TRACER® 2631
User Manual

RADIO FREQUENCY INTERFACE STATEMENT

This equipment has been tested and found to comply with the limits for an intentional radiator, pursuant to Part 15, Subpart C of the Federal Communications Commission (FCC) Rules. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause interference to radio communications.

The limits are designed to provide reasonable protection against such interference in a residential situation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna of the affected radio or television.
- Increase the separation between the equipment and the affected receiver.
- Connect the equipment and the affected receiver to power outlets on separate circuits.
- Consult the dealer or an experienced radio/TV technician for help.

W A R N I N G

Changes or modifications not expressly approved by ADTRAN could void the user's authority to operate the equipment.

Shielded Cables

A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference with nearby radio and television reception when using the AC voltage adapter. It is essential that only the ADTRAN-provided power cord be used.

FCC Output Power Restrictions

The FCC does not require licensing to implement this device. However, the FCC has established restrictions regarding maximum output power and the adjustments required when employing directional gain antennas. (Refer to *Setting the Transmitter Power* in Section 2 of this manual). These restrictions are detailed in FCC Part 15.247 (b)(1), (b)(3)(i), and (3)(iii). It is the responsibility of the individuals designing and implementing the radio system to assure compliance with these and any other pertinent FCC Rules and Regulations. **This device must be professionally installed.**

Exposure to Radio Frequency Fields

The TRACER 10BaseT is designed in three versions with the following power options:

2.4 GHz @ 100 mW
2.4 GHz @ 1 W
5.8 GHz @100 mW

Radio Frequency Interference Statement

These levels of RF energy are below the Maximum Permissible Exposure (MPE) levels specified in FCC OET 65:97-01. The installation of high gain antenna equipment in the system configuration may create the opportunity for exposure to levels higher than recommended for the general population at a distance less than 15 feet (4.6 meter) from the center of the antenna. **The following precautions must be taken during installation of this equipment**:

- The installed antenna must not be located in a manner that allows exposure of the general population to the direct beam path of the antenna at a distance less than 15 feet (4.6 meters). Installation on towers, masts, or rooftops not accessible to the general population is recommended; or
- Mount the antenna in a manner that prevents any personnel from entering the area within 15 feet (4.6 meter) from the front of the antenna.
- It is recommended that the installer place radio frequency hazard warnings signs on the barrier that prevents access to the antenna.
- Prior to installing the antenna to the RFC output, make sure the power is adjusted to the settings specified in Section 2 of this manual.
- During antenna installation, be sure that power to the TRACER 10BaseT equipment is turned off in order to prevent any energy presence on the coaxial connector.
- During installation and alignment of the antenna, do not stand in front of the antenna assembly.
- During installation and alignment of the antenna, do not handle or touch the front of the antenna.

These simple precautions must be taken to prevent general population and installation personnel from exposure to RF energy in excess of specified MPE levels.

Page

Section 1. TRACER 2631 Description

Section 2. Installation

Section 3. Operation

Figures

List of Figures

Tables

List of Tables

INTRODUCTION

The TRACER 2631 provides T1 transport and Ethernet routing capability by way of a spread spectrum microwave link for distances of 30 miles or more depending on path engineering. System performance is partially determined by the engineering of the microwave link. Each end of a TRACER 2631 link is composed of two units – the baseband processor (BBP) and the radio frequency (RF) converter. A DS1/DSX-1 (T1) interface and a 10BaseT Ethernet interface are provided on the rear of the BBP, which can be mounted in a 19-inch rack. The DS1/DSX-1 interface provides connections up to 6000 feet from T1 equipment, and the Ethernet interface is fully compliant with the IEEE 802.3 standard. A single coaxial cable connects the BBP to the RF converter and another coaxial cable connects the RF converter to the antenna.

ISM BAND SPREAD SPECTRUM

The Federal Communications Commission (FCC) has established several portions of the RF spectrum for use in Industrial, Scientific, and Medical (ISM) applications. Part 15.247 of the FCC rules describes the requirements of systems that operate in these bands. The three bands set aside, 902-928 MHz, 2400-2483.5 MHz, and 5725-5850 MHz, are designated for use by spread spectrum transmitters, either frequency hopping or direct sequence. Spread spectrum is a form of communication in which the bandwidth of a message signal is intentionally increased or "spread." The TRACER 2631 operates in the 2400-2483.5 MHz or 5725-5850 MHz band using direct sequence spread spectrum (DSSS) transmission.

APPLICATIONS

Any application that would typically require a metallic T1 transport and/or a 10BaseT router interface could use the TRACER 2631 to provide both. **Figure 1-1** illustrates a typical application.

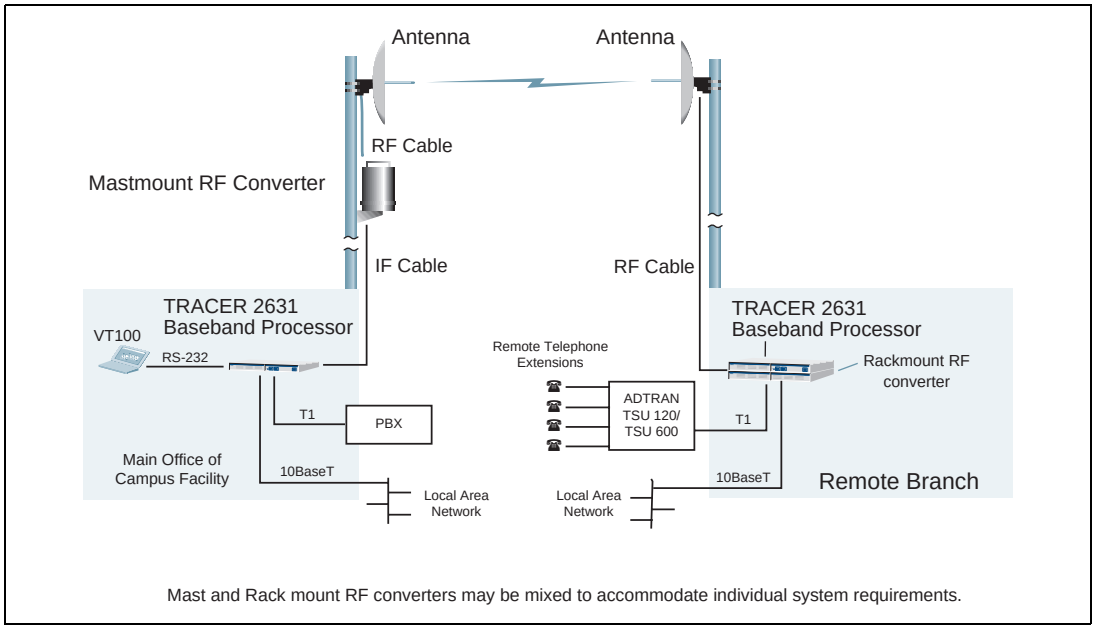

Figure 1-1. Typical Application

The TRACER 2631 can be used in any application that requires data to be shared at a high rate of speed. In addition to telephony applications, TRACER 2631 can be used in data communications such as inter-networking, video conferencing, and telemetry.

Direct Sequence

A direct sequence transmitter spreads the link signal by mixing the data with the output of a pseudorandom number generator which changes state at a rate higher than the data rate. This rate is called the “chipping” rate. The TRACER 2631 chipping rate is twelve times the data rate.

Coding

Many different pseudorandom sequences exist. The sequences are called pseudorandom because, although they appear noise-like, they are determinant and repeat after a specific number of chips. The longer a code is, the better correlation characteristics it possesses. These traits allow multiple spread spectrum systems to operate in the presence of one another with minimal interference if they are operating with different sequences. The TRACER 2631 provides ten different 120-bit long sequences to help ensure minimal interference operation in high traffic areas.

CHANNEL SELECTION

The FCC has allocated 83.5 MHz of spectrum in the 2.4 GHz band and 125 MHz in the 5.8 GHz band in which TRACER 2631 operates. A TRACER 2631 system divides the band into two portions, transmitting in one and receiving in the other. **Figure 1-2** illustrates the bandwidth division.

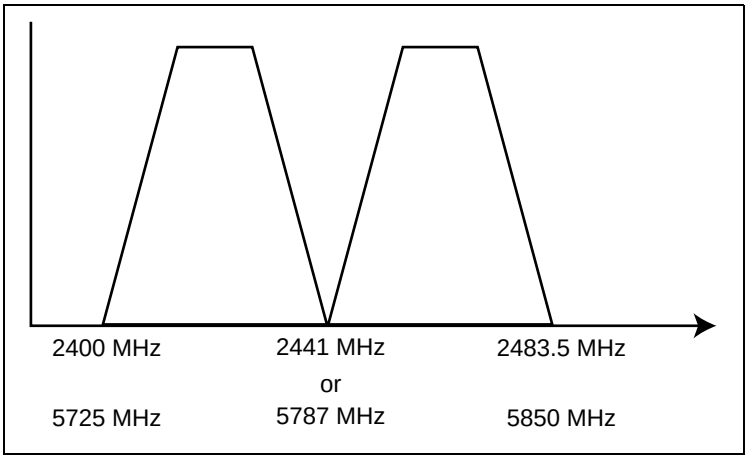

Figure 1-2. Bandwidth Division

The transmitter at one end of a link will transmit in the lower portion of the spectrum. Consequently, the receiver at the other end will receive in the lower portion of the band and transmit in the upper portion. Thus, a system will operate in one of two frequency plans -- transmit in the upper and receive in the lower or vice versa. These two plans are called Plan A and Plan B. One end of a path will be on Plan A and the other will be on Plan B. Shipment of a link will consist of an A and a B unless otherwise specified.

FORWARD ERROR CORRECTION

With the addition of overhead data, error detection and correction capability can be added to a data stream. Error correction can be accomplished by allowing the receiver to request the re-transmission of a detected errored block. The TRACER 2631, on the other hand, implements forward error correction (FEC) which adds enough overhead data for the receiver to detect and correct errors in the data stream without the necessity of retransmission. The addition of FEC decreases the required signal-to-noise (S/N) ratio by approximately 5.5 dB to achieve a given bit error rate (BER).

T1 OPERATION

Framing

The data in a T1 stream is delimited by framing bits. The pattern of the framing bits follows one of two formats – extended superframe (ESF) or superframe (SF). The T1 interface must be prepared for the format that will be used.

Line Code

A mark in the data stream is coded as a pulse on the T1 line. A space is coded as "no activity" on the T1 line. As a form of error detection, subsequent marks in the data stream are coded as pulses of alternating polarity, either positive going or negative going. This type of line coding is called alternate mark inversion (AMI).

For the T1 receiver to operate correctly, a minimum number of "1s" must exist on the T1 facility. If the data cannot be guaranteed to meet this requirement, then another line coding format is used. In the bipolar 8 zero substitution (B8ZS) scheme, a string of eight "0s" is replaced by a special sequence of eight bits that contains a bipolar violation. The receiver, upon recognizing this sequence, reinserts the eight "0s" and the data is recovered intact.

DS1/DSX-1 Interface

When connecting the interface to the public switched network (PSN), an ADTRAN-provided cross-over cable (P/N 3125M011) is required to meet FCC part 68 and IC CS03 requirements. This cable is required to cross-over the TX and RX pairs to meet the connecting arrangement of a network interface device. This cable is included with the BBP and is labelled **T1 CROSSOVER**.

Line Buildout or LBO

The DS1/DSX-1 interface provides two different types of line buildouts (LBOs). When set for DS1, LBOs for 0 dB, -7.5 dB, -15 dB, and -22 dB are available. The DS1 interface can operate on line lengths up to 6,000 feet. When set for DSX-1 interface, LBOs for 0-133 feet, 266-399 feet, 399-533 feet, and 533-655 feet are available.

ROUTER OPERATION

Rear Panel

There are two sets of switches on the back panel. The **TO HUB/TO NIC** switch allows the TRACER 2631 to connect directly to a Network Interface Card (NIC) or a HUB without the need for special cabling.

The **OFF/ON** switch block is for factory default and firmware downloading. With switch 1 in the up or **OFF** position, the TRACER 2631 will immediately go into a download mode when power is enabled. Switch 1 must be in the down or **ON** position in order to boot up normally. Switch 2 in the up or **OFF** position will force the entire configuration to be factory defaulted.

Configuration

The router options on the TRACER 2631 are configured using a menu-based interface. This interface can be accessed via the maintenance port using any asynchronous VT-100 terminal or personal computer running a terminal emulation program, or via the LAN using a Telnet client program. To use the Telnet interface, the TRACER 2631 must first have an IP address programmed into it via the maintenance port. The factory default is 10.0.0.1.

Security

Security on network devices is a major concern for almost anyone with a network. The TRACER 2631 provides many tools for securing the local network from hostile users. Connections can be authenticated using passwords. When accessing router functions, a RADIUS client can also be used for authentication.

The Telnet configuration can also be protected using the same authentication methods. Each router menu item in the TRACER 2631 has a security level associated with it. A Telnet session is assigned a privilege level which determines which menu items are accessible to the Telnet client. See *Security Levels* on page 34 for more information on menu security levels.

Filters can be defined to prevent certain addresses or protocols from being transferred from LAN-to-WAN, WAN-to-LAN, or WAN-to-WAN.

TRACER 2631 SYSTEM CONFIGURATION

A TRACER 2631 system is composed of three major subsystems – a baseband processor, a radio frequency convertor, and an antenna. The following sections describe the system components.

Baseband Processor (BBP)

The BBP (ADTRAN P/N 1280TRCRT1L1) is a 1-U, 19-inch rackmountable unit that provides the system electrical interfaces, user controls and indicators, and performs the spread spectrum processing for the system. The rear panel provides all of the electrical interface points – DS1/DSX-1 interface, DS1/DSX-1 monitor, 10BaseT interface, option switches, VT-100 terminal, alarm contacts, IF signal, DC power (from facility), and AC power (from DC adapter). The BBP front and rear panels are illustrated in **Figure 1-3** and **Figure 1-4**.

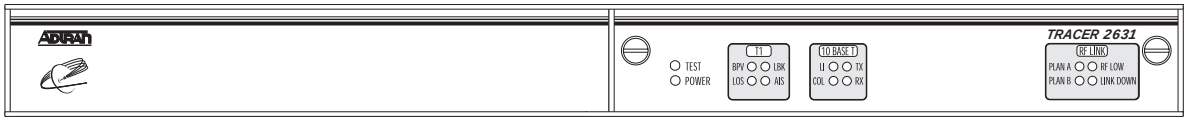

Figure 1-3. BBP Front Panel

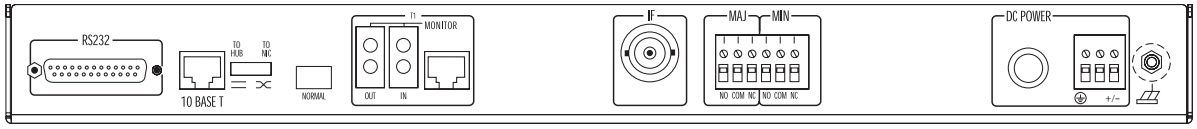

Figure 1-4. BBP Rear Panel

10BaseT Bridge/Router Interface

The TRACER 2631 provides the following basic functions:

1. **LAN Bridge:** Bridging provides a point-to-point connection between two LANs. The bridge learning function scans the source and destination media access control (MAC) addresses of all packets on its local LAN and determines which packets should be transmitted over the wireless link. Applications include connectivity between single user or small offices to corporate LANs. The TRACER 2631 uses the Spanning Tree Algorithm (IEEE 802.1d-ISO/IEC10038), which provides a loop-free topology and redundancy.
2. **IP Router:** The TRACER 2631 can function as an IP router using the Routing Information Protocol (RIP) for advertising and learning routes among other routers. Static routes may also be entered into the routing table.
3. **IPX Router:** IPX routers and services can be exchanged between the TRACER 2631 and other devices using RIP and Service Advertising Protocol (SAP). Watchdog serialization filtering and spoofing can permit the wireless link to be idle during no application traffic periods.
4. **Network Address Translation (NAT):** Single networks can connect to the Internet with this function. The TRACER 2631 translates outgoing IP packets over the wireless link to the IP router at the Internet Service Provider (ISP). Many popular Internet applications are supported.
5. **Point-to-Point Protocol (PPP) or Frame Relay:** The layer two protocol used to transfer packets can be PPP or Frame Relay (RFC 1490). PPP allows a point-to-point connection, whereas Frame Relay can provide up to ten permanent virtual circuits.

Routing and Bridging with the TRACER 2631

The TRACER 2631 is a Router and Transparent Learning Bridge. Its features can be easily configured and used once several basic concepts are understood.

Factory Default

The TRACER 2631 comes from the factory configured for MAC Bridging, IP routing and IPX routing with no filters or connection information defined. An IP address of 10.0.0.1 with a network mask of 255.255.255.0 is preloaded. The factory default layer two configuration is PPP, which provides the least amount of reconfiguration due to its negotiation-oriented nature.

I M P O R T A N T

To disable routing functionality and configure the TRACER 2631 as a bridge, configure the **LAN/CONFIGURATION/IP ROUTER/MODE** menu option to **OFF**. Next, configure the **LAN/CONFIGURATION/IPX ROUTER/MODE** menu option to **OFF**.

Bridging

In Bridge Mode, the TRACER 2631 can be used to connect two LAN segments. In this mode, all protocols are supported because they are transported across the wireless link at the MAC layer. The Spanning Tree Algorithm can be used to guarantee a loop-free topology. MAC addresses are "learned" by each TRACER 2631 to prevent non-WAN packets from being bridged.

IP Routing

The TRACER 2631 operates as an IP router when the **LAN/CONFIGURATION/IP/IP ROUTER/MODE** option is configured to **ON**. In PPP mode, the TRACER 2631 uses an IP unnumbered WAN interface; the IP address and mask assigned to the unit's LAN interface apply to all routing and IP operations for the unit. In Frame Relay mode, each PVC can be specified as a numbered or unnumbered link. If a default gateway is specified on the network of the Ethernet interface, the unit attempts to reach the gateway through that interface. If no default gateway is specified (i.e., 0.0.0.0) the WAN interface becomes the default gateway (recommended for remote applications when there are no other routers on the remote LAN).

IPX Routing

Network routes and services are learned and advertised using Novell's RIP and SAP.

Concurrent Routing And Bridging

The TRACER 2631 can route IP and IPX as well as bridge non-IP/IPX packets simultaneously. The PPP profile will by default negotiate PPP network protocols to support the transmission and reception of IP, IPX, and Bridge packets. If the PPP peer does not accept a protocol, the TRACER 2631 will fall back to any combination of routing and bridging.

Network Address Translation Mode

NAT is a special mode of operation in which the TRACER 2631 obtains a dynamically assigned IP address from the peer router (typically an ISP). This allows a network of computers to appear as a single IP address.

NAT is enabled if the layer two protocol is PPP and the PPP profile has the IP parameter **NAT** set to **YES**, or the layer two protocol is Frame Relay and a DLCI mapping has the **IP MAP/NAT** parameter set to **YES**. The network computer's IP stack may use DHCP to request an IP address, default gateway address, and domain name server addresses from the TRACER 2631.

DS1/DSX-1 Interface

The DS1/DSX-1 interface (designated "T1") is provided for connecting to the T1 equipment. Two types of physical interfaces are provided – RJ-48C and bantam jacks.

The interfaces are illustrated in **Figure 1-5**. The functions of the BBP are partitioned into two printed circuit boards or PCBs, all contained in the same enclosure.

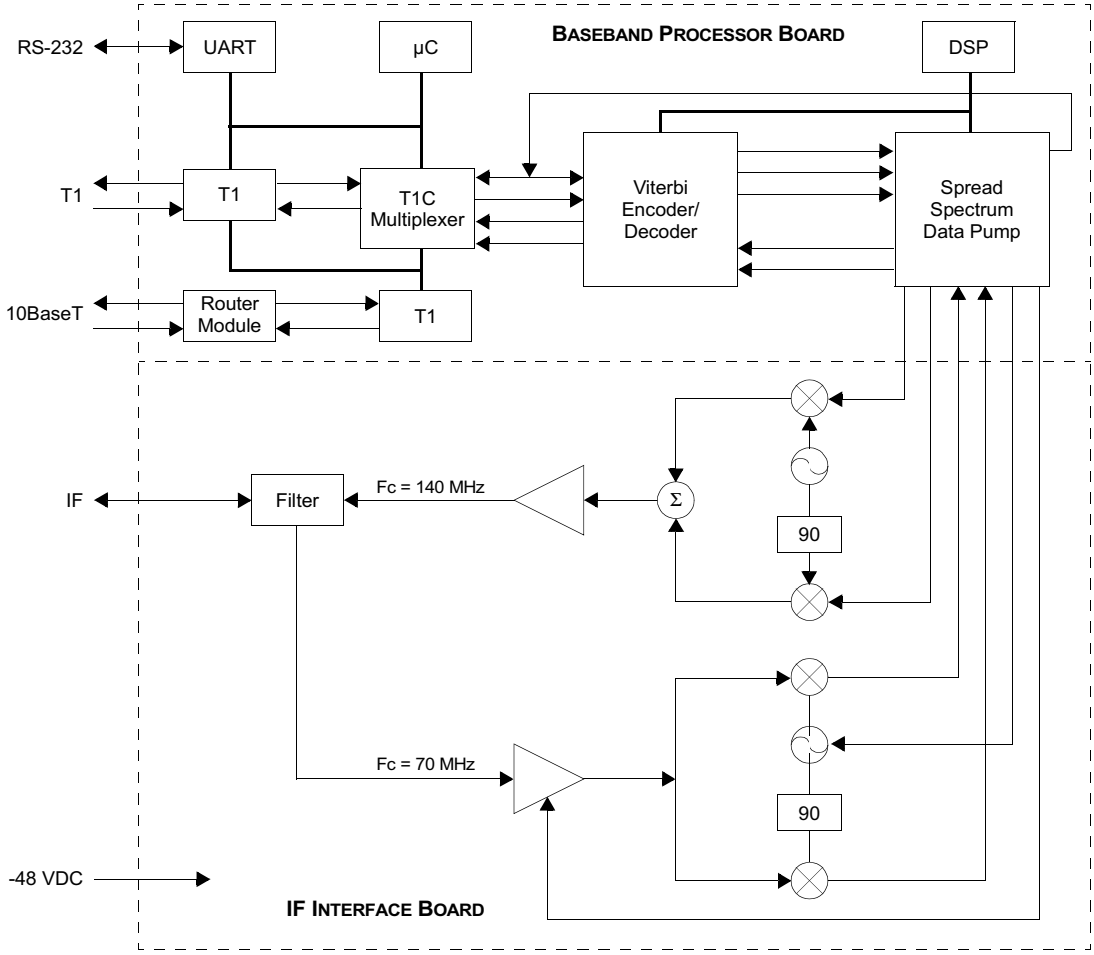

Figure 1-5. BBP Block Diagram

The upper bantam connectors, labeled **MONITOR**, provide isolated monitor points for testing. The lower bantam jacks provide signal insertion points. The insertion of a bantam jack disconnects the RJ-48C connector from the circuit. The DS1/DSX-1 interface can operate on line lengths up to 6000 feet.

When connecting the T1 interface to the Public Switched Network, an ADTRAN-provided cross-over cable (P/N 3125M011) is required to meet FCC part 68 and IC CS03 requirements. This cable is included with the BBP and is labeled **T1 CROSSOVER**. This cable is required to cross-over the TX and RX pairs to meet the connecting arrangement of a network interface device.

For connections to other CPE-type equipment, such as the ADTRAN TSU-100, a straight-through T1 cable is provided by ADTRAN (P/N 3127004) and is included with the BBP.

VT-100 RS-232 Interface

A serial interface port using RS-232C signal levels is provided for attaching a VT-100 compatible terminal. The connection is made via a DB-25 connector on the rear panel. The data rate is configured for 9600 bps, 8 data bits, no parity, and 1 stop bit. Flow control on the serial interface should be configured for **NONE**.

A 7-day error history of the T1 interface and radio link is also provided. For the most recent 24 hours of operation, 15-minute histories are provided.

Alarm Contacts

Two sets of alarm contacts are provided on the rear of the BBP – major alarm and minor alarm. A major alarm indicates the radio link is not operational. A minor alarm indicates that system performance is degraded or that the T1 interface is experiencing errors. Normally-open and Normally-closed contacts are provided for both alarm types. Under normal operating conditions there is no continuity between the Normally-open and Common contacts. Under an alarm condition, continuity between those contacts exists. The Normally-closed and Common contacts normally have continuity; while under alarm conditions, these contacts are open.

IF Signal

The N-Type connector (labeled **IF**) on the rear panel provides the interface point between the BBP and the RF converter. This connection provides the data signal, power, and configuration information to the RF converter. A coaxial cable (ADTRAN P/N 3125RF027) is provided for connecting the BBP to the RF converter for the rackmount model. Cable for connecting the BBP to a mastmount RF converter must be provided by the customer after the length of cable has been determined.

Power

The unit receives power via one of two connectors. Power for the entire system is provided by these interfaces. The three-pin circular DIN connector is provided to connect an optional ADTRAN desktop AC adapter (ADTRAN P/N 1360DSK24VL1), providing 24 volts DC. The three-pin terminal block allows the connection of any DC power source providing between 21 and 60 volts DC. The power consumption of the entire system is 30 watts.

Controls and Indicators

The system may be configured via the front panel, which is accessible behind a drop-down panel on the right half of the BBP. The front panel is illustrated in **Figure 1-6** and **Figure 1-7**.

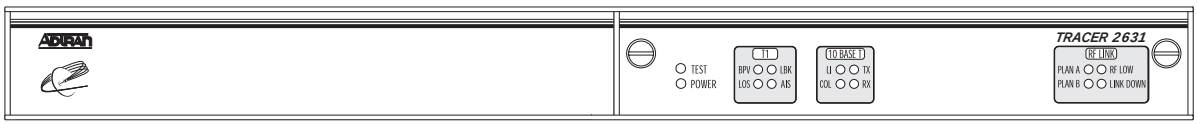

Figure 1-6. BBP Front Panel (with door closed)

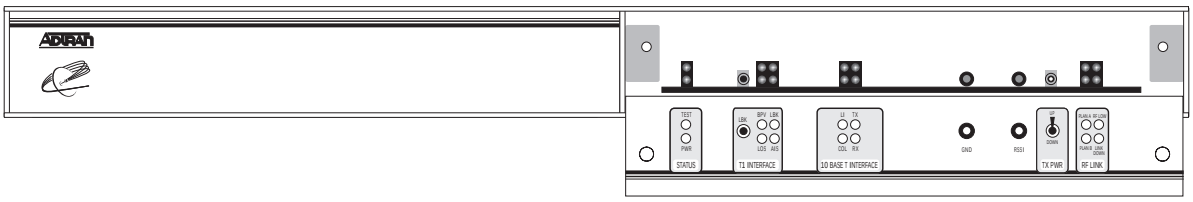

Figure 1-7. BBP Front Panel (with door open)

Options that are set from the front panel can be overridden via the terminal interface. As a rule, a *green* LED indicates a normal situation, a *red* LED indicates an error situation, and a *yellow* LED indicates a configuration option. LEDs indicating overall system integrity are listed in **Table 1-1**.

Table 1-1. System Integrity LEDs

LED	Description
Test	*Red* indicates that the self-test has completed and failed
PWR	*Green* indicates that DC voltage is applied

The LEDs associated with the DS1/DSX-1 interface are listed in **Table 1-2**.

Table 1-2. DS1/DSX-1 Interface LEDs

LED	Description
BPV	*Red* if the incoming T1 stream contains bipolar violations
RED	*Red* if there is no signal present at the T1 interface
LPBK	*Yellow* if the T1 interface is in loopback
AIS	Flashes to indicate a T1 Yellow Alarm; remains *On* (solid) to indicate an AIS alarm (when the DS1/DSX-1 is receiving a Blue code)

The LEDs indicating RF link status are listed in **Table 1-3**.

Table 1-3. RF Link Status LEDs

LED	Description
RF Low	*Red* indicates the received RF carrier level within approximately 10 dB of the minimum receive level
Link Down	*Red* indicates the radio path is down
Plan A	*Yellow* if frequency Plan A is selected
Plan B	*Yellow* if frequency Plan B is selected

The LEDs indicating 10BaseT status are listed in **Table 1-4**.

