RAD
data communications

Installation and Operation Manual

WEB RANger-II

Internet/Intranet Access Router

WEB RANger-II

Internet/Intranet Access Router

Installation and Operation Manual

Notice

For further information contact RAD at the address below or contact your local distributor.

International Headquarters
RAD Data Communications Ltd.

24 Raoul Wallenberg St.
Tel Aviv 69719 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com

U.S. Headquarters
RAD Data Communications Inc.

900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100, Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com

 Publication No. 766-201-03/04

Limited Warranty

RAD warrants to DISTRIBUTOR that the hardware in the WEB RANger-II to be delivered hereunder shall be free of defects in material and workmanship under normal use and service for a period of twelve (12) months following the date of shipment to DISTRIBUTOR.

If, during the warranty period, any component part of the equipment becomes defective by reason of material or workmanship, and DISTRIBUTOR immediately notifies RAD of such defect, RAD shall have the option to choose the appropriate corrective action: a) supply a replacement part, or b) request return of equipment to its plant for repair, or c) perform necessary repair at the equipment's location. In the event that RAD requests the return of equipment, each party shall pay one-way shipping costs.

RAD shall be released from all obligations under its warranty in the event that the equipment has been subjected to misuse, neglect, accident or improper installation, or if repairs or modifications were made by persons other than RAD's own authorized service personnel, unless such repairs by others were made with the written consent of RAD.

The above warranty is in lieu of all other warranties, expressed or implied. There are no warranties which extend beyond the face hereof, including, but not limited to, warranties of merchantability and fitness for a particular purpose, and in no event shall RAD be liable for consequential damages.

RAD shall not be liable to any person for any special or indirect damages, including, but not limited to, lost profits from any cause whatsoever arising from or in any way connected with the manufacture, sale, handling, repair, maintenance or use of the WEB RANger-II, and in no event shall RAD's liability exceed the purchase price of the WEB RANger-II.

DISTRIBUTOR shall be responsible to its customers for any and all warranties which it makes relating to WEB RANger-II and for ensuring that replacements and other adjustments required in connection with the said warranties are satisfactory.

Software components in the WEB RANger-II are provided "as is" and without warranty of any kind. RAD disclaims all warranties including the implied warranties of merchantability and fitness for a particular purpose. RAD shall not be liable for any loss of use, interruption of business or indirect, special, incidental or consequential damages of any kind. In spite of the above RAD shall do its best to provide error-free software products and shall offer free Software updates during the warranty period under this Agreement.

RAD's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement and the WEB RANger-II shall not exceed the sum paid to RAD for the purchase of the WEB RANger-II. In no event shall RAD be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if RAD has been advised of the possibility of such damages.

This Agreement shall be construed and governed in accordance with the laws of the State of Israel.

General Safety Instructions

The following instructions serve as a general guide for the safe installation and operation of telecommunications products. Additional instructions, if applicable, are included inside the manual.

Safety Symbols

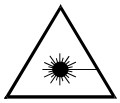
Warning

This symbol may appear on the equipment or in the text. It indicates potential safety hazards regarding product operation or maintenance to operator or service personnel.

Danger of electric shock! Avoid any contact with the marked surface while the product is energized or connected to outdoor telecommunication lines.

.

Protective earth: the marked lug or terminal should be connected to the building protective earth bus.



Warning

Some products may be equipped with a laser diode. In such cases, a label with the laser class and other warnings as applicable will be attached near the optical transmitter. The laser warning symbol may be also attached. Please observe the following precautions:

- **Before turning on the equipment, make sure that the fiber optic cable is intact and is connected to the transmitter.**
- **Do not attempt to adjust the laser drive current.**
- **Do not use broken or unterminated fiber-optic cables/connectors or look straight at the laser beam.**
- **The use of optical devices with the equipment will increase eye hazard.**
- **Use of controls, adjustments or performing procedures other than those specified herein, may result in hazardous radiation exposure.**

ATTENTION: The laser beam may be invisible!

Always observe standard safety precautions during installation, operation and maintenance of this product. Only qualified and authorized service personnel should carry out adjustment, maintenance or repairs to this product. No installation, adjustment, maintenance or repairs should be performed by either the operator or the user.

Handling Energized Products

General Safety Practices

Do not touch or tamper with the power supply when the power cord is connected. Line voltages may be present inside certain products even when the power switch (if installed) is in the OFF position or a fuse is blown. For DC-powered products, although the voltages levels are usually not hazardous, energy hazards may still exist.

Before working on equipment connected to power lines or telecommunication lines, remove jewelry or any other metallic object that may come into contact with energized parts.

Unless otherwise specified, all products are intended to be grounded during normal use. Grounding is provided by connecting the mains plug to a wall socket with a protective earth terminal. If an earth lug is provided on the product, it should be connected to the protective earth at all times, by a wire with a diameter of 18 AWG or wider. Rack-mounted equipment should be mounted only in earthed racks and cabinets.

Always make the ground connection first and disconnect it last. Do not connect telecommunication cables to ungrounded equipment. Make sure that all other cables are disconnected before disconnecting the ground.

Connection of AC Mains

Make sure that the electrical installation complies with local codes.

Always connect the AC plug to a wall socket with a protective ground.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Always connect the power cord first to the equipment and then to the wall socket. If a power switch is provided in the equipment, set it to the OFF position. If the power cord cannot be readily disconnected in case of emergency, make sure that a readily accessible circuit breaker or emergency switch is installed in the building installation.

Connection of DC Mains

Unless otherwise specified in the manual, the DC input to the equipment is floating in reference to the ground. Any single pole can be externally grounded.

Due to the high current capability of DC mains systems, care should be taken when connecting the DC supply to avoid short-circuits and fire hazards.

DC units should be installed in a restricted access area, i.e. an area where access is authorized only to qualified service and maintenance personnel.

Make sure that the DC supply is electrically isolated from any AC source and that the installation complies with the local codes.

The maximum permissible current capability of the branch distribution circuit that supplies power to the product is 16A. The circuit breaker in the building installation should have high breaking capacity and must operate at short-circuit current exceeding 35A.

Before connecting the DC supply wires, ensure that power is removed form the DC circuit. Locate the circuit breaker of the panel board that services the equipment and switch it to the OFF position. When connecting the DC supply wires, first connect the ground wire to the corresponding terminal, then the positive pole and last the negative pole. Switch the circuit breaker back to the ON position.

A readily accessible disconnect device that is suitably rated and approved should be incorporated in the building installation.

Connection of Data and Telecommunications Cables

Data and telecommunication interfaces are classified according to their safety status.

The following table lists the status of several standard interfaces. If the status of a given port differs from the standard one, a notice will be given in the manual.

Ports	Safety Status	
V.11, V.28, V.35, V.36, X.21, RS-530, 10 BaseT, 100 BaseT, Unbalanced E1, E2, E3, STM, DS-2, DS-3, S-Interface ISDN, Analog voice E&M	SELV	Safety Extra Low Voltage: Ports which do not present a safety hazard. Usually up to 30 VAC or 60 VDC.
xDSL (without feeding voltage), Balanced E1, T1, Sub E1/T1	TNV-1	Telecommunication Network Voltage-1: Ports whose normal operating voltage is within the limits of SELV, on which overvoltages from telecommunications networks are possible.
FXS (Foreign Exchange Subscriber)	TNV-2	Telecommunication Network Voltage-2: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are not possible. These ports are not permitted to be directly connected to external telephone and data lines.
FXO (Foreign Exchange Office), xDSL (with feeding voltage), U-Interface ISDN	TNV-3	Telecommunication Network Voltage-3: Ports whose normal operating voltage exceeds the limits of SELV (usually up to 120 VDC or telephone ringing voltages), on which overvoltages from telecommunication networks are possible.

Always connect a given port to a port of the same safety status. If in doubt, seek the assistance of a qualified safety engineer.

Always make sure that the equipment is grounded before connecting telecommunication cables. Do not disconnect the ground connection before disconnecting all telecommunications cables.

Some SELV and non-SELV circuits use the same connectors. Use caution when connecting cables. Extra caution should be exercised during thunderstorms.

When using shielded or coaxial cables, verify that there is a good ground connection at both ends. The earthing and bonding of the ground connections should comply with the local codes.

The telecommunication wiring in the building may be damaged or present a fire hazard in case of contact between exposed external wires and the AC power lines. In order to reduce the risk, there are restrictions on the diameter of wires in the telecom cables, between the equipment and the mating connectors.

Caution To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cords.

Attention Pour réduire les risques s'incendie, utiliser seulement des conducteurs de télécommunications 26 AWG ou de section supérieure.

Some ports are suitable for connection to intra-building or non-exposed wiring or cabling only. In such cases, a notice will be given in the installation instructions.

Do not attempt to tamper with any carrier-provided equipment or connection hardware.

Electromagnetic Compatibility (EMC)

The equipment is designed and approved to comply with the electromagnetic regulations of major regulatory bodies. The following instructions may enhance the performance of the equipment and will provide better protection against excessive emission and better immunity against disturbances.

A good earth connection is essential. When installing the equipment in a rack, make sure to remove all traces of paint from the mounting points. Use suitable lock-washers and torque. If an external grounding lug is provided, connect it to the earth bus using braided wire as short as possible.

The equipment is designed to comply with EMC requirements when connecting it with unshielded twisted pair (UTP) cables. However, the use of shielded wires is always recommended, especially for high-rate data. In some cases, when unshielded wires are used, ferrite cores should be installed on certain cables. In such cases, special instructions are provided in the manual.

Disconnect all wires which are not in permanent use, such as cables used for one-time configuration.

The compliance of the equipment with the regulations for conducted emission on the data lines is dependent on the cable quality. The emission is tested for UTP with 80 dB longitudinal conversion loss (LCL).

Unless otherwise specified or described in the manual, TNV-1 and TNV-3 ports provide secondary protection against surges on the data lines. Primary protectors should be provided in the building installation.

The equipment is designed to provide adequate protection against electro-static discharge (ESD). However, it is good working practice to use caution when connecting cables terminated with plastic connectors (without a grounded metal hood, such as flat cables) to sensitive data lines. Before connecting such cables, discharge yourself by touching earth ground or wear an ESD preventive wrist strap.

FCC-15 User Information

This equipment has been tested and found to comply with the limits of the Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Installation and Operation manual, may cause harmful interference to the radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Emission Requirements

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Warning per EN 55022 (CISPR-22)

Warning	This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user will be required to take adequate measures.
Avertissement	Cet appareil est un appareil de Classe A. Dans un environnement résidentiel, cet appareil peut provoquer des brouillages radioélectriques. Dans ces cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.
Achtung	Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkströrungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

WEB RANger-II with RS-530 or X.21 Ports
Installation Instructions for
Compliance with EMC Requirements

To comply with electromagnetic compatibility requirements, a ferrite core (such as FAIR RITE catalog number 0443167151 or equivalent) should be installed on any unshielded data cable connected to the RS-530 or X.21 ports.

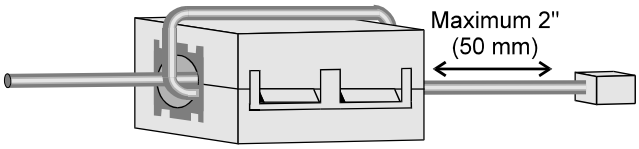
This limits the electromagnetic energy emitted from the cable.

Alternatively, replace unshielded data cable with shielded data cable.

Note: If using a shielded data cable, the cable shield should be connected to the metallic hood.

To install the ferrite core:

- Run the cable through the open core.
- If cable thickness allows, wrap it around the core and run it through again.
  Allow no more than 2 inches (5 cm) between the core and the cable connector to the unit.
- Snap the core shut.



Declaration of Conformity

Manufacturer's Name: RAD Data Communications Ltd.

Manufacturer's Address: 24 Raoul Wallenberg St.
Tel Aviv 69719
Israel

declares that the product:

Product Name: WEB RANger-II

conforms to the following standard(s) or other normative document(s):

EMC:	EN 55022 (1994)	Limits and methods of measurement of radio disturbance characteristics of information technology equipment.
	EN 50082-1 (1992)	Electromagnetic compatibility – Generic immunity standards for residential, commercial and light industry.
Safety:	EN 60950/A4 (1996)	Safety on information technology equipment, including electrical business equipment.

Supplementary Information:

The product herewith complies with the requirements of the EMC Directive 89/336/EEC and the Low Voltage Directive 73/23/EEC. The product was tested in a typical configuration.

Tel Aviv, February 16th, 1998

Haim Karshen
VP Quality

European Contact: RAD Data Communications GmbH, Otto-Hahn-Str. 28-30,
85521 Ottobrunn-Riemerling, Germany

Preface

Foreword

This manual describes the technical characteristics, applications, installation and operation of the WEB RANger-II.

Manual Organization

This manual is organized as follows:

Chapter 1. Introduction
presents the main features and describes the various equipment versions, and lists the technical characteristics of WEB RANger-II.

Chapter 2. Installation
provides detailed installation instructions for WEB RANger-II.

Chapter 3. Operation

provides detailed operation instructions for WEB RANger-II.

Chapter 4. Configuration
provides typical configuration procedures for WEB RANger-II.

Chapter 5. Troubleshooting and Diagnostics
describes the diagnostic and performance monitoring functions supported by WEB RANger-II.

Appendix A. Interface Specifications and Cable Diagrams

provides connection data for the interfaces used by WEB RANger-II.

Appendix B. Boot Manager
explains the download procedure for different versions of software.

Appendix C. SNMP Management

describes the SNMP and IP environments, and provides background information regarding the handling of management traffic.

Appendix D. Glossary
provides glossary of technical terms.

Conventions

Note	*A note draws attention to a general rule for a procedure, or to exceptions to a rule.*
Caution	A caution warns of possible damage to the equipment if a procedure is not followed correctly.
 ***Warning***	**A warning alerts to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the equipment. If these instructions are not followed exactly, possible bodily injury may occur.**

Quick Start Guide

If you are familiar with WEB RANger-II, use this guide to prepare it for operation.

1. Jumper Settings

In most cases, there is no need to perform hardware configuration.
WEB RANger-II jumpers are set by the factory to **DTE** and **Balanced.**

When working in V.24 or V.35 link interface setting DCE mode, or for E1 unbalanced interface, perform the following steps:

1. Disconnect all cables from WEB RANger-II.
2. Remove the cover by loosening the four screws located at the bottom of the unit.
3. Slide off the top cover.
4. Perform required internal settings.
5. Refit the WEB RANger-II case.

2. Cable and Power Connections

Before using WEB RANger-II, make the following cable connections:

1. Connect WEB RANger-II to the power source. Use the 5 ft (1.5m) standard power cable provided with the unit. Make sure the POWER switch on the rear panel is set to OFF, then connect the cable first to the WEB RANger-II rear panel, then to the power source.
2. Connect WEB RANger-II to the link.
3. Connect WEB RANger-II to the supervisory terminal (if needed).
4. Connect WEB RANger-II to the LAN.

3. Configuration

You can configure and operate WEB RANger-II from an ASCII terminal or a PC terminal emulator.

1. Set the terminal to 9.6 kbps, No parity, 8 Data Bits.
2. Set Hardware Flow Control to OFF.
3. Turn WEB RANger-II POWER to ON.

   The operational status screen appears.

4. Press **<Enter>** or **<Space>** several times to invoke the login prompt.
5. Press **<Enter>**.
6. Enter the password. (The default password for first-time connection is **1234**. You can change or remove it later.)

   The Main Menu screen appears.
7. From the Main Menu you can select the Quick Setup menu or the Advanced Setup menu, with submenus, which provide further parameters that can be configured. Follow the instructions on each screen.

Contents

Chapter 4. Configuration

Chapter 5. Troubleshooting and Diagnostics

Appendix A. Interface Specifications and Cable Diagrams

Appendix B. BOOT Manager

Appendix A. SNMP Management

Appendix D. Glossary

Index

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Overview

WEB RANger-II is a standalone access router that connects small to medium-sized networks to the Internet or Intranet. WEB RANger-II supports IP, IPX routing and bridging. Quick setup and configuration menus provide on-screen instructions that guide you through installation and configuration procedures.

WEB RANger-II connects an Ethernet LAN to the Internet or Intranet. The connection is made via Frame Relay, synchronous, Digital Data Service (DDS), or E1/T1 links, operating at data rates of up to 2.048 Mbps.

WEB RANger-II also supports two Ethernet LAN connections.

Options

WEB RANger-II connects your Ethernet LAN to the Internet or Intranet. The connection is made via Frame Relay, ISDN, DDS or Leased Line. A second WAN interface is available. Optional sub-E1/T1 or analog voice drop & insert ports for voice connectivity over E1/T1 services are available.

Versions

A variety of data interfaces are available: V.35, V.24, V.35, RS-530, V.36, X.21, built-in 4-wire modem, and Ethernet BNC or UTP.

Sub-E1/T1, analog voice, and ISDN backup interface options include FXS, FXO, E&M, and ISDN “S” or “U” interface.

The interface provides connection to one or two LANs.

Applications

WEB RANger-II is adaptable to several different applications. Order your unit according to your specific application requirements.

In *Figure 1-1* WEB RANger-II uses the E1/T1 interface to connect to both Internet services and voice (telephone) services.

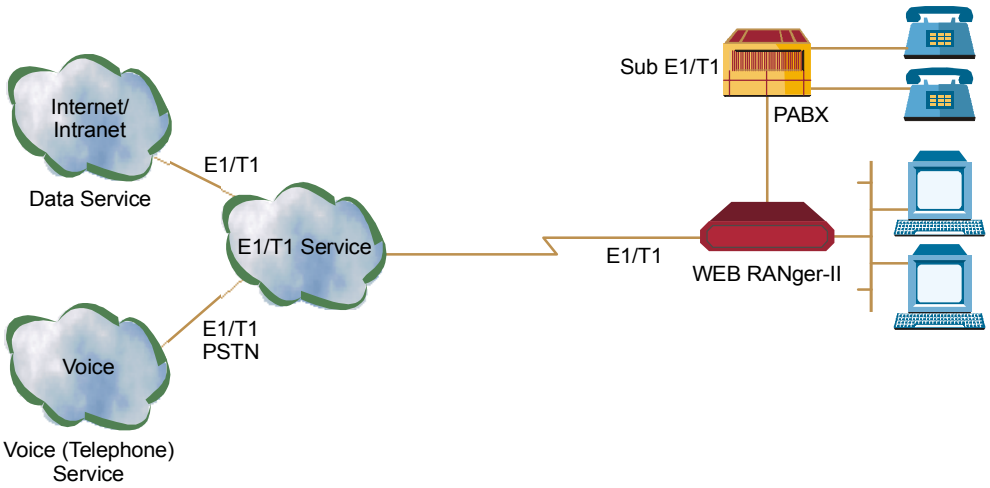


Figure 1-1. WEB RANger-II with E1/T1 Interface including LAN and PABX

In *Figure 1-2* WEB RANger-II connects four telephones and LAN to E1/T1 service.

