).
4. Add *ip1* as external interface.
5. Add *rfc1483-0* as internal interface.
6. Enable *NAT* to internal interfaces.

This should NAT all IP traffic that is being sent (from the internal side of this network) out the Ethernet port on the 3201 Central unit.

> **Note** Once you enable NAT on the Ethernet (external) port, you will be unable to manage this device from the Ethernet IP address. Do the following at the Remote side of the network to make it so you can manage this device from the Ethernet IP address.

1. Access the web page using the WAN IP address of the Central 3201.
2. Click Security. You will see Security Interfaces.
3. Click Advanced NAT Configuration.
4. Click Add Reserved Mapping.
5. Add Internal IP Address: 192.168.164.1.
6. Change Transport Type to TCP.

7. Add Port Number 80.

You should be able to reach the web interface from the Central side using the Ethernet IP address.

# Chapter 8 Monitoring Status

## *Chapter contents*

## Status LEDs

The LEDs indicate the status of the Power, the WAN (DSL) inter-modem link, and the Ethernet connection.

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

Table 5. Status LED descriptions

| | | | |
|---|---|---|---|
| **Power** | Yellow | | *ON* indicates that power is applied.<br>*off* indicates that no power is applied.<br>*2 Hz flash* occurs during POST<br>*1 Hz flash* occurs for non-fatal error.<br>*8 Hz flash* on **all LEDs** for fatal POST outcome or critical error. |
| **WAN (DSL)** | Link | Yellow | *Solid yellow:* connected<br>*2 Hz flash:* training<br>*8 Hz flash:* DSL error<br>*No indication:* no signal detected. |
| | TX | Yellow | *Flashing:* when transmitting data from the unit to the WAN. |
| | RX | Yellow | *Flashing:* when receiving data from the WAN to the unit. |
| **Ethernet** | Link | Yellow | *On:* Ethernet is linked. |
| | 100M | Yellow | *On:* 100 Mbps Ethernet is selected. |
| | TX | Yellow | *Flashing:* when data is transmitted from the unit to the LAN. |
| | RX | Yellow | *Flashing:* when data is received from the LAN. |

# Chapter 9 Diagnostics and Software Upgrades

## *Chapter contents*

## Ping

The ping command is executed from the Command Line Interface (CLI). Ping in the 3201/3241 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