Table 1-4. 10BaseT Status LEDs

LED	Description
TX	*Green* if data is being transmitted on the 10BaseT interface
RX	*Green* if data is received on the 10BaseT interface
LI	Link integrity; *green* when there is a connection between TRACER 2631 and a hub or NIC
COL	Collision; *yellow* when there is a data collision on the 10BaseT interface

The front panel controls are listed in **Table 1-5**.

Table 1-5. Front Panel Controls

Control	Description
LBK	Toggles the T1 between no loopback and line loopback
TX PWR	UP increments radio transmit power up; DOWN increments radio transmit power down; VT-100 terminal will indicate TX Power setting

Non-volatile Memory

The TRACER 2631 system contains non-volatile memory to retain certain configuration settings. These settings include:

- Frequency plan
- Chipping code
- Password
- Password enabling
- Site name
- T1 line coding
- T1 framing
- All router configuration parameters

Built-In Tests

The TRACER 2631 has several features to aid in site setup and troubleshooting. These diagnostics include T1 loopbacks and a router loopback with 2047 BERT (Bit Error Rate Test) data.

The monitor points provided on the front panel of the system are listed in **Table 1-6**.

Table 1-6. Front Panel Monitor Points

I	Demodulated received baseband output
Q	Demodulated received baseband output
RSSI	DC voltage indicating strength of the received signal at the antenna
GND	System ground

Radio Frequency (RF) Converter

The RF converter provides the RF interface between the BBP and the antenna. The RF converter is partitioned into two major components – the transmitter and the receiver.

The major connections illustrated in **Figure 1-8** are transmit signal (**TX**), receive signal (**RX**), and the IF signal (**IF**) connection.

The RF converter unit is enclosed in a metal enclosure approximately 9.5 inches x 5.5 inches x 1 inch and is mounted in a 1-U, 19-inch rackmountable housing or mastmountable, weatherproof enclosure.

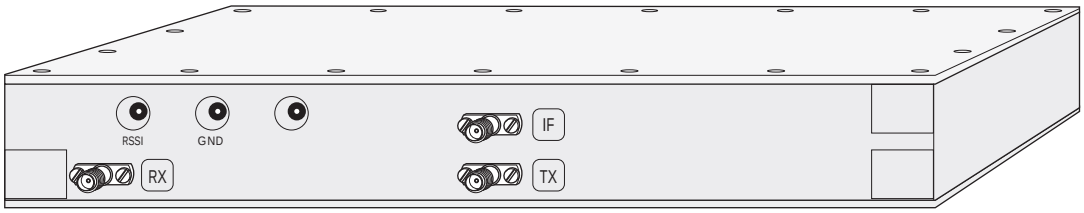

Figure 1-8. RF Converter Module

Three SMA connectors, located on the RF converter module, provide RF and IF connection points. A test point is provided for monitoring the received signal strength indicator (RSSI). The voltage (relative to the GND test point) present on this test point represents the level of the received signal. This signal is used to align the antenna when installing the system and to verify the link is performing as designed. The RSSI test point is also available on the front panel of the BBP. The only connections that must be made in the field are a coax connection between the BBP and the RF converter and a coax connection between the RF converter and the antenna. These connections require male, type N coax connectors.

I M P O R T A N T

The voltage level present at the RSSI test point represents only a relative signal level of receive strength from the far end. No direct correlation can be made between RSSI voltage level and actual receive level in dBm. This test point is provided to assess relative signal level for alignment of antennas.

The **IF** connector provides the connection between the BBP and the rackmounted or mastmounted RF converter. Make sure that the connector labeled **IF** on the BBP is connected to the connector labeled **IF** on the RF converter. An 8-inch IF cable [ADTRAN P/N 3125RF027] is provided for rackmount systems. The **TO ANTENNA** connection provides the connection between the RF converter and the antenna. A block diagram of RF converter functions is shown in **Figure 1-9**.

C A U T I O N

When connecting an RF converter to a baseband processor, verify that the connector labeled **IF** on the rear panel of the baseband processor is connected via coax to the connector labeled **IF** on the RF converter. Connecting the baseband processor to the incorrect connector on the RF converter will cause the internal 1 amp 250 volt fuse to blow in the baseband processor. This fuse is accessed by removing the top of the baseband processor, and is located on the left side of the chassis when facing the front panel.

The RF converter module is enclosed in either a 19-inch EIA rackmount housing, or a weather-tight enclosure suitable for mastmounting near the antenna for enhanced system performance. The RF converter mastmount and rackmount housings are illustrated in **Figure 1-10** and in **Figure 1-11** on page 13.

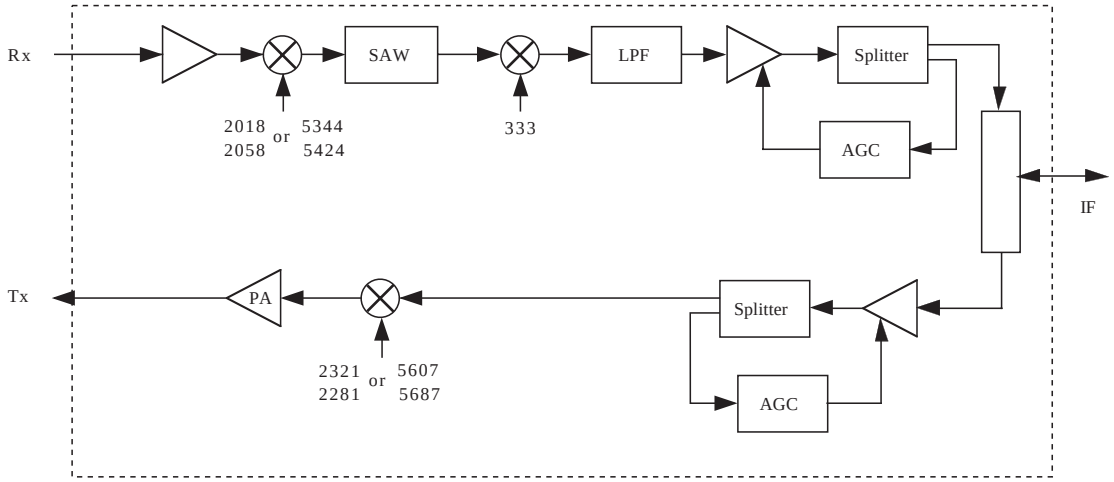

Figure 1-9. RF Converter Function Block Diagram

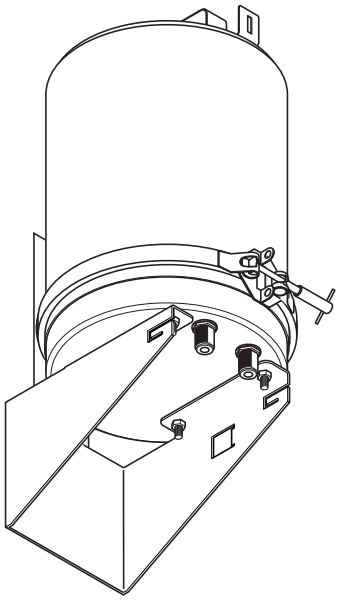

Figure 1-10. Mastmount RF Converter Housing

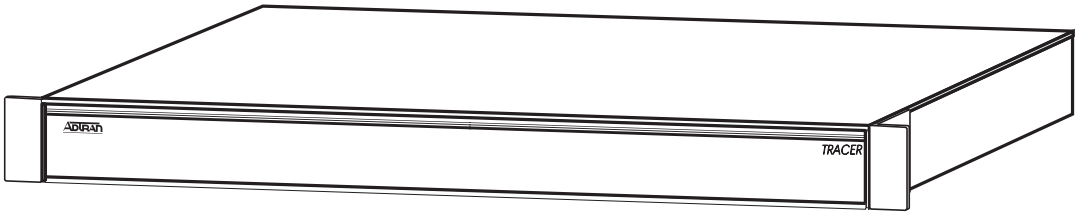

Figure 1-11. Rackmount RF Converter Housing

Antenna

TRACER 2631 is intended to be coupled with an antenna that is directional and provides signal gain. There are several reasons for this requirement.

- TRACER 2631 operates in point-to-point applications; therefore, an omnidirectional antenna is not needed.
- The FCC provides no recourse in this band in the event of nearby interference, so a directional antenna reduces the likelihood of interference in the antenna pattern.
- The low power transmitter is intended to be used with a high-gain antenna for long links.

The antenna requirements are listed in **Table 1-7**.

Table 1-7. Antenna Requirements

Antenna	**100 mW**	**1 W**
Minimum gain	15 dBi	6 dBi
Minimum return loss	15 dB	15 dB
Connector	N-type	N-type
Impedance	50Ω	50Ω

UNPACK, INSPECT

Carefully inspect the TRACER 2631 for any damage. If damage is suspected, file a claim with the carrier, then contact ADTRAN's Customer Service Department. If possible, keep the original shipping container for use in shipping the TRACER 2631 back for repair or for verification of damage during shipment.

Before beginning installation, verify that all of the following components are present.

Rackmounted RF Converter Configuration

Provided by ADTRAN
- Baseband processor
- Rackmounted RF converter
- BBP to RF converter IF interconnect cable
- DS1/DSX-1 interface cables (straight-through and crossover; RJ-48C to RJ-48C)
- Category 5 10BaseT cable (RJ-45 to RJ-45)

Provided by customer
- Antenna feedline cable
- Antenna and mounting hardware
- VT-100 terminal and RS-232 interface cable
- 21 to 60 volt DC power source (available from ADTRAN), either polarity referenced to ground

Mastmounted RF Converter Configuration

Provided by ADTRAN
- Baseband processor
- Mastmounted RF converter
- DS1/DSX-1 interface cable (straight-through and crossover; RJ-48C to RJ-48C)
- Category 5 10BaseT cable (RJ-45 to RJ-45)

Provided by Customer
- Antenna feedline cable
- Antenna and mounting hardware
- BBP to mastmounted RF converter IF interconnect cable
- VT-100 terminal and RS-232 interface cable
- 21 to 60 volt DC power source (available from ADTRAN), either polarity referenced to ground

INSTALLATION

Location and Mounting

Install the TRACER 2631 in a location that requires minimal antenna feedline length (the loss in this cable directly affects overall system performance). The BBP is designed to be mounted in a rack above the rackmount RF converter (if the rackmount RF converter option is applicable). Although no space is needed between the units, certain regulations may require at least 0.75 inches of space above and below the BBP.

Power Requirements

The TRACER 2631 can operate from a supply between 21 and 60 volts DC, with either polarity referenced to ground. Typical power consumption is 30 watts. Amperage is determined by dividing the wattage by the input voltage. For example, at 48 volts, TRACER 2631 would draw approximately 30 watts/48 volts = 0.625 amps.

Grounding

The following grounding instructions are derived from the Underwriters' Laboratory *UL 1459 Standard for Safety: Telephone Equipment* dated September 20, 1993.

An equipment grounding conductor that is no smaller in size than the ungrounded branch-circuit supply conductors is to be installed as part of the circuit that supplies the product or system.

Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green, or green with one or more yellow stripes.

The equipment grounding conductor is to be connected to ground at the service equipment.

The attachment-plug receptacles in the vicinity of the product or system are all to be of a grounding type, and the equipment grounding conductors serving these receptacles are to be connected to earth ground at the service equipment.

A supplementary equipment grounding conductor shall be installed between the product or system and ground that is in addition to the equipment grounding conductor in the power supply cord.

The supplementary equipment grounding conductor shall not be smaller in size than the ungrounded branch-circuit supply conductors. The supplementary equipment grounding conductor shall be connected to the product at the terminal provided, and shall be connected to ground in a manner that will retain the ground connection when the product is unplugged from the receptacle. The connection to ground of the supplementary equipment grounding conductor shall be in compliance with the rules for terminating bonding jumpers at Part K or Article 250 of the National Electrical Code, ANSI/NFPA 70. Termination of the supplementary equipment grounding conductor is permitted to be made to building steel, to a metal electrical raceway system, or to any grounded item that is permanently and reliably connected to the electrical service equipment ground.

Bare, covered, or insulated grounding conductors are acceptable. Individually covered or insulated equipment grounding conductors shall have a continuous outer finish that is either green, or green with one or more yellow stripes.

The supplemental equipment grounding terminals are located on the rear of the BBP adjacent to the power connectors and on the rear of the rackmounted RF converter.

DS1/DSX-1 Interface

The rear panel of the TRACER 2631 has a jack labeled **T1** that provides the T1 interface. The pin assignments for the eight-position modular jack are listed in **Table 2-1**.

Table 2-1. DS1/DSX-1 Pin Assignments

Pin	Name	Function
1	R	Send data (ring)
2	T	Send data (tip)
3	N/A	Not Used
4	R1	Receive data (ring)
5	T1	Receive data (tip)
6	N/A	Not Used
7	N/A	Not Used
8	N/A	Not Used

Bantam jack connections are provided for test equipment access. Data is received on the jack labeled **IN** and is transmitted on the jack labeled **OUT**. Bantam jacks are provided for both inserting and monitoring the interfaces. When a plug is placed in the insert jack, the connection between the modular jack and the interface circuitry is broken. The monitor jacks provide access to monitor the transmitted and received signals without interference.

When connecting the T1 interface to the Public Switched Network, an ADTRAN-provided crossover cable (P/N 3125M011) is required to meet FCC part 68 and IC CS03 requirements. This cable is required to cross-over the TX and RX pairs to meet the connecting arrangement of a network interface device. This cable, labeled **T1 CROSSOVER**, is included with the BBP.

For connections to other customer premise equipment, such as an ADTRAN TSU, a straight-through T1 cable (ADTRAN P/N 3127004) is included with the BBP.

The DS1/DSX-1 interface must be configured for line code and framing from the VT-100 terminal. The choices for line code are AMI and B8ZS. The options for framing are SF and ESF. The interface should be configured to match the attached T1 equipment.

The LBO must be set for the DS1/DSX-1 interface. The LBO setting allows the DS1/DSX-1 interface transmitter to drive the interface with the correct signal strength and equalization based on the line attenuation between TRACER 2631 and the attached equipment. The LBO is set for the interface via the VT-100 terminal. Two sets of configurations are provided – DSX-1 for short-haul interface (less than 655 feet) and DS1 for long-haul interfaces (655-6000 feet). The settings are detailed in **Table 2-2** on page 18.

Table 2-2. LBO Settings

Interface Type	LBO
DSX-1	0-133 feet
DSX-1	133-266 feet
DSX-1	266-399 feet
DSX-1	399-533 feet
DSX-1	533-655 feet
DS1	0 dB
DS1	-7.5 dB
DS1	-15 dB
DS1	-22.5 dB

10BaseT Ethernet Interface

The rear panel of the TRACER 2631 has a jack labeled **10BASET** as well as a switch marked **TO HUB** and **TO NIC**. The pinout of the eight-position modular jack is dependent upon the position of this switch as shown in **Table 2-3**.

The **TO HUB**/**TO NIC** switch allows the TRACER 2631 to connect directly to a Network Interface Card (NIC) or a hub without the need for special cabling. The ADTRAN-provided Category 5 unshielded twisted pair (UTP) cable (ADTRAN P/N 3127026) can be used for either of these configurations.

Table 2-3. 10BaseT Pinout & Switch Position

Pin	Switch Position	
	TO NIC	TO HUB
1	TX1	RX1
2	TX2	RX2
3	RX1	TX1
4	Not Used	Not Used
5	Not Used	Not Used
6	RX2	TX2
7	Not Used	Not Used
8	Not Used	Not Used

LINK PLANNING

I M P O R T A N T

The appropriate transmitter power must be calculated as part of the link planning.

The factors that must be taken into account when planning a link are optimal received signal level, transmitter power, antenna feedline loss (each end), antenna gain (each end), free space path loss, and required fade margin.

I M P O R T A N T

The optimal signal level for the receiver is -60dBm.

Antenna Feedline Loss

Feedline loss is a function of feedline type and length. Feedline loss per 100 feet for several types of coax at IF and microwave frequencies is detailed in **Table 2-4**. The IF loss applies to BBP/RF converter interconnection, and the microwave loss applies to RF converter/antenna interconnection. Antenna manufacturers' specifications may vary.

Table 2-4. Antenna Feedline Loss

Cable	IF Loss/100 ft (in dB)	2.4 GHz Loss/100 ft (in dB)	5.8 GHz Loss/100 ft (in dB)
RG58	5.7	80	N/A
RG8 (air)	2.7	20	N/A
RG8 (foam)	2	9	N/A
1/4” Coax	1.42	5.91	11.36
3/8” Coax	1.25	5.76	9.65
1/2” Coax	0.81	3.83	6.49
7/8” Coax	0.44	2.2	N/A
1 1/4” Coax	0.33	1.62	N/A
1 5/8” Coax	0.27	1.41	N/A
5.8 GHz Elliptical Waveguide	N/A	N/A	1.23

Antenna Gain

Best performance will result from the use of a parabolic dish antenna. Antenna gain is determined by the size of the dish, with typical figures detailed in **Table 2-5**. Dish manufacturers will be able to supply gains for other types of antenna.

Table 2-5. Antenna Gain

Antenna Diameter (in feet)	Gain at 2.4 Ghz (in dB)	Gain at 5.8 Ghz (in dB)
2	21	28.5
4	27	34.2
6	31	37.5
8	33	40.7
10	35	42.5
12	37	44.2

Path Loss

The free space path loss is given by

$$Loss(dB) = 96.6 + 20 \log_{10} f + 20 \log_{10} D$$

where D is distance in miles

f is operating frequency in GHz

A tabulation of various path loss is given in **Table 2-6**.

Table 2-6. Path Loss

Link Distance (in miles)	2.4 GHz Path Loss (in dB)	Link Distance (in miles)	2.4 GHz Path Loss (in dB)	Link Distance (in miles)	5.8 GHz Path Loss (in dB)	Link Distance (in miles)	5.8 GHz Path Loss (in dB)
1	104	13	126	1	112	13	134
2	110	14	127	2	118	14	135
3	114	15	128	3	121	15	135
4	116	16	128	4	124	16	136
5	118	17	129	5	126	17	136
6	120	18	129	6	127	18	137
7	121	19	129	7	129	19	137
8	122	20	130	8	130	20	138
9	123	21	130	9	131	21	138
10	124	22	131	10	132	22	139
11	125	23	131	11	133	23	139
12	126	24	132	12	133	24	139

Path Availability

The availability of a path can be expressed by:

$$availability = (1 - C \times T \times 2.5 \times 10^{-6} \times f \times D^3 \times 10^{-f/10}) \times 100\%$$

where C is the climate factor
T is the terrain factor
f is the frequency in GHz
D is the path length in miles
F is the fade margin in dB

Climate factors are given in **Table 2-7** and terrain factors are given in **Table 2-8**.

Table 2-7. Climate Factors

Climate	Climate Factor
Very Dry	1/8
Temperate	1/4
Humid	1/2

Table 2-8. Terrain Factors

Terrain	Terrain Factor
Smooth	4
Average	1
Mountainous	1/4

The nominal received signal level is -60 dBm. For help in link planning, use the path loss calculation worksheet below.

-91 dBm (-89 dBm for 5.8 GHz)	Minimum Signal Power
+ _____	Transmitter Feedline Loss
- _____	Transmitter Antenna Gain
+_____	Path Loss
- _____	Receiver Antenna Gain
+ _____	Receiver Feedline Loss
+ _____	Required Fade Margin
= _____	(dBm) Transmitter Power Setting

SETTING THE TRANSMITTER POWER

The FCC specifies the maximum transmitter power that may be used for antennas of a given gain. FCC rules Part 15, Subpart 247 allow for a maximum power of 1 watt into antennas of a gain less than or equal to 6 dBi. At 2.4 GHz, the transmitter power must be reduced by 1 dB for every 3 dB of antenna

gain over 6 dBi. **Table 2-9** lists the maximum transmitter power for given antennas gains. For the 5.8 GHz band, there is no reduction in transmitter output power required for antennas gains greater than 6 dBi.

Table 2-9. Maximum Transmitter Power

Antenna Gain	Power
6 dBi	30 dBm (TRACER 2631 & 2.4 GHz 1 watt output option)
12 dBi	28 dBm (TRACER 2631 & 2.4 GHz 1 watt output option)
18 dBi	26 dBm (TRACER 2631 & 2.4 GHz 1 watt output option)
24 dBi	24 dBm (TRACER 2631 & 2.4 GHz 1 watt output option)
30 dBi	22 dBm (TRACER 2631 & 2.4 GHz 1 watt output option)
36 dBi	20 dBm (TRACER 2631 & 2.4 GHz standard 100 milliwatt output option

The transmitter power is set via a momentary switch on the front panel of the BBP or via the **WAN SYSTEM CONFIGURATION** menu of the VT-100 interface. The RF converter must be attached via the IF cable during this operation. Attach an RF power meter to the N-type antenna connector on the RF converter and adjust the power via the front panel switch or VT-100 menus until the desired transmitter power is obtained. If a mastmount RF converter is used, the transmitter power adjustment should be made before the RF converter is installed on the mast.

2.4 GHZ, 1 WATT TRANSMITTER OPTION

The 2.4 GHz TRACER 2631 model is offered with a standard +20 dBm (100 milliwatt) power output (at 2.4 GHz or 5.8 GHz) or optional +30 dBm (1 watt) power output version (at 2.4 GHz only). The 1 watt version includes an add-on amplifier that is installed in the rackmount RF converter chassis. This amplifier is connected to the transmit cable of the RF converter module and amplifies the +20 dBm output power to a maximum level of +30 dBm (1 watt), factory set to +27 dBm. The output power is proportional to the output level from the RF converter module. The level is adjusted via the baseband processor front panel or VT-100 terminal.

Because the 1 watt amplifier is frequency specific, the frequency plans cannot be manually changed by swapping the TX and RX cables in the RF converter chassis as described in the following section. If a frequency reversal is required, the rackmount RF converters will have to be relocated to the opposite ends of the microwave path. The 1 watt version is available only for the 2.4 GHz, rackmount RF converter.

SETTING THE RF CONVERTER FREQUENCY PLAN ON 100 MILLIWATT 2.4 GHZ MODELS

The frequency plan designates on which frequencies the TRACER 2631 transmits and receives. Plan A corresponds to a TX center frequency of 2422 MHz and an RX center frequency of 2462 MHz. Plan B corresponds to a TX center frequency of 2462 MHz and an RX center frequency of 2422 MHz. Shipment of a link consists of one RF converter set to Plan A and the other set to Plan B unless specified otherwise. The RF converter plan can, however, be changed in the field if required if the 1 watt amplifier is not present. This procedure involves reconfiguring the RF converter interconnect cables.

For rackmounted systems, do the following to reconfigure the RF converter interconnect:

1. Remove the six screws which retain the RF converter cover, then remove the cover.
2. The RF unit may be identified by following the connection from the port labeled **IF** on the rear of the RF converter. This connection terminates at the RF unit. The diplexer may be identified by following the connection from the **ANT** port on the rear of the RF converter. This connection terminates at the diplexer, illustrated in **Figure 2-1**.

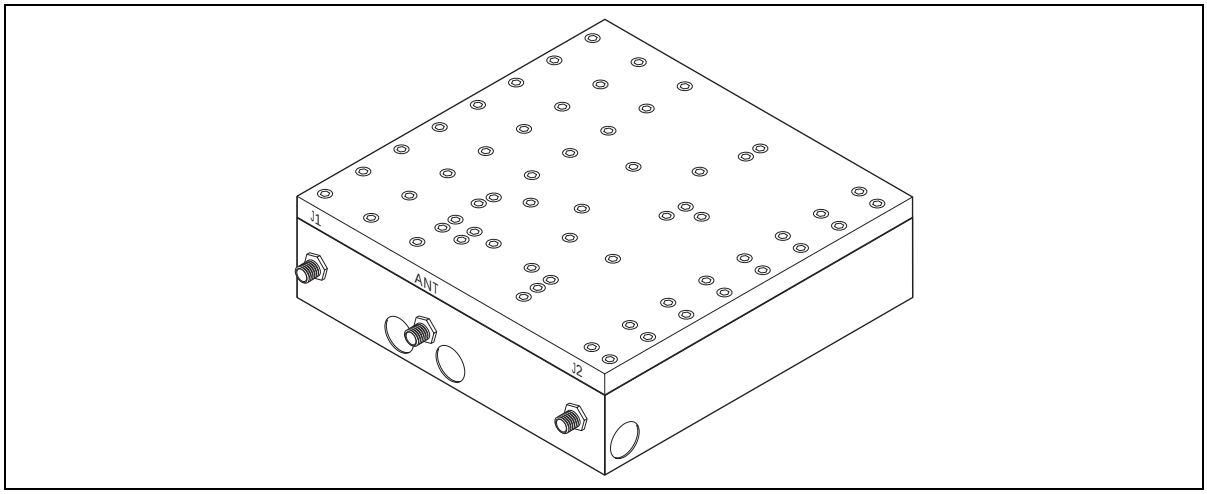

Figure 2-1. 2.4 GHz Diplexer

3. Unscrew the cable assemblies from the ports labeled **TX** and **RX** on the RF converter, and the ports labeled **J1** and **J2** on the diplexer, depending on the frequency Plan (Plan A or Plan B).
4. Unscrew the cable assembly from the port labeled **ANT** on the diplexer.
5. Remove the four screws from the bottom of the RF converter that hold the diplexer in place.
6. Turn the diplexer over revealing the opposite frequency plan (from Plan A to Plan B, or vice versa).
7. Realign the diplexer with the screw holes and replace the four screws that attach it to the bottom of the RF converter.
8. Reattach the loose cable assembly (from step 4) to the port labeled **ANT** on the diplexer. Minimum bend radius on cables is 3/4 inches. Exercise care in handling and forming bends in these cables.
9. Reattach the cable assemblies from the ports labeled **TX** and **RX** on the RF converter, and the ports labeled **J1** and **J2** on the diplexer. Cable connections should be aligned to each other as shown in **Table 2-10**.

Table 2-10. 2.4 GHz Frequency Plan Cable Connections

Plan A	Plan B
RF Converter TX connected to diplexer port J1	RF Converter TX connected to diplexer port J2
RF Converter RX connected to diplexer port J2	RF Converter RX connected to diplexer port J1

10. Replace and secure the RF converter cover.

For mastmounted systems, the following steps reconfigure the RF converter interconnect:

1. Remove the lid of the mast RF converter.
2. Disconnect the three cables attached to the diplexer. The diplexer may be identified by following the antenna connector to the middle connector of the diplexer. Leave the cables in the same positions.
3. Remove the two screws securing the diplexer and rotate the diplexer to reveal the opposite frequency plan label.
4. Reinstall the two screws and reattach the cables in the same positions. Minimum bend radius on cables is 3/4 inches. Exercise care in handling and forming bends in these cables.
5. Reinstall the lid of the mast RF converter.

SETTING THE RF CONVERTER FREQUENCY PLAN ON 5.8 GHZ MODELS

The 5.8 GHz RF converter operates on Plan A, TX = 5747 MHz center frequency, RX = 5827 MHz center frequency or Plan B, TX = 5827 MHz center frequency, RX = 5747 MHz center frequency. See **Figure 2-2** for an illustration of the 5.8 GHz diplexer.