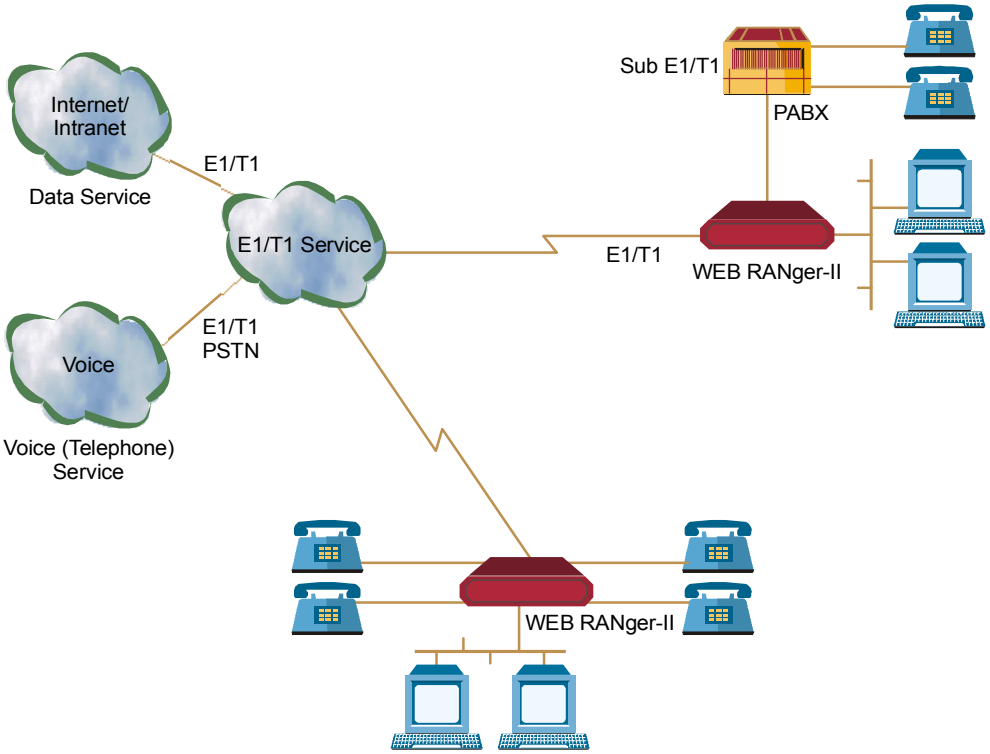


Figure 1-2. WEB RANger-II with Four Telephones and LAN

In *Figure 1-3* WEB RANger-II supports two separate LAN configurations. WEB RANger-II connects these networks to the Internet with a V.35 interface, using the PPP or Frame Relay protocols.

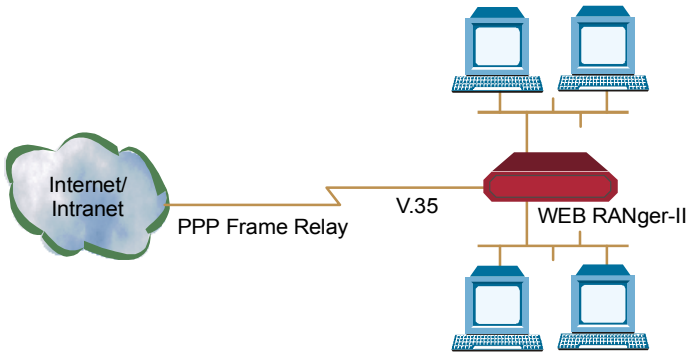


Figure 1-3. WEB RANger-II with V.35 and 2 LANs

In *Figure 1-4* WEB RANger-II supports a single LAN connection to the Internet using the V.35 interface and the PPP or Frame Relay protocols, with ISDN backup link.

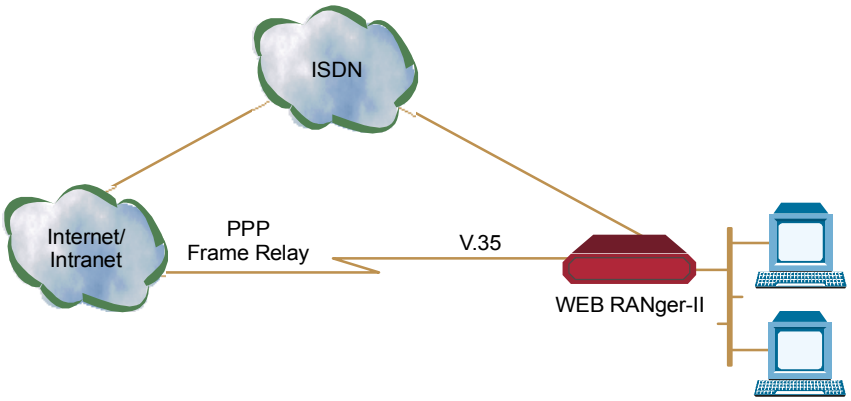


Figure 1-4. WEB RANger-II with V.35 Interface, Single LAN, and ISDN Backup

Features

WEB RANger-II features IP/IPX routing and standard bridging. WEB RANger-II supports Frame Relay, PPP, MLPPP, NAT and Single IP address translation, Integral E1 with or without LTU or Integral T1 CSU/DSU.

Easy configuration is performed through a Quick Setup menu.

Fast installation can be performed from a terminal emulator or via TELNET. An SNMP agent provides management by RADview or any other standard SNMP management station. Inband and out-of-band remote management is available.

Software downloading is available using XMODEM or TFTP. Dual image flash enables downloading two software versions. WEB RANger-II also supports RADIUS.

The quad analog voice or sub-E1/T1 drop & insert ports provide toll-quality voice transmission. Modulation is PCM encoded, A-Law, or µ-Law.

Security features include Solid Firewall protection and PAP/CHAP authentication. The Solid Firewall feature allows the user to block all access from the outside into the LAN.

Undesired access to WEB RANger-II via TELNET or SNMP can also be blocked or password protected.

The fail-safe bypass of the sub-E1/T1 link ensures continuity of voice services in case of power supply failures.

Connection-On-Demand and Bandwidth-On-Demand, together with advanced filtering, reduce communication expenses in ISDN services.

1.2 Physical Description

WEB RANger-II units are delivered completely assembled. The units are designed for desktop installation, or mounted in a 19-inch rack. Refer to the *Rack Mounting Kit for 19-inch Racks* guide that comes with the RM kit.

Installation procedures for WEB RANger-II models and respective versions are provided in *Chapter 2*.

Figure 1-5 shows a 3-dimensional view of one of the WEB RANger-II versions.

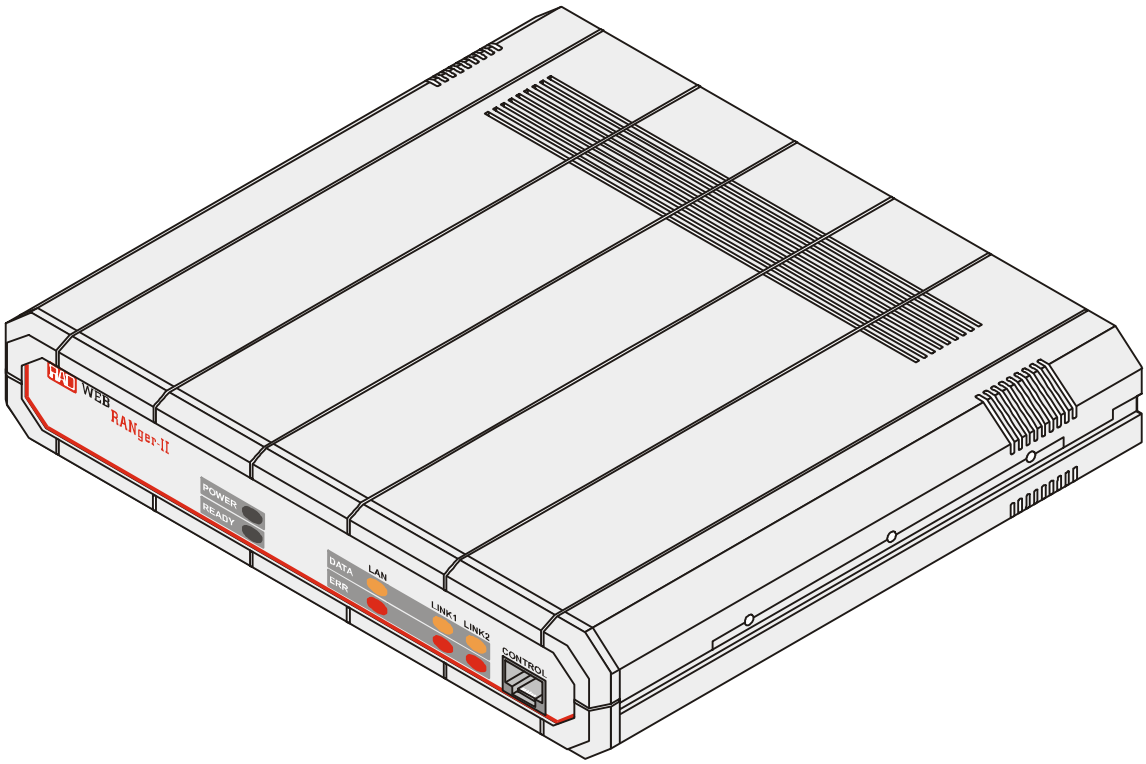


Figure 1-5. A WEB RANger-II Version – 3D view

LEDs

Controls and indicators of the various versions of WEB RANger-II and their functions are described in *Chapter 3*. LED indicators on the front panel indicate the operating status of WEB RANger-II; these include status of the user's data port, data activity in the user's data connector, alert conditions, and test loop activity. The WEB RANger-II front panel always contains LEDs for Power, Ready, Link1/2 and LAN. Additional LEDs are provided if your unit has 2 LANs. If your unit contains an E1 link, the LEDs indicate Local Sync Loss or Remote Sync Loss. If the unit contains a T1 link, LEDs indicate Red Alarm and Yellow Alarm status. For a description of the front panel, with all the available options, refer to *Table 3-1*.

Connectors

The power and interface connectors are located on the rear panel of WEB RANger-II. For a description of the rear panel, refer to *Interfaces and Connections* in Chapter 2.

Jumpers

The internal jumpers of WEB RANger-II are set according to the options ordered. The only time you may need to set jumpers is when working with V.24 or V.35 link interface DCE mode, or for E1 balanced interface. For more information see *Setting Internal Jumpers and Switches* in Chapter 2.

1.3 Functional Description

This section describes the functional components of WEB RANger-II.

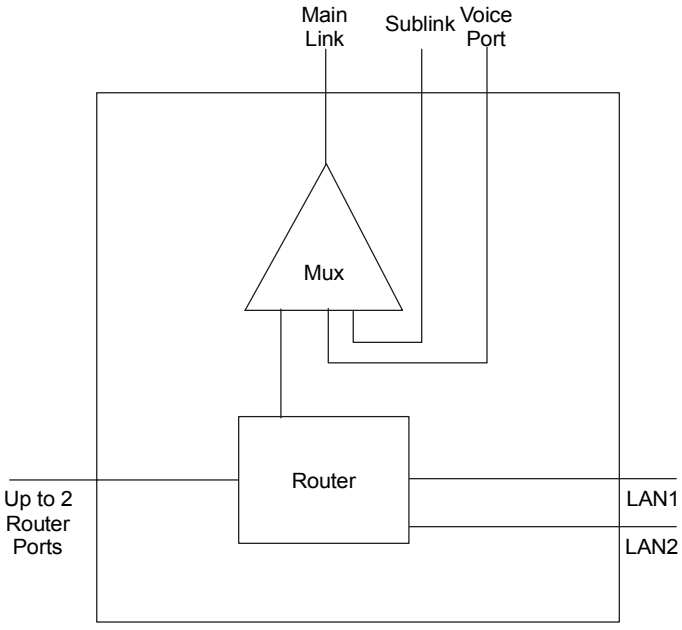


Figure 1-6. WEB RANger-II Functional Block Diagram

Protocols

PPP Point-to-point Protocol supports a variety of links and connection options.

Frame Relay This network interface provides high speed frame or packet transmission with minimum delay and maximum bandwidth utilization.

IP/IPX Routing

WEB RANger-II as an IP router supports Static IP net configuration, Dynamic IP net learning using the RIP and RIP-2 protocols, CIDR topologies, Multiple IP nets on the LAN, numbered and unnumbered interfaces and IP fragmentation.

In addition to IP routing, WEB RANger-II also supports standard IPX routing and includes support for RIP and SAP.

Bridging

WEB RANger-II supports bridging. The bridge is used to interconnect a number of LANs, by accessing layer 2 (MAC layer). WEB RANger-II automatically extends the scope of any interface, allowing the interface to interconnect several networks - if all supported interfaces are set to Bridge mode.
WEB RANger-II interconnects:

- Any LAN to link
- Two LANs of the same Bridge (only in options WR2\2B for 2x10Base2, or WR2\2T for 2x10BaseT)
- Two LANs and link (only in options WR2\2B for 2x10Base2, or WR2\2T for 2x10BaseT).

WEB RANger-II interconnects all its interfaces to one extended LAN.

WEB RANger-II supports standard bridging, as specified in IEEE 802.1D, and can operate opposite any other third party bridge. Spanning Tree Algorithm is not supported. Bridging works over PPP, Frame Relay RFC-1490 and also a 'Native' protocol. MAC frames pass in an HDLC format.

Address Translation (Single IP)

WEB RANger-II offers a feature called Single IP. Single IP allows users in a Small Office LAN to connect to the Internet/Intranet quickly and transparently. Single IP requires only one legal IP address. It may be assigned statically by configuration or obtained dynamically from the Internet/Intranet Access Router using standard IPCP.

WEB RANger-II and Single IP

Single IP is a WEB RANger-II feature, designed by RAD, which translates IP addresses. Single IP can be enabled or disabled. When enabled, WEB RANger-II allows users in a Small Office to connect to the Internet/Intranet quickly and transparently. WEB RANger-II provides security against Internet hackers using the Solid Firewall feature.

Normally, a LAN requires a complete statically assigned, unique and legal subnet for connection to the Internet or Intranet. Single IP allows an entire Small Office to connect to the Internet or Corporate Intranet using only one dynamically or statically assigned IP.

The Internet/Intranet provider does not need to specially coordinate with the office or allocate subnets.

WEB RANger-II is designed to support multiple concurrent users on the Small Office LAN.

Solid Firewall

The Solid Firewall feature prevents access from the Internet/Intranet into the Small Office LAN. This feature makes the Small Office LAN invisible to outside users. The Solid Firewall feature is a simple and foolproof way of protecting security-sensitive Small Offices (e.g. doctors and lawyers) from Internet hackers. Refer to *Security Setup Menu* in Chapter 4 for further information about the Firewall.

1.4 Technical Specifications

LAN Interface	*Standard*	Conforms to IEEE 802.3
	Type	10Base2 with coax connector 10BaseT with RJ-45 connector
Link Interface	*Interface (refer to Ordering Information)*	V.35
	Connectors	V.35 with 34-pin female V.24/RS-232 or RS-530 with 25-pin D-type, female X.21 with 15-pin D-type, female via adapter cable V.36/RS-422 with 37-pin D-type, female via adapter cable
	Data Rates	T1: up to 1.5 Mbps V.35, E1: up to 2.048 Mbps
	Protocol	Synchronous PPP and MLPPP, Frame Relay/RFC 1490, HDLC
Control Interface	*Type*	RS-232
	Connector	RJ-45 female (front panel)
	Data Rate	9.6 kbps, 8 bits, No Parity

T1 Interface

Framing	D4, ESF
Bit Rate	1.544 Mbps
Line Code	AMI
Zero Suppression	Transparent, B7ZS, B8ZS
Impedance	100Ω, balanced
Signal Level	Receive: 0 to -36 dB with CSU 0 to -10 dB without CSU Transmit: 0, -7.5, -15, -22.5 dB with CSU Soft adjustable at 0 to 655 ft without CSU
Jitter Performance	As per AT&T TR-62411
Connector	RJ-48c 8-pin Two BNC coaxial, unbalanced
Compliance	AT&T TR-62411, ANSI T1.403
Diagnostics	User-activated local and remote loopbacks Network activated loops and FDL loops (RLB, LLB)

E1 Interface

Framing	256N (no MF, CCS) 256N (no MF, CCS) with CRC-4 256S (TS16 MF, CAS) 256S (TS16 MF, CAS) with CRC-4
Bit Rate	2.048 Mbps
Line Code	AMI
Zero Suppression	HDB3
Impedance	120Ω, balanced 75Ω, unbalanced
Signal Level	Receive: 0 to -36 dB / with LTU 0 to -12 dB / without LTU Transmit: 3V (±10%), balanced 2.37V (±10%), unbalanced
Jitter Performance	As per ITU G.823
Connector	RJ-48c 8 pin, balanced Two BNC coaxial, unbalanced
Compliance	ITU G.703, G.704, G.706, G.732
Diagnostics	User-activated local and remote loopbacks

Analog Voice

Number of Voice Channels	4
Modulation method	PCM (per ITU-T G.711 and AT&T PUB-43801), μ-Law or A-Law
Interfaces	E&M: 2-wire or 4-wire, supporting different types of E&M signaling: RS-464 Types I, II, III, V, and BT SSDC5, configured by software
	FXS: Loop start, WINK start (reverse polarity) for direct connection to a 2-wire telephone
	FXO: Loop start, WINK start (reverse polarity) connection to a 2-wire telephone exchange subscriber line
Nominal level	0 dBm
Nominal impedance	600Ω
Return loss	(ERL), better than 20 dB
Frequency response (Ref: 1020 Hz)	±0.5 dB, 300 to 3000 Hz
	±1.1 dB, 250 to 3400 Hz
Signal to total distortion, G.712, G.713 method 2	0 to –30 dBm0 – better than 33 dB
	+3 to –45 dBm0 – better than 22 dB
Idle channel noise:	better than –70 dBm0 (+20 dBrnc)
Transformer isolation	1500 VRMS
Diagnostics	Local digital loopback towards the analog side
	Remote analog loopback towards the remote side, activated from local side
	1 kHz tone injection towards analog side Activity indicators
	1 kHz tone injection towards the E1/T1 side

ISDN

Interfaces	ISDN BRI, “S” and “U”
Compliance	ETS 300012, I.430, NTT, 5ESS, DMS-100, NI1

Routing

Types	STATIC, RIP-I, RIP-2, RIP/SAP

Fiber Optic Interfaces	*Types*	850 nm LED for use over multimode fiber at distances up to 5 km (3 miles) 1300 nm LED for use over single mode fiber at distances up to 47 km (29 miles) 1300 nm laser diode for use over single mode fiber at distances up to 62 km (38 miles) 1550 nm laser diode for use over single mode fiber for extended range up to 100 km (62 miles).
	Connectors	ST, FC/PC, SC
	Compliance	ITU G.921, G.956
LED General Indicators	*POWER (green)*	On – powered
	READY (green)	On – packets can be transferred
	LAN DATA (yellow)	On – a packet is received or transmitted on LAN side
	LAN ERROR (red)	On – LAN interface indicates an error
	LINK DATA (yellow)	On – a packet is received or transmitted on LINK side
	LINK ERROR (red)	On – LINK interface indicates an error
LED Indicators: T1	*RED ALARM (red)*	On – T1 interface detects red alarm
	YEL ALARM (yellow)	On – T1 interface detects yellow alarm
E1	*LOCAL SYNC LOSS (red)*	On – E1 interface detects local sync loss
	REMOTE SYNC LOSS (red)	On – E1 interface detects remote sync loss
Panel Controls	*Power ON/OFF*	Rear panel
Power Supply	*Voltage*	100-230 VAC, 24 VDC , 48 VDC,
	Frequency	50–60 Hz
	Power	13 VA max

Physical	*Height*	4.4 cm / 1.8 in (1U)
	Length	24 cm / 9.6 in
	Width	21.6 cm / 8.5 in
	Weight	1.16 kg / 2.55 lb
Environment	*Temperature*	0°–50°C / 32°–122°F
	Humidity	0 to 90%, non-condensing

Chapter 2

Installation and Setup

Topics covered in this chapter include:

- Introduction
- Unpacking WEB RANger-II
- Site requirements
- Package contents
- Equipment needed
- Installation and setup
- Interfaces and connections
- Power
- Operating procedure.

2.1 Introduction

This chapter details the steps for WEB RANger-II installation.

➤ **To install WEB RANger-II:**

1. Unpack WEB RANger-II.
2. Connect to the power source.
3. Connect to the LAN(s).
4. Connect to the Link(s).
5. Connect to the Terminal Emulator.

After installation you must configure the unit before further operation. Refer to *Chapter 3* for operation and *Chapter 4* for configuration instructions. If you encounter a problem, refer to *Chapter 5* for troubleshooting and diagnostics.

2.2 Unpacking WEB RANger-II

Inspect the container before unpacking. Report evidence of damage immediately to your RAD distributor.

➤ **To unpack WEB RANger-II:**

1. Place the container on a clean flat surface, cut all straps, and open the top.
2. Take out WEB RANger-II carefully and place it securely on a clean surface.
3. Inspect the product for damage. Report any damage found immediately.

Warning

No internal settings, adjustment, maintenance, or repairs may be performed by either the operator or the user; such repairs may be performed only by a skilled technician who is aware of the hazards involved. Always observe standard safety precautions during installation, operation, and maintenance of this product.