 →
```

## 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 3201'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 3201.
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 3201/3241 via TFTP. .

> **Note** The Patton 3201/3241 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 *script.bat*. (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.

# Chapter 10 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 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 5 days a week, from 8:00am to 5:00pm EST 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) 975-1007** 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 **Specifications**

## *Chapter contents*

## General Characteristics

- Compact low-cost plug-and-play router
- 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.
- 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.
- External UI, 120 VAC, 230 VAC, or 48 VDC Power Supply Options. UI are standard and included in price of unit. 120/230 VAC and 48 VDC are extra charge options.
- Field Factory Default Option.
- Standard 1 year warranty.

## G.SHDSL Characteristics (Model 3201/3241)

- 2.3 Mbps speed (Model 3201) over 2 wire.
- 4.6 Mbps speed (Model 3241) over 2 wire.
- DTE Rates 192 kbps to 2.32 Mbps operation.
- Distance from 30,000 ft (9,144 m) at 192 kbps to 16,400 ft (5,000 m) at 2.3 Mbps on 24 AWG (0.5 mm) wire
- Annex A (ANSI), Annex B (ETSI) PSD selection.
- 2 wire support per ITU G.991.2 and ETSI TS 101524 with G.994.1 handshake.
- When connecting two routers and modems in a point-to-point application, one modem must be set for central mode, the other for remote mode.
- 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.

## 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 and Traceroute 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.

## 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.
- FRF.12 Frame Relay Fragmentation support, LMI For Frame Relay PVC Link Management, FRF.5 Frame Relay to ATM Network internetworking, and FRF.8 Frame Relay to ATM Service Internetworking.

## 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)
- 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)

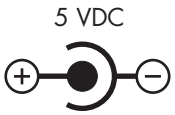
## Power and Power Supply Specifications

The 3201 may come with either an AC or DC power supply.

- The supply's connection to the 3201 is a 2.5 mm barrel receptacle with the center conductor positive.
- There is one fuse in the equipment rated at 250V, 500 mA, 2 sec.
- Model 3201's Rated voltage: 5 VDC
- Model 3201's Rated current: 1 A DC

External AC universal power supply

- Output from power supply: 5 VDC, 2A




- Input to power supply: universal input 100 – 240 VAC 50/60 Hz 0.3A

CAUTION

An approved external power supply that incorporates a disconnect device must be used and positioned within easy reach of the operator's position

CAUTION

Connect the equipment to a 5 VDC source that is electrically isolated from the ac source. The 5 VDC source is to be reliably connected to earth.

- External 48 VDC power supply
  - Input
    - Rated voltage: 36–60 VDC
    - Rated current: 0.25 A DC
    - 3-pin locking connector, 3.5 mm pitch
    - Reverse polarity protection
    - Transient over-voltage protection, 100 VDC at 2 ms
  - Output
    - Rated voltage: 5 VDC ± 5%, 5W
    - Rated current: 1 A DC
    - 6-inch cable terminated with 2.5 mm barrel plug, center positive


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.

- Isolation 500 VDC
- Environment 0–50°C; 5–95% relative humidity, non-condensing
- Size 3.0 x 1.63 x 0.75 in. (76 x 42 x 19 mm)

# Appendix B Cable Recommendations

## *Chapter contents*

## DSL Cable

10 foot (3 m), RJ-11/RJ-11 (refer to “RJ-11 non-shielded port” on page 122)

## Ethernet Cable

Ethernet cable (P/N 10-2500) (refer to “RJ-45 shielded 10/100 Ethernet port” on page 122)

## Adapter

EIA-561 to DB-9 (P/N 16F-561) (refer to “RJ-45 non-shielded RS-232 console port (EIA-561)” on page 122)

# Appendix C **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 |

## Power input

2.5 mm barrel plug/jack

# Appendix D 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:

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

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

To continue our example:

```
→ ethernet list ?
    ports
    transports
→ ethernet list
```

Then

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

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

Another example shows when the user must provide a parameter.

```
→ ip ?
    list
    clear
    add
    delete
    set
    attach
    attachbridge
    detach
    show
    interface
    ping
→ 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.

```
→ ip interface ip1 ?
    add
    delete
    clear
    list
→ ip interface ip1 list ?
    secondaryipaddresses
→ 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.

```
→ system config save
```

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

```
→ 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: ***
→
```

**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. 3201 or 3201 |
| ModemState | RO | Idle<br>Deactivated<br>Norm Oper<br>In-Progress | Show the state of the handshaking process:<br>Idle – The DSL chip is in idle state<br>Deactivated – The DSL chip is deactivated<br>Normal Operation – The DSL chip is in operating (Link established)<br>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. |
| DataRatel | 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<br>Remote | Central – CO unit<br>Remote – CPE unit |
| Interface | RW | Hdlc | Utopia – Data will be packaged in ATM cell format and send through the UTOPIA interface of the processor<br>Hdlc – Data will be packaged in HDLC frame and send through the PCM Bus |
| Action | WO | Start<br>Deactivate | Start – Command the box to configure the DSL chip and start the handshaking process<br>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

```
→ gshdsl set terminal central
→ gshdsl set interface utopia
→ gshdsl set dataRateN 32
→ gshdsl set dataRateI 0
→ gshdsl set Action Start
```

For CPE (remote) unit

```
→ gshdsl set terminal remote
→ gshdsl set interface utopia
→ gshdsl set dataRateN 32
→ gshdsl set dataRateI 0
→ gshdsl set Action Start
```

Default Setting of the unit

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