Plan A	**Plan B**
RF Converter **TX** connected to diplexer **CHAN 1**	RF Converter **TX** connected to diplexer **CHAN 2**
RF Converter **RX** connected to diplexer **CHAN 2**	RF Converter **RX** connected to diplexer **CHAN 1**

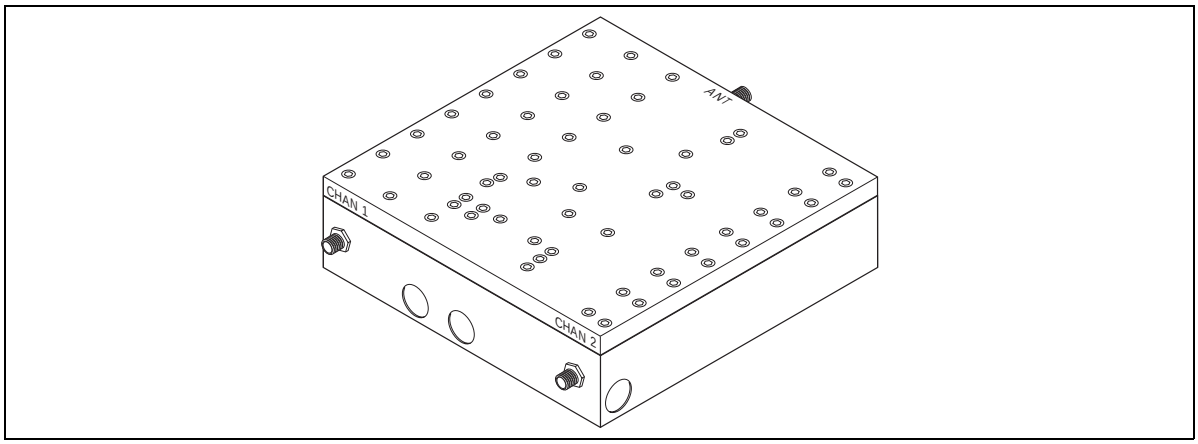

Figure 2-2. 5.8 GHz Diplexer

Changing the Frequency Plan on the Rackmount RF Converter

1. Remove RF converter top cover by removing six screws.
2. Disconnect the cables at the **TX** and **RX** RF converter module ports. Swap and reconnect these two cables to the RF converter module ports. Minimum bend radius on these cables is 3/4 inches. Use care in handling and forming bends in these cables.
3. Reinstall the RF converter top cover with the six screws previously removed.

Changing the Frequency Plan on the Mastmount RF Converter

1. Remove the lid of the Mast RF converter.
2. Disconnect the two cables at both ends; at the diplexer and RF converter module.
3. Swap and reconnect these cables. Minimum bend radius on these cables is 3/4 inches. Use care in handling and forming bends in these cables.
4. Reinstall the lid of the Mast RF converter.

CONNECTING THE BBP AND THE RF CONVERTER

The BBP and the RF converter are connected by an IF cable, either supplied by ADTRAN (for rackmount assembly) or by the customer (for mastmount assembly). This single connection provides everything the RF converter requires. The cable assembly attaches to the ports labeled **IF** on the BBP and the RF converter.

C A U T I O N

When connecting an RF converter to a baseband processor, verify that the connector labeled **IF** on the rear panel of the baseband processor is connected via coax to the connector labeled **IF** on the RF converter. Connecting the baseband processor to the incorrect connector on the RF converter will cause the internal 1 amp 250 volt fuse to blow in the baseband processor. This fuse is accessed by removing the top of the baseband processor, and is located on the left side of the chassis when facing the front panel.

APPLYING POWER

If the ADTRAN supplied tabletop power source is used, simply plug it into the circular receptacle located in the **DC Power** area on the rear of the BBP. If a source of 21 to 60 volts DC (30 watts) is available, either polarity referenced to ground, it may be attached to the terminal block located on the rear of the BBP. Ground should be applied to the terminal with the ground symbol (terminal 1) and positive or negative voltage should be applied to the +/- terminal (terminal 3). When a positive voltage reference power supply is used (+24V for example), connect the ground (or -) cable from the power supply to the ground terminal (terminal 1) and the + cable from the power supply to the +/- terminal (terminal 3). When a negative voltage reference power supply is used (-48V for example), connect the ground cable from the power supply to the ground terminal (terminal 1) and the - cable from the power supply to the +/- terminal (terminal 3).

C A U T I O N

Power sources must not be attached to both the circular connector and the terminal blocks at the same time or damage will occur.

AUTOMATIC BBP FREQUENCY PLAN

Upon the initial application of power, the BBP will default to the factory-preset frequency plan, and then auto-detect the frequency plan determined by the cable configuration of the RF converter. The LED will indicate which frequency plan is active. The BBP will also auto-detect the frequency plan on subsequent reboots.

CHIPPING CODE

The chipping code for each end must be the same. The choice of chipping code is selectable by the operator or the installer. TRACER 2631 is shipped in a matched (default) configuration. Chipping code is set in the **WAN SYSTEM CONFIGURATION** menu (see *WAN System Configuration Menu* on page 88).

W A R N I N G

Chipping code can be set through the VT-100 interface from the other end of the link. If the remote end chipping code is accidentally changed, the link will be lost. If the new chipping code is unknown, step the local end of the link through all the other chipping codes until the link is re-established.

CO-LOCATING MULTIPLE SYSTEMS

When multiple transmitters are to be co-located (installed in the same equipment room or on the same tower), it is advised to set all systems as follows:

1. If more than one system is transmitting from the same location, set the antenna polarity of one system *horizontal* and the other system(s) *vertical* if the systems are operating in the same frequency bands. (The antennas should be marked as to which mounting position is vertical or horizontal.) This will provide approximately 30 dB of isolation between the different antennas.
2. If more than one TRACER 2631 system is installed, set the co-located transmitters to the same frequency plan (example: Plan A, TX=2422 or 5747 MHz; or Plan B, TX=2462 or 5827 MHz) and set each to a different chipping code. This keeps the transmitters on the additional system(s) from interfering with the co-located receiver(s).
3. If the systems are from different manufacturers, set the transmit frequencies as close as possible with different chipping codes. Other manufacturers may not use the exact frequency plans as the TRACER 2631 system, but keeping the frequencies close will reduce the probability of the transmitter(s) interfering with the co-located receiver(s).

This equipment is authorized under FCC Part 15.247. With this authorization by the FCC, this equipment shall not be co-located with a similar transmitter that transmits identical information.

ANTENNA ALIGNMENT

After the transmitter power for each end has been adjusted and the BBP and RF converter have been installed and connected, the antenna should be connected to the RF converter via the feedline. Verify that the antenna on each end of the link is arranged on the same polarity – vertical or horizontal. The antennas should be aimed toward one another as precisely as possible and the RSSI voltage measured. The RSSI voltage is a function of the signal strength at the receiver and is used to provide a relative signal strength indication. RSSI varies approximately from 0 to greater than 4 volts, with 0 volts corresponding to a weaker received signal and 4 volts or better corresponding to a stronger received signal.

I M P O R T A N T

The voltage level present at the RSSI test point represents only a relative signal level of receive strength from the far end. No direct correlation can be made between RSSI voltage level and actual receive level in dBm. This test point is provided to assess relative signal level for alignment of antennas.

RF LOW

The **RF LOW** LED indicates that the received signal is within 10 dB of the minimum received signal strength (approximately -80 dBm). If this indicator is on, the link performance may be marginal. The antennas should be peaked in azimuth and elevation until the desired signal level is achieved. RSSI may be monitored on either the RF unit or the front of the BBP. If the received signal is too strong and RSSI reaches a maximum such that the peak cannot be discerned, then the transmitter on the far end should be turned down.

At this point the radio link should be operational. Proper operation can be determined by the status of the **LINK DOWN** LED. If this LED is *on*, the link is *not* operational. If this LED is *not on*, the link *is* operating. Certain types of interference can cause one end of a path to operate and the other end to fail. In some instances, this may be corrected by swapping the frequency plan at each end, thus avoiding the interference if it is stronger at one end than the other. Changing the chipping code at each end may also allow interference to be mitigated.

ALARM CONTACTS

Two sets of alarm contacts are provided on the rear of the BBP – major alarm and minor alarm. A major alarm indicates the radio link is not operational. A minor alarm indicates that system performance is degraded or that the T1 interface is experiencing errors. Normally-open and Normally-closed contacts are provided for both alarm types. See **Table 2-11** for a summary of major and minor alarms. Under normal operating conditions there is no continuity between the Normally-open and Common contacts. Under an alarm condition, continuity between those contacts exists. The Normally-closed and Common contacts usually have continuity; while under alarm conditions, these contacts are open.

Table 2-11. Discrete Alarm Summary

Alarm Type	Interface	Description
Major	RF	T1 Mux Sync Fail (Link Error)
Minor	RF	RF Low
Minor	T1	Yellow Alarm
Minor	T1	Bipolar Violations
Minor	T1	Received AIS (Blue Alarm)
Minor	T1	Carrier Loss
Minor	T1	Sync Loss
Minor	T1	Data Loss

VT-100 USER INTERFACE

TRACER 2631 may be accessed with a VT-100 compatible terminal set to 9600 bits per second, 8 data bits, and no parity, connected to the RS-232 port on the back of the unit. Flow control on the serial interface should be configured to **NONE** for proper operation. Once a terminal is connected, pressing **Ctrl-R** will redraw the current screen.

RS-232 INTERFACE

TRACER 2631 has an RS-232 interface for system management via an attached VT-100 terminal or personal computer with terminal emulation software. The RS-232 port is configured as a DCE with the pin assignments shown in **Table 3-1**.

Table 3-1. RS-232 Interface Pin Assignments

Signal Name	Pin Number	Direction
TXD	2	To TRACER 2631
RXD	3	From TRACER 2631
Ground	7	N/A

PASSWORD PROTECTION

If password protection has been **ENABLED** on the maintenance port, the **LOGIN** window will appear. TRACER 2631 is shipped with password protection **DISABLED**. Password configuration is accessed via the **LAN CONFIGURATION/MANAGEMENT/MAINTENANCE PORT** menu.

CABLE CONNECTIONS

The cable connections required for various configurations are detailed in Appendix A of this manual.

TERMINAL MENU OPERATION AND STRUCTURE

The TRACER 2631 menu system is partitioned into two configuration sets – local area network (LAN) and wide area network (WAN). On system power-up or reset, TRACER 2631 goes through a series of self-tests, and then enters the LAN menu set.

I M P O R T A N T

To gain access to the WAN menu set, go to the **LAN/CONFIGURATION/WAN/CONFIGURE WAN & T1** menu and press the **Return** or **Enter** key.

To return to the LAN menu set, type **L** from the TRACER 2631 WAN **SYSTEM STATUS** menu.

NAVIGATING THE LAN MENUS

LAN Menu Window

The TRACER 2631 uses a multi-level menu structure that contains both menu items and data fields. All menu items and data fields display in the terminal menu window (see Figure 3-1), through which you have complete control of the TRACER 2631 LAN interface.

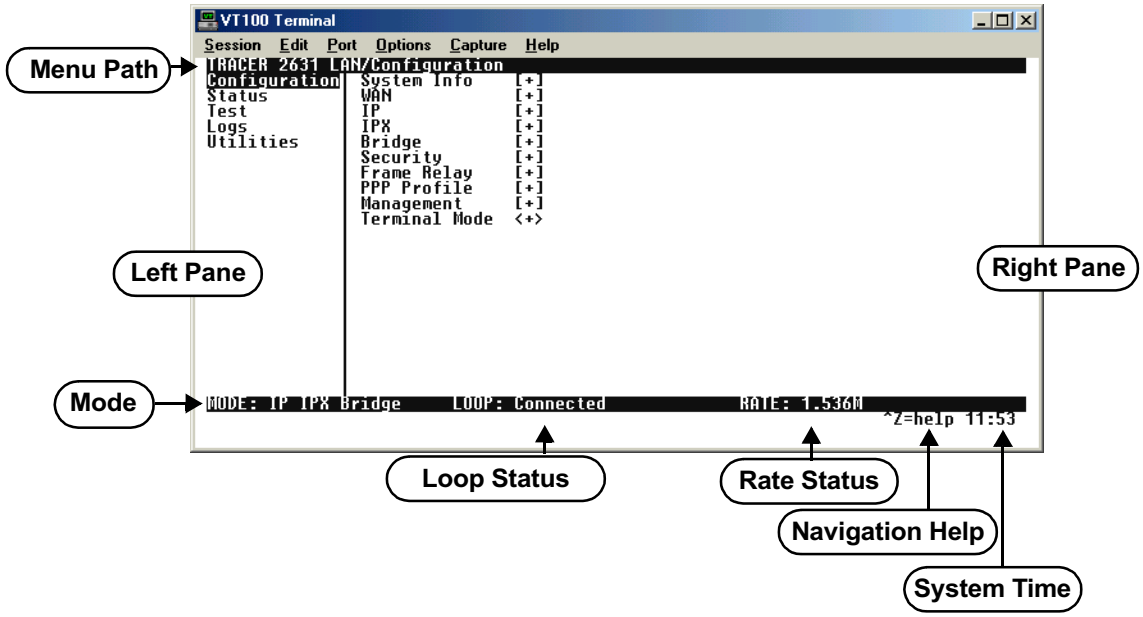

Figure 3-1. LAN Top-Level Terminal Menu Window

Menu Path

The first line of the terminal menu window (the menu path) shows the session's current position (path) in the LAN menu structure. For example, Figure 3-1 shows the top-level menu with the cursor on the **CONFIGURATION** submenu; therefore, the menu path reads **TRACER 2631 LAN/Configuration**.

Window Panes

When you first start a terminal menu session, the terminal menu window is divided into left and right panes. The left pane shows the list of available submenus, while the right pane shows the contents of the currently selected submenu.

Window Pane Navigation

Use the following chart to assist you in moving between and within the two window panes.

To do this...	Press this key...
Move from left pane to right pane	Tab Enter Right arrow
Move from right pane to left pane	Tab Escape Left arrow Backspace
Move within each pane	Up arrow Down arrow Left arrow Right arrow

Right Window Pane Notation

The right window pane shows the contents of the currently selected menu. These contents can include both submenu items and data fields. Some submenus contain additional submenus and some data fields contain additional data fields. The following chart explains the notation used to identify these additional items.

This notation...	Means that...
[+]	More items are available when selected
[DATA]	More items are available when selected
<+>	An action is to be taken, such as activating a test
Highlighted menu item	You can enter data in this field
Underlined field	The field contains read-only information

Navigating Using the Keyboard Keys

You can use various keystrokes to move through the terminal menu, to manage a terminal menu session, and to configure the system. Press **<Ctrl+Z>** to activate a pop-up screen listing the navigation keystrokes.

Moving through the Menus

To do this...	Press this key...
Return to the home screen	H
Jump between two menu items Press <J> while the cursor is located on a menu item, and you jump back to the main screen. Go to another menu item, press <J>, and you jump back to the screen that was displayed the first time you pressed <J>. Press <J> anytime you want to jump between these items.	J
Select items	Arrows
Edit a selected menu item	Enter
Cancel an edit	Escape
Close pop-up help screen	Escape
Move between the left and right panes	Tab Arrows
Move to the top of a screen	A
Move to the bottom of a screen	Z
Ascend one menu level	Backspace

Session Management Keystrokes

To do this...	Press this key...
Log out of a session	**Ctrl+L**
Invalidate the password entry and return to the login screen	**Ctrl+S**
Refresh the screen	**Ctrl+R**
View Extended Data Display data fields too large for display window.	**Ctlr+V**

Configuration Keystrokes

To do this...	Press this key...
Restore factory default settings. This setting restores the factory defaults based on the location of the cursor.	F
Copy selected items to the clipboard. The amount of information you can copy depends on the cursor location when you press <C>: If the cursor is over an editable field, only that item is copied. If the cursor is over the index number of a list, then all of the items in the row of the list are copied.	C
Paste the item stored in the clipboard, if the information is compatible. You must confirm all pastes - except those to a single editable field.	P
Increment the value of certain types of fields by one when you paste information into those fields.	>
Decrement the value of certain types of fields by one when you paste information into those fields.	<
Insert a new list item.	I
Delete a list item.	D

Getting Help

The bottom line of the terminal menu window contains context-sensitive help information. When the cursor is positioned over a set of configuration items, a help message displays (when available) providing a description of the item. When more detailed help is available for a particular item, **^A** displays at the bottom of the window. At this point, if you press **<Ctrl+A>**, a pop-up help screen displays with information about the item.

Press **<Ctrl+Z>** to activate a help screen that displays the available keystrokes you can use to navigate the terminal menu.

TERMINAL MENU AND SYSTEM CONTROL

Selecting the Appropriate Menu

The terminal menu is the access point to all other operations. Each terminal menu item has several functions and submenus that identify and provide access to specific operations and parameters.

Security Levels

To edit terminal menu items, you must have a password and the appropriate security level. **Table 3-2** describes the six security levels.

Table 3-2. Password Security Level

Security Level	Description
5	Access status menus only - **minimum rights**
4	Access to all status menus and permission to use test commands
3	Access to all commands except passwords, flash download, authentication methods, and interface configurations
2	Access to all commands except passwords, flash download, and authentication methods
1	Access to all commands except passwords
0	Permission to edit every menu item, including creating and editing passwords - **maximum rights**

TOP LEVEL LAN MENU

The main LAN menu is utilized to access all other LAN functions. Each main LAN menu item has several functions and submenus to identify and access specific parameters. **Figure 3-1** on page 30 shows the top level main LAN menu.

LAN/CONFIGURATION MENU

Configuration/System Info

The **SYSTEM INFO** menu provides basic information about the unit and displays data fields for editing information. **Figure 3-2** displays the submenus available under this menu item.

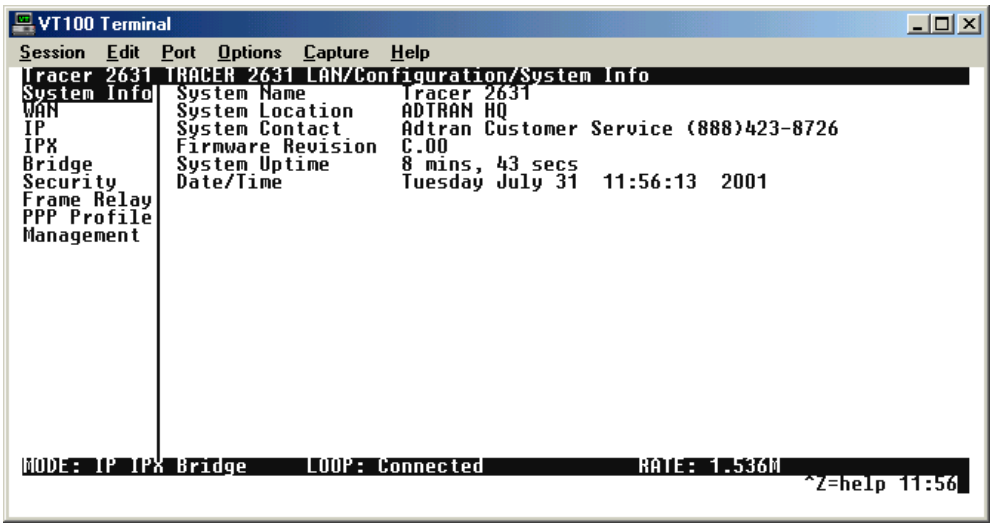

Figure 3-2. LAN/Configuration/System Info Screen

System Info/System Name

Write security: 3; Read security: 5

Provides a user-configurable text string for the name of the TRACER 2631. This name can help distinguish between different installations. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an under bar). The system name is also used for PPP authentication and IPX service name.

System Info/System Location

Write security: 3; Read security: 5

Provides a user configurable text string for the location of the TRACER 2631. This helps to keep track of the physical location of the unit. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an under bar).

System Info/System Contact

Write security: 3; Read security: 5

Provides a user-configurable text string for the contact name. This field can contain a name, phone number, or e-mail address of a person responsible for the TRACER 2631. You can enter up to 31 alpha-numeric characters in this field, including spaces and special characters (such as an under bar).

System Info/Firmware Revision

Read security: 5

Displays the current firmware revision level of the TRACER 2631. This is a read-only field.

System Info/System Uptime

Read security: 5

Displays the length of time TRACER 2631 has been running since power up or reset. This is a read-only field.

System Info/Date/Time

Write security: 3; Read security: 5

Displays the current date and time as programmed in the real-time clock. This field can be edited. Enter the time in 24-hour format (such as 23:00:00 to represent 11:00 PM). Enter the date in mm-dd-yyyy format (for example, 09-30-1997).

Configuration/WAN

The **WAN** menu is used to set up all parameters associated with the wide area network interface, including all wireless and T1 parameters. **Figure 3-3** shows the **WAN** menu.

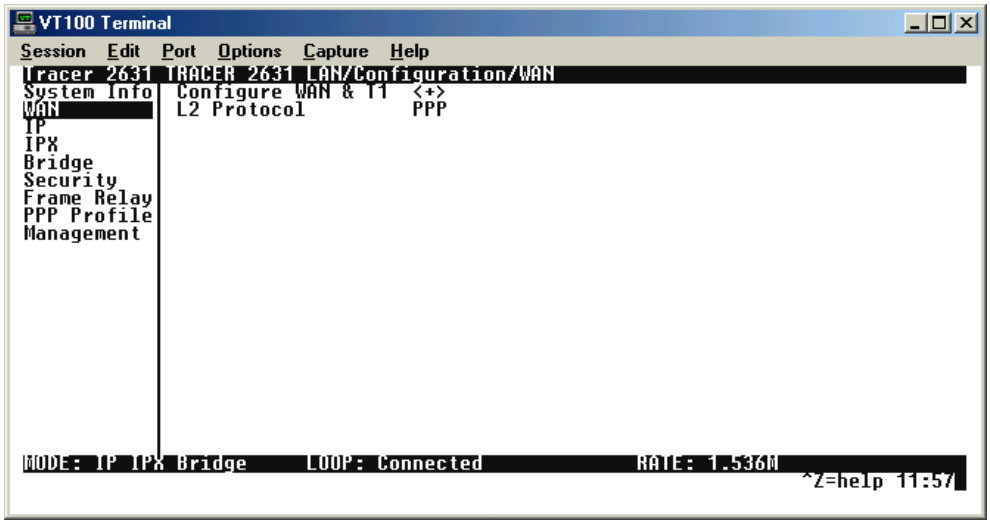

Figure 3-3. LAN/Configuration/WAN Screen

WAN/Configure WAN & T1

This is an activator that switches the TRACER 2631 to the WAN menu set. All T1 and wireless options are configured via the WAN menus, which are discussed starting on page 85.

WAN/L2 Protocol

Write security: 3, Read security: 5

This parameter specifies the layer 2 data link layer transport used. When selected as **PPP** (default), TRACER 2631 will negotiate PPP over the wireless link. Parameters for controlling the PPP negotiation are in the **LAN/CONFIGURATION/PPP PROFILE** menu. **FRAME RELAY** should be selected when TRACER 2631 is connected to a Frame Relay switch. The **LAN/CONFIGURATION/WAN/FRAME RELAY** menu is used for controlling the Frame Relay parameters.

Configuration/IP

The **IP** menu is used to set up the IP parameters for the TRACER 2631. Any general IP-related configuration item is under this menu. **Figure 3-4** shows the **IP** menu.

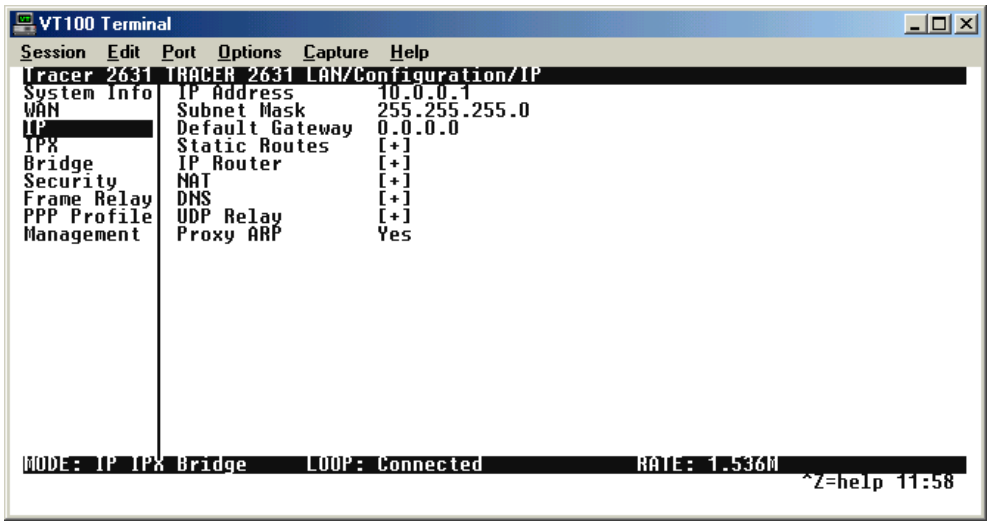

Figure 3-4. LAN/Configuration/IP Screen

IP/IP Address

Write security: 2; Read security: 5

The IP address assigned to the TRACER 2631's Ethernet port is set here. This address must be unique within the network. Factory default is 10.0.0.1.

IP/Subnet Mask

Write security: 2; Read security: 5

The IP network mask to be applied to the TRACER 2631's Ethernet port is set here. Factory default is 255.255.255.0.

IP/Default Gateway

Write security: 3; Read security: 5

The default gateway is used by TRACER 2631 for sending IP packets whose destination address is not found in the route table. If this address is all zeros, then the first WAN connection becomes the default gateway.

IP/Static Routes

Static Routes can be inserted under this menu.

Static Routes/Active

Write security: 4; Read security: 5

Adds this static route entry to the IP routing table when set to **YES** (default) and removes it (if it was previously added) if set to **NO**.

Static Routes/IP Address

Write security: 4; Read security: 5

This is the IP address of the host or network address of the device being routed to.

Static Routes/Subnet Mask

Write security: 4; Read security: 5

This mask determines the bits in the previous IP address that are used. If this is to be a host route, it must be set to all ones (255.255.255.255).

Static Routes/Gateway

Write security: 4; Read security: 5

This is the IP address of the router to receive the forwarded IP packet.

Static Routes/Hops

Write security: 4; Read security: 5

This is the number of router hops required to get to the network or host. Maximum distance is 15 hops.

Static Routes/Private

Write security: 4; Read security: 5

When set to **NO**, TRACER 2631 will advertise this static route using RIP. When set to **YES**, the route is kept private.

IP/IP Router

The IP router is configured under this menu as follows.

IP Router/Mode

Write security: 3; Read security: 5

When this option is set to **ON** (default), TRACER 2631 will advertise and listen to routes from other IP routers. If **OFF**, the route table is still used but only static routes are used for routing IP packets and only the Ethernet port is used. IP packets can be sent over the WAN, but only when bridged.

IP/RIP

Write security: 3; Read security: 5

RIP is supported by TRACER 2631. The following parameters are required for setting up the mode on the Ethernet port.

RIP/Mode

Write security: 3; Read security: 5

This option turns RIP **ON** (default) or **OFF**.

RIP/Protocol

Write security: 3; Read security: 5

Version can be **V1** (default) (which is RIP version 1) or **V2** (which is RIP version 2).

RIP/Method

Write security: 3; Read security: 5

Split Horizon	Only routes not learned on the Ethernet port are advertised.
Poison Reverse (default)	All routes are advertised, including routes learned from the Ethernet port. These routes are poisoned.
None	All routes are advertised, including routes learned from the Ethernet port. No attempt is made to poison these routes.

RIP/Direction

Write security: 3; Read security: 5

TX and RX (default)	RIP advertisements are transmitted and listened to on the Ethernet port.
TX only	RIP advertisements are transmitted and not listened to.
RX only	RIP advertisements are listened to but not transmitted.

RIP/V2 Secret

Write security: 0; Read security: 0

This is a text string used for authenticating advertised routes.

IP/NAT

The Network Address Translation (NAT) general parameters are set up under this menu.

NAT/DHCP Mode

Write security: 3; Read security: 5

When this option is set to **ON**, TRACER 2631 acts as a DHCP server and will dynamically assign IP, network mask, default gateway, and DNS addresses to any device which transmits a broadcast DHCP request. The addresses assigned are based on the TRACER 2631's own IP address and will be within the same network. This mode is most commonly used with the NAT functionality. The default is **OFF**.

NAT/DHCP Renewal Time

Write security: 3; Read security: 5

This is the number of hours that the DHCP server should allow the device before it is required to send a new DHCP request. The default is 15 hours, and 0 represents an infinite lease.

NAT/Web Server

Write security: 3; Read security: 5

This is the IP address of a web server on the Ethernet network. When an active NAT connection is made to the Internet, any HTTP, FTP, or SMTP server requests from the WAN are translated and sent to this web server. Normally, communication across NAT must be initiated from the LAN side of TRACER 2631. Web Server allows a single machine on the NAT side to be accessed from the Internet side of NAT. This provides outside access to a webserver, mail, or ftp server.

NAT/Default IP

This is the IP address used by TRACER 2631 for NAT when nothing is assigned during the PPP negotiation when PPP mode is active or when nothing is specified in the DLCI Mapping's Link IP Address.