2.3 Site Requirements and Prerequisites

WEB RANger-II is designed for installation on top of a bench or shelf, or mounting in a 19-inch rack (RM-17 kit). Refer to the Rack Mounting Kit for 19-inch Racks guide that comes with the RM kit.

Install AC-powered WEB RANger-II units within 1.5m (5 feet) of a grounded AC outlet, furnishing 115V or 230V (in accordance with your order). DC-powered units require a 24 or 48 VDC power source, in accordance with your order.

Allow at least 10 cm (4 inches) clearance, in front of and behind the unit for interface cable connections. Allow at least 90 cm (36 inches) of frontal clearance for operator access.

The ambient temperature should be 0°–50°C (32°–122°F) at a relative humidity of up to 90%, non-condensing.

2.4 Package Contents

Inspect the equipment package before unpacking. Note and report damage immediately. The WEB RANger-II package includes the following items:

- WEB RANger-II unit
- Technical documentation CD
- Configuration cable
- Power cable
- Adapter cable for link
- RM-17 rack mount kit (if ordered).

2.5 Equipment Needed

The cables you need depend on the application. Cables terminated in appropriate connectors provide support for the following data port interfaces:

- **V.35 interface** – the interface adapter cable ends in a 34-pin female connector
- **V.36/422 interface** – the interface adapter cable ends in a 37-pin D-type female connector
- **V.24/RS-232 or RS-530 interface** – the interface adapter cable ends in a 15-pin D-type female connector
- **X.21 interface** - the interface adapter cable ends in a 15-pin D-type female connector.

The required cables are available from RAD, or can be prepared in accordance with the port connector wiring information given in *Appendix A*.

2.6 Installation and Setup

The WEB RANger-II units are delivered completely assembled. The units are designed for installation on top of a bench or shelf, or mounted in a 19-inch rack (RM-17). Refer to the *Rack Mounting Kit for 19-inch Racks* guide that comes with the RM kit.

Installation procedures for WEB RANger-II are provided in the following paragraphs.

Setting Internal Jumpers and Switches

In most cases, there is no need to perform Hardware Configuration. It is only necessary when working in V.24 or V.35 Link Interface Setting DCE mode, or for E1 Balanced Interface.

Warning

To avoid accidental electric shock, disconnect the telephone wires and the WEB RANger-II power cord before opening the top cover.

➤ **To perform Hardware Configuration:**

1. Disconnect the WEB RANger-II power cord from the wall socket. Turning OFF the POWER switch on the rear panel is not sufficient.
2. Remove the cover by loosening the four screws located on the bottom of the unit.
3. Set the jumpers according to the instructions in *V.24 and V.35 Link Interface Setting – DTE/DCE Jumper* or *E1 and T1 Link Interface Setting*, as shown below.
4. Refit the cover.

V.24 and V.35 Link Interface Setting – DTE/DCE Jumper

The WEB RANger-II link interface can be configured as DTE or DCE. The factory setting is DTE. Refer to *Figure 2-1* and *Figure 2-2* for jumper locations.

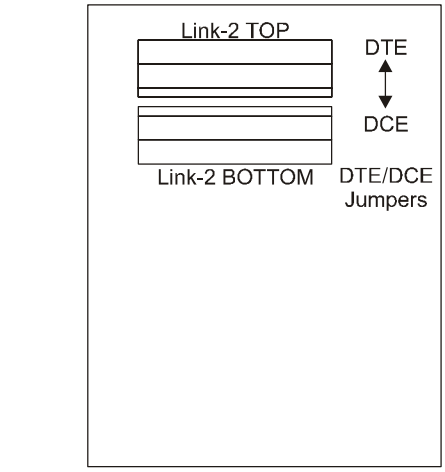


Figure 2-1. V.24D, V.35D, V.24 Link Interface Card

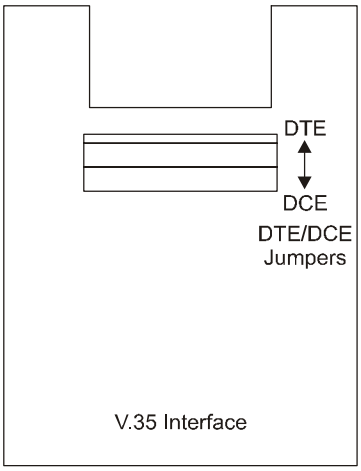


Figure 2-2. V.35 Link Interface Card

E1 and T1 Link Interface Setting

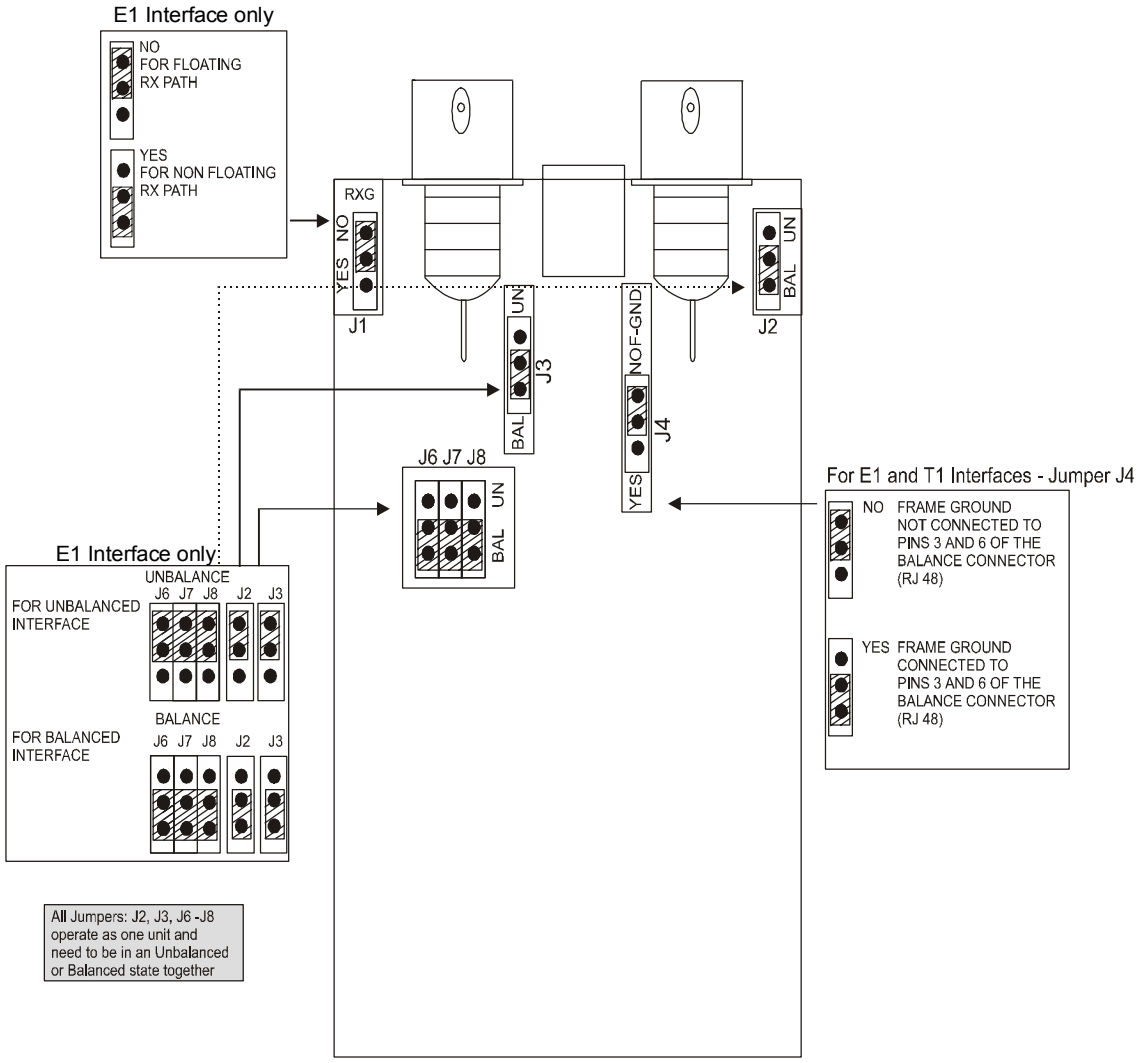


Figure 2-3. E1 and T1 Interface Setting

Table 2-1. Jumpers for E1 and T1 Link Interface Setting

Jumper Number	Description	Options	Factory Setting
Link Interface Jumpers: **J2, J3** **J6 - J8**	Selects the link interface (E1 only) for BAL/UN	**Balanced Interface** (RJ-48) – set all jumpers to BAL **Unbalanced Interface** (BNC) – set all jumpers to UN Set all the jumpers to the same position.	**Balanced**
Receive Path Jumper: **J1**	Controls the ground reference of the link receive input when the unbalanced interface is used (E1 interface only).	**YES** - Receive ground reference is connected to the frame (chassis) ground **NO -** Receive ground reference is not connected to the frame ground (floating).	**NO**
Frame/Signal Ground Jumper **J4**	Controls the connection of Pins 3 and 6 in the RJ-48 connector (Balance option) to the frame (chassis) ground	**YES** - Pins 3 and 6 in RJ-48 are connected to the frame (chassis) ground **NO -** Pins 3 and 6 in RJ-48 are not connected to the frame ground	**NO**

Warning

Australian and New Zealand users: Leave J4 at NO.

2.7 Interfaces and Connections

➤ **To connect the cable:**

1. Connect the power cable to the power port located on the right hand side of the WEB RANger-II rear panel.
2. Connect the three-prong plug to a grounded AC outlet.

Connecting to the Link

A connector is provided to connect the interface to the communication link(s). Refer to *Table B-1* for Link connector pin assignments.

Note *X.21 and V.36 connections are provided by adapter cables to the RS-530 (25-pin connector) on the WEB RANger-II rear panel.*

➤ **To connect to the link(s):**

1. Attach the cable with the interface connector to the link port of the WEB RANger-II rear panel.

There are many different rear panel options for WEB RANger-II. A schematic diagram of the Main Link, Sublink, and LAN options is shown in *Figure 2-4*.

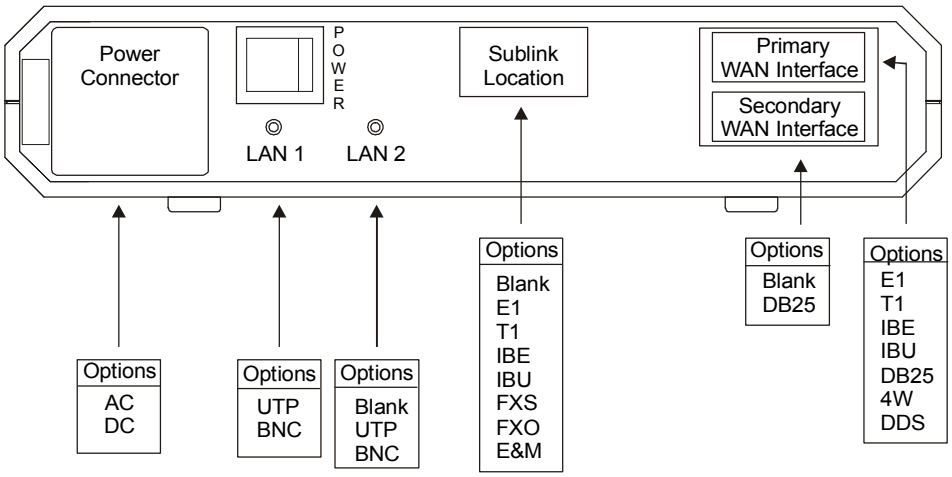


Figure 2-4. Rear Panel Schematic Diagram Showing WEB RANger-II Options

2. Attach the other side of the cable to the wall outlet. *Figure 2-5* shows connection to the Public Access Service.

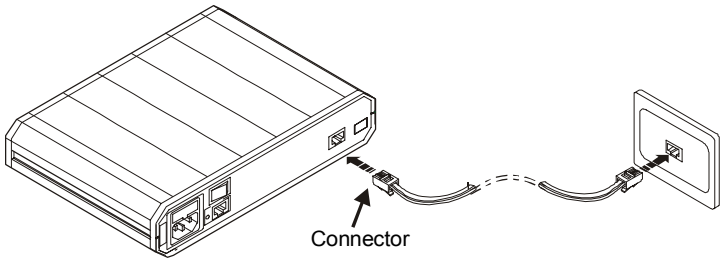


Figure 2-5. Connecting to the Public Access Service

Connecting to the Terminal Emulator

You can run the WEB RANger-II setup program from an ASCII terminal or a PC terminal emulator. Connect the terminal to the RJ-45 CONTROL port on the WEB RANger-II front panel.

➤ **To connect to the terminal emulator:**

1. Attach the cable to the RS-232 port on the PC.
2. Attach the other end of the cable to the control port on the WEB RANger-II front panel (refer to *Figure 2-6*).

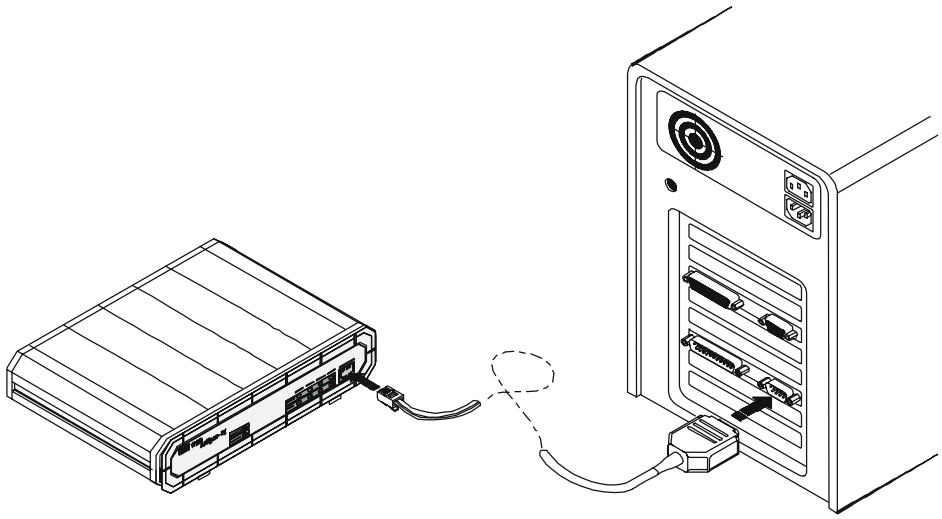


Figure 2-6. Connecting to the Terminal Emulator

Connecting to the LAN

A standard 10Base2 (BNC), or 10BaseT (RJ-45) connector is provided for connecting LANs.

➤ **To connect to the LAN(s):**

1. Attach an Ethernet cable to the 10BaseT, or 10Base2 port on the WEB RANger-II rear panel.
2. Attach the other end of the cable to the Hub/Repeater (see *Figure 2-7*). Use a cross Ethernet cable if you are connecting between WEB RANger-II and the LAN.

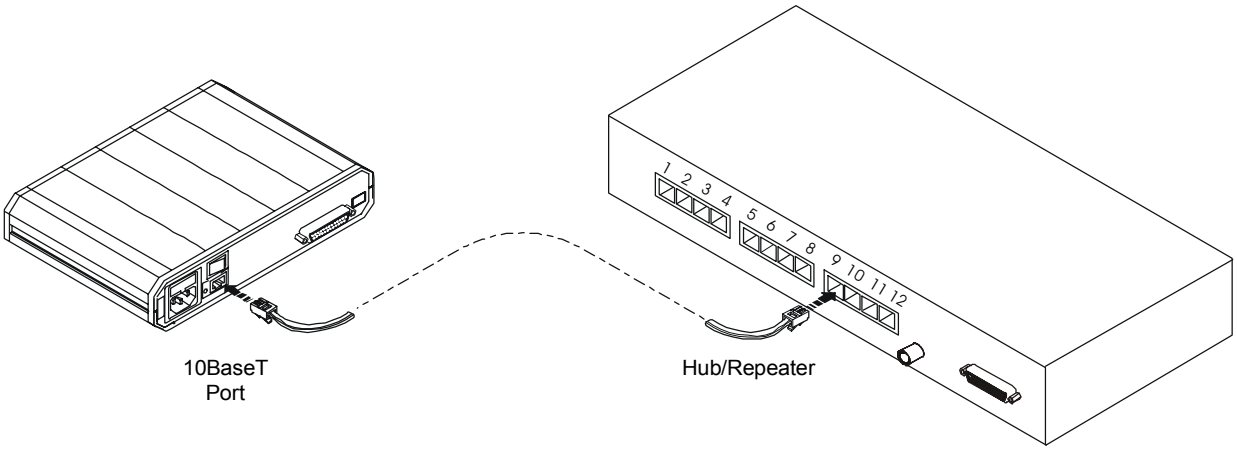


Figure 2-7. Connecting to the LAN

2.8 Operating Procedure

Power

Warning

GROUNDING - Always ground this unit through the protective earth lead of the power cable. Before connecting AC power to this unit, the mains plug should be inserted in a socket outlet provided with a protective earth contact only. The protective action must not be negated by use of an extension cord (power cable) without a protective conductor (grounding). Interrupting the protective (grounding) conductor (inside or outside the unit), or disconnecting the protective earth terminal can make this unit dangerous.

AC power should be supplied to WEB RANger-II through a standard power cable terminated by a standard three-prong plug.

A 1A slow-blow fuse is installed in the power supply unit.

Warning

To prevent electrical fire hazard, always replace the fuse with the same type and rating as indicated.

➤ **To connect the AC power:**

1. Check that the ON/OFF switch on the WEB RANger-II rear panel is set to OFF.
2. Connect the power cable to the connector on the WEB RANger-II rear panel.
3. Connect the power cable to the mains outlet.

➤ **To connect the DC power:**

1. Check that the ON/OFF switch on the WEB RANger-II rear panel is set to OFF.
2. Connect the power cable to the DC power connector.

Power-On

On the rear panel, switch POWER to the ON position. The POWER indicator lights up, indicating that WEB RANger-II is on.

Normal Operation

During normal operation, when the remote workstations are active, the READY indicator remains lit continuously, the activity indicators blink and the LAN and LINK error indicators remain off (refer to *Chapter 3*).

Power-Off

On the rear panel, switch POWER to the OFF position.

Chapter 3

Operation

Topics covered in this chapter include:

- Front panel options
- Initial operation and checks
- Connecting to the Internet/Intranet
- Initial setup program.

3.1 Initial Operation and Basic Checks

Figure 3-1 shows the various front panel options of WEB RANger-II with the controls and indicators. *Table 3-1* lists the controls and indicators that appear on WEB RANger-II front panels.