IP/DNS

The Domain Name Server (DNS) parameters used by TRACER 2631 are specified here. The DNS server addresses can be exchanged between PPP peers. When a connection occurs and IPCP is negotiated, TRACER 2631 will get the DNS server addresses from the PPP peer. If the configured DNS server addresses (**Server 1** and **Server 2**) are all zeros, the addresses from the PPP peer are used. In NAT mode, the PPP peer's DNS addresses are always used. The DNS addresses set in **Server 1** and **Server 2** are offered to a PPP peer if so requested.

DNS/Domain Name

Write security: 3; Read security: 5

This is a text string used to represent the domain name used by TRACER 2631.

DNS/Server 1

Write security: 3; Read security: 5

This is the IP address for the primary DNS device. It is the first server that domain name requests are sent.

DNS/Server 2

Write security: 3; Read security: 5

This is the IP address for the secondary DNS device. It is used as a back-up in case the primary address does not respond to the request.

IP/UDP Relay

TRACER 2631 can be configured as a relay agent for UDP broadcast packets. Normally, a router will not forward UDP broadcast packets. However, many network applications use UDP broadcasts to configure addresses, host names, and other information. If hosts using these protocols are not on the

same network segment as the servers providing the information, the client programs will not receive a response without enabling the UDP relay agent.

UDP Relay/Mode

Write security: 3; Read security: 5

When this option is set to **ON** (default), TRACER 2631 will act as a relay agent.

UDP Relay/UDP Relay List

Up to four relay destination servers can be specified in this list.

UDP Relay List/Relay Address

Write security: 3; Read security: 5

This is the IP address of the server that will receive the relay packet.

UDP Relay List/UDP Port Type

Write security: 3; Read security: 5

Standard (default)	The following standard UDP protocols are relayed when set: DHCP, TFTP, DNS, NTP (Network Time Protocol, port 123). NBNS (NetBIOS Name Server, port 137), NBDG (NetBIOS Datagram, port 138), and BootP.
Specified	When set, the UDP port (1 to 65535) can be specified in the UDP Port columns (up to a maximum of three per server).

UDP Relay List/UDP Ports 1, 2, and 3

Write security: 3; Read security: 5

UDP Port 1, UDP Port 2, and UDP Port 3 are used for specifying UDP ports to be relayed. These fields only apply when **UDP PORT TYPE** is set to **SPECIFIED**.

IP/Proxy ARP

Write security: 4; Read security: 5

This feature allows the network portion of a group of addresses to be shared among several physical network segments. The Address Resolution Protocol (ARP) itself provides a way for devices to create a mapping between physical (i.e., Ethernet) addresses and logical IP addresses. Proxy ARP makes use of this mapping feature by instructing a router to answer ARP requests as a “proxy” for the IP addresses behind one of its ports. The device which sent the ARP request will then correctly assume that it can reach the requested IP address by sending packets to the physical address that was returned to it. This technique effectively hides the fact that a network has been (further) subnetted. If this option is set to **YES** (default), when an ARP request is received on the Ethernet port the address is looked up in the IP routing table. If the forwarding port is not on the Ethernet port and the route is not the default route, TRACER 2631 will answer the request with its own hardware address. If set to **NO**, TRACER 2631 will only respond to ARP requests received for its own IP address.

Configuration/IPX

The **IPX** menu is used to set up the IPX parameters for the TRACER 2631. Any general IPX-related configuration item can be found under this menu. **Figure 3-5** shows the **IPX** menu.

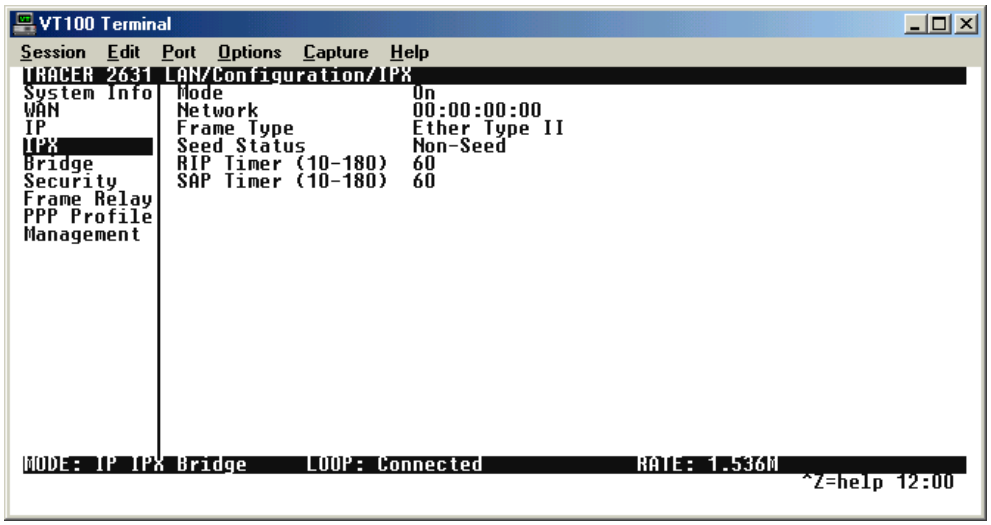

Figure 3-5. LAN/Configuration/IPX Screen

IPX/Mode

Write security: 2; Read security: 5

When this option is set to **ON** (default), TRACER 2631 will route IPX. Setting the option to **OFF** will disable all IPX functionality.

IPX/Network

Write security: 2; Read security: 5

The IPX network address for the Ethernet port is set here. This is an eight-digit hexadecimal value that uniquely identifies the network segment of the Ethernet port. Accidental selection of an IPX network which is already in use on another network segment may cause hard-to-diagnose problems. IPX network numbers should be carefully tracked.

IPX/Frame Type

Write security: 2; Read security: 5

TRACER 2631 supports all four defined IPX frame types. The possible frame types are **ETHER TYPE II** (default), **ETHER 802.3 (RAW)**, **ETHER 802.2**, or **ETHER SNAP** (802.2 SNAP). Only one frame type can be used at one time.

IPX/Seed Status

Write security: 2; Read security: 5

The seed status defines what TRACER 2631 will do with the network information on the selected frame type during startup. There are three possible seeding selections specified.

Seed	TRACER 2631 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, TRACER 2631 will use the configured IPX network number for the Ethernet segment.
Non-Seed (default)	TRACER 2631 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, TRACER 2631 will wait indefinitely until a number is sent by another router on the Ethernet segment.
Auto-Seed	TRACER 2631 will listen for an IPX network number being sent by another router (including Novell software routers residing on servers) on the Ethernet segment connected to this port and use this number if it exists. If it does not discover a number in use, TRACER 2631 will auto-generate a valid number using its routing tables.

IPX/RIP Timer

Write security: 3; Read security: 5

This value specifies how often TRACER 2631 sends out IPX RIP packets on the network segment attached to the Ethernet port. The RIP packets sent contain routing information about the networks for which TRACER 2631 is responsible. The default value is 60 seconds.

IPX/SAP Timer

Write security: 3; Read security: 5

This value specifies how often TRACER 2631 sends out IPX SAP packets on the network segment attached to the Ethernet port. The SAP packets sent contain information about the services (such as servers, printers, etc.) for which TRACER 2631 is responsible. The default value is 60 seconds.

Configuration/Bridge

The **BRIDGE** menu is used to set up the bridge parameters for TRACER 2631. The bridging function runs at the MAC level which allows any protocol packets that run over Ethernet to be forwarded. Bridging can run concurrently with IP and IPX routing. However, certain rules apply for when packets are bridged across a WAN connection. When IP routing is active, IP packets (which include ARP packets) are not bridged. When IPX routing is active, IPX packets are not bridged. Also, the WAN IP Bridge and

WAN IPX Bridge menus allow the WAN connection to bridge packets to TRACER 2631, but get routed as soon as they arrive at the unit. **Figure 3-6** shows the **BRIDGE** menu.

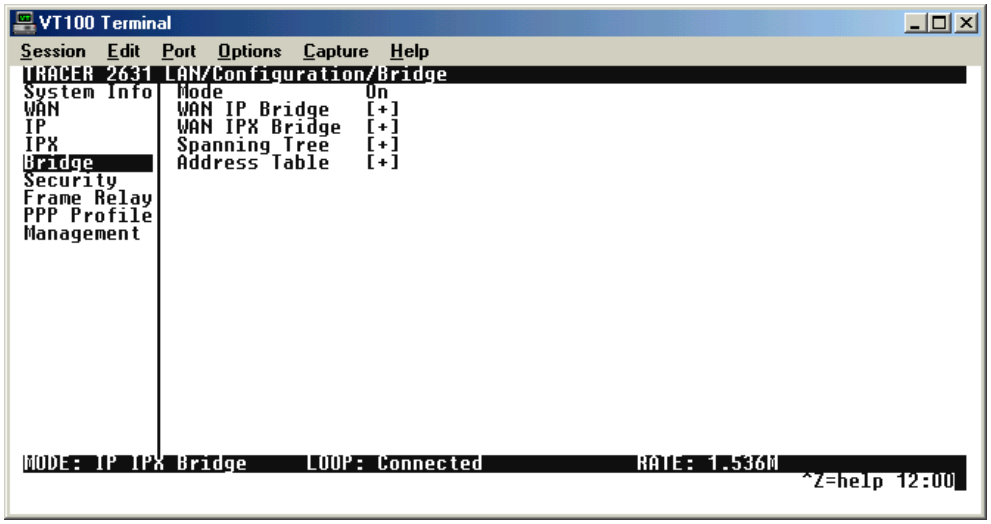

Figure 3-6. LAN/Configuration/Bridge Screen

Bridge/Mode

Write security: 2; Read security: 5

When this option is set to **ON** (default), TRACER 2631 bridge functionality will be enabled. Setting it to **OFF** will disable all bridge functionality.

Bridge/WAN IP Bridge

When IP routing is active, TRACER 2631 will allow another WAN device to bridge IP packets to it using PPP Bridge Control Protocol (BCP). Normally, two IP routers would negotiate PPP IPCP to exchange IP packets. However, if a device can only support PPP BCP, IP packets are encapsulated by the device as bridge packets. TRACER 2631 can treat the WAN IP Bridge as a virtual Ethernet port connected only to a WAN device which has negotiated PPP BCP. This menu allows the IP parameters for this virtual Ethernet to be set up.

WAN IP Bridge/Network

Write security: 2; Read security: 5

This is the IP address of the virtual Ethernet port.

WAN IP Bridge/Netmask

Write security: 2; Read security: 5

This is the network mask to be applied to the virtual Ethernet port.

WAN IP Bridge/Triggered
Write security: 2; Read security: 5

When set to **YES**, only IP RIP updates are sent when the routing table has changed. When set to **NO** (default), updates are sent periodically.

N O T E

RIP version, method, and direction are determined by the Ethernet parameters set in the **LAN/CONFIGURATION/IP/IP ROUTER/RIP** menu.

WAN IP Bridge/Proxy ARP
If this option is set to **YES** (default), TRACER 2631 will proxy ARP on the bridge IP port. See the section *IP/Proxy ARP* on page 41 for an explanation of the proxy ARP function.

Bridge/WAN IPX Bridge

When IPX routing is active, TRACER 2631 will allow another WAN device to bridge IPX packets to it using PPP BCP. Normally, two IPX routers would negotiate PPP IPXCP to exchange IPX packets. However, if a device can only support PPP BCP, IPX packets are encapsulated by the device as bridge packets. TRACER 2631 can treat the WAN IPX Bridge as a virtual Ethernet port connected only to a WAN device which has negotiated PPP BCP. This menu allows the IPX parameters for this virtual Ethernet to be set up.

WAN IPX Bridge/Network
Write security: 2; Read security: 5

This is the network address of the virtual Ethernet port. See *IPX/Network* on page 42 for an explanation of the IPX network number.

WAN IPX Bridge/Frame Type
Write security: 2; Read security: 5

This is the frame type used for the virtual Ethernet port. See *IPX/Frame Type* on page 42 for an explanation of the IPX frame type.

WAN IPX Bridge/Seed Status
Write security: 2; Read security: 5

This is the seed status used for the virtual Ethernet port. See *IPX/Seed Status* on page 43 menu for an explanation of the IPX seed status.

WAN IPX Bridge/Triggered

Write security: 2; Read security: 5

When set to **YES**, only IPX RIP and SAP updates are sent when the routing or service table has changed. When set to **NO** (default), updates are sent periodically.

N O T E

RIP and SAP periodic rates set for the Ethernet port (see *IPX/RIP Timer* on page 43 and *IPX/SAP Timer* on page 43) are used for the WAN IPX bridge port.

Bridge/Spanning Tree

The Spanning Tree Algorithm and Protocol ensures a loop-free topology and provides redundancy. The protocol parameters can be specifically tuned from their defaults, though most applications require no adjustment.

Spanning Tree/Mode

Write security: 2; Read security: 5

When the mode is set to **ON**, TRACER 2631 will participate in the Spanning Tree protocol between other bridges. When **OFF** (default), all bridge ports remain permanently open for forwarding.

Spanning Tree/Priority

Write security: 2; Read security: 5

This assigns a priority to TRACER 2631 that permits the relative priority of multiple bridges to be managed. The range is 0 to 65535 with a default of 32768.

Spanning Tree/Maximum Age

Write security: 2; Read security: 5

This is the timeout value used by TRACER 2631 to test against the root device. The value is in one-tenth seconds with a range between 60 (6.0 seconds) and 400 (40.0 seconds). The default is 200 (20.0 seconds).

Spanning Tree/Hello Time

Write security: 2; Read security: 5

This is the time between the generation of configuration Bridging Protocol Data Units (BPDUs) by the root bridge. The value is in one-tenth seconds with a range between 10 (1.0 second) and 100 (10.0 seconds). The default is 20 (2.0 seconds).

Spanning Tree/Forward Delay

Write security: 2; Read security: 5

This is the time spent in the listening and learning state while moving from the blocking state to the forwarding state. The value is in one-tenth seconds with a range between 40 (4.0 seconds) and 300 (30.0 seconds). The default is 150 (15.0 seconds).

Spanning Tree/LAN Port

The path cost and priority parameters for the Ethernet port are specified under this menu.

LAN Port/Active

Write security: 2; Read security: 5

The Ethernet port can be disabled when set to **NO**. In this mode, no bridge traffic will be forwarded in or out. Setting to **YES** (default) allows the port to participate in the spanning tree topology.

LAN Port/Path Cost

Write security: 2; Read security: 5

This is the cost of using the Ethernet port in the total cost of the path. The range is from 1 to 65535 with a default of 100 (for 10 Mbits/second).

LAN Port/Priority

Write security: 2; Read security: 5

The priority adjusts the relative priority of the Ethernet port among the multiple bridge ports. The range is 0 to 255 with a default of 128.

Spanning Tree/Bridge Group 1

The Bridge Group 1 is either the first PPP BCP connection or part of multiple DLCI destinations when running Bridge (RFC 1490) over Frame Relay.

Bridge Group 1/Active

Write security: 2; Read security: 5

The Bridge Group 1 port can be disabled when set to **NO**. In this mode, no bridge traffic will be forwarded in or out. Setting to **YES** (default) allows the port to participate in the Spanning Tree topology.

Bridge Group 1/Path Cost

Write security: 2; Read security: 5

This is the cost of using the Bridge Group 1 in the total cost of the path. The range is from 1 to 65535 with a default of 1302 (for 768 kbits/second).

Bridge Group 1/Priority

Write security: 2; Read security: 5

The priority adjusts the relative priority of the Bridge Group 1 among the multiple bridge ports. The range is 0 to 255 with a default of 128.

Spanning Tree/Bridge Group 2

Bridge Group 2 is part of multiple DLCI destinations when running Bridge (RFC 1490) over Frame Relay.

Bridge Group 2/Active

Write security: 2; Read security: 5

This setup is exactly like Bridge Group 1 above.

Bridge Group 2/Path Cost

Write security: 2; Read security: 5

This setup is exactly like Bridge Group 1 above.

Bridge Group 1/Priority

Write security: 2; Read security: 5

This setup is exactly like Bridge Group 1 above.

Bridge/Address Table

TRACER 2631 automatically maintains a table of MAC addresses detected and associates those addresses with the LAN, WAN0, or WAN1 port from which they were received. WAN 0 represents Bridge Group 1, and WAN1 represents Bridge Group 2. This menu permits the user to adjust the parameters or rules for the table as addresses are learned.

Address Table/Aging

Write security: 3; Read security: 5

This is the maximum time an idle MAC address remains in the table before being removed. The value is in minutes and can range from 0 (which means never age) to 65535. The default is 5.

Address Table/Forward Policy

Write security: 3; Read security: 5

When this parameter is set to **UNKNOWN** (default), any bridge packet with a destination MAC address that is not in the bridge table is forwarded to all other ports. When set to **KNOWN**, the packet with the unknown destination MAC address is dropped and is not forwarded.

Configuration/Security

The **SECURITY** menu is used to set up the authentication parameters needed to authenticate PPP connection. Filter defines are also placed under this menu. **Figure 3-7** shows the **SECURITY** menu.

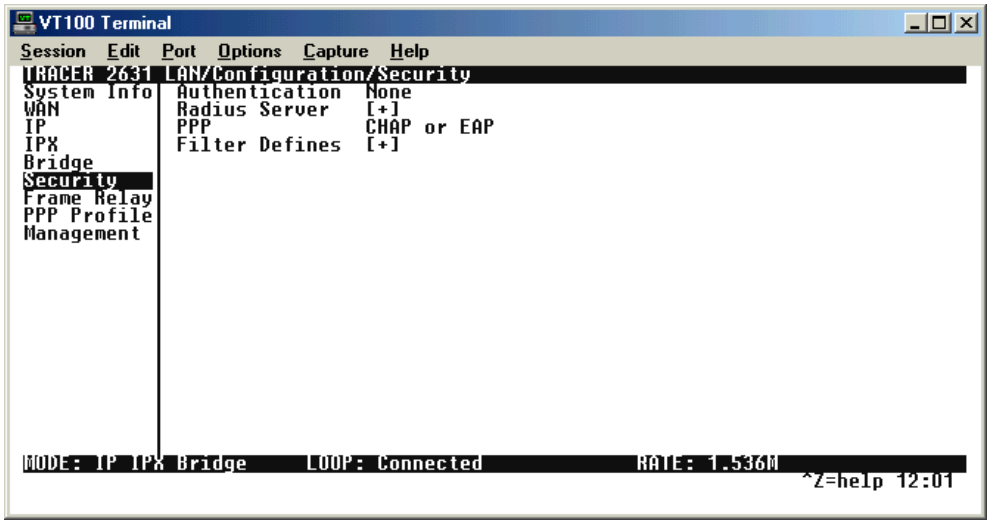

Figure 3-7. LAN/Configuration/Security Screen

Security/Authentication

Write security: 1; Read security: 2

The method used for authenticating the PPP peer is selected here. Possible values are:

None (default)	No attempt is made to authenticate the PPP peer.
RADIUS	The TRACER 2631 will act as a RADIUS client and authenticate the PPP peer using the RADIUS server. The RADIUS server parameters must be set up properly for this to work.
PPP Profile	The PPP profile is used to authenticate the PPP peer.

See *Configuration/PPP Profile* on page 60 for more information on authenticating.

Security/RADIUS Server

The parameters for the radius server are configured in this menu. The RADIUS server can be used for authenticating a PPP peer (if defined under **SECURITY/AUTHENTICATION**) and for Telnet server sessions.

RADIUS Server/Primary Server

Write security: 1; Read security: 2

This is the IP address of the first RADIUS server that TRACER 2631 should attempt to communicate with when authenticating a PPP peer.

RADIUS Server/Secondary Server

Write security: 1; Read security: 2

This is the IP address of the back-up RADIUS server that TRACER 2631 should attempt to communicate with when the primary server does not respond.

RADIUS Server/UDP Port

Write security: 1; Read security: 2

This is the UDP port that TRACER 2631 should use when communicating with the RADIUS server. The default is 1645, which is the commonly used port.

RADIUS Server/Secret

Write security: 0; Read security: 1

The RADIUS server and TRACER 2631 share this text string, which is used by the RADIUS sever to authenticate the TRACER 2631 that is the RADIUS client. The factory default is not to use a secret string.

RADIUS Server/Retry Count

Write security: 1; Read security: 2

This is the number of times TRACER 2631 should send a request packet to the RADIUS server without a response before giving up. If the number of attempts to communicate with the primary server is equal to the retry count, the secondary server (if defined) is tried. If the secondary server does not respond within the retry count, the PPP peer (or Telnet session) is not authenticated and is dropped. The default is 5.

Security/PPP

Write security: 1; Read security: 2

The PPP peer can be authenticated using three standard methods: PAP (Password Authentication Protocol), CHAP (Challenge Handshake Protocol) and EAP (Extensible Authentication Protocol). The strength of the authentication is determined in the order EAP, CHAP, followed by PAP, where EAP is the strongest and PAP is the weakest. PAP is a clear-text protocol, which means the password is sent over the PPP link in a readable format. Care must be taken not to allow highly sensitive passwords to become compromised using this method. CHAP and EAP use a one-way hashing algorithm which makes it virtually impossible to determine the password. EAP has other capabilities which allow more flexibility than CHAP.

The following selections are possible:

PAP, CHAP or EAP (default)	TRACER 2631 will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP or PAP.
CHAP or EAP	TRACER 2631 will ask for EAP during the first PPP LCP negotiation and allow the PPP peer to negotiate down to CHAP but not PAP.
EAP	TRACER 2631 will only allow EAP to be negotiated. If the PPP peer is not capable of doing EAP, then the connection will not succeed.

Security/Filter Defines

TRACER 2631 can filter packets based on certain parameters within the packet. The method used by TRACER 2631 allows the highest flexibility for defining filters and assigning them to a profile. The filters are set up in two steps: (1) defining the packet types, and (2) adding them to a list under the PPP profile or DLCI map. See the section *DLCI Mapping/Filters* on page 58 for examples of how to set up filter profiles. This menu is used to define the individual filter defines based on packet type.

Filter Defines /MAC Filter Defines

Write security: 2; Read security: 3

The MAC filter is applied to bridge packets only. Bridge packets which are forwarded by the bridge functionality of TRACER 2631 are defined here. Up to 32 MAC defines can be specified.

Name	Identifies the filter entry
Src Addr	48-bit MAC source address used for comparison (hexadecimal format)
Src Mask	Bits in the MAC source address which are compared (hexadecimal format)
Dest Addr	48-bit MAC destination address used for comparison (hexadecimal format)
Dest Mask	Bits in the MAC destination address used for comparison (hexadecimal format)
MAC Type	16-bit MAC type field used for comparison (hexadecimal format)
Type Msk	Bits in the MAC type field used for comparison (hexadecimal format)

Filter Defines /Pattern Filter Defines

Write security: 2; Read security: 3

The pattern filter is applied to bridge packets only. That is any packet which is forwarded by the bridge functionality of TRACER 2631. Up to 32 pattern defines can be specified.

Name	Identifies the filter entry
Offset	Offset from beginning of packet of where to start the pattern comparison
Pattern	64 bits used for comparison (hexadecimal format)

Filter Defines /IP Filter Defines

Write security: 2; Read security: 3

The IP filter defines apply to any IP packet, whether it is routed or bridged. Up to 32 IP defines can be specified.

Name	Identifies the filter entry
IP Src	IP address compared to the source address (dotted decimal format)
Src Mask	Bits which are used in the source comparison (dotted decimal format)

IP Dest	IP address compared to the destination address (dotted decimal format)
Dest Mask	Bits which are used in the destination comparison (dotted decimal format)
Src Port	IP source port number used for comparison
	Range: 0 to 65535 (decimal format)
Src Port Cmpr	Type of comparison that is performed
=	Means ports equal to
not =	Means ports not equal to
>	Means ports greater than
<	Means ports less than
None	Means the source port is not compared
Dst Port	IP destination port number used for comparison Range: 0 to 65535 (decimal format)
Dst Port Cmpr	Type of comparison that is performed
=	Means ports equal to
not =	Means ports not equal to
>	Means ports greater than
<	Means ports less than
None	Means the destination port is not compared
Proto	Protocol used for comparison; Range: 0 to 255 (decimal format)
Proto Cmpr	Type of comparison that is performed
=	Means protocols equal to
not =	Means protocols not equal to
>	Means protocols greater than
<	Means protocols less than
None	Means the protocol is not compared
TCP Est	
Yes	Only when TCP established
No	Only when TCP not established
Ignore	Ignore TCP flags

Filter Defines /IPX Filter Defines

Write security: 2; Read security: 3

The IPX filter defines apply to any IPX packet whether it is routed or bridged. Also, any IPX encapsulation type will be accounted for. Up to 32 IPX defines can be specified.

Name	Identifies the filter entry (15 characters max)
Src Net	32-bit source network address
Src Mask	Bits in the source network address which are compared (hexadecimal format)
Dest Net	32-bit destination network address
Dest Mask	Bits in the destination network address which are compared (hexadecimal format)
Src Socket	16-bit value which is the source socket
	Range: 0-65535
Src Socket Comp	Type of comparison that is performed
=	Means socket equal to
Not =	Means socket not equal to
>	Means socket greater than
<	Means socket less than
None	No comparison is done on source socket
Dest Socket	16-bit value which is the destination socket
	Range: 0-65535.
Dest Socket Comp	Type of comparison that is performed
=	Means socket equal to
Not =	Means socket not equal to
>	Means socket greater than
<	Means socket less than
None	No comparison is done on destination socket
Type	8-bit value which is the IPX type
Type Comp	Type of comparison that is performed
=	Means type equal to
Not =	Means type not equal to
>	Means type greater than
<	Means type less than
None	No comparison is done on IPX type

Configuration/Frame Relay

Frame Relay is a connection-oriented service requiring circuits to be configured by your carrier to establish a physical link between two or more locations. Multiple virtual circuits (which appear as virtual point-to-point links) can be run through the same physical connection.

There are two types of virtual circuits supported in Frame Relay – Permanent Virtual Circuits (PVC) and Switched Virtual Circuit (SVC). PVCs are like dedicated point-to-point private lines. Since the physical connection is always there in the form of a leased line, call setup and tear down is done by a carrier via a network management system. SVCs require setup and tear down and are generally not available from Frame Relay carriers. Virtually all Frame Relay communication is done using PVCs. TRACER 2631 supports PVCs only.

A number called the Data Link Connection Identifier (DLCI) identifies each virtual circuit within a shared physical channel.

Figure 3-8 shows the **FRAME RELAY** menu.

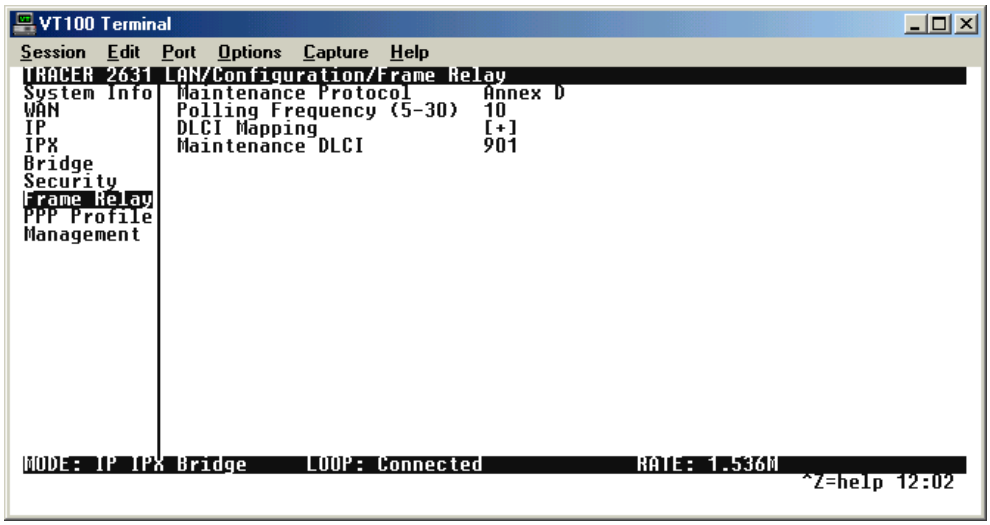

Figure 3-8. LAN/Configuration/Frame Relay Screen

Frame Relay/Maintenance Protocol

Write security: 3, Read security: 5

The Frame Relay maintenance protocol is used over the wireless link. The maintenance protocol is used to send link status and virtual circuit information between Frame Relay switches and other devices (such as routers) that communicate with them. Possible choices are listed below.