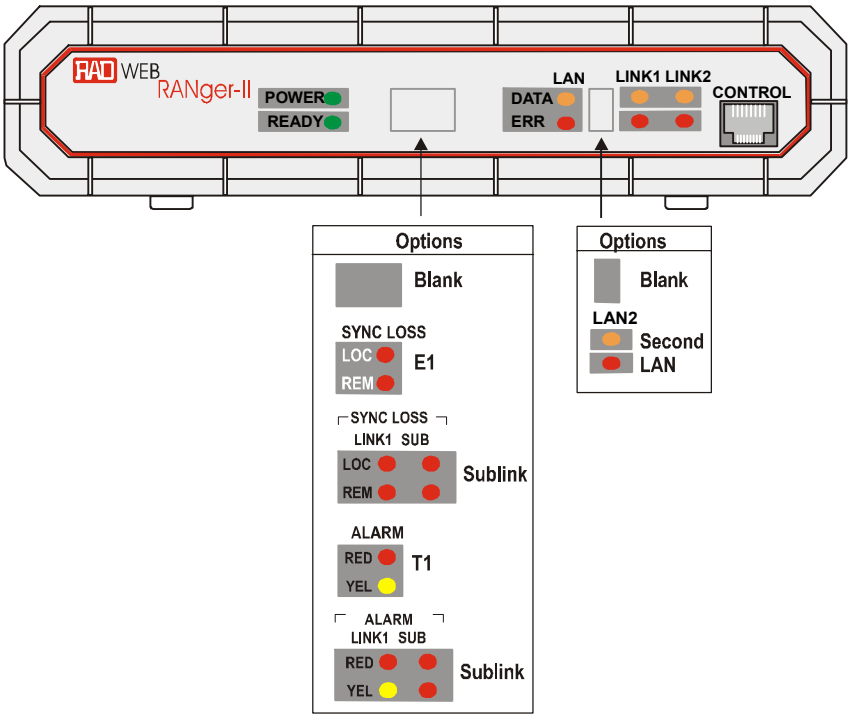


Figure 3-1. WEB RANger-II Front Panel Options

Table 3-1. WEB RANger-II Controls and Indicators

Object	Description	Function
POWER	Green LED	On – WEB RANger-II is powered on.
READY	Green LED	On – Packets can be transferred. (At least two interfaces are connected in the physical layer.)
LAN 1 DATA LAN 2 DATA	Yellow LED	On – a packet is received or transmitted on the LAN side.
LAN 1 ERR LAN 2 ERR	Red LED	On – a LAN interface indicates an error.
LINK 1 DATA LINK 2 DATA	Yellow LED	On briefly – a packet is received or transmitted on the LINK side.
LINK1 ERR LINK2 ERR	Red LED	Off – there is a physical connection and no LINK interface error. On briefly – LINK interface indicates an error. On continuously – there is no physical connection.
LINK1 RED ALARM	Red LED	On – T1 link is in RED ALARM. Local unit lost frame synchronization for more than 2.5 consecutive seconds.
SUB RED ALARM	Red LED	On – T1 link is in RED ALARM. Sublink of the local unit lost frame synchronization for more than 2.5 consecutive seconds.
LINK1 YELLOW ALARM	Yellow LED	On – T1 link is in YELLOW ALARM. Yellow alarm signal is sent from Remote Unit to inform the local unit that a RED ALARM exists at the remote end.
SUB YELLOW ALARM	Yellow LED	On – T1 sub link is in YELLOW ALARM. Yellow alarm signal is sent from Remote Unit to inform the sublink of the local unit that a RED ALARM exists at the remote end.
LINK1 LOC SYNC LOSS	Red LED	On – E1 link is in local sync loss alarm. Local unit lost frame synchronization for more than 2.5 consecutive seconds.
SUB LOC SYNC LOSS	Red LED	On – E1 sublink is in local sync loss alarm. Sublink of the local unit lost frame synchronization for more than 2.5 consecutive seconds.
LINK1 REM SYNC LOSS	Red LED	On – E1 link is in remote sync loss alarm. Remote sync loss signal is sent from remote unit to inform the local unit that a sync loss exists at the remote end.

Table 3-1. WEB RANger-II Controls and Indicators (Cont.)

Object	Description	Function
SUB REM SYNC LOSS	Red LED	On – E1 sublink is in remote sync loss alarm. Remote sync loss signal is sent from Remote Unit to inform the sublink of the local unit that a sync loss exists at the remote end.
CONTROL	Port (DCE)	Connects to a terminal for management.

3.2 Connecting to the Internet/Intranet

Use the following checklist to make sure you are ready to connect to the Internet/Intranet.

Internet Check List

1. Subscribe to the Internet Service Provider (ISP) and request a **static IP subnet**.
2. Make sure the **line** (Frame Relay or Leased) to the ISP is working properly.
3. Use the **static IP subnet** you have obtained to configure the WEB RANger-II **LAN IP host addresses** (see *Setup Menu* in Chapter 4).

Preparing Your PCs

1. Make sure your PCs have a correctly installed **TCP/IP stack.**
2. Assign an **IP address,** from the static IP subnet to each PC.
3. Ensure that each PC has the correct **subnet mask**.
4. Configure each PC with the WEB RANger-II as the **Default Gateway**.
5. Configure each PC with the ISP's DNS IP address.
6. Check that your Small Office LAN is correctly set up to work with IP.

3.3 Initial Setup Program

WEB RANger-II features a setup program that is invoked and run from an ASCII terminal or a PC terminal emulator. The terminal/terminal-emulator is connected to the RJ-45 CONTROL port on the WEB RANger-II front panel. Refer to *Chapter 2* for instructions on setting up this connection.

This section describes the procedures necessary to connect to the terminal and to access the setup program Main menu.

Connecting to the Terminal

➤ **To connect WEB RANger-II to the terminal:**

1. Set the terminal to work at baud rate 9.6 kbps, No Parity, 8 Data Bits, No Flow Control.
2. Connect a control cable between the WEB RANger-II RJ-45 CONTROL port and the connector on the terminal, or between the WEB RANger-II RJ-45 CONTROL port and the PC communication port.

   In general, some running operational messages will appear on the screen before you access configuration menus.

➤ **To invoke the login message:**

- Press one of the following keys several times: **<Enter>, <Space>,** or **<Esc>.**

Password Protection

Using a password prevents unauthorized personnel from changing configuration parameters.

Before you can access any WEB RANger-II configuration menus you will be prompted for login (see *Figure 3-2*).

```
Login:
```

Figure 3-2. Login Screen

Enter the correct password. The password can be changed or removed during configuration (see *Section 4-4*).

Factory default password: 1234

Notes

1. *Use of Password protection for the configuration module is recommended. Always use the **Exit** option in the Main Menu once the unit has been configured. Using the **Exit** option will force personnel requiring access to the configuration module to use password.*
2. *Password verification is case sensitive. Once the password is set, use the same case that you used when typing in the password.*
3. *The default password set by the factory is **1234**.*

The Main menu appears after you have completed the Login procedure. Select from the Quick Setup, Advanced Configuration, View, Security, or Diagnostic Tools menus.

Chapter 4

Configuration

Topics covered in this chapter include:

- Main menu
- Quick Setup Menu
- Security Setup Menu
- Advanced Options Menu
- Setup Menu
  - Host Parameters
  - Routing/Bridging
  - Interface Parameters
  - E1 and Voice Menu
  - Access Control
  - WAN Economy Menu
  - Factory Default Options
- Device Control Menu
  - Download Software Parameters
  - Upload Device Parameters.

4.1 Main Menu

The Main Menu hierarchy is shown in *Figure 4-1*.

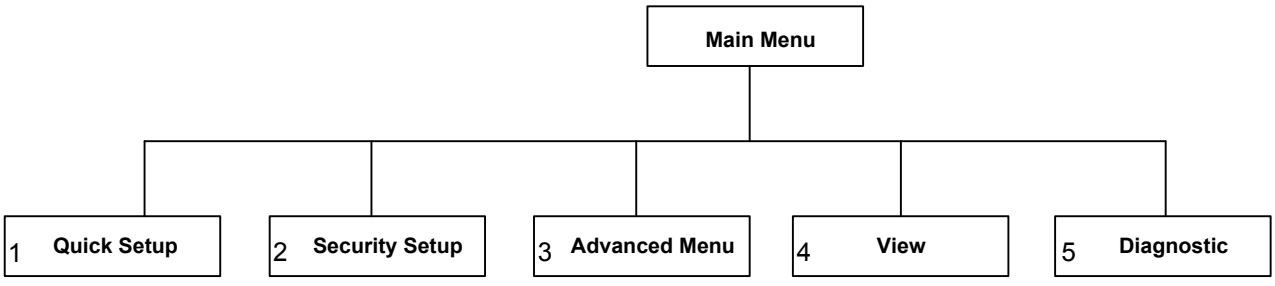


Figure 4-1. Main Menu Hierarchy

Quick Setup	Used to define the basic parameters for your WEB RANger-II unit. The Quick Setup menu allows you to adjust setup and link configuration parameters while WEB RANger-II is in operation. Line-by-line prompts guide you throughout the procedure. On-screen instructions and explanations guide you through the setup procedure. For a complete description of the Quick Setup menu refer to *Section 4.2*.
Security Setup	Used to control WEB RANger-II management and entry to your LAN by unauthorized users (see *Section 4.3*).
Advanced Menu	Lists WEB RANger-II configuration parameters and their current values. You can change these parameters and perform advanced configuration operations, not available through the Quick Setup menu. Resetting the device and software downloads are also performed via the Advanced Menu (see *Section 4.4*).
View	Used to view configuration screens and information on interface connections, routing tables and statistics (see *Chapter 5*).
Diagnostic Tools	Used to verify WAN and LAN connectivity. The Ping feature allows you to request another user on the LAN or WAN. If the remote user replies, connectivity is confirmed up to and including the IP level (see *Chapter 5*). This feature is recommended for devices configured as IP routers.
Exit	Select this option to return to the Operational Status Messages screen. In this mode you can view real-time information about the unit's activities.

Figure 4-2 shows the Main Menu. The name of the device connected to the terminal (WEB II) is listed at the top of the screen.

```
      MAIN  MENU   ( Device name - WEB II  )

  1.  Quick setup
  2.  Security setup
  3.  Advanced setup
  4.  View
  5.  Diagnostic tools


  0.  Exit
 Press number to select or ESC to return to the previous menu
```

Figure 4-2. WEB RANger-II Main Menu

➤ **To choose an option from the Main Menu:**

- Type the number preceding the option.

4.2 Quick Setup Menu

Introduction

The parameters listed on the Quick Setup Menu include most of the internetworking features of WEB RANger-II:

- WAN Interface
- IP Parameters
- Physical connections
- Protocol
- Routing type.

Setting Parameters

The Quick Setup screen presents messages that prompt you to accept or modify the current parameters. The parameter options are enclosed in brackets **[ ].**

➤ **To accept the current parameter:**

- Press **<Enter>**.

➤ **To view the options:**

- Toggle with the **<Space Bar>** and press **<Enter>.**

➤ **To enter new information:**

1. Type new information in the new parameters.
2. Press **<Enter>.**

➤ **To change the existing value:**

1. Press **<Backspace>**
2. Type new information.

After all parameters have been accepted or changed, you can view them on the screen. A confirmation message appears requesting that you confirm all the setup changes. The device may reset after saving these changes.

➤ **To configure the setup parameters:**

1. From the Main Menu, select option **1**, Quick Setup.
2. Follow the on-screen instructions to accept or modify the setup parameters.
3. Press **Y** to save the setup parameters.

Quick Setup Parameters

The Quick Setup menu contains both general parameters and those parameters specific to interfaces. This section organizes the parameter into various categories. The screen for each interface and a description of the options in the Quick Setup menu can be found in the sections that follow. Refer to the section that applies to the interface you ordered.

Table 4-1. Quick Setup Parameters

WAN Parameters	***General***	Link status
		Link mode
		Routing
		Protocol
		WAN IP Address (optional)
		WAN IP Mask (optional)
	E1/T1	E1/T1 Configuration
	Frame Relay	DCLI number
	ISDN	Protocol (ISDN)
		Bandwidth
		Connection Type
		Channel A – Destination Phone No.
		Channel B – Destination Phone No.
	V24 Async	Modem Type
		Baud Rate
LAN Parameters	***General***	LAN IP Address
		LAN IP Mask
		Default Gateway
		Default Gateway Interface
		Routing
	Security Parameters	Device Access Name
		Password
		Security Type

The Quick Setup Menu varies according to the options of WEB RANger-II that you have ordered. The following pages illustrate some of the Quick Setup menus that are available.

The fields in the Quick Setup screens are described below.

WAN Parameters

Link Status

This parameter specifies the link status.

Enable Transmits and receives frames. Normally you want all links in enabled status.

Disable Frames are not transmitted or received. The link may be permanently disabled, for example, when testing. A disabled line freezes all link operation, including connection attempts and forwarding.

Backup If a link is defined as backup to another, then whenever the main link operates normally, the backup link is *disabled*. If the main link fails, the backup link begins to operate and become *enabled*. You must that the routing settings are correct so that traffic will be forwarded to the desired destination via the backup link. When you restore the main link connection, the backup link becomes *disabled* again.

Link Mode

This parameter determines how data is transmitted across the link.

Synchronous Data bits are transmitted at a fixed rate. The sender and the receiver are synchronized.

Frame Relay A packet-switching protocol for connecting devices on a WAN (see *Figure 4-3*).

Asynchronous (for V.24 interface only).

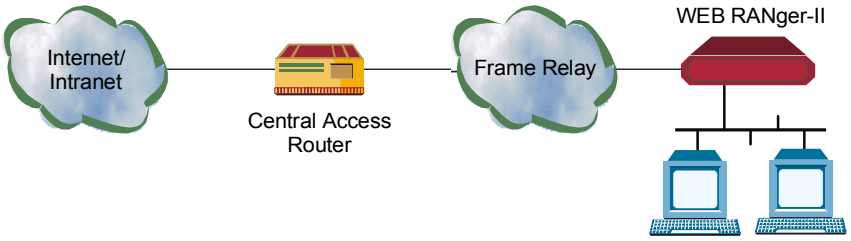


Figure 4-3. Frame Relay Hardware Setup

Routing

This parameter assigns a link forwarding type. Use the **<Space bar>** to toggle between values:

- **Bridge, IP, IPX**
- Any combination of these types.

Protocol

PPP Point to Point Protocol. PPP consists of 3 components:

- Encapsulation method for IP datagrams on a serial link. PPP supports either:
  - Asynchronous link with 8 bits of data and no parity.
  - HDLC synchronous links.
- LCP: Link control procedure to establish, configure, and test the data-link connection. Having an LCP allows each end to negotiate various options.
- NCP(s): A family of network control protocols specific to different network layer protocols. The NCPs allow each end to configure network control parameters.

PPP is often used across slow serial lines. It is therefore important to reduce the number of bytes per frame in order to reduce the latency time. Using LCP, most implementations negotiate to omitting the constant address and control fields and reducing the size of the protocol fields from 2 bytes to 1 byte. In addition, when using IP NCP, most implementations use Van Jacobson header compression to reduce the size of IP and TCP headers.

RFC-1490 Encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. RFC-1490 also supports a simple fragmentation procedure for carrying large frames over a frame relay network with a smaller MTU.

- **DLCI:** Every network interface card (NIC) has a Data Link Communication Identifier (DLCI) that uniquely identifies the node on the network. DLCI enables connection to the Frame Relay network without configuring Frame Relay parameters.
  DLCI executes congestion control when an explicit congestion notification is received for the DLCI from the Frame Relay network. The unit reduces the transmitted information rate of the DLCI and increases it when the congestion condition is cleared.

Factory setting: PPP

DLCI Number

This parameter permits you to enter new DLCIs for a link configured as Frame Relay.

LAN Parameters

Set the parameters in this section for each LAN connection.

Routing

This parameter sets the routing option. Refer to *Routing* on the previous page for more information.

Note *This parameter appears for the WR2/2U device only.*

LAN IP Address

Select this parameter to enter the IP address. Every device on a TCP/IP network must have an identification address. The IP address is a value consisting of the network address and the host address on that network. The value assigned to a network depends on the number of computers on that network.

The IP address is a 32-bit number. The number consists of 4 parts, where each part consists of 3 digits. One part of the address identifies the network and another part of the address identifies the host. The numbers in the address that identify the host depend on the class.

There are five classes of IP addresses. Each class represents a network having a certain number of computers. For example, a Class C address is given to a network having between 1–255 computers. *Table 4-2* gives the ranges for different classes of IP addresses.

Table 4-2. LAN IP Address - IP Classes

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

The numbers in each part of the code are translated into binary. The binary code identifies the network and the host.

IP addresses are assigned by the Internet Network Information Center (InterNIC). InterNIC assigns the network ID. Host IDs are assigned by the network administrator.

Figure 4-4 illustrates choosing LAN IP Addresses in Single IP or Regular Routing Mode.

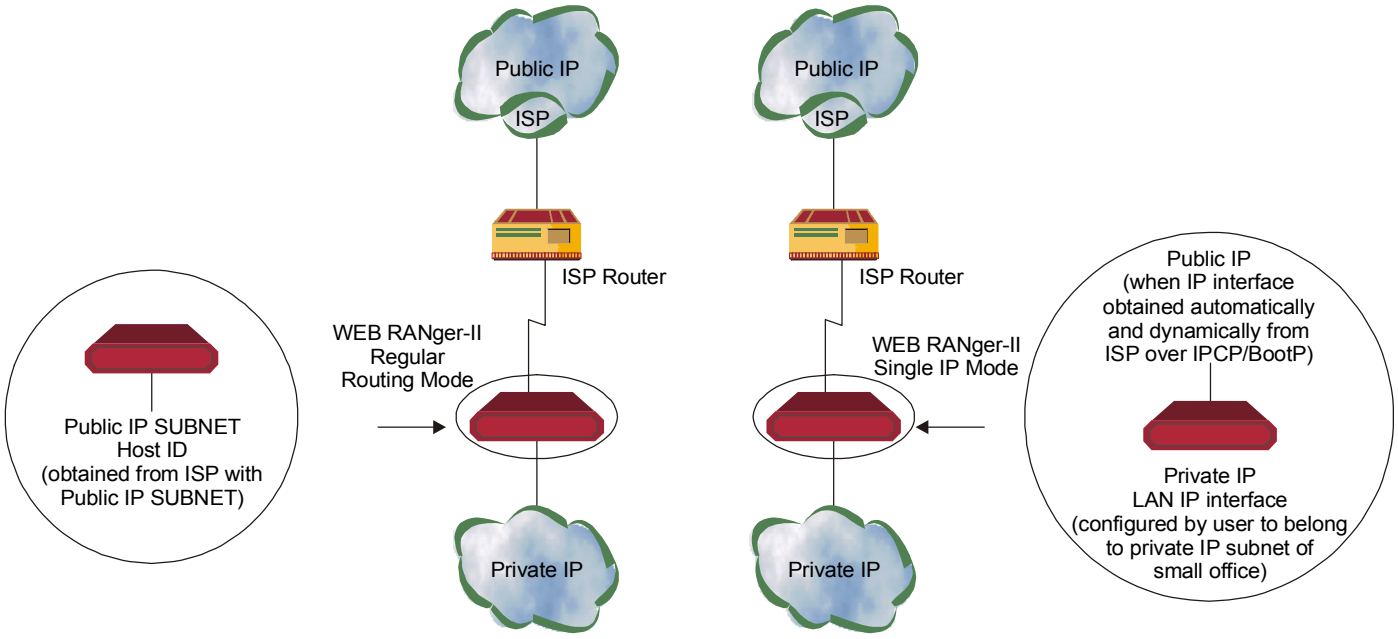


Figure 4-4. Choosing LAN IP Addresses in Single IP or Regular Routing Mode

LAN IP Mask

Select this parameter to enter the IP mask. The mask is configured automatically from the IP address class. If you want to change the default mask, enter a new mask. For example, the IP mask is usually 225.225.225.0. A mask like this would allow 254 hosts on the LAN. If you want to create a subnet that allows 6 users, including WEB RANger-II, configure the mask as 225.225.225.248. on WEB RANger-II, as well as each host included on the subnet (refer to *Figure 4-5*).

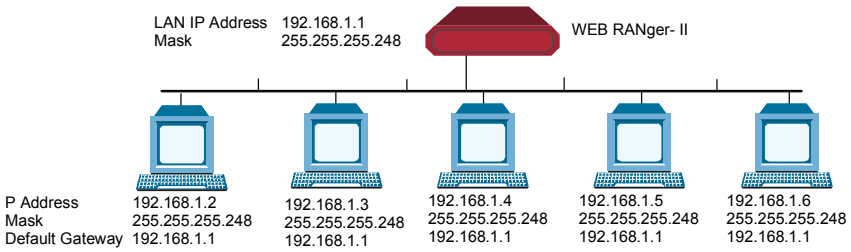


Figure 4-5. Setting up the IP Mask

Default Gateway Setting

Select this parameter to set the Default Gateway configuration. The default gateway is the address to which frames are sent, if no other address is defined in the routing table.

The default gateway can be an IP address or a WAN interface. If you choose an IP address, enter the address of the router that will deliver the frames. Specifying an IP address for the default gateway is done with shared media, such as LAN interface.

If you choose a WAN interface, the connection to the router is point-to-point. Choose **by interface** and enter interface/DLCI number (for Frame Relay).