Annex D (default)	This is an ANSI standard and is the most commonly used standard in the US.
Annex A	This is the CCITT European standard.
LMI	Local Management Interface. This was developed by a vendor consortium and is also known as the “consortium” management interface specification. It is still used by some carriers in the U.S.

Static	This should be selected when there is no Frame Relay switch in the circuit. The DLCIs are assigned in the DLCI Mapping and must be the same for the device it will communicate with.

Frame Relay/Polling Frequency

Write security: 3, Read security: 5

This parameter is the interval that TRACER 2631 polls the Frame Relay switch using the maintenance protocol selected above. TRACER 2631 is required to poll the Frame Relay switch periodically to determine whether the link is active. The value is in seconds and ranges from 5 to 30 seconds with a default of 15 seconds.

Frame Relay/DLCI Mapping

This menu allows each DLCI to be mapped to a particular Frame Relay maintenance protocol. Each protocol parameter can be individually configured for each DLCI. By factory default, the DLCI map is empty.

When empty and a maintenance protocol other than static is used, TRACER 2631 will poll the switch to determine which DLCIs are active. These active DLCIs will attempt to determine the IP and IPX addresses on the other end of the virtual circuit using Inverse ARP (IARP). If there is a response, the network learned will be added to the router tables and the virtual circuit will be treated as an unnumbered interface. Bridge mode is not attempted in this case.

When more than one DLCI mapping is listed, TRACER 2631 will try to match the DLCIs learned from the Frame Relay switch with the DLCI values in the map. If there is a match, the protocols specified in the map are used. However, if an active DLCI is not in the list it looks for an entry that has 0 in the DLCI field. This entry is considered the default entry to use when no match occurs. If this default entry is not present, TRACER 2631 falls back to using IARP as in the previous paragraph to determine the protocols to use with that particular virtual circuit. If a static maintenance protocol is used, at least one DLCI mapping must be specified.

N O T E

To insert a new profile, press the **I** key when over the **NUM** column. A new inserted profile will always be set up with the default parameters. To copy parameters from an old profile to this newly inserted profile, use the copy (**C**) and paste (**P**) keys. Entire configuration trees can be copied with this method.

N O T E

To delete an unused profile, use the **D** key when the cursor is over the number in the **NUM** column. Once deleted, the profile is gone permanently as soon as the DLCI Mapping is saved. Items may be deleted when **DEL** appears below the status bar.

DLCI Mapping/Active

Write security: 3, Read security: 5

When this parameter is set to **YES** (default), the mapping is used to determine the protocols used. If set to **NO**, TRACER 2631 will ignore the virtual circuit with this DLCI.

DLCI Mapping/DLCI

Write security: 3, Read security: 5

This is the DLCI associated with this virtual circuit. This value can range from 16 to 1007.

DLCI Mapping/IP Map

Write security: 3, Read security: 5

This menu represents the IP protocol mapping that is to take place for this DLCI.

IP Map/Active

Write security: 3, Read security: 5

When this is set to **YES** (default), TRACER 2631 will attempt to transport IP packets for this DLCI. A setting of **NO** means that no IP traffic or route will be exchanged.

IP Map/IARP

Write security: 3, Read security: 5

When this is set to **YES** (default), TRACER 2631 will send IARP packets in order to determine the IP address on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IP route table. A setting of **NO** means that the route address is to be assigned statically using the **IP MAP/FAR-END IP ADDRESS** parameter. TRACER 2631 will always respond to IARP requests.

IP Map/Far-End IP Address

Write security: 3, Read security: 5

This is the IP address of the device on the other end of the virtual circuit. When this DLCI becomes active, TRACER 2631 will add a route in the IP routing table.

IP Map/IP Netmask

Write security: 3, Read security: 5

The IP network mask to apply to the **FAR-END IP ADDRESS** and **LINK IP ADDRESS** is specified here.

IP Map/Link IP Address

Write security: 3, Read security: 5

The virtual circuit may require an IP address to be specified at this DLCI interface. This is called a numbered interface. This address is used by TRACER 2631 to respond to IARP requests. If this IP address is left as 0.0.0.0, the link is treated as unnumbered and TRACER 2631 responds to the IARP with its Ethernet IP address.

IP Map/RIP Protocol

Write security: 3, Read security: 5

The RIP protocol can be specified per DLCI. The possible selections are **OFF** (meaning no RIP packets are listened to or sent), **V1** (which is RIP version 1) (default) or **V2** (which is RIP version 2).

IP Map/RIP Method

Write security: 3, Read security: 5

The way the RIP protocol sends out its advertisements is specified here:

None	All routes in the router table are advertised out this virtual circuit with no modification of the metrics.
Split Horizon (default)	Only routes not learned from this particular virtual circuit are advertised.
Poison Reverse	All routes are advertised, but the routes learned from this port are "poisoned" with an infinite metric.

IP Map/RIP Direction

Write security: 3, Read security: 5

This parameter allows the direction at which RIP advertisements are sent and listened to be specified.

TX and RX (default)	RIP advertisements are periodically transmitted and are listened to on this virtual circuit.
TX Only	RIP advertisements are periodically transmitted but are not listened to on this virtual circuit.
RX Only	RIP is not transmitted on this virtual circuit but they are listened to.

IP Map/NAT

TRACER 2631 can perform NAT over a PVC. Setting this option to **ON** will cause TRACER 2631 to translate between the Ethernet addresses and the configured **LINK IP ADDRESS**. Only one PVC may be used for translation at one time. If more than one IP Map is configured for NAT, the first PVC which is activated becomes the NAT port.

DLCI Mapping/IPX Map

This menu represents the IPX protocol mapping that is to take place for this DLCI.

IPX Map/Active

Write security: 3, Read security: 5

When this is set to **YES** (default), TRACER 2631 will attempt to transport IPX packets for this DLCI. A setting of **NO** means that no IPX traffic or route will be exchanged.

IPX Map/IARP

Write security: 3, Read security: 5

When this is set to **YES** (default), TRACER 2631 will send IARP packets to determine the IPX network on the other end of the virtual circuit. If the IARP is responded to, a route is placed in the IPX route table. A setting of **NO** means that the IPX network is to be assigned to the link statically using the IPX Map/Link Network parameter. TRACER 2631 will always respond to IARP requests.

IPX Map/Link Network

Write security: 3, Read security: 5

This is the IPX network of the link or of the other device's LAN. When this DLCI becomes active, TRACER 2631 will add a route to this network in the IPX routing table. This address is also used by TRACER 2631 to respond to IARP requests. If this IPX address is left as 0, the link is treated as unnumbered and TRACER 2631 responds to the IARP with its Ethernet IPX address.

DLCI Mapping/Bridge Map

This menu is used to permit bridging of packets over this DLCI. Each DLCI or virtual circuit must be assigned a bridge group. The bridge group treats all virtual circuits as one circuit. Bridge packets destined to be transmitted out a particular bridge group are copied and transmitted individually out each DLCI in the bridge group. However, incoming bridge packets received from one DLCI are not retransmitted out the other DLCIs in the same bridge group. Any device in the bridge group must transmit to each DLCI. This requires a fully meshed circuit, meaning each device has a virtual circuit to each other.

Bridge Map/Active

Write security: 3, Read security: 5

When this is set to **YES** (default), TRACER 2631 will bridge packets to and from this DLCI. Bridge packets are any packets that are not IP or IPX packets except when the router is turned off, in which case that particular router's protocol packets are bridged. A setting of **NO** means that no bridging will occur.

Bridge Map/Bridge Group

Write security: 3, Read security: 5

The bridge group that this DLCI is part of is specified here as **GROUP 1** or **GROUP 2**. These groups correspond to the spanning tree protocols Bridge Group 1 and Bridge Group 2.

DLCI Mapping/Filters

TRACER 2631 can block packets in and out of a PVC port by use of the filters. They are set up in two steps: 1) Define the types of packets that would be of interest in the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES** menu; and 2) Set up the filter type and combination of defines that will cause a packet block.

Filters/In from PVC

Write security: 2; Read security: 5

The packets which come into TRACER 2631 via this PVC can be filtered in three ways:

Disabled (default)	Turns off packet input filtering. No incoming packets from this PVC are blocked.
Block All	All incoming packets from this PVC are blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.
Forward All	All incoming packets from this PVC are not blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.

Filters/In Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

Active	Turns this entry active when set to **ON**.
Type	Selects the filter define list to reference:
MAC	from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/MAC FILTER DEFINES** list.
Pattern	from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/ PATTERN FILTER DEFINES** list.
IP	from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/IP FILTER DEFINES** list.
IPX	from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/IPX FILTER DEFINES** list.
Filter List Name	Selects between filters defined in the list.
Next Oper	the next operation to use to combine with the next filter in the list:
END	the last filter to combine
AND	logically AND this filter with the next filter in the list
OR	logically OR this filter with the next filter in the list

Filters/Out to PVC

Write security: 2; Read security: 5

The packets which transmit out this PVC from TRACER 2631 can be filtered in three ways:

Disabled (default)	Turns off packet output filtering. No outgoing packets to this PVC are blocked.
Block All	All outgoing packets to this PVC are blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list.
Forward All	All outgoing packets to this PVC are not blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list.

Filters/Out Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries. The setup is exactly the same as the **FILTER/IN EXCEPTIONS** list.

Configuration/PPP Profile

TRACER 2631 uses the PPP profile to specify the profile used when connected using PPP. **Figure 3-9** shows the **PPP PROFILE** menu.

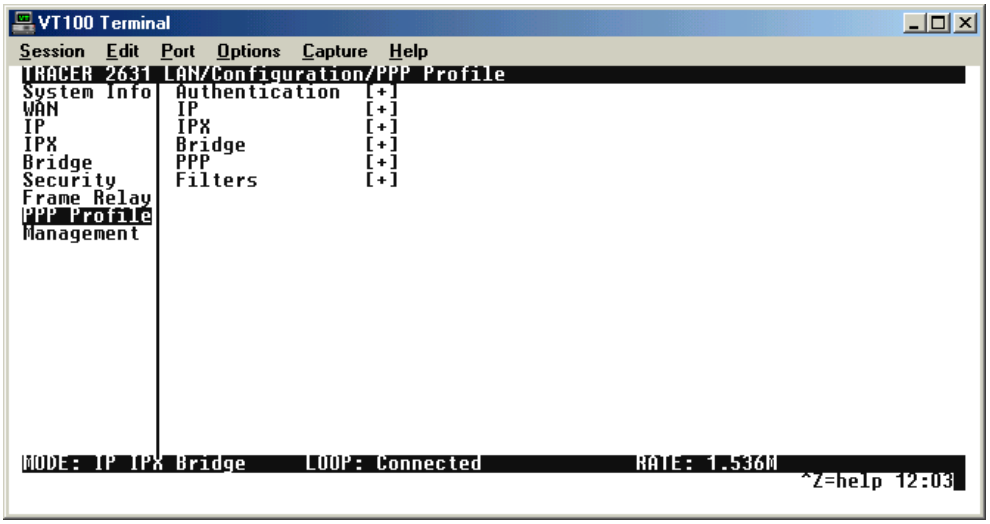

Figure 3-9. LAN/Configuration/PPP Profile Screen

PPP Profile/Authentication

The authentication menu contains the required parameters for the authentication of the PPP peer and for being authenticated by the PPP peer. Authentication is applied between TRACER 2631 and the PPP peer as follows

Authentication/TX Method

Write security: 2; Read security: 3

This parameter specifies how TRACER 2631 is to be authenticated by the PPP peer. There are four possible selections. See *Security/PPP* on page 50 for an explanation of the three PPP standard authentication types.

None	The connection will not allow the PPP peer to authenticate it.
PAP, CHAP or EAP (default)	The connection can be authenticated using PAP, CHAP or EAP.
CHAP or EAP	The connection can be authenticated using CHAP or EAP only.
EAP	The connection will only allow authentication by the peer using EAP.

Authentication/TX Username

Write security: 1; Read security: 3

This is the username that is used when being authenticated by the PPP peer.

Authentication/TX Password

Write security: 0; Read security: 1

This is the password or secret that is used when being authenticated by the PPP peer.

Authentication/RX Username

Write security: 1; Read security: 3

This is the username used to authenticate the PPP peer.

Authentication/RX Password

Write security: 0; Read security: 1

This is the password or secret that is used to authenticate the PPP peer.

PPP Profile/IP

The **IP** menu contains the parameters for exchanging IP data with the PPP peer.

IP/Mode

Write security: 3; Read security: 5

Setting to **ON** (default) will permit this connection profile to negotiate PPP IPCP with the PPP peer for exchanging of IP packets.

IP/NAT

Write security: 3; Read security: 5

TRACER 2631 can perform NAT. This feature is most widely used when connecting to the Internet. The Ethernet network can consist of private network numbers. When this profile is connected, all IP addresses on the Ethernet side are translated into the one real IP address negotiated with the PPP peer (ISP). Multiple stations on the Ethernet side can access the Internet simultaneously. See the section

IP/NAT on page 3-15 for more global options. Setting this option to **ON** will cause TRACER 2631 to perform NAT. When this option is **OFF** (default), the unit will route across the connection normally.

IP/Route

The IP parameters are configured in this menu. TRACER 2631 will automatically discover the PPP peer's networks using PPP IPCP and/or RIP.

Route/IP/Net

Write security: 3; Read security: 5

If known, the PPP peer's IP address or network can be set here. Leaving this at 0.0.0.0 means that TRACER 2631 will determine the PPP peer's IP and network using the PPP IPCP.

Route/Netmask

Write security: 3; Read security: 5

This network mask is applied to the **IP/NET** address for determining the PPP peer's network. If left as 0.0.0.0, a standard network mask is used.

Route/Force IP

Write security: 3; Read security: 5

When set to **YES**, the TRACER 2631 will force the PPP peer to use the IP address in the **IP/NET** for this profile as its WAN IP address. Normally, this option is set to **NO** (default).

IP/RIP

The RIP parameters can be adjusted from their defaults under this menu.

RIP/Mode

Write security: 3; Read security: 5

TRACER 2631 will perform RIP over the WAN connection when this is set to **ON** (default).

RIP/Protocol

Write security: 3; Read security: 5

TRACER 2631 can perform version 1, **V1** (default) (which is RIP version 1), or version 2 , **V2**, of RIP on this WAN connection.

RIP/Method

Write security: 3; Read security: 5

Split Horizon	Only routes not learned on the WAN connection are advertised.
Poison Reverse (default)	All routes are advertised, including routes learned from the WAN connection. These routes are poisoned.
None	All routes are advertised, including routes learned from the WAN connection. No attempt is made to poison these routes.

RIP/Direction

Write security: 3; Read security: 5

TX and RX (default)	RIP advertisements are transmitted and listened to on the WAN connection.
TX only	RIP advertisements are transmitted and not listened to.
RX only	RIP advertisements are listened to but not transmitted.

RIP/Triggered

Write security: 3; Read security: 5

When set to **YES**, only IP RIP updates are sent when the routing table has changed and learned routes are not "aged." When set to **NO** (default), updates are sent periodically.

PPP Profile/IPX

The **IPX** menu contains the parameters for exchanging IPX data with the PPP peer.

IPX/Mode

Write security: 3; Read security: 5

Setting to **ON** (default) will permit this connection profile to negotiate PPP IPXCP with the PPP peer for exchanging of IPX packets.

IPX/Remote Network

Write security: 3; Read security: 5

A non-zero value in this remote network number will allow TRACER 2631 to add a route to the PPP peer's network to the routing table.

The TRACER 2631 normally will treat the wireless link as an unnumbered link. This is usually referred to as being a "half-router." However, a PPP peer which wants to assign a network address to the WAN link can do so, in which case TRACER 2631 will go into "full-router" mode.

IPX/Triggered

Write security: 3; Read security: 5

When set to **YES**, only IPX RIP and SAP updates are sent when the routing or service table has changed and learned routes are not "aged." When set to **NO** (default), updates are sent periodically based on the RIP and SAP timers set in **LAN/CONFIGURATION/IPX/RIP TIMER** and **CONFIGURATION/ IPX/SAP TIMER**.

IPX/Type 20 Packets

Write security: 3; Read security: 5

In order for certain protocol implementations, like NetBIOS, to function in the NetWare environment, routes must allow a broadcast packet to be propagated throughout the IPX networks. The Type 20 IPX packet is used specifically for this purpose. This causes special handling of this packet by TRACER 2631. When a router receives this type of packet, it rebroadcasts it across all interfaces except the one it is received on and includes the network number of that interface in the data portion of the packet. The IPX Router Specification from Novell notes that Type 20 packets should not be propagated across slower links with bandwidths of less than 1Mbps. However, when set to **PASS** (default), TRACER 2631 will allow these packets to propagate over the wireless link. This facilitates dial-on-demand applications. When set to **BLOCK,** all Type 20 packets are not propagated across the WAN connection.

PPP Profile/Bridge

The **BRIDGE** menu contains the parameters needed for exchanging bridged packets with the PPP peer.

Bridge/Mode

Write security: 3; Read security: 5

When set to **ON** (default), the TRACER 2631 will attempt to negotiate PPP BCP with the PPP peer. Bridging can be used even in route mode only if the PPP peer cannot support certain PPP protocols for that particular routing protocol. See *Bridge/WAN IP Bridge* on page 44 and *Bridge/WAN IPX Bridge* on page 45 for further details.

PPP Profile/PPP

TRACER 2631 supports the Internet Engineering Task Force (IETF) standards for the Point-to-Point Protocol. The PPP state machine running in TRACER 2631 can be fine-tuned to support many applications that can be employed. The configurable items under this menu can be changed from their default values for special cases.

PPP/VJ Compression

Write security: 3; Read security: 5

When this item is set to **ON**, TRACER 2631 will perform TCP/IP header compression known as Van Jacobson compression to the PPP peer. Normally, this is not necessary and can be set to **OFF** (default) to disable it.

PPP/Max Config

Write security: 3; Read security: 5

This value is the number of unanswered configuration-requests that should be transmitted before giving up on a connection. The possible values are **5**, **10** (default), **15** and **20**.

PPP/Max Timer

Write security: 3; Read security: 5

This value is the number of seconds to wait between unanswered configuration-requests. The possible values are **1 SEC**, **2 SECS** (default), **3 SECS**, **5 SECS** and **10 SECS**.

PPP/Max Failure

Write security: 3; Read security: 5

Due to the nature of PPP, configuration options may not be agreed upon between two PPP peers. This value is the number of configuration-naks that should occur before an option is configuration-rejected. This allows a connection to succeed that might otherwise fail. The possible values are **5** (default), **10**, **15** and **20**.

PPP Profile/Filters

TRACER 2631 can block packets in and out of a WAN port by use of the filters. They are set up in two steps: 1) Define the types of packets that would be of interest in the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES** menu; and 2) Set up the filter type and combination of defines that will cause a packet block.

Filters/WAN-to-LAN (In)

Write security: 2; Read security: 5

The packets which come into TRACER 2631 can be filtered in three ways:

Disabled (default)	Turns off packet input filtering. No incoming packets are blocked.
Block All	All incoming packets from the WAN are blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.
Forward All	All incoming packets from the WAN are not blocked except as defined in the **FILTERS/IN EXCEPTIONS** list.

Filters/In Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries which can be combined using the operations field. The operations are performed in the order they appear on the list.

Active — Turns this entry active when set to **ON.**

Type — Selects the filter define list to reference:

- **MAC** — from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/MAC FILTER DEFINES** list
- **Pattern** — from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/PATTERN FILTER DEFINES** list
- **IP** — from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/IP FILTER DEFINES** list
- **IPX** — from the **LAN/CONFIGURATION/SECURITY/FILTER DEFINES/IPX FILTER DEFINES** list

Filter List Name — Selects between filters defined in the list.

Next Oper — The next operation to use to combine with the next filter in the list:

- **END** — the last filter to combine
- **AND** — logically AND this filter with the next filter in the list
- **OR** — logically OR this filter with the next filter in the list

Filters/LAN-to-WAN (Out)

Write security: 2; Read security: 5

The packets which come out toward the WAN from TRACER 2631 can be filtered in three ways:

Disabled (default) — Turns off packet output filtering. No outgoing packets are blocked.

Block All — All outgoing packets to the WAN are blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list.

Forward All — All outgoing packets to the WAN are not blocked except as defined in the **FILTERS/OUT EXCEPTIONS** list.

Filters/Out Exceptions

Write security: 2; Read security: 5

This is a list of up to 32 filter entries. The setup is exactly the same as the **FILTER/IN EXCEPTIONS** list.

Configuration/Management

The LAN functions of TRACER 2631 can be managed using Telnet, Simple Network Management Protocol (SNMP), or the maintenance port. See Appendix D for a description of the MIBs supported by TRACER 2631. Each of the three methods can be protected using authentication. **Figure 3-10** shows the **CONFIGURATION/MANAGEMENT** menu.

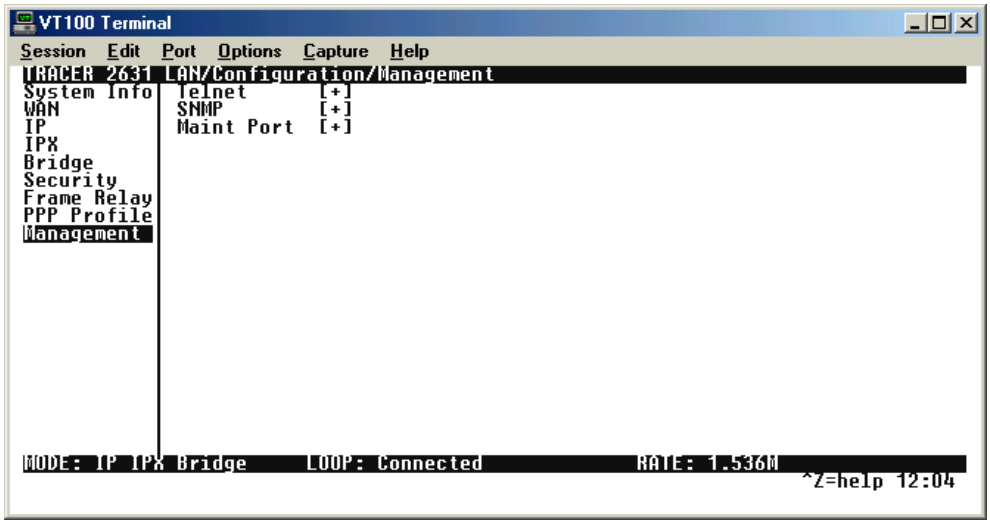

Figure 3-10. LAN/Configuration/Management Screen

Management/Telnet

Any Telnet client application can bring up a session to TRACER 2631's Telnet server using the standard Telnet TCP port. Only one session is supported at a time. All sessions require a username and password.

Telnet/Server Access

Write security: 2; Read security: 5

This option must be set to **ON** (default) to access TRACER 2631 via Telnet. Turning it **OFF** means that access is denied.

Telnet/User List

Up to four users can be configured for access to TRACER 2631. Each user can be assigned a privilege and timeout.

User List/Name

Write security: 1; Read security: 3

A text string of the username for this session.

User List/Authen Method

Write security: 1; Read security: 3

The user can be authenticated in two ways:

Password	The **PASSWORD** field is used to authenticate the user.
RADIUS	The RADIUS client is used for authenticating the user.

User List/Password

Write security: 0; Read security: 3

When the authenticating method is password, this text string is used for the password.

User List/Idle Time

Write security: 1; Read security: 3

When set to non-zero, the session is automatically logged out when no activity occurs for this amount of time. The range is 0 to 255 and is in minutes. The default is 10 minutes, and a setting of 0 will never time-out the session. When a timeout occurs during an edit session, all changes are saved.

User List/Level

Write security: 0; Read security: 1

This is the security level privilege that is assigned for this user. See *Security Levels* on page 34 for an explanation of what those levels imply. Level 0 is the default.

Management/SNMP

TRACER 2631 is an SNMP agent. It can respond to Get-Requests, Set-Requests, and generate traps. These two lists set up the manager, communities, and levels. See Appendix D for more information on SNMP.

SNMP Access

Write security: 3; Read security: 5

When set to **OFF**, SNMP access is denied. When set to **ON** (default), TRACER 2631 will respond to SNMP managers based on the following lists.

SNMP/Communities

This list is used to set up to eight SNMP community names that TRACER 2631 will allow. Factory default sets the community **PUBLIC** with **GET** privileges.

Communities/Name

Write security: 1; Read security: 3

This is a text string for the community name.

Communities/Privilege

Write security: 1; Read security: 3

The access for this manager can be assigned one of the three following levels.

None	No access is allowed for this community or manager.
Get	Manager can only read items.
Get/Set	Manager can read and set items.

Communities/Manager IP

Write security: 1; Read security: 3

This is the IP address of SNMP manager. If set to 0.0.0.0, any SNMP manager can access the TRACER 2631 for this community.

SNMP/Traps

TRACER 2631 can generate SNMP traps. See Appendix D for trap types supported. This list allows up to four managers to be listed to receive traps.

Traps/Manager Name

Write security: 2; Read security: 4

This is the text string describing the name of the entry. It is intended for easy reference and has no bearing on the SNMP trap function.

Traps/Manager IP

Write security: 2; Read security: 4

This is the IP address of the manager that is to receive the traps.

Management/Maint Port

TRACER 2631 has an EIA-232 connector on the back of the unit. The **SECURITY** setup for that port is under this menu.

Maint Port/Password Protect

Write security: 0; Read security: 1

When set to **NO** (default), the maintenance port is not password protected. When **YES**, TRACER 2631 will prompt for a password upon startup.

Maint Port/Password

Write security: 0; Read security: 1

This is the text string that is used for comparison when password protecting the maintenance port. By default, no password is entered.

N O T E

The security level for the maintenance port is always set to 0. This gives full access to all menus.

Configuration/Terminal Mode

This is an activator which places the TRACER 2631 terminal session into a command prompt mode. All menu options are accessible during this mode. See Appendix E for the command structure and command list. Type **Exit** to leave the terminal mode and return to the menus.

LAN/STATUS MENU

The TRACER 2631's **STATUS** menu contains comprehensive status and diagnostic information used in verifying configuration and identifying problems on the LAN interface. The menus are divided into protocol types and sessions. **Figure 3-11** shows the **STATUS** menu.

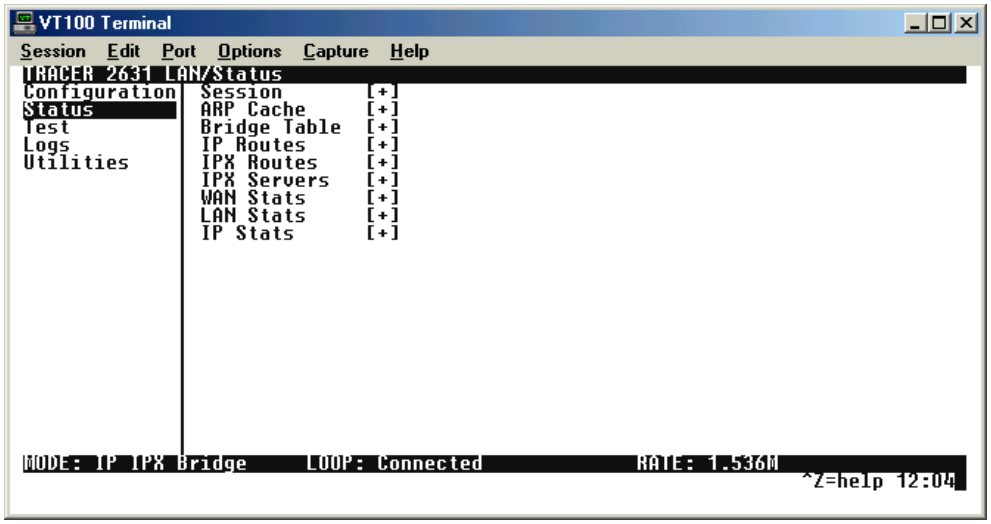

Figure 3-11. LAN/Status Screen

Status/Session

This menu contains the current status of all sessions and spanning tree ports.