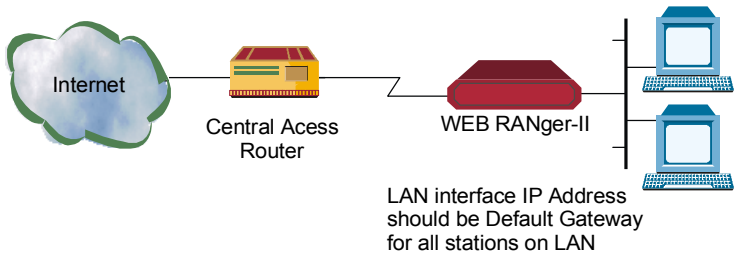


Figure 4-6. Default Gateway

Note *It is very important to obtain the correct parameters from the system administrator or ISP. The most common problem when establishing an IP connection is incorrect configuration of the IP parameters and Default Gateway.* ***Do not*** *try to guess these parameters.*

E1/T1 Parameters

E1/T1 Configuration

WEB RANger-II enables the user to setup the E1/T1 parameters if the hardware interface detected is E1 or T1.

ISDN Parameters

Protocol (ISDN)

This parameter assigns a protocol provided by the ISDN service in your area. Some additional parameters may be requested, depending on the selected protocol.

Bandwidth

This parameter assigns a bandwidth. The bandwidth is the rate at which data passes through the link. The greater the bandwidth, the more information can be sent through the link. WEB RANger-II allows you to work with a bandwidth of 56, 64, 112, or 128 kbps. If you select 112 or 128 kbps for protocols other than Leased or IDSL, MLPPP will be evoked.

Connection Type

This parameter specifies the type of connection to the Internet or Intranet.

Answer only Link used for receiving remote access connections

Answer&Originate Link used for both incoming and outgoing connections (not simultaneously)

Originate only Link used for outgoing connections only.

Destination Phone No.

This parameter defines phone number. To edit the phone number, erase the number with the **<Back space>** key and enter the new number. This parameter appears for **Originate** connection type only.

Connection

This parameter determines when the link between the local LAN and the Internet should be activated. Selecting **any frame to forward** activates the link only when there is traffic to be sent on the link. Selecting **always** keeps the link active, independent of traffic. The Connection parameter is important in reducing operating costs.

Frame Relay Parameters

DLCI Number

Enter new DLCI numbers with this parameter. To change or remove existing numbers, use the Advanced Menu.

V.24 Async Parameters

Modem Type

Select this parameter to select the modem type.

Baud Rate

Select this parameter to display the rate at which data is sent between WEB RANger-II and the modem. Use the **<Space Bar>** to toggle between the different baud rates. The Quick Setup default value is recommended for your modem.

Security Parameters

Device Access Name

Select this parameter to display the name assigned to WEB RANger-II for identification by the Internet Provider. To change the device access name, type in the new name and press **<Enter>**.

Device Access Password

Select this parameter to assign or update a password. The password is used to access the Internet.

Security Type

Select this parameter to permit access to all users (disable) or restrict access to allow/deny users whose profiles are defined (enable) in the system.

Quick Setup Menu Examples

The following pages illustrate some of the Quick Setup menus, dependent upon the interface that has been ordered.

Quick Setup for T1 (PPP, IP)

Figure 4-7 shows the Quick Setup menu for T1.

```
    QUICK SETUP

WARNING: This device automatically exits to Operational
          Messages 10 minutes after last keyboard action without
          saving parameters


'Enter' - Accept parameter, 'SPACE' - Change parameter.


WAN interface Link 1 - T1
 Link status          : [Enable  ]
 Link mode            : [Synchronous  ]
 Routing              : [IP ROUTER    ], Protocol: [PPP      ]
 WAN IP address       : 10.0.0.1, enter new : 10.0.0.1
 WAN IP mask          : 255.255.255.252, enter new: 255.255.255.252
 Do you want to configure the T1 Interface parameters (Y/N)?:
Host IP setup:
 LAN IP address       : 192.168.1.1, enter new : 192.168.1.1
 LAN IP mask          : 255.255.255.000, enter new : 255.255.255.000
 Default gateway setting by: [Interface ]
 Default gateway interface: 1
SECURITY Setup
 Device access name   : WR II
 No password at present – do you want to create password (Y/N)?: [N]
 Security type        : [Disabled]

Saving the changes might cause RESET the unit.
Do you want to save QUICK SETUP (Y/N) ? Y
```

Figure 4-7. T1 Interface Quick Setup Screen

Quick Setup for E1 (PPP, IP) + ISDN (Backup, 128K, PPP, IP)

Figure 4-8 shows the Quick Setup menu for E1.

```
    QUICK SETUP

WARNING: This device automatically exits to Operational
         Messages 10 minutes after last keyboard action without
         saving parameters


 'Enter' - Accept parameter , 'SPACE' - Change parameter.

 WAN interface Link 1 - E1
  Link status          : [Enable  ]
  Link mode            : [Synchronous  ]
  Routing              : [IP ROUTER    ], Protocol: [PPP      ]
  WAN IP address       : 10.0.0.1, enter new : 10.0.0.1
  WAN IP mask          : 255.255.255.252, enter new: 255.255.255.252
  Do you want to configure the E1 Interface parameters (Y/N)?:

 WAN interface Link 2/CH1 - BRI
  Link status          : [Backup  ] to interface:  [LINK 1   ]
  Routing              : [IP ROUTER    ], Protocol: [PPP      ]
  WAN IP address       : 0.0.0.0, enter new : 0.0.0.
  Protocol             : [ETSI    ]
  Bandwidth            : [128 ]
  Connection Type      : [Originate only   ]
  Channel A - Destination phone number: 1234
  Channel B - Destination phone number: 5678
  Connection           : [Always        ]

 Host IP setup:
  LAN IP address : 192.168.1.1, enter new : 192.168.1.1
  LAN IP mask    : 255.255.255.000, enter new : 255.255.255.000
  Default gateway setting by: [Interface ]
  Default gateway interface: [LINK 1   ]

 SECURITY Setup
  Device access name : WR II
  No password at present - do you want to create password (Y/N)?: [N]
  Security type: [Disabled]

 Saving the changes might cause the unit to RESET.
 Do you want to save QUICK SETUP (Y/N) ? N
```

Figure 4-8. E1 Interface Quick Setup Screen

Quick Setup for V.35 (Frame relay, IP+IPX) + 2 LANs (IP+IPX)

Figure 4-9 shows the Quick Setup menu for V.35.

```
   QUICK SETUP

WARNING: This device automatically exits to Operational
          Messages 10 minutes after last keyboard action without
          saving parameters


'Enter' - Accept parameter, 'SPACE' - Change parameter.


WAN interface Link 1 - V.35
 Link status          : [Enable  ]
 Link mode            : [Frame relay  ]
 Routing              : [IP & IPX ROUTER    ], Protocol: [RFC 1490      ]
 Number of DLCIs to configure: 2
 Enter DLCI id number (16-991): 16
 WAN IP address       : 10.0.0.1, enter new : 10.0.0.1
 WAN IP mask          : 255.255.255.252, enter new: 255.255.255.252
 Enter DLCI id number (16-991): 17
 WAN IP address       : 20.0.0.1, enter new : 20.0.0.1
 WAN IP mask          : 255.255.255.252, enter new: 255.255.255.252

LAN 1 settings:
 Routing              : [IP & IPX ROUTER ]
 LAN IP address       : 192.168.1.1, enter new : 192.168.1.1
 LAN IP mask          : 255.255.255.000, enter new : 255.255.255.000
LAN 2 settings:
 Routing              : [IP & IPX ROUTER ]
 LAN IP address       : 192.168.2.2, enter new : 192.168.2.2
 LAN IP mask          : 255.255.255.000, enter new : 255.255.255.000
 Default gateway setting by: [Interface ]
 Default gateway interface: 1 DLCI: 16

Saving the changes might cause RESET the unit.
Do you want to save QUICK SETUP (Y/N)? Y
```

Figure 4-9. V.35 Interface Quick Setup Screen

Quick Setup for V.24 (Asynchronous, PPP, IP, Answer Only, Security Enabled) + V.35 (PPP, IP)

Figure 4-10 shows the Quick Setup menu for V.24.

```
    QUICK SETUP

WARNING: This device automatically exits to Operational
         Messages 10 minutes after last keyboard action without
         saving parameters
'Enter' - Accept parameter, 'SPACE' - Change parameter.


WAN interface Link 1 – V.24
 Link status          : [Enable  ]
 Link mode            : [Asynchronous  ]
 Routing              : [IP ROUTER    ], Protocol: [PPP      ]
 WAN IP address       : 0.0.0.0, enter new : 0.0.0.0
 Modem type: Unlisted Modem
   Do you want to change modem type (Y/N)? : [N]
 Baud rate            : [19,2 ] kbps
 Connection type      : [Answer only    ]
 Connection           : Always       ]
WAN interface LINK 2    – V.35
 Link status          : [Enable  ]
 Link mode            : [Synchronous  ]
 Routing              : [IP ROUTER    ], Protocol: [PPP      ]
 WAN IP address       : 0.0.0.0, enter new : 0.0.0.0
Host IP setup:
 LAN IP address       : 192.168.1.1, enter new : 192.168.1.1
 LAN IP mask          : 255.255.255.000, enter new : 255.255.255.000
 Default gateway setting by: [Interface ]
 Default gateway interface: [LINK 2  ]
SECURITY Setup
 Device access name   : WR II
 No password at present – do you want to create password (Y/N)?: [N]
 Security type        : [Enabled]

Saving the changes might cause RESET the unit.
Do you want to save QUICK SETUP (Y/N) ? Y
```

Figure 4-10. V.24 Interface Quick Setup Screen

Settings for V.35+1 LAN, V.35+2 LANs

Figure 4-11 shows the Quick Setup menu for 1 or 2 LANs.

```
     QUICK SETUP

WARNING: This device automatically exits to Operational
           Messages 10 minutes after last keyboard action without
           saving parameters
  'Enter' - Accept parameter, 'SPACE' - Change parameter.


  WAN interface #1 - V.35
    Connection type: [Uplink  ]
    Link mode: [Frame Relay    ]
    Routing: [IP & IPX ROUTER ], Protocol: [RFC 1490   ]
    Number of DLCIs to configure: 2
    Enter DLCI id number (16-991): 16
    WAN IP address: 10.0.0.1 , enter new : 10.0.0.1
    WAN IP mask   : 255.255.255.252 , enter new : 255.255.255.252
    Do you want to enable SINGLE IP option (Y/N)? : [N]
    Enter DLCI id number (16-991): 18
    WAN IP address: 10.1.1.5 , enter new : 10.1.1.5
    WAN IP mask   : 255.255.255.252 , enter new : 255.255.255.252
    Do you want to enable SINGLE IP option (Y/N)? : [N]


  LAN 1 settings:
    Routing: [IP & IPX ROUTER ]
    IP address : 192.168.2.1 , enter new : 192.168.2.1
    IP mask    : 255.255.255.0 , enter new : 255.255.255.0
  LAN 2 settings:
    Routing: [IP & IPX ROUTER ]
    IP address : 192.168.3.1 , enter new : 192.168.3.1
    IP mask    : 255.255.255.0 , enter new : 255.255.255.0
  Default gateway setting by: [Interface ]
    Default gateway interface: 1 DLCI: 18


  Saving the changes might cause RESET the unit.
  Do you want to save QUICK SETUP (Y/N) ? Y
```

Figure 4-11. V.35+ 2 LANs Quick Setup Screen

4.3 Security Setup Menu

Topics covered in this section include:

- Device Access Restriction
  - Enabling TELNET Access
  - Enabling SNMP Access
  - Changing Login Password
  - Firewall Options
- IP Address translation.

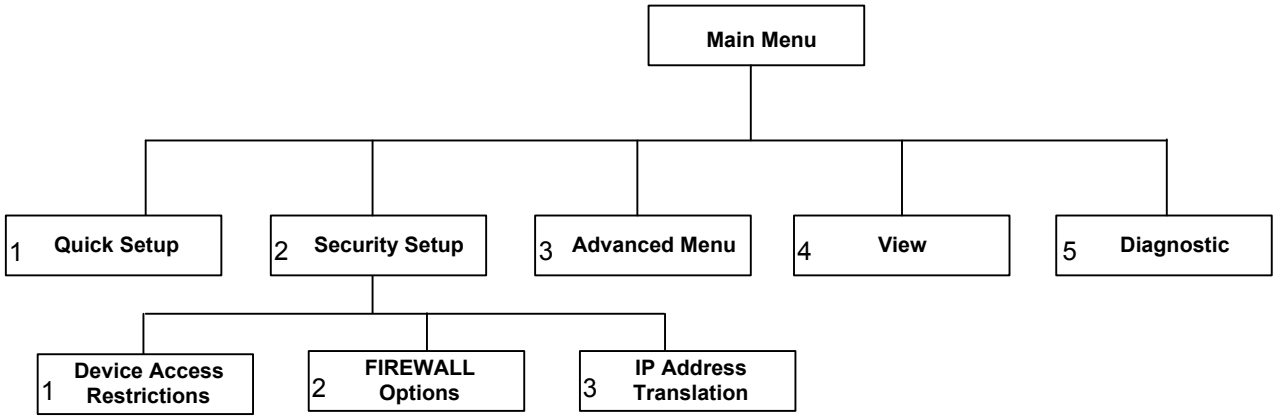


Figure 4-12. Security Setup Menu Outline

The Security Setup menu allows you to control access to WEB RANger-II and access to the LAN. WEB RANger-II is protected against access by unauthorized users by disabling access via SNMP and TELNET. The Solid Firewall is used to protect the LAN against undesired entry.

➤ **To access the Security Setup Menu:**

1. In the Main menu, press **2**.

   The Security Setup menu appears (see *Figure 4-13*).

```
      SECURITY SETUP  ( Device name - WEB II  )


   1.  Device access restrictions
   2.  FIREWALL options
   3.  IP address translation
   ESC - Return to previous menu

  Choose one of the above:
```

Figure 4-13. Security Setup Menu

The Security Setup options are described below.

Device Access Restriction

Security Setup
↓1
Device Access Restriction

Parameters listed on this screen allow you to control access to WEB RANger II configuration from the control port or from LAN/WAN (via Telnet and SNMP).

Enabling TELNET Access

WEB RANger-II supports TELNET. This allows WEB RANger-II to be configured and controlled over the WAN and LAN using TCP/IP.

Access to TELNET requires authentication by the device, using the password.

By default, TELNET access to WEB RANger-II is disabled to prevent changes being made to the unit's configuration parameters.

➤ **To enable TELNET access:**

1. From the Security Setup menu, select option **1**, Device Access Restrictions.
2. From the Device Access Restrictions menu, select option **1**, TELNET Access Status and change it to **Enable**.
3. Select options **2** and **3** to change the user name and password, if required.

WEB RANger-II can now be accessed using your TELNET username and password.

Enabling SNMP Access

By default, access to WEB RANger-II via SNMP is disabled. Blocking SNMP access prevents changes being made to the unit's configuration parameters.

➤ **To enable SNMP access:**

1. From the Security Setup menu, select option **1**, Devise Access Restrictions.
2. From the Devise Access Restrictions menu, select option **4**, SNMP Access Status and change it to **Enable**.
3. Select options **5**, **6**, and **7** to change Read, Write and Trap communities, if required.

WEB RANger-II can now be accessed for SNMP operation using the appropriate communities.

Changing Login Password

Entrance to configuration screens, via terminal from the control port, is set by the factory default as *Protected by Password*. The **default password** is ***1234***.

➤ **To change the password or remove password protection:**

1. From the Security Setup menu, select option **1**, Device Access Restrictions.
2. From Device Access Restrictions menu, select option **8**, Monitor User Password.
3. Enter a new value for Password.

Note *Leaving Password blank removes login protection.*

Firewall Options

Firewall Option

Security Setup
↓2
Firewall Options

Solid Firewall is a rule-based security mechanism, which monitors incoming and outgoing traffic and allows or restricts access according to the user-defined criteria (rules).

You can configure the Solid Firewall to monitor incoming or outgoing traffic on any WAN and LAN link. The firewall blocks all traffic coming from the unprotected network segment to the protected section, and allows traffic from protected to unprotected segments. Only those applications that are enabled via the application list (e.g. HTTP, FTP, POP3 servers, etc.) are allowed for use. By default, the Solid Firewall is disabled.

➤ **To select the Solid Firewall interface and direction:**

1. From the Main menu, select option **2**, Security Setup.
2. From the Security Setup menu, select option **2**, Firewall Options.
   The Firewall Setup menu appears (see *Figure 4-15*).
3. From the Firewall Setup menu, type **1**.
   The Firewall Interface menu appears (see *Figure 4-16*).
4. From the Firewall Interface menu, type **A** and define the link on which you intend to set the firewall and traffic type to monitor:
   - **Inbound** – The firewall blocks the traffic coming into WEB RANger-II via the link on which the firewall is enabled. The firewall forwards the traffic going out of the firewall-protected interface to its destination.
   - **Outbound** – The firewall blocks the traffic going out of WEB RANger-II via the link on which the firewall is enabled. The firewall grants access to the traffic coming into WEB RANger-II from the network segment attached to the firewall-protected interface.
5. Press <ESC> and save new values.

➤ **To define the Solid Firewall rules:**

1. From the Firewall Setup menu, type **2**.
   The Firewall Rules menu appears (see *Figure 4-17*).
2. From the Firewall Rules menu, type **A** and do the following:
   - Define a link on which the rule will be applied
   - Specify the source IP address range by defining the start and end addresses.
   - Specify the destination IP address range by defining the start and end addresses.
   - Enable the application used by the rule (**user defined**, **Telnet**, **Ping**, **HTTP**, **FTP**, **TFTP**, **POP3**, **SMTP**, **SNMP**, **SNMP Trap**, **BOOTP/DHCP**, **DNS Client to Server**, or **DNS Server to Server**).

- If you select a user-defined application, you must specify the following parameters:
  - Protocol type: **TCP**, **UPD** or **ICMP**
  - **Minimum** and **maximum port value** for TCP and UDP protocols, or **ICMP message type** for ICMP protocol.

3. Press <ESC> and save new firewall rule values.

   For example, two LANs are connected to the WEB RANger-II 10BaseT ports (see *Figure 4-14*). LAN 1 includes company's Web, mail and FTP servers, which cab be accessed from the outside. Employees' PCs sitting on LAN 2 must not be reached from the outside, but they must be allowed to access the servers. In order to grant access to LAN 1 and restrict it to LAN 2, you must set up two firewalls:

   Firewall 1

   - Select interface – main link
   - Select direction – inbound
   - Define rule 1 for Web server:
     - Start and end source IP address – 000.000.000.000 to 255.255.255.255
     - Start and end destination IP address – 192.111.111.111
     - Protocol – HTTP.
   - Define rule 2 for mail server, which is identical to rule 1, except for destination IP addresses (192.111.111.112) and protocol (SMTP).
   - Define rule 3 for FTP server, which is identical to rule 1, except for destination IP addresses (192.111.111.113) and protocol (FTP).

   Firewall 2

   - Select interface – LAN 2
   - Select direction – outbound.

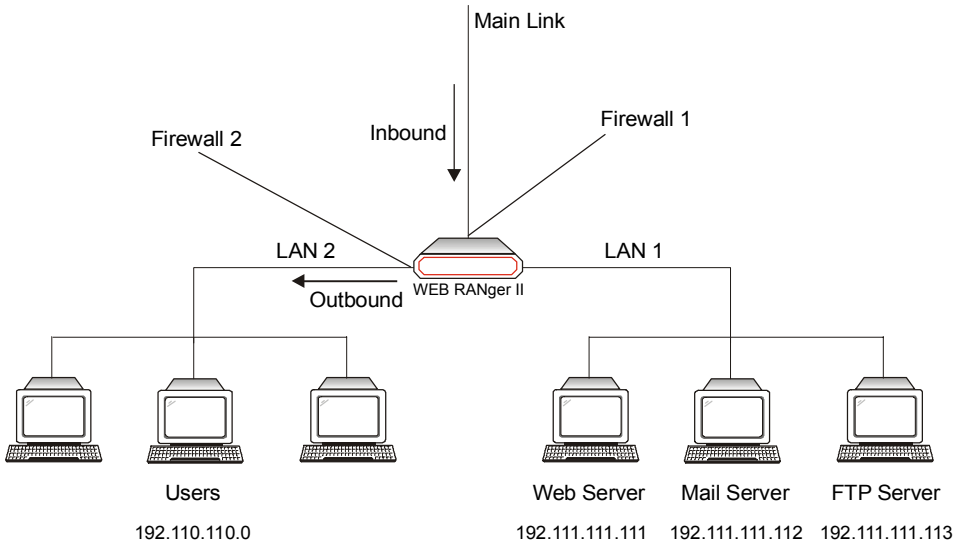


Figure 4-14. Configuring Firewalls

```
 FIREWALL SETUP  ( Device name - WEB RANger-II )
--------------

     1.  FIREWALL Interfaces
     2.  FIREWALL Rules

     ESC - Return to previous menu




     Choose one of the above:
```

Figure 4-15. Firewall Setup Menu

```
 FIREWALL INTERFACES  ( Device name - WEB RANger-II )
--------------
     Interface      Direction



     OPTIONS: A-Add

Press one of the above or ESC to return to previous screen:
        Select interface: [LINK 1    ]
        Select Direction: [Inbound  ]
```

Figure 4-16. Firewall Interfaces Menu

```
 FIREWALL RULES  ( Device name - WEB RANger-II )
--------------
     Interface      Direction

OPTIONS: A-Add

Press one of the above or ESC to return to previous screen:
   Select interface: [LINK 1    ]
   Enter start source IP address: 000.000.000.000
   Enter end source IP address  : 222.222.222.222
   Enter start destination IP address   :
   Enter end destination IP address     :
   Select application type: [Telnet       ]
```

Figure 4-17. Firewall Rules Menu

IP Address Translation (NAT)

Security Setup
↓2
IP Address Translation

IP Address Translation allows a NET, that uses a private IP Address, to connect to the Public Internet/Intranet (Single IP is one of the IP Address Translation types).

```
IP ADDRESS TRANSLATION (Device name - WEB RANger-II)
----------------------
   Type    Interface   Status                    Range


OPTIONS: A-Add
Press one of the above or ESC to return to previous screen:
```

Figure 4-18. IP Address Translation Menu

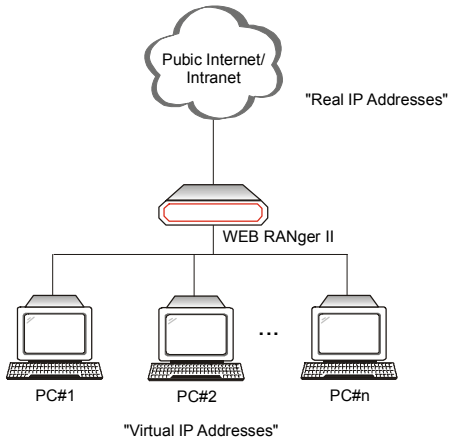


Figure 4-19. IP Address Translation

IP Address Translation permits some, or all, PCs on your private LAN to be represented with legal IP Addresses that are defined on the internet/Intranet (refer to *Figure 4-19).*

WEB RANger-II supports the following types of IP Address Translation types:

- **Static Single** – a PC with its Virtual Address specified will have access to the Internet/Intranet with a legal, real IP Address. Bidirectional one-to-one access is allowed.
- **Static Range** – PCs with their Virtual Addresses within the specified range will have access to the Internet/Intranet with a legal, real IP Address range. Bidirectional N-to-N access is allowed.
- **Concurrent** – a number of PCs (n) with their Virtual Addresses within the specified range will have access, but only some of them (m) can work simultaneously (m<n). The application must be started from the private LAN.
- **Transparent** – address translation is not performed for a specified range of IP Addresses. This setup may be used for the application shown in *Figure 4-20*.
- **PAT (Port Address Translation)** – WEB RANger-II connects a UDP or TCP port to a specified IP address. PAT is available for single IP only.

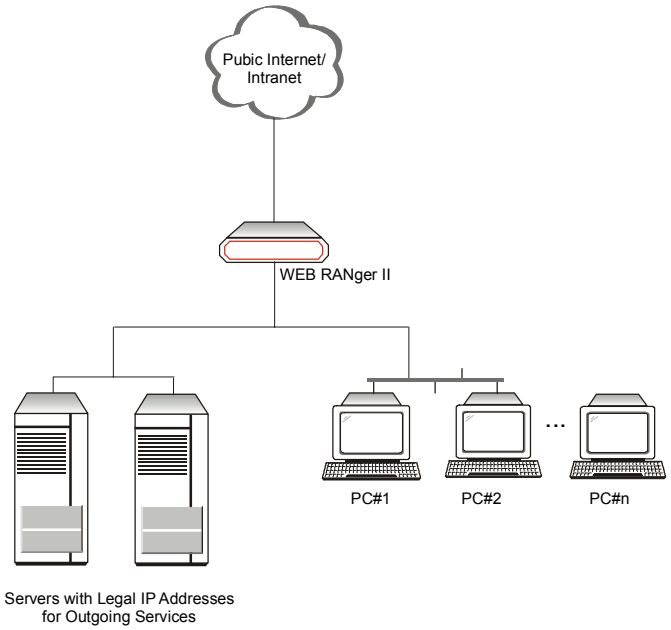


Figure 4-20. IP Address Transparent

- **Single IP** – the whole Private LAN is represented as a single legal IP Address on Internet/Intranet.

Note *For Static and Concurrent Address Translation, all PCs on your LAN with IP Addresses not covered by the listed definitions will not obtain access to the Internet/Intranet.*
You may enter more than one entry of each type.
Each definition in a list may be Enabled or Disabled separately.

4.4 Advanced Options

The Advanced Menu contains the majority of WEB RANger-II configuration parameters. You can change these parameters and perform advanced configuration operations that are not available through the Quick Setup menu. Resetting the WEB RANger-II and software downloads are also performed via the Advanced Menu.

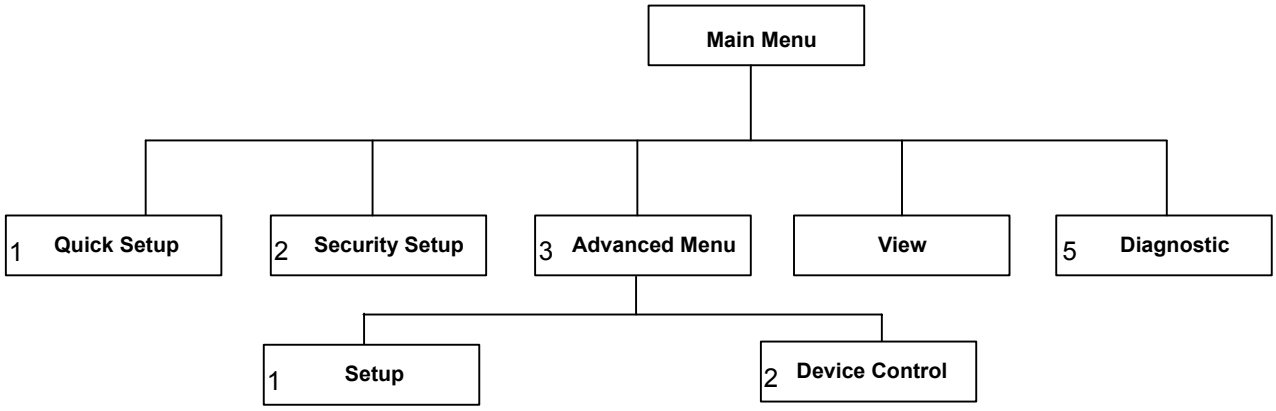


Figure 4-21. Advanced Menu Outline

➤ **To access the Advanced Menu:**

1. In the Main Menu, press **3**.

   The Advanced Menu appears (see *Figure 4-22*).

```
     ADVANCED  MENU  ( Device name - WEB II  )


1.  Setup
2.  Device control
ESC - Return to previous menu


Choose one of the above:
```

Figure 4-22. Advanced Menu

The options in the Advanced Menu are:

- Setup - modifies setup parameters.
- Device Control - downloads software and parameters, performs reset operations.

These options are described in the sections below.

4.5 Setup Menu

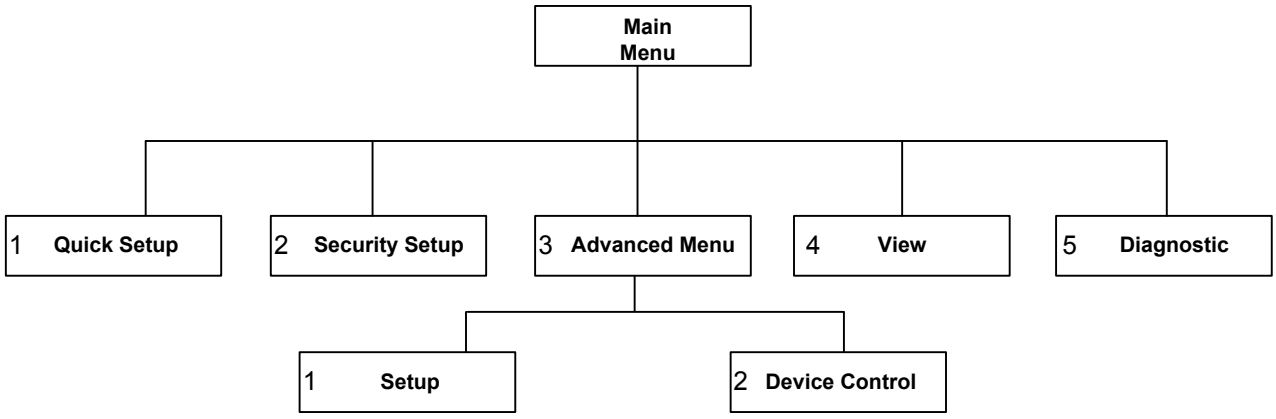


Figure 4-23. Setup Menu Map

➤ **To access the Setup menu:**

- In the Advanced Menu, press **1**.

The Setup menu appears (see *Figure 4-24*).

```
     SETUP  ( Device name - WEB II  )


 1.  Host parameters
 2.  Routing / Bridging
 3.  Interface parameters
 4.  Access control (Security)
 5.  WAN economy
 6.  Factory default options
Press number to select or ESC to return to the previous menu:
```

Figure 4-24. Setup Menu

The options in the Setup menu are briefly described below. For a detailed description of the sub-menus, refer to the sections that follow.

Host Parameters To enter reference information about the device, the IP Host, the SNMP agent and TFTP.

Routing To enter WEB RANger-II routing information.

Interface Parameters To set general parameters and link, Frame Relay, ISDN or E1/T1 parameters.

Access Control (Security) To perform security operations.

WAN Economy To reduce traffic over the WAN and to keep the link up only when necessary.

Factory Default Options To return settings to the factory default.

Host Parameters

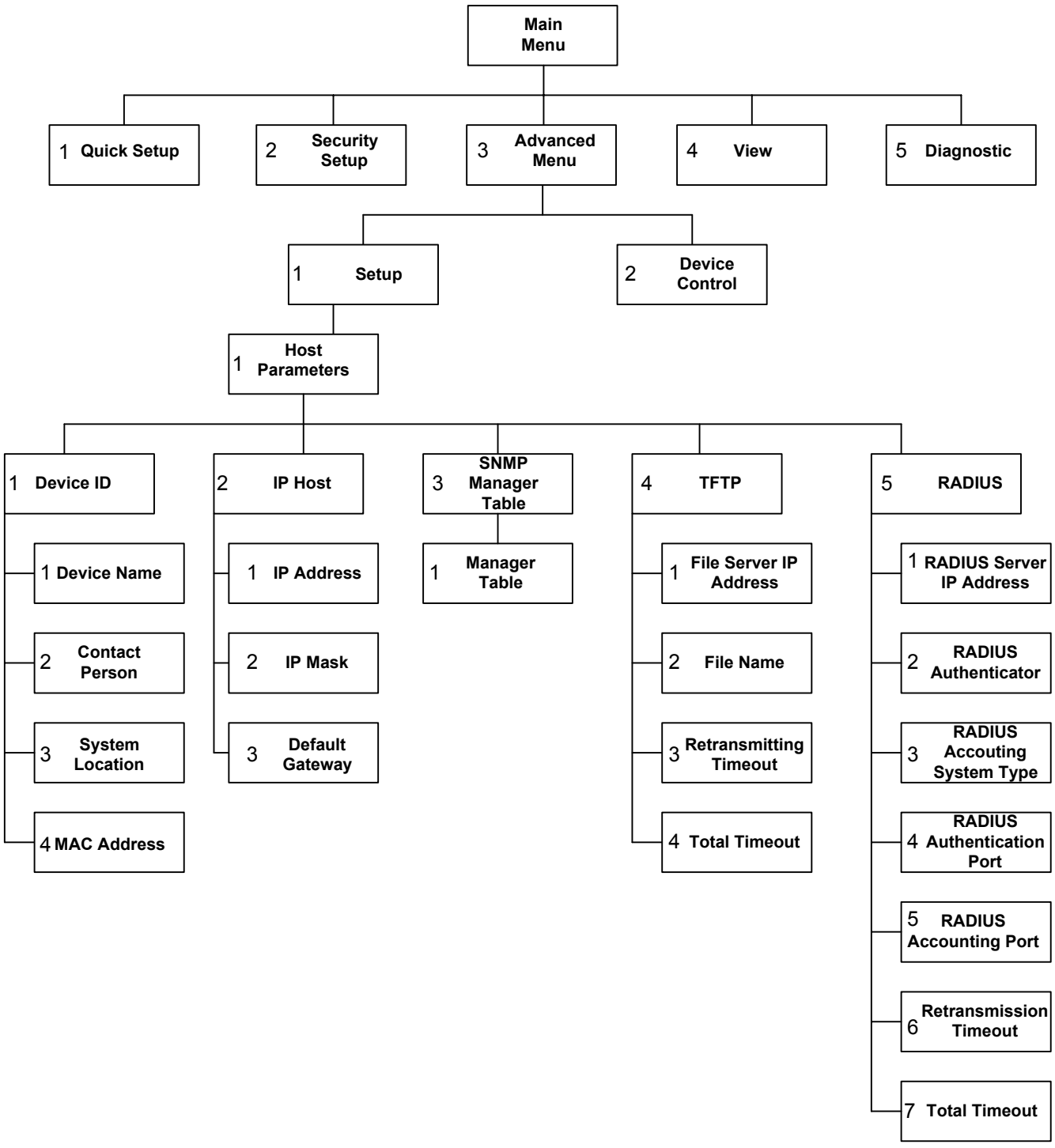


Figure 4-25. Host Parameters Menu Outline

➤ **To access the Host Parameters menu:**

1. In the Advanced Menu, press **1**.
   The Setup menu appears.
2. In the Setup menu, press **1**.
   The Host Parameters menu appears (see *Figure 4-26*).

```
     HOST PARAMETERS  ( Device name - WEB II  )


  1.  Device ID
  2.  IP host
  3.  SNMP manager table
  4.  TFTP
  5.  RADIUS


  ESC - Return to previous menu


  Choose one of the above:
```

Figure 4-26. Host Parameters Menu

The options in the Host Parameters menu are described below.

Device ID

Advanced Menu
↓1
Setup
↓1
Host Parameters
↓1
Device ID

Select this option to view and/or modify the following parameters.

Device Name

Select this parameter to assign an arbitrary name to WEB RANger-II for identification by the system manager; for example "accounting".

Contact Person

Select this parameter to enter the name of the person to be contacted with matters pertaining to the system; for example "John Doe".

System Location

Select this parameter to enter the physical location of the device; for example "Building 3 Floor 4".

MAC Address

Select this parameter to assign a MAC address locally. This allows you additional control of the devices in the LAN. WEB RANger-II can be used with the burned-in (default) address provided by the manufacturer or with a locally administered address; for example 4020 2D16 1234. Locally administered addresses are very useful for managing large networks.

IP Host

Advanced Menu
↓1
Setup
↓1
Host Parameters
↓2
IP Host

Select this option to configure the following IP parameters.

IP Address

Every device on a TCP/IP network must have an address for identification. The IP address is a value consisting of the network address and the host address on that network. The value assigned to a network depends on the number of computers on that network.

The IP address is a 32-bit number. The number is made up of 4 parts, with each part consisting of 3 digits. One part of the address identifies the network and another part of the address identifies the host. The numbers in the address, which identify the host, are dependent on the class.

There are 5 classes of IP addresses. Each class represents a network having a certain number of computers. For example, a Class C address is given to a network having between 1-255 computers. *Table 4-3* gives the range for different classes of IP addresses.

Table 4-3. IP Host - IP Classes

Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 247.255.255.255

The numbers in each part of the code are translated into binary. The binary code identifies the network and the host.

IP addresses are assigned by the Internet Network Information Center (InterNIC). InterNIC assigns the network ID. Host IDs are assigned by the network administrator.

IP Mask

A subnet is a portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices whose IP addresses begin with 133.100.100. are part of the same subnet. An IP mask allows you to filter IP addresses on a subnet.

When an IP address is configured, the IP mask is automatically configured according to *Table 4-4*.

Table 4-4. IP Masks

IP Network Class	IP Address Range	Default IP mask
A	0.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	255.255.255.225

The default IP mask can be edited.

Default Gateway

The default gateway defines where frames will be sent, if no explicit routing is defined in the routing table.

The default gateway can be an IP address or a WAN interface. If you choose to use an IP address, enter the address of the router that will deliver the frames. Specifying an IP address for the default gateway is done with shared media, such as LAN interface.

If you choose to use a WAN interface, the connection to the router is point-to-point. Select **by interface** and enter the interface/DLCI number.

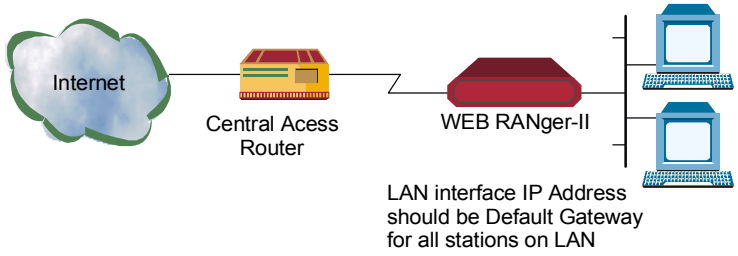


Figure 4-27. Default Gateway

Note *It is very important to obtain the correct parameters from the system administrator or ISP. The most common problem when establishing an IP connection is incorrect configuration of the IP parameters and default gateway.* ***Do not*** *try to guess these parameters.*

SNMP Manager Table

Advanced Menu
↓1
Setup
↓1
Host Parameters
↓3
SNMP Manager Table

Select this option to add, clear or delete parameters from the manager table. The manager table lists the SNMP manager IP addresses and masks.

Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP to access management information data (such as packets per second and network error rates), network administrators can more easily manage network performance and find and solve network problems.

TFTP (Trivial File Transfer Protocol)

Advanced Menu
↓1
Setup
↓1
Host Parameters
↓4
TFTP

TFTP is a simple file transfer protocol running over IP that permits unsecured and unauthorized file exchange over the Internet/Intranet. TFTP is widely used time to upgrade software and configuration parameters for various standalone units. TFTP is a client-server type protocol; WEB RANger-II operates as the TFTP client. In order to use the TFTP-based features of WEB RANger-II you need TFTP server software running on some of your PCs.

This screen permits you to configure common TFTP session parameters that are used for software upgrades and upload/download features (see *Device Control Menu*).

Retransmission Timeout

Select this parameter to enter the amount of time that is allowed to pass before the last non-acknowledged request is transmitted, for example 30 seconds.

Total Timeout

Select this parameter to enter the amount of time WEB RANger-II should wait for an acknowledgment from the TFTP server (for example 60 seconds) in case a frame is lost, or there are other problems.

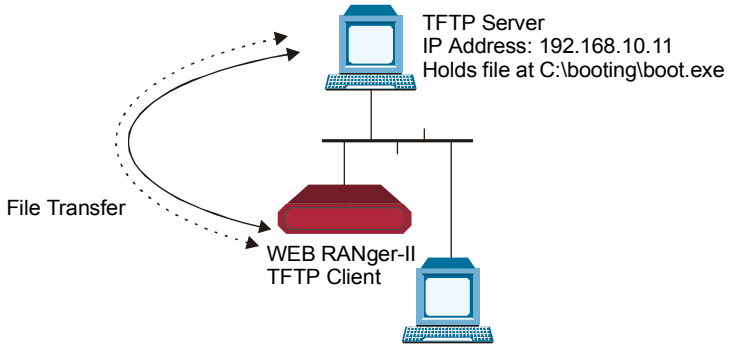


Figure 4-28. File Transfer to and from TFTP Server

RADIUS Authentication and Billing

Advanced Menu
↓1
Setup
↓1
Host Parameters
↓5
RADIUS

The RADIUS (Remote Authentication Dial-In User Service) is a client/server security protocol. Security information is stored in a central location, known as the RADIUS server. RADIUS clients, such as WEB RANger-II, communicate with the RADIUS server to authenticate users. Although the term RADIUS refers to the network protocol that the client and server use to communicate, it is often used to refer to the entire client/server system.