Session/PPP Session

Read security: 5

This menu reflects the results of PPP negotiations, username, time connected, and data rates for the session.

LCP	Shows UP if PPP Link Control Protocol has negotiated successfully
BCP	Shows UP if PPP Bridge Control Protocol has negotiated successfully
IPCP	Shows UP if PPP IP Control Protocol has negotiated successfully
IPXCP	Shows UP if PPP IPX Control Protocol has negotiated successfully
Up Time	Displays how long the link has been up
TX Pkts	Number of packets transmitted
RX Pkts	Number of packets received
TX Bytes	Number of bytes transmitted
RX Bytes	Number of bytes received
TX Rate	Current application data transmission rate
RX Rate	Current application data reception rate

Session/DLCI Table

The status of all virtual circuits is displayed here.

DLCI	The DLCI that is associated with this virtual circuit.
State	The state of the virtual circuit:
Inactive	Means the circuit exists but has been deactivated by the Frame Relay switch.
Exists	Means the circuit exists at this point and should be activated soon.
Active	Means the circuit is fully active.
Off	Means the circuit has been turned of by the DLCI mapping active selection.
TX Frames	Number of Frame Relay packets that have been transmitted via this DLCI.
RX Frames	Number of Frame Relay packets that have been received via this DLCI.
TX Bytes	Number of Frame Relay bytes that have been transmitted via this DLCI.
RX Bytes	Number of Frame Relay bytes that have been received via this DLCI.
IP Sublfc	The IP router port assigned for this DLCI. Possible ports are fr0, fr1, … , fr9. None means that this DLCI not used for routing IP.
IPX Sublfc	The IPX router port assigned for this DLCI. Possible ports are fr0, fr1, … , fr9. None means that this DLCI not used for routing IPX.
Bridge Group	The bridge group that this DLCI belongs to (Group 1 or Group 2). None means that this DLCI is not used for bridging.

Session/Spanning Tree

Read security: 5

When Bridge mode and Spanning Tree mode are active, this reflects the current state of the LAN and WAN ports. The following can appear:

Off	Appears when Spanning Tree mode is disabled
Disabled	Port is not connected (for WAN) or disabled in configuration
Listening	Port is in the listening state
Learning	Port is in the learning state
Forwarding	Port is in the forwarding state with the following possible properties:
root	is the root port
designated	is designated port
Blocking	Port is in the blocked state

Status/ARP Cache

Read security: 5

This lists the contents of TRACER 2631's ARP table. All resolved cache entries time out after 20 minutes. Unresolved entries time out in 3 minutes.

ARP Cache/IP Address

IP address used for resolving MAC address.

ARP Cache /MAC Address

Ethernet address resolved (0 = no resolution).

ARP Cache/Time

Minutes since entry was first entered.

Status/Bridge Table

Read security: 5

This lists the contents of TRACER 2631's bridge table.

Bridge Cache/MAC Address

Ethernet address for device learned.

Bridge Cache/Port

Port device learned from: **LAN, WAN0,** or **WAN1**

Bridge Cache/TTL
Seconds until address is removed from table.

Status/IP Routes
Read security: 5

This lists the contents of the TRACER 2631's IP router table.

IP Routes /IP Address
Network or host destination address.

IP Routes /Netmask
Network mask applied to the destination address.

IP Routes /Gateway
Host or router to receive this packet.

IP Routes /Port
Port gateway is located on:

local	Sent directly to the TRACER 2631 router
eth0	TRACER 2631's Ethernet port
wan0	TRACER 2631's first PPP bundle
fr 0 . . . fr 9	TRACER 2631 is connected up to 10 DLCIs

IP Routes /Use
Number of times TRACER 2631 has referenced the route

IP Routes/Flags
Important tags associated with this route entry

H	Route is a host route
G	Route is a gateway route
D	Route learned dynamically from RIP
I	Route learned from an ICMP redirect
P	Route is private and is not advertised with RIP
T	Route is to a triggered port (updates only when table changes)

IP Routes/Hops
Number of routers that must be gone through to get to the destination. Ranges from 0-15 or 16 for infinite (cannot get there from here).

IP Routes/TTL
Time to live seconds until address is removed from table or "zombied." Value of **999** means route is static.

Status/IPX Routes
Read security: 5

This lists the contents of TRACER 2631's IPX router table.

IPX Routes /Network
Network destination address.

IPX Routes /Gateway
Node or Ethernet address of gateway to receive this packet.

IPX Routes /Port
Port gateway is located on:

local	Sent directly to the TRACER 2631 router
eth0	TRACER 2631's Ethernet port
wan0	TRACER 2631's first PPP bundle
fr 0 . . . fr 9	TRACER 2631 is connected up to 10 DLCIs

IPX Routes/Use
Number of times TRACER 2631 has referenced the route.

IPX Routes/Hops
Number of routers that must be gone through to get to the destination. Ranges from 0-15 or 16 for infinite (can't get there from here).

IPX Routes/Ticks
Router determined value for representing time packets take to reach the network destination. One tick is equivalent to one-eighteenth of a second.

IPX Routes/TTL
Time to live seconds until address is removed from table. Value of **999** means route is static.

Status/IPX Servers

Read security: 5

This lists the contents of TRACER 2631's IPX server table.

IPX Servers/Type

The server type.

IPX Servers/Name

The server name.

IPX Servers/Network

The server network address.

IPX Servers /Address

The server's node address.

IPX Servers/Socket

The server's socket address.

IPX Servers/Hops

Number of routers that must be gone through to get to the server. Ranges from **0-15** or **16** for infinite.

IPX Servers/TTL

Time to live seconds until address is removed from table. Value of **999** means server is static.

Status/WAN Stats

Read security: 5

This menu contains generic WAN statistics on the HDLC hardware port.

HDLC Port	
TX Bytes	Total number of raw bytes sent out HDLC port 1
RX Bytes	Total number of raw bytes received in HDLC port 1
RX CRCs	Total number of CRC errors detected on HDLC port 1
Clear Counts	When activated, clears all WAN stat counts

Status/LAN Stats

Read security: 5

This menu contains statistics for the Ethernet port.

TX Packets	Packets transmitted out the Ethernet port
RX Packets	Packets received from the Ethernet port
TX Errors	Total transmit errors encountered on Ethernet port
Single Collisions	Total single collisions before successful transmission
Multiple Collisions	Total multiple collisions before successful transmission
Excessive Collisions	Total collisions that resulted in packet being dropped
Deferred Transmissions	Total packets deferred due to collisions
Carrier Sense Errors	Total carrier sense errors encountered (no link integrity)
RX Errors	Total packets received in error and dropped
CRCs	Total packets detected with CRC errors
Giants	Total packets received that were greater than 1518 bytes
Runts	Total packets received that were less than 64 bytes
RX Collisions	Total collisions that occurred during reception
Clear Counts	When activated, clears all LAN Stat counts.

Status/IP Stats

Read security: 5

This menu contains IP statistics that can be useful when diagnosing problems. All are taken from the SNMP MIB-2 variables.

Active TCP connections
Bad header packets
Bad IP addresses
Bad protocol discards
Clear Counts - clears all IP stats
Datagrams discarded
Default TTL
Disassembled fragments
Discarded routing entries
Errorfree discards
Failed fragments
ICMP messages received

ICMP messages sent
ICMP packet errors
ICMP redirected messages
ICMP specif if errors
ICMP timeouts received
IP datagrams reassembled
IP datagrams received
IP datagrams sent
IP reassembly failures
IP reassembly timeout
No application at dest. port
Routeless discards
Sent datagrams to upper layers
Successful fragments
TCP current connections
TCP failed attempts
TCP passive connections
TCP segments received
TCP segments sent
Total forwarded datagrams
Total IP fragments
Total TCP resets
Total TCP retransmits
UDP bad packets
UDP datagrams received
UDP datagrams sent

LAN/TEST MENU

TRACER 2631's **TEST** menu contains built-in tests that can be used to diagnose problems on the LAN interface. **Figure 3-12** shows the **TEST** menu screen.

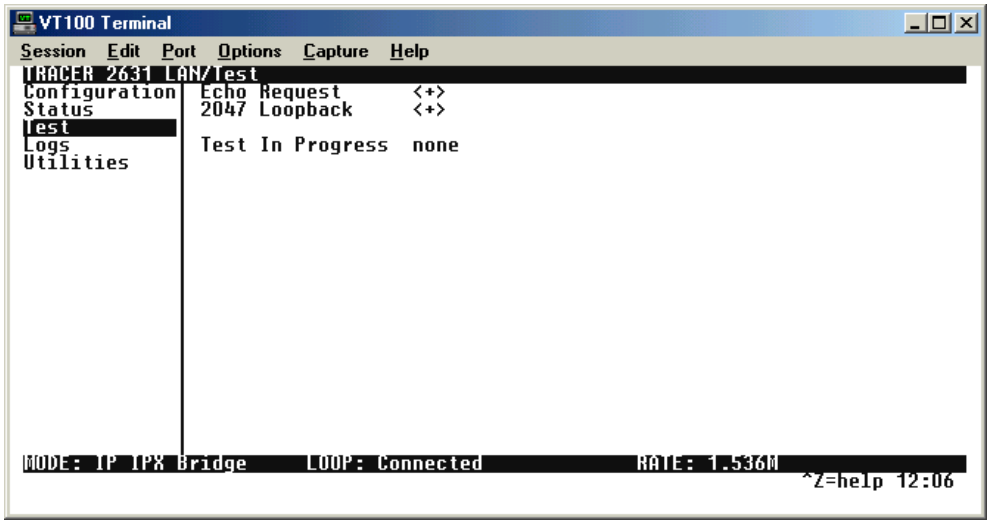

Figure 3-12. LAN/Test Screen

The following tests can be run:

Test/Echo Request

Write security: 4, Read security: 5

When activated, the echo request test will begin sending continuous PPP echo request packets to any open LCP ports. Results are displayed on the screen. This is not used in the Frame Relay mode.

Test/2047 Loopback

Write security: 4, Read security: 5

When activated, a loopback command is sent to the far-end TRACER and an internal 2047 pattern is continually transmitted towards the remote end. Loopbacked data is checked and an error count is maintained.

N O T E

When this test is de-activated, the router will go through a soft reset. Routing functionality will be lost until the unit comes out of reset (approximately 10 seconds). Any non-saved options will be lost.

LAN/LOGS MENU

The **LOGS** menu contains logs displaying important information about the running condition of the TRACER 2631. The logs can be set to capture diagnostics of error conditions only by way of a log level. **Table 3-3** lists the division of levels.

Table 3-3. Log Levels

Level 0	Fatal event (causes reset)
Level 1	Critical event
Level 2	Error event
Level 3	Warning event
Level 4	Notify event
Level 5	Informational event
Level 6	Debugging event

Figure 3-13 shows the **LOGS** menu. The three logs available are listed after the figure.

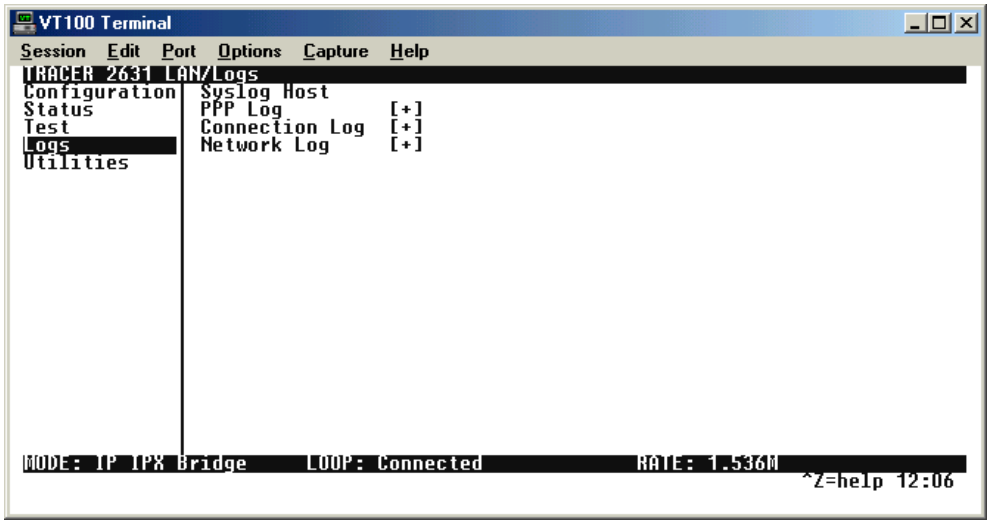

Figure 3-13. LAN/Logs Screen

Logs/Syslog Host

Set this to the IP address or domain name (if DNS configured) of the Syslog host device. All log events are sent to this device.

Logs/PPP Log

Information pertaining to the PPP negotiation and authentication will be logged here.

PPP Log/Active

When set to **YES** (default), PPP events below or equal the log level are logged into the log.

PPP Log/Wrap
When set to **YES** (default), new PPP events will overwrite old PPP events when the log is full. All logging will stop when the log is full and set to **NO**.

PPP Log/Level
In order to log events, they must be at or below this level. Range is **0** to **6**. The default is **3**.

PPP Log/View
This menu displays the log list. The fields are as follows:

Date/Time	Date and time event occurred
Level	Level associated with this event (0-6)
Message	Text message for this event; if message is too long to fit on the line, another event appears below it continuing the message

PPP Log/Clear
This clears the log when activated.

Logs/Connection Log
Information pertaining to the connection over the wireless link.

Connection Log/Active
When set to **YES** (default), connection events below or equal the log level are logged into the log.

Connection Log/Wrap
When set to **YES** (default), new connection events will overwrite old connection events when the log is full. All logging will stop when the log is full and set to **NO**.

Connection Log/Level
In order to log events, they must be at or below this level. Range is **0** to **6**. The default is **3**.

Connection Log/View
This menu displays the log list. The fields are as follows:

Date/Time	Date and time event occurred
Level	Level associated with this event (0-6)
Message	Text message for this event; if message is too long to fit on the line, another event appears below it continuing the message

Connection Log/Clear
This clears the log when activated.

Logs/Network Log

Information pertaining to the routing protocols is placed in this log.

Network Log/Active

When set to **YES** (default), call events below or equal the log level are logged into the log.

Network Log/Wrap

When set to **YES** (default), new Network events will overwrite old Network events when the log is full. All logging will stop when the log is full and set to **NO**.

Network Log/Level

In order to log events, they must be at or below this level. Range is **0** to **6**. The default is **3**.

Network Log/View

This menu displays the log list. The fields are as follows:

Date/Time	Date and time event occurred
Level	Level associated with this event (0-6)
Message	Text message for this event; if message is too long to fit on the line, another event appears below it continuing the message

Network Log/Clear

This clears the log when activated.

LAN/UTILITIES MENU

TRACER 2631 has utilities embedded in it to help in managing and testing the network and to facilitate router software upgrades. **Figure 3-14** shows the **UTILITIES** menu.

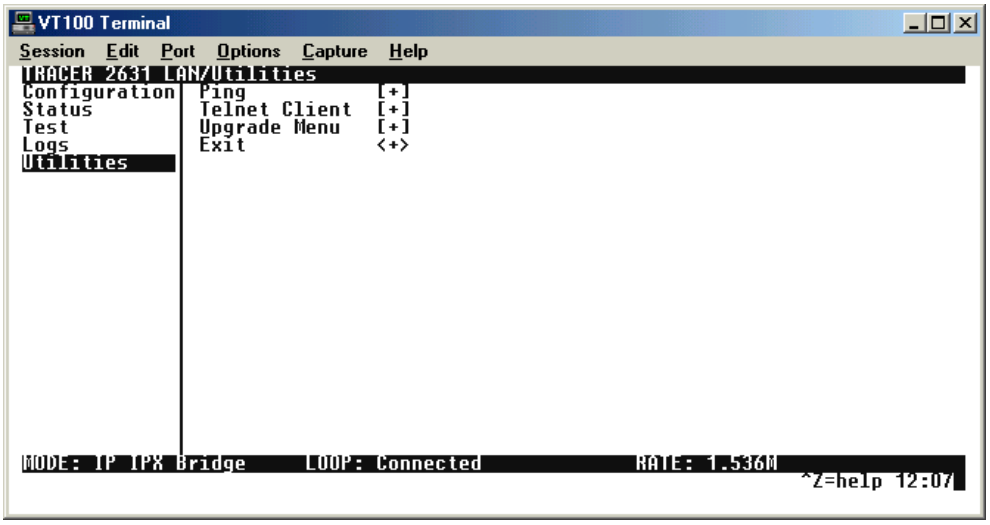

Figure 3-14. LAN/Utilities Screen

Utilities/Ping

Write security: 4; Read security: 5

The ping menu is used to send ICMP ping messages to hosts. The following items are under this menu:

Start/Stop	Activator to start and cancel a ping test
Host Address	IP address or domain name (if DNS is configured) of device to receive the ping
Size	Total size of ping to send; Range is 40 (default) to 1500 bytes.
# of Packets	Total packets to send every two seconds
# of Transmits	Total packets sent (read only)
# of Receives	Total packets received (read only)
% Loss	Percentage loss based on pings returned from host (read only)

Utilities/Telnet Client

Write security: 4; Read security: 5

The **TELNET** menu can be used to activate the Telnet client function in TRACER 2631.

Host	IP address or domain name (if DNS is configured) of Telnet server. By default, the standard TCP server port is used. However, a nonstandard port can be specified here with the IP address or domain name separated by a colon (:).

Activate	Starts Telnet client function. The key combination **Control]** cancels the session.

Utilities/Upgrade Menu

Write security: 2; Read security: 3

The TRACER 2631 router firmware can be upgraded using this menu.

N O T E

Only router functionality is capable of being upgraded by flash download.

Upgrade/Transfer Method

The two methods for upgrading are **TFTP** and **XMODEM**. **TFTP** requires a TFTP server running somewhere on the network. TRACER 2631 starts a TFTP client function which gets the upgrade code from the TFTP server. Selecting **XMODEM** will load the upgrade code through the maintenance port using any PC terminal emulator with xmodem capability.

Upgrade/TFTP Host

This is required when the transfer method is TFTP. It is the IP address or domain name (if DNS is configured) of the TFTP server.

Upgrade/Filename

This is required when the transfer method is TFTP. It is the case-sensitive file name which is the upgrade code.

Upgrade/Status

This appears when TFTP is used. It displays the status of the transfer as it happens. Any error or success message will be displayed here.

Upgrade/Start Transfer

This activator is used when the configurable items in this menu are complete.

N O T E

Once started, TRACER 2631 will prompt for erasing the flash. When the flash is erased and the upgrade transfer fails, do not turn off the unit. Retry the transfer until successful. Otherwise, if power is removed before upgrade has finished, the upgrade will have to occur from the maintenance port using XMODEM. If this happens, set a PC terminal emulation program to 9600 baud and attach to TRACER 2631's RS-232 port. Press **Enter** to display a simple terminal menu for upgrading. This menu appears when the flash code has been erased or is corrupt. The menu will also appear if power is applied with the rear panel DIP switch position 1 in the up (on) position.

Upgrade/Abort Transfer

Use this activator to cancel any TFTP transfer in progress.

Upgrade/TFTP Server

Setting this to **YES** allows another TRACER 2631 to upgrade its router code using TFTP client. This turns on the TRACER 2631 TFTP server function and allows its router code to be "cloned." Setting to **NO** (default) will deny any request from TFTP clients.

Utilities/Exit

Write security: 5; Read security: 5

Activating this feature will exit the terminal session from the maintenance port or Telnet. It is equivalent to the key combination **Ctrl-L**.

NAVIGATING THE WAN MENUS

The following sections provide information on how to navigate through the WAN menu set.

General Layout

TRACER 2631 **WAN SYSTEM STATUS** is the root level WAN menu, and contains real-time information on the status of the wireless WAN link. This menu is illustrated in **Figure 3-15** on page 86. All other WAN menus are similar in layout to this menu.

Menu Path

The top line of the display shows the current WAN menu.

Keyboard Navigation

Entering the WAN Main Menu

From the **WAN SYSTEM STATUS** menu, press **W** to enter the **WAN MAIN MENU**. This menu may also be entered by pressing **M** (for **M**ain menu).

Returning to the LAN Menu Set

From the **WAN SYSTEM STATUS** menu, press **L** to return to the LAN menu set. This may also be accomplished by pressing **R** (for **R**outer menu). When returning to the LAN menu set, the cursor is placed back in the **LAN/CONFIGURATION/WAN/CONFIGURE WAN & T1** menu.

I M P O R T A N T

The **WAN SYSTEM STATUS** menu is the only menu that can be used to return to the LAN menu set.

Navigation Summary

The **Enter** key, arrow keys, spacebar, **Tab**, and various single letter shortcuts are used to navigate the WAN menu system. These keystrokes are summarized as follows:

Arrow Keys	Selects items and moves between options.
Enter	Selects an item or writes changes to an item.
Tab	Moves between options, same as up and down arrows.
Spacebar	Selects items and toggles through options on selected items.
Ctrl-R	Redraws the entire menu.
L	Return to the LAN menu set (same as **R**). Only available from the **WAN MAIN MENU**.
M	Return to the **WAN MAIN MENU** from any other WAN menu (same as **W**).
N	View the next set of 15 minute increment history data in any of the **WAN HISTORY** menus.

R	Return to the LAN menu set (same as **L**). Only available from the WAN Main Menu.
W	Return to the **WAN MAIN MENU** from any other WAN menu (same as **M**).

WAN SYSTEM STATUS MENU

The menu shown in **Figure 3-15** displays the status of the WAN system components, including the wireless link, the T1 interface, and the router link. System status for both sides of the link is displayed. This is a status screen only; no configuration can be performed from this menu.

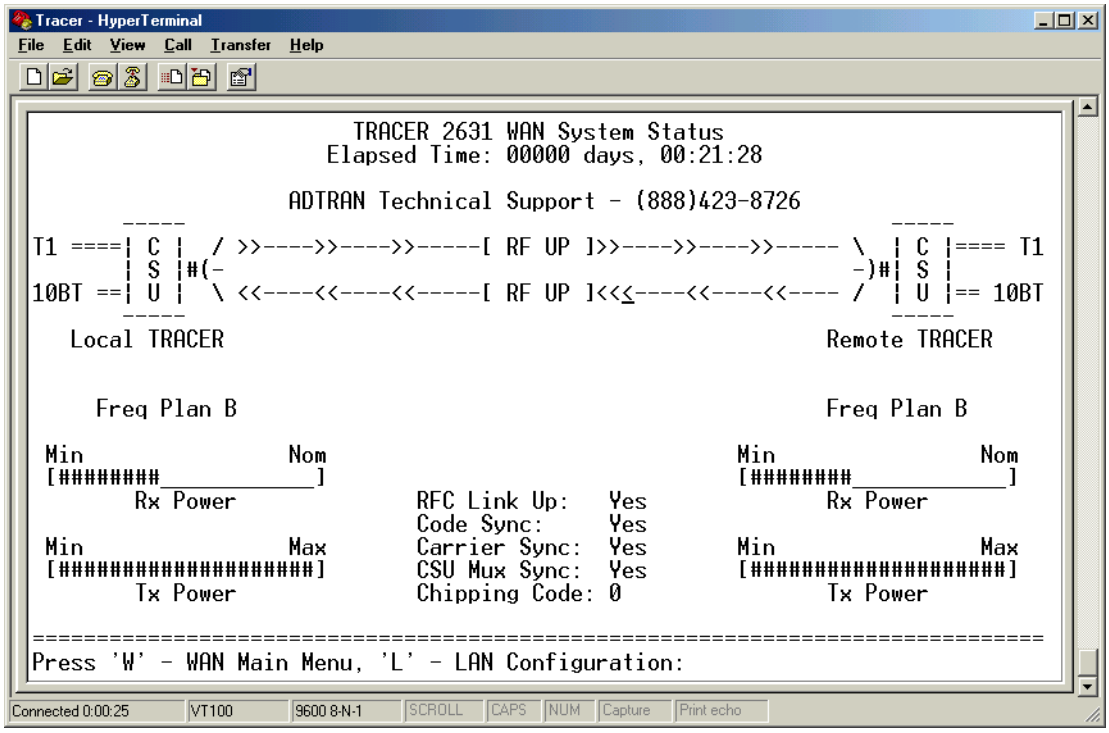

Figure 3-15. WAN System Status Screen

To enter the **WAN MAIN MENU**, press **W**. To return to the LAN menu set (**LAN/CONFIGURATION/WAN/ CONFIGURE WAN & T1)**, press **L**. The **WAN SYSTEM STATUS MENU** is the only menu that can be used to return to the LAN menu set.

The upper portion of the screen indicates how long the system has been running since the last reset operation. The **T1** and/or **10BT** labels will be highlighted if any error conditions exist on either of those interfaces.

The status of the wireless link is indicated as **RF UP** or **RF DOWN**. The left portion of the screen reports the status of the local system (the system to which the terminal is attached). The right portion of the screen reports the status of the remote system. During **RF DOWN** situations, remote status cannot be obtained. The approximate transmitter and receiver signal levels are shown via the “fuel gauges” on the left and right sides of the screen. The **CODE SYNC**, **CARRIER SYNC**, and **T1 MUX SYNC** will all be **YES** for an operational link. **RFC LINK UP** indicates that the baseband processor is communicating properly with the RF converter. **CHIPPING CODE** indicates the code to which the system is set.

If the **RFC LINK**, **CODE SYNC**, **CARRIER SYNC**, or **CSU MUX SYNC** is not **UP**, various portions of the spread spectrum data pump are not operating. Any of these conditions being **DOWN** will cause a major alarm to be activated at the alarm contacts.

WAN MAIN MENU

Pressing **W** while in any of the WAN menus will take the user to the **WAN MAIN MENU** (shown in **Figure 3-16**), from which all other WAN menus are accessed.

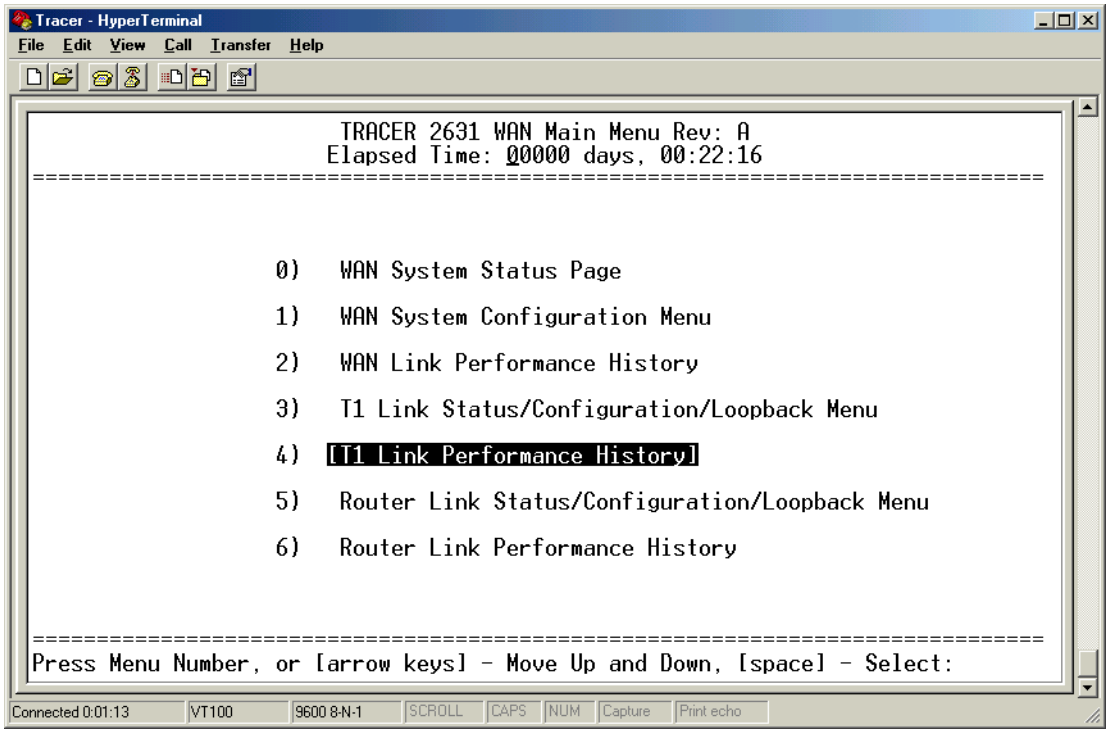

Figure 3-16. WAN Main Menu

To return to the **WAN SYSTEM STATUS PAGE**, press 0 from this menu or use the arrow keys to move to option 0, and then press **Enter**. This is the only way to return to the **WAN SYSTEM STATUS PAGE.**

WAN SYSTEM CONFIGURATION MENU

Pressing 1 from the **WAN MAIN MENU** or using the arrow keys to move to option 1 and then pressing enter will select the **WAN SYSTEM CONFIGURATION MENU**.

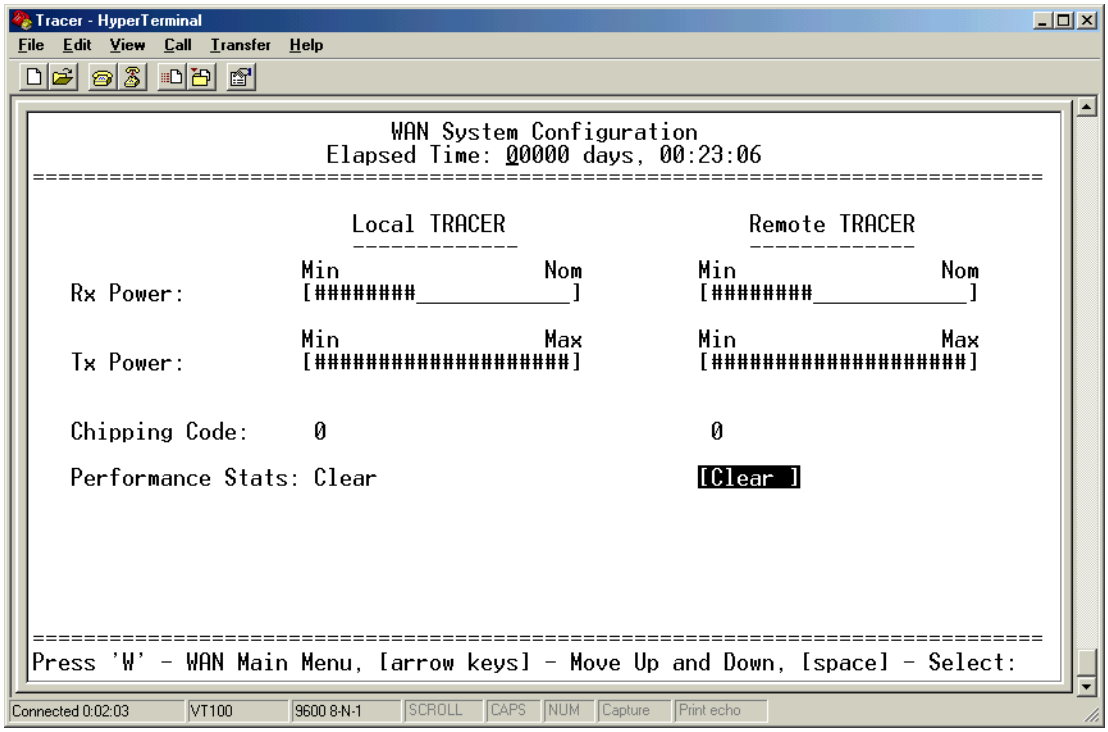

Figure 3-17. WAN System Configuration

The upper potion of this screen shows transmit and receive power on both ends of the TRACER 2631 link. Local and remote transmit power levels can be adjusted from this menu, while the receive power levels are a function of the link characteristics and cannot be changed.

Chipping code can also be set for either end from this menu. *Each end of the link must be configured for the same chipping code.*

I M P O R T A N T

If the remote end chipping code is accidentally changed from this menu, the link will be lost. If the new chipping code is unknown, step the local end of the link through all the other chipping codes until the link is re-established.

To clear all performance statistics on either end of the link, scroll down to the **CLEAR** activator and press **Enter** twice. This clears all 24 hour and 15 minute registers in the **WAN LINK PERFORMANCE HISTORY, T1 LINK PERFORMANCE HISTORY,** and **ROUTER LINK PERFORMANCE HISTORY** menus. To return to the **WAN MAIN MENU**, press **W.**

WAN LINK PERFORMANCE HISTORY MENU

Pressing 2 from the **WAN MAIN MENU** or using the arrow keys to move to option 2 and then pressing enter will select the **WAN LINK PERFORMANCE HISTORY MENU.**

The screen in **Figure 3-18** presents detailed error statistics for the RF link. The data is presented as **RFC** (Radio Frequency Converter) and **LNK** (RF Link) errors, representing seconds out of service for each. **RFC** represents the communications channel between the BBP and the RF converter that runs via the IF interconnect cable. **LNK** represents errored seconds received on the wireless link and is generally an indication of path or interference problems. The counts for the most recent 24 hours are recorded in 15-minute increments. Twenty-four hour totals are recorded for the most recent days. To view the next eight hours (32 15-minute intervals) of performance history, press **N.** To view the previous eight hours, press **P.** This information is available for both ends of the link. To return to the **WAN MAIN MENU**, press **W.**

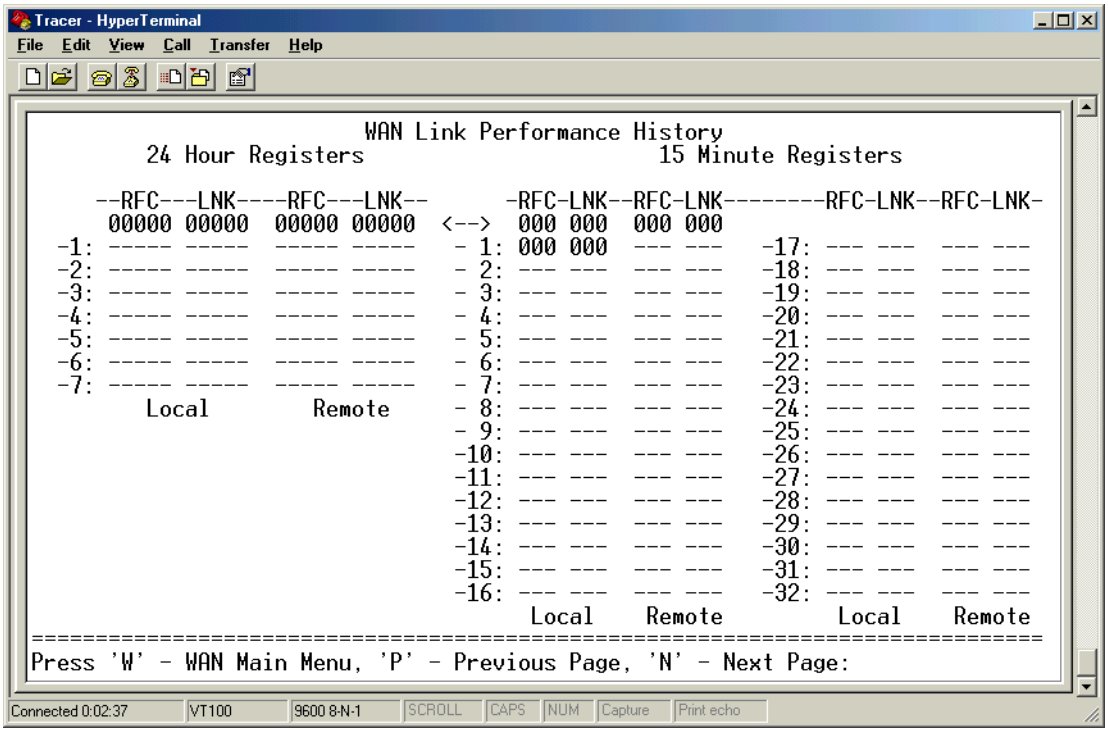

Figure 3-18. WAN Link Performance History

T1 LINK STATUS/CONFIGURATION/LOOPBACK MENU

Pressing 3 from the **WAN MAIN MENU** or using the arrow keys to move to option 3 and then pressing enter will select the **T1 LINK STATUS/CONFIGURATION/LOOPBACK MENU.**

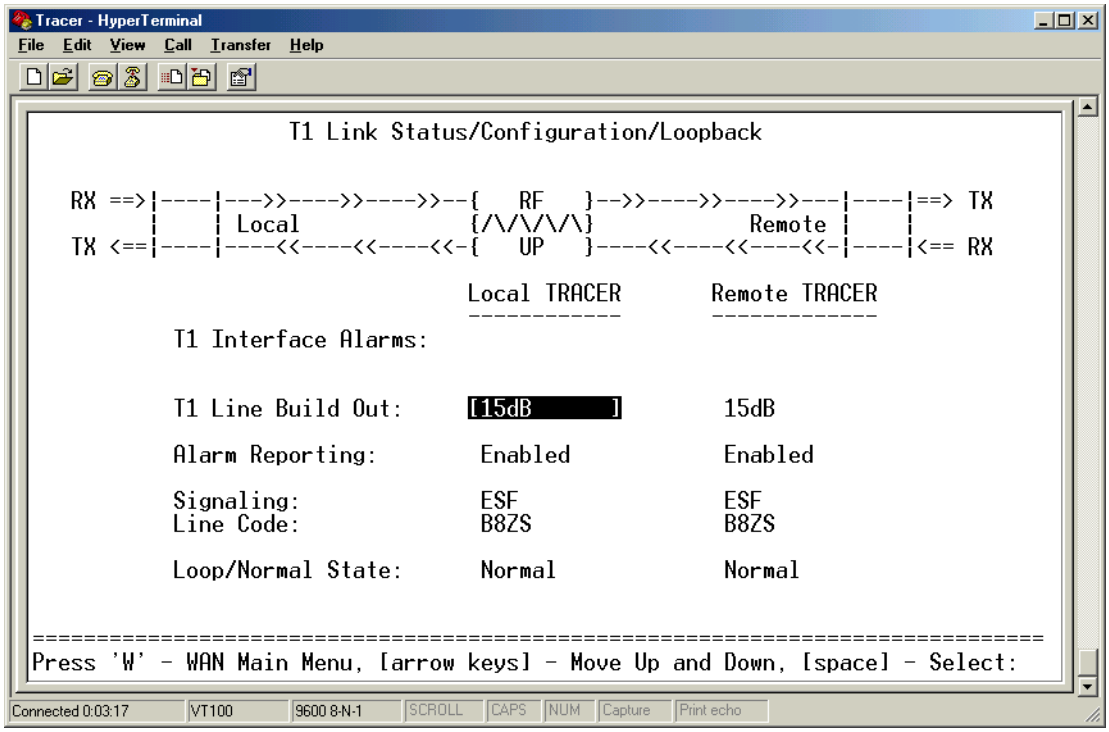

Figure 3-19. T1 Link Status/Configuration/Loopback

The upper portion of this screen shows a real time representation of the T1 link.

Any active T1 alarms will be displayed for both ends of the link immediately below the link status, if both ends of the link have alarm reporting enabled. These alarms include Red, Blue, Yellow, AIS, and bipolar violations (BPV). See Section 4, *Troubleshooting*, for further information on these alarms. If any of the T1 alarms are active on the local side, a minor alarm will be indicated at the alarm contacts.

T1 LBO allows the T1 interface to be configured for the appropriate line buildout, based on the distance to the T1 equipment.

ALARM REPORTING can be enabled or disabled at either end. If alarm reporting is disabled, no alarms will be registered on this page. Each end of the link operates independently with regard to alarm reporting. Therefore, it is possible to have alarms enabled on the remote side and disabled locally, or vice-versa.

SIGNALING allows the T1 interface to be configured for either **D4** or **ESF** framing.

LINE CODE allows the T1 interface to be set to either **AMI** or **B8ZS**.

LOOP/NORMAL STATE controls the loop status of the T1 link. Supported loopbacks include:

Link	The local unit is looped at the T1 framer so that data is looped back to the far end.

Line	The local unit is looped at the T1 interface so that data is looped back locally to the device attached to the T1 port.
Normal	No loopback present.

Configuration and loopback parameters on both sides of the link can be modified from this menu. To return to the **WAN MAIN MENU**, press **W**.

T1 LINK PERFORMANCE HISTORY MENU

Pressing 4 from the **WAN MAIN MENU** or using the arrow keys to move to option 4 and then pressing enter will select the **T1 LINK PERFORMANCE HISTORY MENU.**

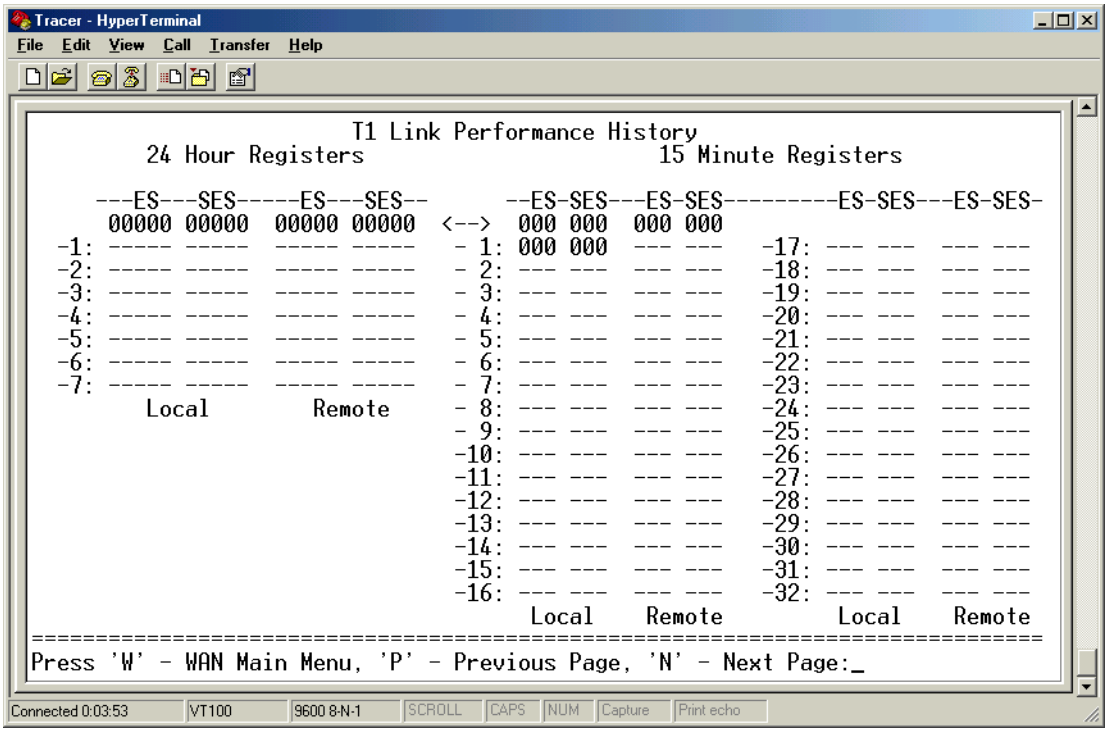

Figure 3-20. T1 Link Performance History

This screen presents detailed error statistics for the T1 interface. The data is presented as Errored Seconds (ES) and Severely Errored Seconds (SES). The counts for the most recent 24 hours are recorded in 15-minute increments. Twenty-four hour totals are recorded for the most recent days. To view the next eight hours (32 15-minute intervals) of performance history, press **N**. To view the previous eight hours, press **P.** This information is available for both ends of the link.

ROUTER LINK STATUS/CONFIGURATION/LOOPBACK MENU

Pressing 5 from the **WAN MAIN MENU** or using the arrow keys to move to option 5 and then pressing enter will select the **ROUTER LINK STATUS/CONFIGURATION/LOOPBACK MENU.**

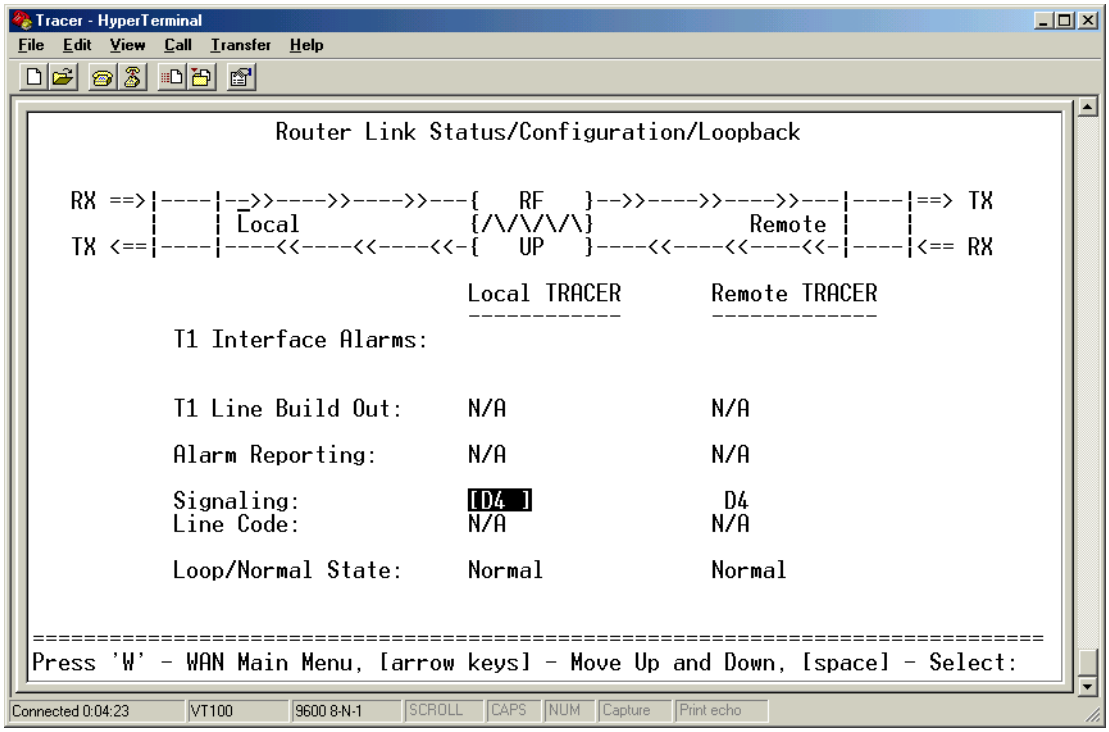

Figure 3-21. Router Link Status/Configuration/Loopback

The upper portion of this screen shows a real time representation of the router link.

If a TRACER 4103 or 4203 is present at the remote end instead of a TRACER 2631, any active T1 alarms will be displayed for the remote end of the link immediately below the link status, if the remote TRACER has alarm reporting enabled. If a TRACER 2631 is present at the remote end, there will be no T1 alarms displayed, since there is no T1 interface involved. See the troubleshooting chapter for further information on T1 alarms.

The following options are not applicable to the TRACER 2631, but have been included among the menu options so that if a TRACER 4103 or 4203 is used on the remote end, configuration of that unit will still be possible:

T1 LINE BUILD OUT
ALARM REPORTING
LINE CODE
LOOP/NORMAL STATE

These options cannot be highlighted to be changed on a TRACER 2631 unit, and will be displayed as **N/A** or **NORMAL**.

SIGNALING allows the Router interface to be configured for either **D4** or **ESF** framing.

Configuration and loopback parameters on both sides of the link can be modified from this menu. To return to the **WAN MAIN MENU**, press **W**.

ROUTER LINK PERFORMANCE HISTORY MENU

Pressing 6 from the **WAN MAIN MENU** or using the arrow keys to move to option 6 and then pressing enter will select the **ROUTER LINK PERFORMANCE HISTORY MENU**.

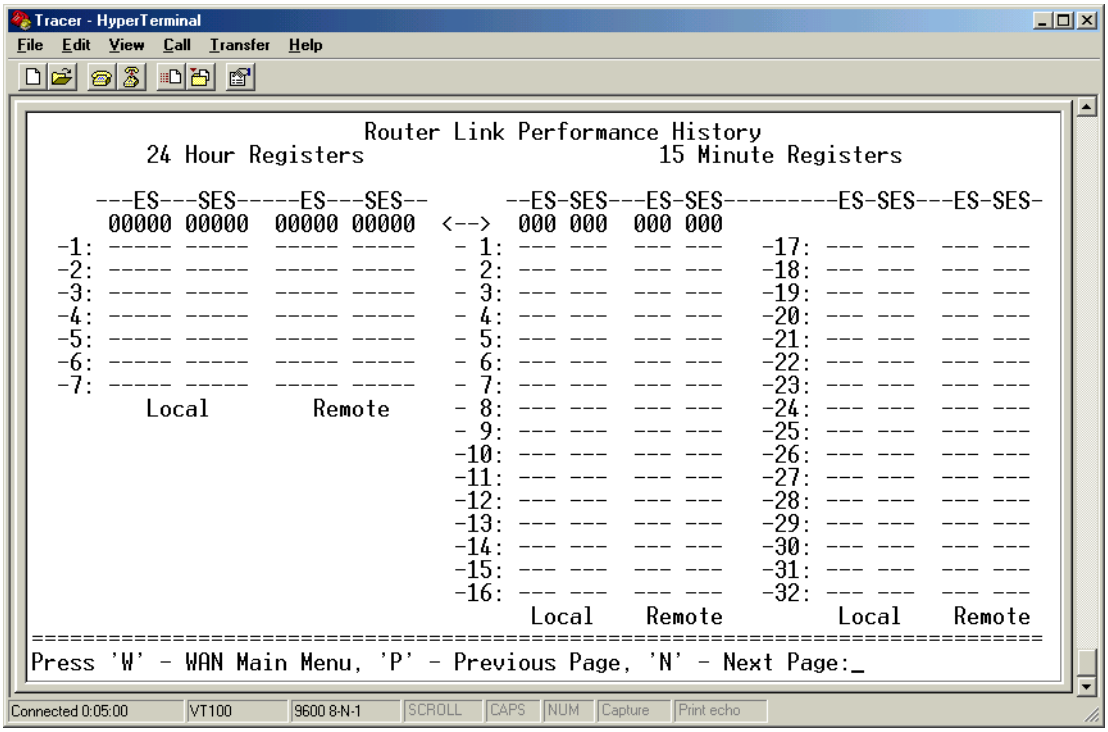

Figure 3-22. Router Link Performance History

This menu is not applicable to the TRACER 2631, but has been included among the menu options so that if a TRACER 4103 or 4203 is used on the remote end, performance history monitoring of that unit will still be possible. If the remote TRACER is a 4103 or 4203 configuration, this menu will display T1 error information from the remote end. Otherwise, this menu will always read no errors, since there is no T1 interface involved. To view the next eight hours (32 15-minute intervals) of performance history, press **N**. To view the previous eight hours, press **P.** This information is available for both ends of the link. To return to the **WAN MAIN MENU**, press **W**.

I M P O R T A N T

If problems persist after you have followed the Recommended Actions, contact ADTRAN Technical Support at (888) 423-8726.

Power LED is not Lit

If the Power LED is not lit, it is an indicator that the BBP is not receiving adequate DC power.

Recommended Actions:

1. Verify that the power source is delivering between and 21-60 VDC.
2. Check the polarity of the power connection by verifying that DC voltage ground is properly connected.

Test LED is Blinking or on (Solid)

The Test LED will remain **ON** (solid) during power-up, indicating a self-test is in progress. If the Test LED is blinking or remains **ON** (solid) after ten seconds, the TRACER 2631 has failed self-test. This is an internal failure, and ADTRAN technical support should be contacted.

Link Down LED is Lit (the RF Link is Down)

Recommended Actions:

1. Check the BBP to RF converter coaxial cable connection.
2. Check the RF converter to antenna coaxial cable connection.
3. Measure the RSSI voltage. If the signal is good ($\geq$ 2.0 VDC at BBP RSSI Test Point), go to step 8.
4. Verify that the RF converter on one end of the link is configured as Plan A and the other end is configured as Plan B.
5. Check the fuse on the IF board. This fuse is accessed by removing the top of the BBP, and is located on the left side of the chassis when facing the front panel. If this fuse is open, verify that the connector labeled **IF** on the rear panel of the BBP is connected via coax to the connector labeled **IF** on the RF converter. Check the BBP to RF converter coaxial cable for a short, and verify that any lightning arrestors installed in the coax line between the BBP and RFC are specified to pass DC voltage. Replace the fuse with a 1 amp, 250 volt slo-blow type fuse.
6. Verify that the antenna polarization is the same at both ends of the RF signal transmit and receive path.
7. Verify that the RF signal path is clear.
8. Verify same PN code on both ends of the RF signal path.
9. Check for possible interference at both ends of the link. If necessary, change polarization and/or code at both ends.

I M P O R T A N T

If problems persist after you have followed the Recommended Actions, contact ADTRAN Technical Support at (888) 423-8726.

RF Low LED is Lit

This indicates that the received signal is within approximately 10 dB of the minimum operable signal. This condition is typically indicative of a path problem.

Recommended actions:

1. Verify the far-end transmitter power setting is the value that the link planning budget allows.
2. Check all coaxial cable connectors for solid connections. Check for water and corrosion around any of the connectors.
3. Verify the RF signal path by verifying the antenna alignment.
4. Check integrity of the cable plant.
5. Verify lightning arresters will pass DC.

LOS LED is Lit (Red Alarm)

A Red Alarm (loss of signal) is generated at the TRACER 2631 T1 interface when the interface cannot sync up to the T1 framing information. This error may be due to a degraded signal or no signal, or it may be caused by improper framing.

Recommended actions:

1. Verify that the T1 cable is connected to the T1 interface on the TRACER 2631.
2. If the RJ-45 connection is used, verify that the connector is wired correctly. If the Bantam jacks are used, verify that they are inserted into the correct sockets.
3. Verify the connections at opposite ends of the T1 cable.
4. Verify that the framing mode (ESF or D4) is on the same setting for both the TRACER 2631 and the connected equipment.

AIS LED is Lit (Yellow Alarm)

A Yellow Alarm, when indicated at TRACER 2631, is generated by the attached equipment. When the attached equipment's T1 interface is in Red Alarm, a Yellow Alarm will be generated at the TRACER 2631 unit.

Recommended Action:

1. Follow the troubleshooting steps for Red Alarm, but do so at the attached equipment.

AIS LED is Blinking (Alarm Indication Signal or Blue Alarm)

A Blue Alarm (also called AIS, Keep Alive, and All-ones), when indicated at TRACER 2631, is generated by the attached equipment. The root cause must be determined at the attached equipment. A typical cause of a Blue Alarm is a lack of input to a CSU.

Recommended Actions:

1. Verify the input to any attached data equipment.

I M P O R T A N T

If problems persist after you have followed the Recommended Actions, contact ADTRAN Technical Support at (888) 423-8726.

BPV LED is Lit (Bipolar Violations)

This alarm will activate when the incoming T1 stream presents Bipolar Violations (BPVs). BPVs indicate an improper configuration or a faulty cable plant.

Recommended Actions:

1. Verify that the TRACER 2631 unit and the attached equipment are configured for the same line coding (AMI or B8ZS).
2. Verify that the line build-out (LBO) of the attached equipment is correct.
3. Inspect the cable plant for split pairs. A split pair is a condition in which the T1 interface is incorrectly wired into the cable plant. Each interface direction, transmit and receive, is carried on two signals – tip and ring. Normally, tip and ring for the transmit signal comprise the two wires for a single twisted pair in the bundle. It is not uncommon for one connection from the transmit interface and one connection from the receive interface to comprise another twisted pair. This condition is referred to as a split pair and can cause signal degradation.

This section lists the specifications for TRACER 2631 system.