The three main functions of RADIUS are:

- Authentication
- Authorization
- Accounting.

To perform these functions, you must configure the parameters below.

RADIUS Server IP Address

Select this parameter to enter the IP address of the RADIUS server, for example, 192.168.1.9. Refer to *Figure 4-29*.

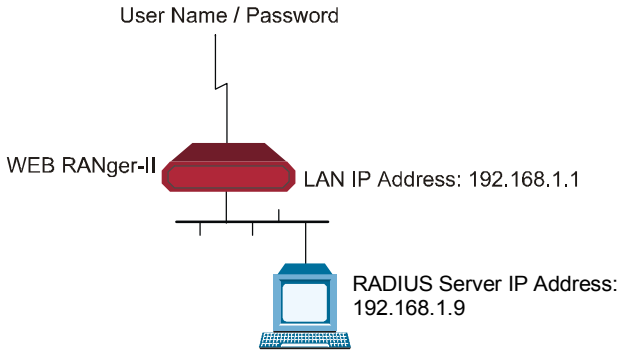


Figure 4-29. Setting up the RADIUS Server

RADIUS Authenticator

Select this parameter to enter the *shared secret*. The *shared secret* is a password used by RADIUS to authenticate the client. It is important to remember that the client is WEB RANger-II. Do not supply the shared secret.

Note *When configuring the RADIUS Authenticator, be sure to use the same value in the RADIUS server and WEB RANger-II.*

RADIUS Accounting System Type

Select this parameter to track link up/link down activity. This information is often used for billing purposes.
Use the space bar to toggle between the options:

- **ON**
- **OFF**.

RADIUS Authentication Port

Select the UDP port number to be used for the RADIUS authentication application. Confirm that the same value is defined in the RADIUS server.

RADIUS Accounting Port

Select the UDP port number to be used by the RADIUS accounting application. Confirm that the same value is defined in the RADIUS server.

Retransmission Timeout

Select this parameter to enter the maximum time WEB RANger-II waits for a single request response from the RADIUS server, for example 30 seconds. After this time the request will be retransmitted.

Total Timeout

Select this parameter to enter the total time WEB RANger-II tries to communicate with the RADIUS server.

Routing/Bridging Menu

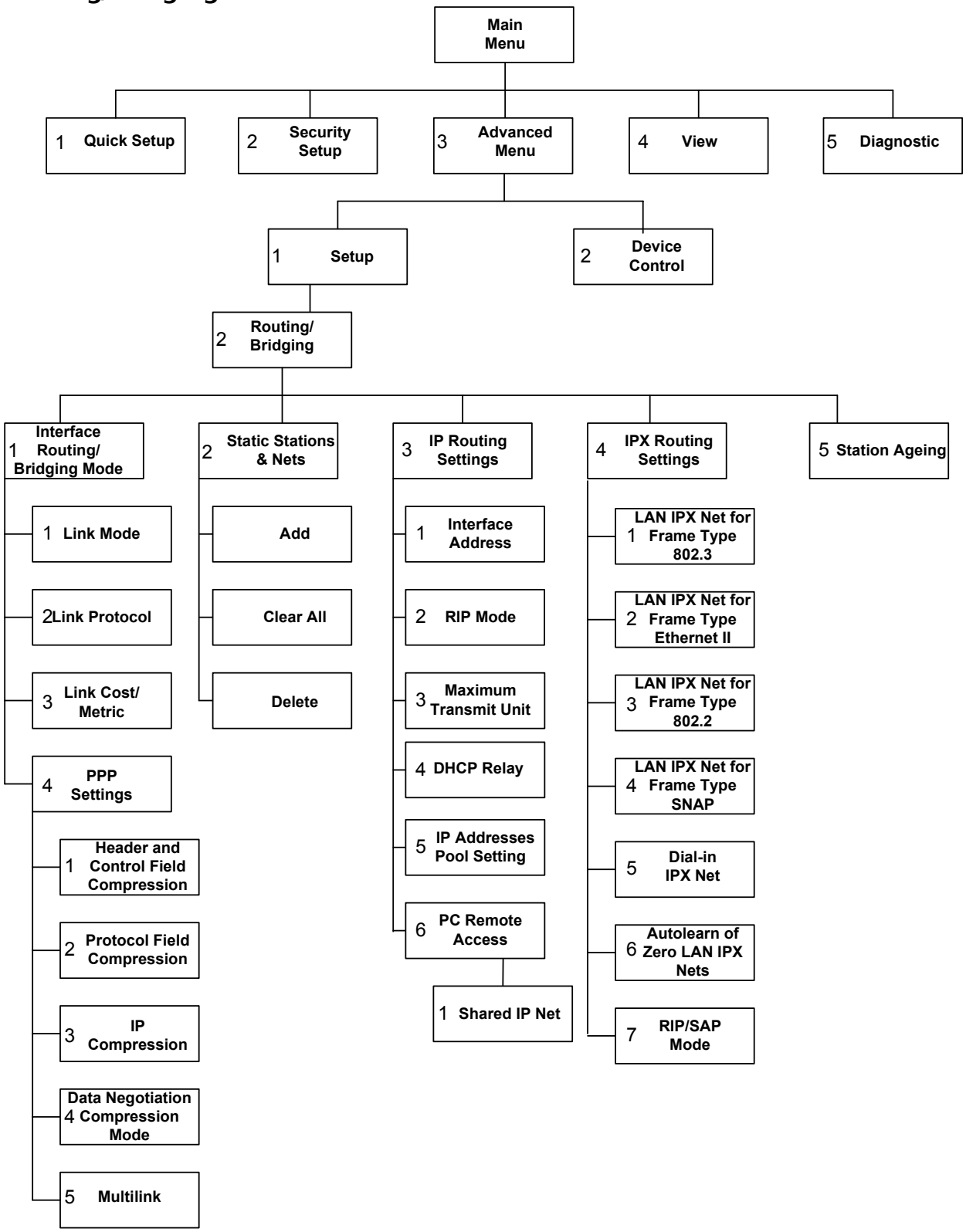


Figure 4-30. Routing Menu Outline

➤ **To access the Routing/Bridging menu:**

1. In the Advanced Menu, press **1**.
   The Setup menu appears.
2. In the Setup menu, press **2**.
   The Routing/Bridging menu appears.

```
      ROUTING/BRIDGING ( Device name - WEB RANger-II  )

           Link 1 - IP & IPX ROUTER  PPP

      Setup Menu

 1. Interface Routing Bridging Mode
 2. Static stations & nets
 3. IP routing settings
 4. IPX routing settings
 5. Station ageing (minutes): 30

  ESC - Return to previous menu

  Choose one of the above:
```

Figure 4-31. Routing/Bridging menu

The options in the Routing/Bridging menu are described below.

Interface Routing / Bridging Mode

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓1
Interface Routing / Bridging Mode

```
    ROUTING MODE: LINK 1   ( Device name - WEB RANger-II   )


1. Link type         - IP Router
2. Link protocol     - PPP
3. Link cost/metric - 1
4. PPP settings
ESC - Return to previous menu


Choose one of the above :
```

Figure 4-32. Interface Routing Bridging Mode

To perform the routing / bridging functions, configure the parameters below.

Link Type

Select this parameter to assign the link type, for each interface. Use the space bar to toggle between the options:

- **IP**
- **IPX routing**
- **Bridging**
- **Any combination of these types**.

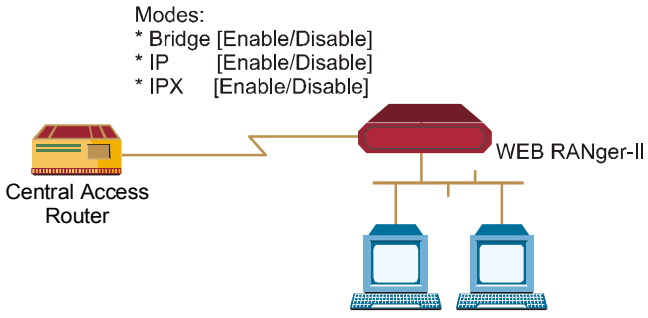


Figure 4-33. Link Routing Types

LAN Type (only for WR2/2U)

Select this parameter if the interface selected was a LAN. You can select any combination of Bridge, IP, or IPX routing.

Link Protocol

Select this parameter to define the type of encapsulation while sending frames through the WAN interface. The settings are different for various link types.

Link protocols available for synchronous links are:

- **PPP**
- **Native**.

Link protocols available for asynchronous links are:

- **PPP**
- **SLIP**
- **CSLIP**.

Note

When the Native protocol is used with a router, protocol packets pass in HDLC format.
When the Native protocol is used with a bridge, MAC frames pass in HDLC format.

Link Cost

Select this parameter to assign a cost to each WAN link for routing purposes. This parameter affects WEB RANger-II's operation of the corresponding interface configured to use RIP routing protocol.

Each routing entry is accompanied by a metric, which is the number of routers through which a packet must go to get to its destination.

Before updating routing tables, WEB RANger-II adds link cost value to all routing metrics received from this link; this may affect further routing decisions.

PPP Settings

This option is only available for PPP link protocol.

The PPP Setting screen has the following options:

Header and Control Field Compression	For troubleshooting only. Change the Header and Control Field Compression setting only if there is a problem with PPP negotiation.
Protocol Field Compression	For troubleshooting only. Change the Protocol Field Compression setting only if there is a problem with PPP negotiation.

IP Compression Activates Van Jacobson TCP Header Compression on a specified link. PPP is often used on slow bandwidth links, such as modems. To make the transmission faster, certain parts of the data packets can be compressed. In Van Jacobson TCP Header Compression the TCP/IP packet header is compressed according to RRC 1144. Other protocols running over IP (for example, UDP, ICMP) are not affected by using Van Jacobson compression. Since PPP is used for point to point transmissions, both the local and remote devices must have Van Jacobson TCP Header Compression enabled for compression to be performed. To verify that Van Jacobson TCP Header Compression is being performed, open the Interface Connections Screen.

Multilink Determines if a line supports multilink PPP (RFC 1990 compliant). Choose between:

- **Disabled** – The line does not support multilink PPP
- **Permanent** – The line supports multilink PPP
- **BOD** – The line enables multilink PPP with Bandwidth-on-Demand support (for ISDN line only).

Permitting multilink PPP means that two neighboring links (or two ISDN B-channels) will work as a single logical channel, thereby increasing the total link bandwidth. If you select *Permanent*, then both links will be connected simultaneously, independent of bandwidth utilization. Using *BOD* permits you to be connected most of the time with only one B-channel and to be connected with the second channel for small periods of high bandwidth utilization. This method reduces connection costs.

Fine Tuning BOD

If you choose BOD, then configure the following parameters:

Sensibility Direction Traffic direction to be counted in determining whether to connect the second line. The direction can be:

- Transmit
- Receive
- Both.

Sensibility Timeout Time interval for the utilization count.

Static Stations and Nets

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓2
Static Stations and Nets

Select this parameter to add, delete, or clear static entries in the IP/IPX Routing table or Bridge Routing table. If the WEB RANger-II is attached to more than one LAN, then select this parameter for each LAN interface, if necessary. Static entries are not removed from the routing tables by the Ageing Mechanism. *Figure 4-34* shows the Static Stations and Nets screen.

```
STATIC STATIONS AND NETS(MAC, IP, IPX) (Device name - WEB RANger-II)

1. IP  - 192.168.182.056 mask-255.255.255.248 interface-2/16   cost-1

2. IPX - 25490880       interface-3      cost-1

   A - Add , C - Clear all , D - Delete
   ESC - Return to previous menu.
```

Figure 4-34. Static Stations and Nets

When adding static entries in the IP/IPX Routing table or Bridge Routing table, they can be defined in 4 ways:

MAC Station A single static entry in the Bridge routing table. The entry is a single MAC Address (6 bytes) entered in hexadecimal format, and the interface that is the frame pathway.

IP Net A network as the destination. IP Net consists of 2 parts:

- Destination – defined by entering the subnet IP address and IP mask. For example, 192.168.182.32 is a subnet IP address and 255.255.255.240 is the IP mask.
- Frame pathway – specified either as an interface (i.e. port) number or as Next Hop IP address. In Next Hop IP the frames are sent to another router; from there they will be sent to their final destination.

IP-Station Defines a single host as the destination. IP Station consists of 2 parts:

- Destination - defined by entering the host IP address; for example, 192.168.182.11
- Frame pathway - specified as in IP Net, above.

IPX Net Used for IPX routing. Define the IPX Net in hexadecimal and the interface number.

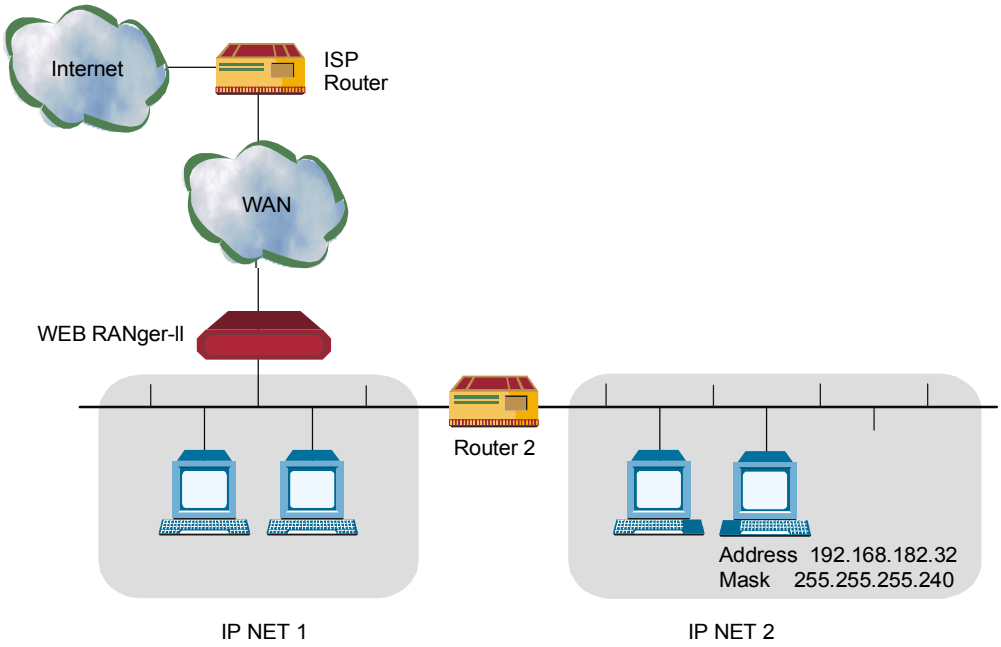


Figure 4-35. Router 2 set to "Next Hop" in WEB RANger-II

IP Routings Settings

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings

Figure 4-36 shows the menu options.

```
IP ROUTING SETTINGS ( Device name - WEB RANger-II  )

1. Interface address
2. RIP mode
3. Maximum transmit unit
4. DHCP Relay
5. IP address pool setting
6. PC remote access

 ESC - Return to previous menu

 Choose one of the above:
```

Figure 4-36. IP Routing Settings

Interface Address

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓1
Interface Address

Select this parameter to enter an IP address for the WAN interface and one or more IP addresses for the LAN interface. Multiple IP addresses on the LAN are useful in environments with multiple IP nets on the LAN (refer to *Figure 4-37*). If your WEB RANger-II setup has two LAN interfaces use this screen to enter one or more IP addresses for the second LAN.

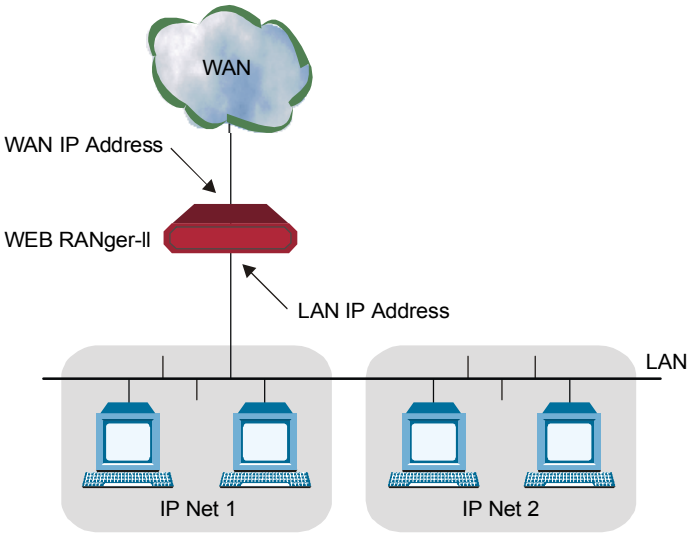


Figure 4-37. WAN and LAN Interface Addresses

RIP Mode

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓2
RIP Mode

This parameter sets the type of routing advertisement protocol to be used for each WEB RANger-II interface (LANs and WANs). For each interface toggle between:

- **RIP1**
- **RIP2**
- **RIP1+2**
- **No RIP**.

If WEB RANger-II is configured as a **RIP enabled router**, it sends/receives information from its routing table to/from corresponding router(s), learning its environment dynamically. Select from:

RIP1	Sends and receives routing information about IP nets only
RIP2	Sends and receives full routing information, including subnets
RIP1+2	Sends information as for RIP2 (full routing information, including subnets), and receives both RIP1 and RIP2 (routing information about IP nets only).

Maximum Transmit Unit

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓3
Maximum Transmit Unit

This parameter sets the maximum transmit unit (MTU) for IP fragmentation. The Set the MTU for each interface (LANs and WANs). If a frame is larger than the MTU, it will be fragmented into smaller units, when it is sent through the specified interface.

DHCP Relay

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓4
DHCP Relay

This parameter enables transmission of DHCP requests to specified IP addresses via WAN and LAN links.

IP Address Pool Setting

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓5
IP Address Pool Setting

This parameter determines the option for how WEB RANger-II assigns IP addresses dynamically to connected workstations. WEB RANger-II uses one of the following mechanisms to assign IP addresses dynamically to workstations:

IPCP Negotiations This is a mechanism where the remote router or a workstation connected to WEB RANger-II via a link requests an IP address. This request is made by specifying zero for the IP address in the IPCP configure request (PPP).

BOOTP This is a method where another router or workstation sends an affirmation for an IP address. WEB RANger-II uses BOOTP to confirm the IP address by sending a BOOTP reply packet via a link or LAN. WEB RANger-II using BOOTP supports basic options only.

DHCP This protocol is an extension to BOOTP and permits WEB RANger-II to supply not only an IP address but also additional parameters, such as Default Gateway, DNS server addresses etc. WEB RANger-II supplies these parameters to the client's workstation. In contrast to BOOTP, DHCP supplies these parameters on a temporary basis. WEB RANger-II using DHCP checks on the workstation periodically. If the workstation is not using the IP address, the IP address can be supplied to other workstations later.

WEB RANger-II supports all these mechanisms simultaneously.

IP Addresses Pool

Select this option to define IP address information.

```
  IP ADDRESSES POOL  ( Device name - WEB II    )
      ----------------------

 Pool of IP addresses dynamically allocated by the device working as
 Remote Access server or DHCP server to workstations over the WAN/LAN.
 Allocation can be made via DHCP, BOOTP and PPP-IPCP request.



 1. IP Address: 001.001.001.001 - 001.001.001.005  Mask: 255.255.255.000
    Default gateway: 001.001.001.001
    Primary DNS: 194.090.001.005, Secondary DNS: 000.000.000.000
    Interface: LAN 1

OPTIONS:  C-Clear all, E-Edit, D-Delete, A-Add
Press one of the above or ESC to return to previous screen:
```

Figure 4-38. IP Addresses Pool

You can define up to five entries. Each entry contains the following parameters:

Low IP Address Defines the lower boundary of the IP address range.