Transmitter

Output Power ..... +20 dBm, max
(5.8 GHz, standard 2.4 GHz option)
+30 dBm, max
(2.4 GHz 1 watt option - factory setting is +27 dBm)
Frequency Range ..... 2400 to 2483.5 MHz, or 5725 to 5850 MHz
Channel Bandwidth ..... 40 MHz
Intermediate Frequency ..... 140 MHz

Receiver

Receive Level, range ..... -30 to -91 dBm (2.4 GHz)
-30 to -89 dBm (5.8 GHz)
Receive Level, maximum ..... -30 dBm
Receive Level, nominal ..... -60 dBm
Intermediate Frequency ..... 70 MHz

Frequency Plan

Plan A 2.4 GHz ..... TX 2.422 GHz, RX 2.462 GHz
Plan B 2.4 GHz ..... TX 2.462 GHz, RX 2.422 GHz
Plan A 5.8 GHz ..... TX 5.747 GHz, RX 5.827 GHz
Plan B 5.8 GHz ..... TX 5.827 GHz, RX 5.747 GHz

Spread Spectrum Data Pump

Modulation ..... QPSK
Spreading Method ..... Direct sequence
Code Length ..... 120 bits
Processing Gain ..... >12 dB
Number of Codes 10
Chipping Rate ..... 12 times

T1 Interface Specifications

Connection ..... RJ-48C, bantam
Line Code ..... AMI, B8ZS
Framing ..... SF, ESF
Alarms ..... AIS, Red, Yellow, BPVs
Loopbacks ..... Local and remote

LAN Interface Specifications

Connection Ethernet/IEEE802.3 10BaseT (RJ-45)

User Interface

Front Panel ..... Alarm LEDs, Configuration Switch, Test Points
Diagnostics ..... T1 and Router Loopbacks
Test Points ..... RSSI, QPSK Constellation
VT-100 Terminal ..... Menu-Driven User Interface, Control of the Remote End Wireless Link, Password Protected (Optional), Event History

VT-100 Terminal Interface

Data Rate ..... 9600 bps
Data Bits 8
Parity ..... None
Stop Bits 1
Terminal Emulation VT-100

Mechanical & Environmental

Baseband Processor

Operating Temperature ..... -25 to 65 °C
Size ..... 19" x 1.75" x 10.5"
Humidity ..... 95%, Non-condensing
Weight ..... 6 lbs.

Rack RF Converter

Operating Temperature ..... -40 to 65 °C
Size ..... 19" x 1.75" x 11.5"
Humidity ..... 95%, Non-condensing
Weight ..... 6 lbs.

Mast Unit

Operating Temperature ..... -40 to 65 °C
Size ..... 21" high x 9" diameter
Humidity 100%
Weight ..... 18 lbs.

Power

Input Voltage ..... 21 to 60 volts DC, either polarity referenced to ground
Power Consumption ..... 30 watts
Connector ..... 3 pin DIN (AC adapter), 3 pin screw clamp terminal block (DC)
Fuse ..... 1 amp, 250 volt slo-blow

WARRANTY

ADTRAN will replace or repair this product within five years from the date of shipment if it does not meet its published specifications or fails due to defects in materials and workmanship.

For detailed warranty, repair, and return information, refer to the ADTRAN Equipment Warranty, Repair, and Return Policy and Procedure located on the ADTRAN web site at http://www.adtran.com.

SALES

For TRACER 2631 sales information, contact Adtran Sales at:

(888) 3ADTRAN or http://www.adtranwirelesss.com

TECHNICAL SUPPORT

Standard support hours are 7 a.m. to 7 p.m. CST, Monday through Friday. Emergency technical support is available 24 hours a day, seven days a week.

For technical support at any time, contact ADTRAN at:

(888) 423-8726

REPAIRS AND RETURNS

Return Material Authorization (RMA) is required prior to returning equipment to ADTRAN.

For RMA information, contact ADTRAN at:

(800) 726-8663

or ADTRAN, Inc.
Customer Service Department
P.O. Box 140000 / 901 Explorer Boulevard
Huntsville, Alabama 35814-4000

When returning faulty equipment, please include the RMA number on the shipping label.

The cable connections required for various configurations are detailed below.

Terminal Connection (DB25)

TRACER 2631 (DCE)			Terminal (DTE)	
Number	**Name**		**Number**	**Name**
2	TXD	⟷	2	TXD
3	RXD	⟷	3	RXD
4	RTS	⟷	4	RTS
5	CTS	⟷	5	CTS
6	DSR	⟷	6	DSR
7	Ground	⟷	7	Ground

Personal Computer Connection (DB9)

TRACER 2631 (DCE)			Computer (DTE)	
Number	**Name**		**Number**	**Name**
2	TXD	⟷	3	TXD
3	RXD	⟷	2	RXD
4	RTS	⟷	7	RTS
5	CTS	⟷	8	CTS
6	DSR	⟷	6	DSR
7	Ground	⟷	5	Ground

		Rear Panel Switch Position	
		TO NIC	TO HUB
	Pin 1	TX1	RX1
	Pin 2	TX2	RX2
	Pin 3	RX1	TX1
	Pin 6	RX2	TX2

N O T E

The switch position can be set for either **TO NIC** or **TO HUB** on the back panel of the TRACER 2631. The rear panel is illustrated in **Figure 1-4** on page 5.

TRACER 2631 displays current loop status of the wireless link on the highlighted status line at the bottom of the LAN menus. The following messages are defined:

Connected
This is seen when the TRACER 2631 wireless link is established and layer 1 protocols are successfully negotiated.

Echo: TX: X RX: Y
The current transmit and receive count for the PPP echo request test.

Layer 1 up
The TRACER 2631 WAN layer 1 is up.

Link Down
The wireless link is not synchronized.

Link In Sync
The wireless link is synchronized but layer 1 is not up.

The TRACER 2631 **LOGS** menu contains messages of events that occur. The definitions for some of those log messages are as follows:

PPP Log Messages

BCP <X> down
Level 5
Bridge Control Protocol port <X> has been dropped between TRACER 2631 and PPP peer.

BCP <X> up
Level 5
Bridge Control Protocol port <X> has been successfully negotiated between TRACER 2631 and PPP peer.

CCP <X> down
Level 5
Compression Control Protocol port <X> has been dropped between TRACER 2631 and PPP peer.

CCP <X> up
Level 5
Compression Control Protocol port <X> has been successfully negotiated between TRACER 2631 and PPP peer.

CHAP authen failed
Level 3
The PPP peer has rejected the TRACER 2631's username and/or password used for authenticating. Check to make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **TX METHOD**, **TX USERNAME**, and **TX PASSWORD** are correct.

EAP authen failed
Level 3
The PPP peer has rejected the TRACER 2631's username and/or password used for authenticating. Check to make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **TX METHOD**, **TX USERNAME**, and **TX PASSWORD** are correct.

IPCP <X> down
Level 5
IP Control Protocol port <X> has been dropped between TRACER 2631 and PPP peer.

IPCP <X> up
Level 5
IP Control Protocol port <X> has been successfully negotiated between TRACER 2631 and PPP peer.

IPXCP <X> down
Level 5
IPX Control Protocol port <X> has been dropped between TRACER 2631 and PPP peer.

IPXCP <X> up
Level 5
IPX Control Protocol port <X> has been successfully negotiated between TRACER 2631 and PPP peer.

LCP <X> down
Level 5
Link Control Protocol port <X> has been dropped between TRACER 2631 and PPP peer.

LCP <X> up
Level 5
Link Control Protocol port <X> has been successfully negotiated between TRACER 2631 and PPP peer.

Link is looped back
Level 3
The TRACER 2631 has encountered a location which is looping back all data. Essentially, the unit has negotiated PPP with itself.

Negot not converging
Level 2
Negotiation of the LCP layer is unattainable due to misconfiguration or the TRACER 2631 or PPP peer is requiring authentication and the other end is refusing.

No IP addr for peer
Level 2
The TRACER 2631 cannot continue the connection because there was no IP address received from the PPP peer or it was not set in **LAN/CONFIGURATION/CONNECTION LIST/IP/ROUTE/IP/NET** parameter.

No Response from peer
Level 2
The TRACER 2631 has not seen any PPP negotiation packets.

PAP authen failed
Level 3
The PPP peer has rejected the TRACER 2631's username and/or password used for authenticating. Check to make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **TX METHOD**, **TX USERNAME**, and **TX PASSWORD** are correct.

Peer failed CHAP authen
Level 3
The PPP peer's reported CHAP username and/or password does not match the TRACER 2631's parameters. This is most likely caused by PPP peer sending an incorrect username and/or password. Make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **RX USERNAME** and **RX PASSWORD** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer failed EAP authen
Level 3
The PPP peer's reported EAP username and/or password does not match the TRACER 2631's parameters. This is most likely caused by PPP peer sending incorrect username and/or password. Make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **RX USERNAME** and **RX PASSWORD** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer failed PAP authen
Level 3
The PPP peer's reported PAP username and/or password does not match the TRACER 2631's parameters. This is most likely caused by PPP peer sending incorrect username and/or password. Make sure the **LAN/CONFIGURATION/CONNECTION LIST/AUTHENTICATION** parameters **RX USERNAME** and **RX PASSWORD** are correctly entered. Also, if using RADIUS, check that the server is configured and running properly.

Peer refused authen
Level 3
The PPP peer would not allow the TRACER 2631 to authenticate it using the method set in **LAN/CONFIGURATION/SECURITY/PPP**.

Peer refused SpanTree
Level 4
The PPP peer would not participate in the Spanning Tree protocol. This is a warning message only. Bridging will still occur across the WAN port so care must be taken that no loop topologies exist across the connection.

PPPtx[x] …
Level 6
Advance debugging decode of transmitted PPP configuration packets.

PPPrx[x] …
Level 6
Advanced debugging decode of received PPP configuration packets.

Call Log Messages

Power Up - last down cause: <reason>
Level 0 (displayed as Level 1 after the unit is reset)
This is the <reason> for the last reset. Most are caused by internal errors. Possible reasons are:

Bus Error - Bad address occurred on the internal bus

Kernel error - General operating system error

No SBCs - Mail resources used up or lost

Router stack error - Fatal error in protocol stack

general panic - general error
no rip - rip tasks could not start
out of memory - out of available memory
out of TCP ports - all TCP ports are used up
unknown error - unknown fatal error has occurred

Set timer error - Cannot set real-time clock

Software Watch Dog Reset - Software watchdog was not updated

Network Log Messages

Attempting to add bad IP iface route: ifnum=<inter> dest=<ip>
Level 4
An IP address <ip> could not be used for the interface number <inter>.

DHCP couldn't alloc mem
Level 1
A DHCP response could not be generated due to memory allocation problems.

DHCP response sent
Level 4
A DHCP response was successfully sent to requesting device.

DHCP socket failed
Level 1
Internal error occurred when attempting to start DHCP server.

DHCP: Host not added to ARP table
Level 2
The DHCP server could not add requesting host to ARP table.

Installing bad default route: ifnum=<inter> metric=<hops> gw=<ip>
Level 6
The TRACER 2631 did not install a default route because the <inter> or <hops> was zero.

Rejecting packet with Source Routing option - src=<srcip> dest=<destip>
Level 4
The TRACER 2631 has dropped a source routed IP packet due to invalid parameters.

setmask: local IP iface(0), not done
Level 6
Debug error used in determining router stack problems.

syslog: bad host
Level 2
Syslog function cannot use host name or IP set in **LAN/CONFIGURATION/LOGS/SYSLOG HOST**.

syslog: no port
Level 2
Syslog function cannot open port to send Log entries.

TEL: Telnet Session Closed
Level 4
Telnet server session has been closed.

telclient bad host
Level 2
Telnet client could not use host name or IP address set in **LAN/CONFIGURATION/UTILITIES/TELNET CLIENT/HOST**.

telclient bad init
Level 2
Telnet client could not initialize a session.

Telnet Client: Clr TCBF_BUFFER flag failed
Level 6
Debugging message related to Telnet client function.

Telnet Client: Set TCBF_DONTBLOCK flag failed
Level 6
Debugging message related to Telnet client function.

Telnet Client socket failed
Level 2
Telnet client function could not open TCP socket.

Telnet server connect to <ip>
Level 4
Telnet server has connected to Telnet client with IP address <ip>.

Telnet Session Closed
Level 4
Telnet server has closed connection.

Telnet Session failed, error <errnum>
Level 2
Telnet server could not connect to Telnet client due to error.

TELNETD: accept failed
Level 2
Telnet server could not open TCP socket to incoming Telnet client.

TELNETD: Set TCPC_LISTENQ failed
Level 6
Debugging message related to Telnet server function.

TELNETD: Clr TCBF_BUFFER flag failed
Level 6
Debugging message related to Telnet client function.

TELNETD: could not obtain peer ip
Level 2
Telnet server function could not get IP address of Telnet client.

TELNETD: Session failed, error
Level 2
A Telnet server session has failed because of an error.

TELNETD: Set TCBF_DONTBLOCK flag failed
Level 6
Debugging message related to Telnet client function.

TELNETD: SOCKET creation error
Level 2
Telnet server could not be started due to TCP socket error.

TFTP: can't get to host
Level 2
TFTP client could not get to host.

TFTP client: unable to open port
Level 2
TFTP client function could not open a UDP port.

TFTP: error rcvd - <message>"
Level 2
Received error with <message> from TFTP server.

TFTP: lost communication
Level 2
Lost communication to TFTP client or server during transfer.

TFTP server: unable to open port
Level 2
TFTP server function could not open a UDP port.

Understanding SNMP

As LAN environments became standardized over the past ten years, multi-vendor equipment grew with competition. It became necessary to manage the various vendor equipment from a single control console. Thus, SNMP emerged as the *de facto* standard for managing commercial Transmission Control Protocol/Internet Protocol (TCP/IP) networks.

The term *SNMP* broadly refers to the message protocols used to exchange information between the network and the managed devices, as well as to the structure of network management databases. SNMP has three basic components:

- **Network Manager:** This is a control program that collects, controls, and presents data pertinent to the operation of the network devices. It resides on a network management station.
- **Agent:** This is a control program that responds to queries and commands from the network manager and returns requested information or invokes configuration changes initiated by the manager. It resides in each network device connected.
- **MIB:** This is an index to the organized data within a network device. It defines the operating parameters that can be controlled or monitored.

When requesting the network manager to retrieve or modify a particular piece of information about a network device, the network manager transmits the request to that network device. The agent in that device interprets the incoming request, performs the requested task, and sends its response to the network manager. The network manager collects all the data from the various network devices and presents it in a consistent form.

Using SNMP Version 1, the network manager can issue three types of commands:

- **GetRequest**: This command retrieves a single item or the first in a series from a network device.
- **GetNextRequest**: This command retrieves the next item in a series from a network device.
- **SetRequest**: This command writes information to a network device.

The network device issues two types of messages:

- **GetResponse**: This message is the response to a network manager **GetRequest** or **GetNextRequest** command.
- **Trap**: This is an unsolicited message issued by a network device to report an operational anomaly or an alarm condition to the network manager.

These messages are typically encased within informational packets and transported over the LAN or WAN.

SNMP Embedded Agent

TRACER 2631 supports the following groups from MIB-II: (RFC 1213)

- System Group
- UDP Group

- Interfaces Group
- ICMP Group
- Address Translation Group
- IP Group
- TCP Group

Also, the Ethernet transmission MIB is supported (RFC 1643).

The following manager requests are supported:

- Get object
- Get next object
- Set object

Communities

TRACER 2631 permits up to eight communities to be defined. The privilege level of each community can be set. The default community is public with read-only privileges. When the IP address is all zeros, any manager of the community can access TRACER 2631.

Traps

Up to four hosts can be set to receive traps. Each host entry requires an IP address of the manager.

Trap types supported are: cold start, link up, link down, and authentication failure.

N O T E

Only the LAN parameters available from the LAN menu set can be accessed via SNMP. All WAN parameters must be accessed through the VT-100 port.

TRACER 2631 supports a command line interface for configuring LAN parameters. All LAN menu options are configurable and readable from the terminal mode. Additional commands are also available.

Menu Commands

Every menu item in the LAN menu structure can be accessed through the terminal mode interface. Terminal commands are as follows:

top_menu sub_menu1 sub_menu2 … config_item

Each config_item is entered as shown below.

Type	Entered As
string	printable characters within double quotes
password	printable characters within double quotes
IP address	xx.xx.xx.xx (0..9) separated by '.'
Hex	xx:xx:xx:xx (0..9,a..f) separated by ':'
enum	sub-string or [#index]
unsigned	digits (0..9)
date	mm-dd-yyyy
time	hh:mm:ss
date/time	mm-dd-yyyy hh:mm:ss
activator	read only
list	followed by index with first record being 1
array	followed by index with first record being 1

One of the following keywords must be used first:

info	Goes directly to **CONFIGURATION/SYSTEM INFO** menu
ip	Goes directly to **CONFIGURATION/IP** menu
ipx	Goes directly to **CONFIGURATION/IPX** menu
bridge	Goes directly to **CONFIGURATION/BRIDGE** menu
security	Goes directly to **CONFIGURATION/SECURITY** menu
ppp	Goes directly to **CONFIGURATION/PPP PROFILE** menu
telnet	Goes directly to **CONFIGURATION/MANAGEMENT/TELNET** menu
snmp	Goes directly to **CONFIGURATION/MANAGEMENT/SNMP** menu
maint	Goes directly to **CONFIGURATION/MANAGEMENT/MAINT** menu
status	Goes directly to **CONFIGURATION/STATUS** menu
test	Goes directly to **CONFIGURATION/TEST** menu
logs	Goes directly to **CONFIGURATION/LOGS** menu
util	Goes directly to **CONFIGURATION/UTILITIES** menu
frame	Goes directly to **CONFIGURATION/WAN/FRAME RELAY** menu

Some examples are listed below:

telnet user 1 name "guest"	Sets user name for Telnet user list entry 1 to "guest"
test 2047	Starts 2047 test
status ip 1 gateway	Returns the gateway address for IP route table entry 1

Additional Commands

Other commands available from the terminal mode are given below:

save	Saves the configuration to non-volatile RAM (flash).
mac	Returns the MAC address for the TRACER 2631
version	Returns the firmware version and routing stack version
reset	Resets the unit
exit	Leaves terminal mode and returns to menus
download	Downloads complete configuration to the terminal screen for capture

Download/Uploading Configuration

TRACER 2631's LAN configuration can be captured to a text file using the download command. The text file can be edited if required. Upload of the LAN configuration can be accomplished by sending the text file to the TRACER 2631 in terminal mode. As soon as the upload has been completed, type **save** to save the new configuration to flash. A **reset** command or power cycle 10 seconds after the save command is recommended to ensure that the new configuration is complete.

AMI ..... Alternate Mark Inversion
ARP ..... Address Resolution Protocol
B8ZS ..... Bipolar 8 Zero Substitution
BCP ..... Bridge Control Protocol
BER ..... Bit Error Rate
BERT ..... Bit Error Rate Test
BBP ..... Baseband Processor
BPDU ..... Bridging Protocol Data Unit
bps ..... Bits per second
Bps ..... Bytes per second
BPV ..... Bipolar Violations
CCITT ..... Consultative Committee for International Telegraphy and Telephony
CHAP ..... Challenge Handshake Protocol
CPE ..... Customer Premises Equipment
DCE ..... Data Communicaitons Equipment
DLCI ..... Data Link Connection Identifier
DSSS ..... Direct Sequence Spread Spectrum
DTE ..... Data Terminal Equipment
EAP ..... Extensible Authentication Protocol
ES ..... Errored Seconds
ESF ..... Extended Superframe
FCC ..... Federal Communications Commission
FEC ..... Forward Error Correction
FTP ..... File Transfer Protocol
IARP ..... Inverse Address Resolution Protocol
IETF ..... Internet Engineering Task Force
IF ..... Intermediate Frequency
IPX ..... Internetwork Packet Exchange
ISDN ..... Integrated Services Digital Network
ISM ..... Industrial, Scientific, and Medical
ISO ..... International Standardization Organization
ISP ..... Internet Service Provider
LAN ..... Local Area Network
LBK ..... Loopback
LBO ..... Line Buildout
MAC ..... Media Access Control
MPE ..... Maximum Permissible Exposure
NAT ..... Network Address Translation
NIC ..... Network Interface Card
PAP ..... Password Authentication Protocol
PPP ..... Point-to-Point Protocol
PCB ..... Printed Circuit Board
PVC ..... Permanent Virtual Circuit
RF ..... Radio Frequency
RFC ..... Request for Comments (as in RFC 1490) generated by the IETF
RFC ..... Radio Frequency Converter
RFCL ..... Radio Frequency Converter Link
RIP ..... Routing Information Packet, Routing Information Protocol

RSSI.....Received Signal Strength Indicator
RX.....Receive
SAP.....Service Advertising Protocol
SF.....Superframe
S/N.....Sound-to-Noise Ratio
SNMP.....Simple Network Management Protocol
SVC.....Switched Virtual Circuit
TCP/IP.....Transmission Control Protocol/Internet Protocol
TFTP.....Trivial File Transfer Protocol
TX.....Transmit
WAN.....Wide Area Network

10Base2

IEEE 802.3 specification, similar to Ethernet, using thin coaxial cable that runs at 10 Mbps, with a maximum distance of 185 meters per segment. Also known as Thin Ethernet or Thinwire Ethernet.

10BaseT

IEEE 802.3 specification, using unshielded twisted-pair cabling and running at 10 Mbps.

BOOTP

The Bootstrap Protocol allows a network node to determine certain startup information such as its IP address.

Bridge

A data communications device that connects two or more networks. A bridge stores and forwards complete packets between the networks. Bridges operate at the data-link layer of the OSI model.

CCITT

Consultative Committee on International Telephony and Telegraphy – A body of the International Telegraph Union (ITU) which prepares recommendations, commonly referred to as international standards, to resolve technical telegraph and telephone problems.

central office (CO)

In telephony, the phone company switching facility or center, usually a Class 5 end office, at which subscribers local loops terminate. Handles a specific geographic area, identified by the first three digits of the local telephone number. Usually the facilities of the local BOC.

CSMA/CD

Carrier Sense Multiple Access Collision Detect – A channel access mechanism where devices check the channel for a carrier before transmitting. If no carrier is sensed for the specified period of time, the device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays their retransmissions for a random length of time. CSMA/CD is used by Ethernet and IEEE 802.3.

D-channel

The ISDN channel that carriers signalling information to control the call setup, teardown, or invocation of supplementary services. The D-Channel may also be used to provide packet mode data service.

DDS

Dataphone Digital Service – AT&T private line service for transmitting data over a digital system. The digital transmission system transmits electrical signals directly, instead of translating the signals into tones of varied frequencies as with traditional analog transmission systems. Digital techniques provide more efficient use of transmission facilities, resulting in lower error rates and costs than analog systems.

Ethernet

A local area network used for connecting computers, printers, workstations, a terminals, servers, etc., within the same building or campus. Ethernet operates over twisted wire and coaxial cable at speeds up to 10 Mbps. Ethernet specifies a CSMA/CD.

hop count

A routing metric used to measure the distance between a source and a destination. Particularly used by RIP.

hub

(1) Communications center, (2) Major routing station for connecting channels, (3) DDS connecting center.

IEEE

Institute of Electrical and Electronic Engineers – Professional organization that defines network standards. IEEE LAN standards are the predominant LAN standards today and include protocols similar or virtually equivalent to Ethernet and Token Ring.

IEEE 802.1d

An algorithm used to prevent bridging loops by creating a spanning tree.

IEEE 802.3

A physical layer standard specifying a linear bus network LAN with a CSMA/CD access method on a bus topology. Ethernet follows the 802.3 standard, transmitting at 10 megabits per second. This is the most common local area network specification. Physical variations of IEEE 802.3 include 10Base2 and 10BaseT.

interexchange carrier

Since divestiture, any carrier registered with the FCC authorized to carry customer transmissions between LATAs interstate, or if approved by a state public utility commission, intrastate. Includes carriers such as AT&T, Qwest, Sprint, and Worldcom.

interworking

Communication between two types of networks or end equipment. This may or may not involve a difference in signalling or protocol elements supported.

Internet Protocol

A TCP/IP protocol describing software that tracks the Internet address of nodes, routes outgoing message, and recognizes incoming messages. Used in gateways to connect networks at OSI network Level 3 and above.

IPX

Internetwork Packet Exchange – A Novell NetWare protocol used to move information across networks.

ISDN

Integrated Services Digital Network – A network architecture that enables end-to-end digital connections. The network supports diverse services through integrated access arrangements and defines a limited set of standard, multipurpose interfaces for equipment vendors, network providers, and customers. Interworking with a public switched telephone network is retained.

LATA

Local Access and Transport Area – One of 161 local telephone serving areas in the United States, generally encompassing the largest standard statistical metropolitan areas. Subdivisions established as a result of the AT&T divestiture that now distinguish local from long distance service. Circuits with both end-points within the LATA (intraLATA) are generally the sole responsibility of the local telephone company, while circuits that cross outside the LATA (interLATA) are passed on to an interexchange carrier.

loopback

A diagnostic procedure where data is sent to the device being tested, and the output of the device is fed directly back to its input, looped around, and the returning data is checked against that which was sent.

Media Access Control (MAC)

As defined by the IEEE, the lower of the two sublayers of the OSI reference model data link layer. The MAC sublayer is concerned with media access issues, such as whether token passing or contention is used.

message

The Layer 3 information that is passed between the CPE and SPCS for signalling.

NAT

Network Address Translation occurs at the borders of stub domains. Its purpose is to translate the IP address of passing packets by changing all references of one IP address to another. Translation is performed as per RFC 1631.

netmask

A 32-bit bit mask which shows how an Internet address is to be divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion.

NT1

Network Termination 1 – A unit that provides physical and electromagnetic termination of the U-interface 2-wire transmission line, converts between Layer 1 formats used at the U- and T- reference points, and performs some maintenance functions.

point-to-point protocol (PPP)

An implementation of TCP/IP which is intended for transmission using telephone lines. PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

RIP

Routing Information Protocol – A protocol used to exchange routing information among a set of computers connected by a LAN. RIP uses hop counts as a routing metric.

router

An interface which finds the best route between two networks. Routers forward packets from one network to another, based on network layer information.

routing metric

The method by which a routing algorithm determines one route is better than another. This information is stored in routing tables. Such tables include reliability, delay bandwidth, load, MTUs, communication costs, and hop count.

service advertising protocol (SAP)

An IPX protocol through which network resources such as servers become known to clients.

serving area

Region surrounding a broadcasting station where signal strength is at or above a stated minimum. The geographic area handled by a telephone central office facility. Generally equivalent to a LATA.

SNMP

Simple Network Management Protocol – SNMP provides a means to monitor and set network configuration and runtime parameters.

spanning tree

A loop-free subset of the topology of a network.

SPCS

Stored Program Controlled Switch – A digital switch that supports call control, routing, and supplementary services provision under software control. All ISDN switches are SPCSs.

spoofing

Spoofing reduces the required bandwidth by having devices, such as bridges or routers, answer for the remote devices. This causes the remote LAN to appear as if it is still connected to the LAN device even though it is not. The spoofing saves the WAN bandwidth, because no packet is ever sent out on the WAN.

synchronous

(1) The condition occurring when two events happen in a specific time relationship with each other, both under control of a master clock; (2) A method of data transmission requiring the transmission of timing pulses to keep the sender and receiver synchronized in their communication used to send blocks of information. Synchronous data transmission is used in high speed data circuits because there is less overhead than asynchronous transmission of characters which contain two extra bits per character to effect timing.

T1

A digital transmission link with a capacity of 1.544 Mbps. T1 uses two pairs of normal twisted wires. T1 normally can handle 24 voice conversations with each conversation being digitized at 64 kbps. With more advanced digital voice encoding techniques, it can handle more voice channels. T1 is a standard for digital transmission in North America.

Telnet

The TCP/IP standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a remote timesharing system at another site as if the user's terminal were connected directly to the remote machine.

TCP/IP

Transmission Control Protocol/Internet Protocol – A set of protocols developed by the Department of Defense to link dissimilar computers across many kinds of networks.

twisted pair

Two wires twisted around each other to reduce induction (interference) from one wire to the other. Several sets of twisted pair wires may be enclosed in a single cable. Twisted pair is the normal cabling from a central office to your home or office, or from your PBX to your office phone. Twisted pair wiring comes in various thicknesses. As a general rule, the thicker the cable is, the better the quality of the conversation and the longer cable can be and still get acceptable conversation quality. However, the thicker it is, the more it costs.

U-interface

A twisted pair subscriber loop that connects the NT1 reference point to the ISDN network, as defined in the I.411 Recommendation. This interface provides Basic Rate Access with an operating frequency of 160 kbps and an information rate of 144 kbps. Under U.S. regulations, this also marks the line of demarcation between customer-owned equipment and the public network.

Zombie Routes

Routes that have been identified by the router to be deleted. They remain in the router’s route table for a specified amount of time with an infinite metric so that all other routers will learn of this router’s intention to delete them.