High IP Address Defines the upper boundary of the IP address range.

IP Mask Defines the IP mask for the IP address range (for DHCP and BOOTP).

Default Gateway The Default Gateway IP address for workstations which receive IP addresses from the range defined by the Low IP Address and High IP Address. The Default Gateway IP address must be within this IP address range (used by DHCP only).

Primary DNS The IP address of the DNS server which can be used by the workstation. The workstation receives an IP address from the range defined by the Low IP Address and High IP Address (for DHCP and IPCP).

Secondary DNS Additional DNS server address that is an alternative to the Primary DNS (for DHCP and IPCP).

Interface This interface determines which requests to the IP address can be accepted. You can determine the interface by toggling between WAN, LAN (any LAN or specifically 2 LAN interface units), and ALL (both WAN and LAN).

PC Remote Access

Advanced Menu
↓1
Setup
↓2
Routing/Bridging
↓3
IP Routing Settings
↓5
PC Remote Access

Select this parameter to define the remote access. The PC Remote Access Option is important if WEB RANger-II is used as a remote access server for remote PCs accessing the LAN. Refer to *Figure 4-39*.

```
      PC Remote Access ( Device name - WEB II  )

1. Shared IP net - 192.168.1.1    mask - 255.255.255.240

 ESC - Return to previous menu

 Choose one of the above:
```

Figure 4-39. PC Remote Access

Shared IP Net
Select this parameter to enter the Shared IP net address. The Shared IP net address is used by all remote workstations that connect to the remote access server on the WAN links.

IPX Routing Settings

Advanced Menu
↓**1**
Setup
↓**2**
Routing/Bridging
↓**4**
IPX Routing Settings

The IPX Routing Settings Menu is shown in *Figure 4-40*.

```
IPX ROUTING SETTINGS (  Device name - WEB RANger-II   )

1.  LAN IPX net for frame type 802.3        - 00000000
2.  LAN IPX net for frame type Ethernet II  - 00000000
3.  LAN IPX net for frame type 802.2        - 00000000
4.  LAN IPX net for frame type SNAP         - 00000000
5.  Dial-in IPX net                         - D2162747
6.  Autolearn of zero LAN IPX nets          - [Enable ]
7.  RIP/SAP mode

ESC - Return to previous menu
Choose one of the above:
```

Figure 4-40. IPX Routing Settings

WEB RANger-II learns IPX Nets in several ways:

LAN IPX Net for Frame Type Each of these parameters specifies the IPX Nets associated with a particular frame type. If WEB RANger-II is in Autolearn enable mode, then non-zero values point to learned Net. WEB RANger-II supplies default values for these frame types that can be added to PC's operating on LANs without other IPX routing.

Dial-in IPX Net This parameter specifies the IPX Net definition for a WAN interface.

Autolearn Zero LAN IPX Nets By setting this parameter to **Enable**, WEB RANger-II learns IPX Nets from RIP/SAP frames sent by other IPX routers on the same LAN. Refer to *Figure 4-41*.
If there are no other IPX routers on WEB RANger-II LAN, this parameter must be set to **Disable**, and you must configure the IPX Nets for each frame type.

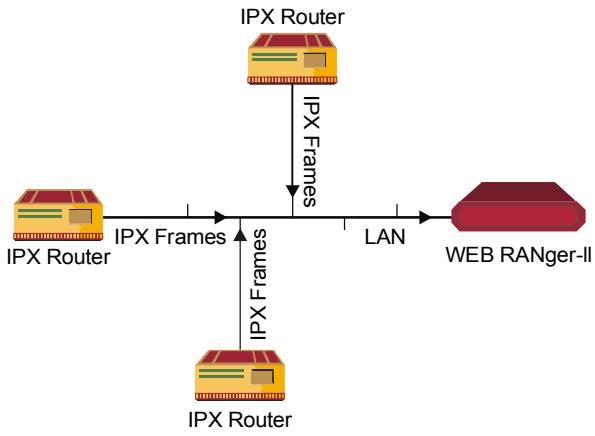


Figure 4-41. Automatic Learning from IPX Frames

RIP / SAP Mode

Advanced Menu
↓**1**
Setup
↓**2**
Routing/Bridging
↓**4**
IPX Routing Settings
↓**7**
RIP/SAP Mode

Figure 4-42 shows the RIP / SAP Mode Setup.

```
RIP / SAP MODE SETUP (Device name - WEB II)

  1. Link 1 RIP/SAP mode: [Enabled ]
  2. LAN    RIP/SAP mode: [Enabled ]

   ESC - Return to previous menu

  Choose one of the above:
```

Figure 4-42. RIP / SAP Mode Setup

Link 1 RIP/SAP Mode

Select this parameter to **Enable**/**Disable** the RIP/SAP mode. The default setting enables sending RIP and SAP tables for all updates and interfaces (Link and LAN).

When disabled WEB RANger-II does not send RIP/SAP frames, but receives and processes RIP/SAP frames sent from other routers.

Station Ageing

Advanced Menu
↓**1**
Setup
↓**2**
Routing/Bridging
↓**5**
Station Ageing

Station ageing determines the amount of time a station is allowed to be inactive before it is removed from the network. A station is inactive when no traffic from it is received by the WEB RANger-II LAN interface. This parameter is used in IP routing mode for ARP table ageing and in bridge mode for MAC station table ageing. Static stations are not removed by the ageing mechanism. The default ageing time is 60 minutes.

Interface Parameters

The Interface Parameters menu is dynamic, depending on the hardware configuration. Only those screens / parameters that are applicable to your interface will appear.

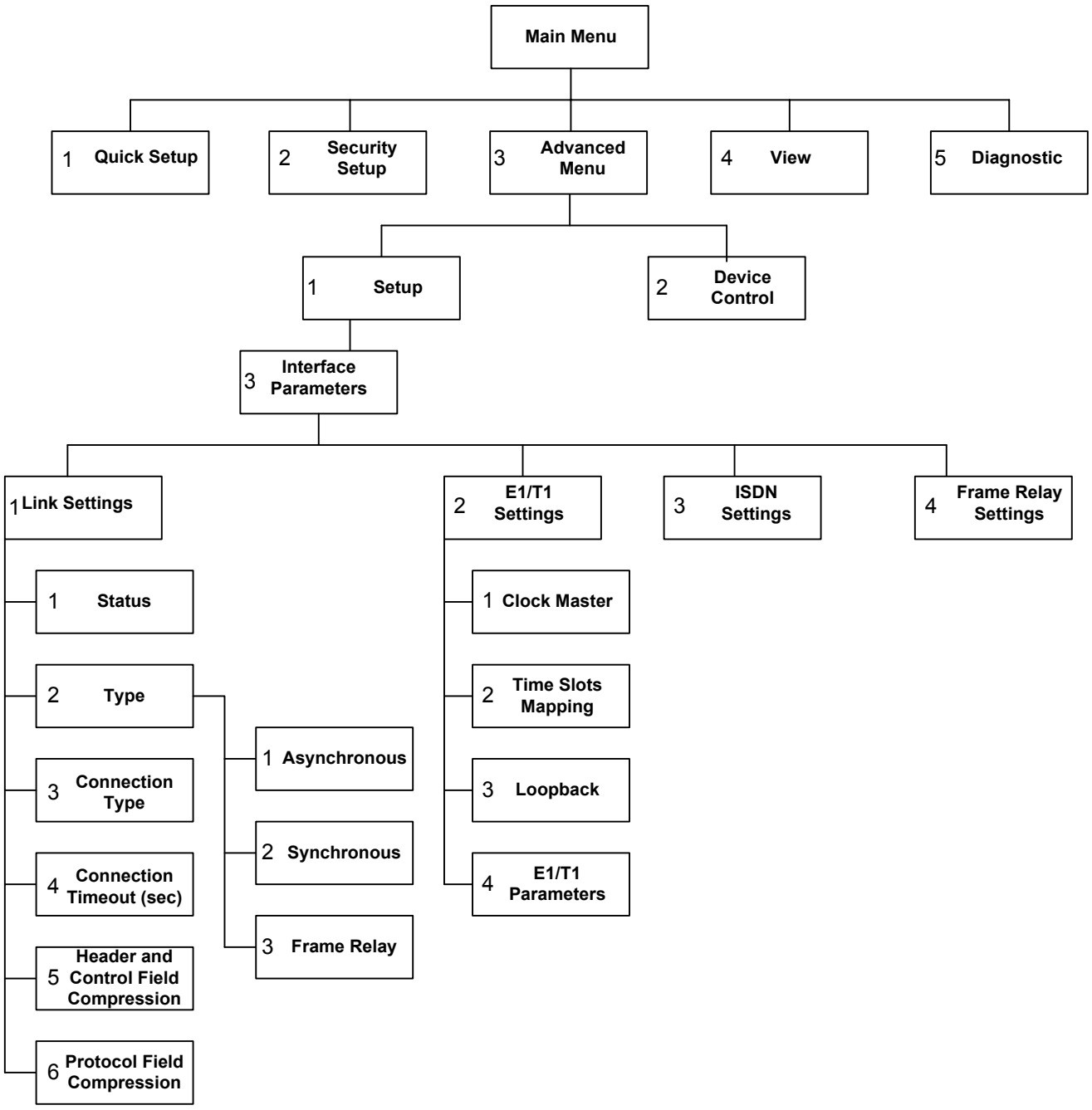


Figure 4-43. Interface Parameters Menu Outline

➤ **To access the Interface Parameters menu:**

3. In the Advanced Menu, press **1**.
   The Setup menu appears.
4. In the Setup menu, press **3**.
   The Interface Parameters menu appears.

```
        INTERFACE PARAMETERS (Device name - WEB RANger-II)

1.  Link settings
2.  E1/T1 settings
3.  ISDN settings
4.  Frame relay DLCI settings

ESC - return to previous menu
Choose one of the above:
```

Figure 4-44. Interface Parameters

The options in the Interface Parameters menu are described below.

Link Settings

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**1**
Link Settings

The Link Settings menu lists parameters that are specific to the line hardware. The menu is dynamic, depending on which hardware interface and protocol you have ordered.

The parameters that follow apply to all link types.

Status

This parameter specifies the status of a link:

Enabled Transmits and receives frames. For normal operations set all links in enabled status.

Disabled Frames are not transmitted or received. The link may be permanently disabled, for example, when testing. A disabled line freezes all link operation, including connection attempts and forwarding.

Backup A backup link is disabled when the main link operates normally.If the main link fails, the backup link begins to operate and become *enabled*. Check that the backup routing settings are correct, so that traffic is forwarded to the desired destination via the backup link. When you restore the main link connection, the backup link becomes *disabled* again.

Type

This parameter specifies the type of interface:

Synchronous Data bits are transmitted at a fixed rate, because the sender and the receiver are synchronized.

Asynchronous Data bits are transmitted one character at a time. Characters are preceded by start bits and followed by stop bits, which provide synchronization at the receive terminal.

Frame Relay A packet-switching protocol for connecting devices on a WAN.

Connection Type

This parameter specifies the type of connection:

Originate only If the link is to be used to connect to the Internet or Intranet.

Answer only If the link is to be used for receiving remote access connections.

Answer&Originate
If the link is to be used for both incoming and out going connections (not simultaneously).

This parameter only affects dial-up link types (asynchronous with modem or ISDN). For leased-line links select *Answer-only*.

Connection Timeout (sec)

This parameter specifies the connection timeout. The remote side has to answer within the time allotted with the Connection Timeout. If within this time there is no response, you are informed that the remote side is no longer active.

Connection timeout is *applicable only when the PPP protocol is used*.

Other parameters depend on link hardware type and protocol.

Control Signals Mode (for Synchronous, Asynchronous, and Frame Relay Links Only)

WEB RANger-II can be set to ignore or acknowledge the following control signals:

RTS Request-to-send

CTS Clear-to-send

CD Carrier Detect

Clock Rate (for Synchronous and Asynchronous DCE lines)

This parameter specifies the rate at which data is sent across the link.

Parity (for Asynchronous Only)

This parameter specifies the parity. Parity is a method of checking for errors. A parity bit is a non-information bit that is added to a group of bits to ensure that the total number of bits in a character is odd or even. If you know that the total number of bits must be odd any group of bits whose total number is even must be erroneous. Toggle between:

- **Odd**
- **Even**
- **None**.

Stop Bit ((for Asynchronous Only)

This parameter specifies the stop bit quantity. The stop bit is a signal at the end of a character that instructs a receiving device to wait for a subsequent signal. Toggle between **1** or **2** stop bits.

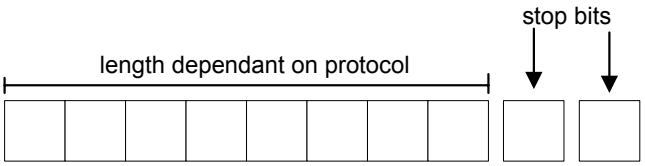


Figure 4-45. Stop Bit

Modem Settings (for Asynchronous Only)

This parameter displays a menu that allows configuration of modem parameters.

Dialing Mode Parameters

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**1**
Link Settings

Destination Phone Number (for ISDN only)

Select this parameter to enter the phone number of the station you want to dial. This parameter is mandatory for dialing out. The other dialing mode parameters are optional.

Destination Sub-Number

Select this parameter to enter the extension number of the destination phone number.

Source Phone Number

Select this parameter to enter the phone number of the person dialing out. The destination station uses this parameter to identify the caller.

Source Sub-Number

Select this parameter to enter the extension number of the person dialing out.

Answering Mode Parameters

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**1**
Link Settings

Local Phone Number

Select this parameter to enter the number to which incoming calls are directed.

Local Sub-Number

Select this parameter to enter the extension to which incoming calls are directed.

Local Number for Dialback (for ISDN only)

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓1
Link Settings

Dialback Phone Number

Select this parameter to enter the phone number that is used by the ISP to dial back WEB RANger-II. When WEB RANger-II wants to dial-up to the ISP, the ISP uses this number to identify and dial back WEB RANger-II (similar to reverse charging). In this way, the PTT bills the ISP and not the caller. This feature is only useful when dialback is enabled on both sides.

Dialback Sub-Number

Select this parameter to enter the extension used by the ISP for dialback purposes.

Frame Relay Settings

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓4
Frame Relay Settings

Frame Relay is a form of WAN that is designed to maximize throughput and minimize cost by simplifying network processing.

Figure 4-46 shows the connection of WEB RANger-II to Internet / Intranet through Frame Relay network.

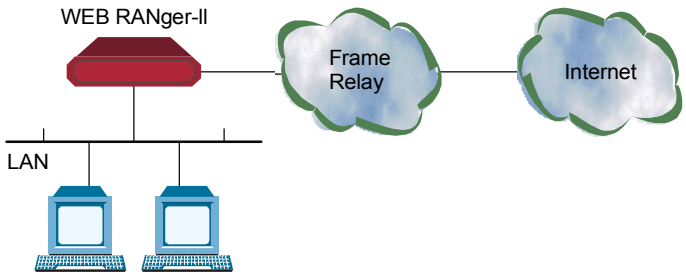


Figure 4-46. Connection to the Internet over Frame Relay

Frame Relay Features

- Supports permanent virtual circuits (PVC)
- Supports Frame Relay (IP/IPX/Bridge) encapsulation based on RFC 1490
- Supports different maintenance protocols:
  - T1.617/ANNEX D
  - Q.933/ANNEX A
  - LMI.
- Supports self-learning of the maintenance protocol and the DLCI that enables connection to the Frame Relay network **without configuring Frame Relay parameters**.
- Executes congestion control when an explicit congestion notification is received for the DLCI from the Frame Relay network. The unit reduces the transmitted information rate of the DLCI and increases it when the congestion condition is cleared.
- Supports the Frame Relay SNMP MIB.

Implementing Frame Relay

Figure 4-47 maps the options in the Advanced Menu, which are used to configure WEB RANger-II for operation over a Frame Relay network.

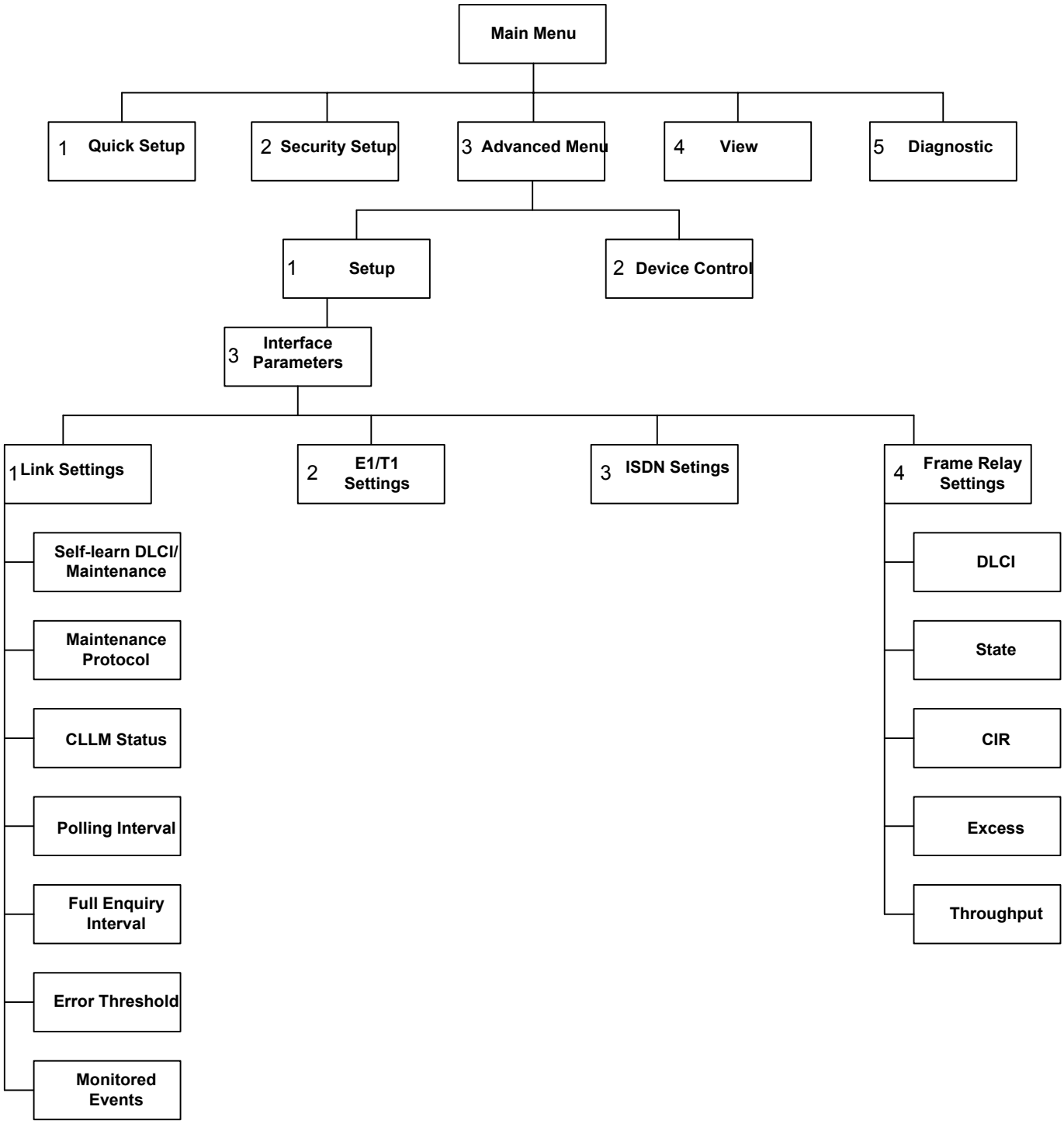


Figure 4-47. Interface Parameters for Frame Relay

Frame Relay Link Parameters

The parameters in the Frame Relay Links Parameters menu are described below.

Self Learn DLCI/Maintenance

Select this parameter to specify whether WEB RANger-II will self learn the maintenance protocol on the Frame Relay link and the existing DLCIs with their status (**UP** or **DOWN**). When this parameter is disabled (OFF), you need to configure the maintenance protocol and the DLCIs manually.

Maintenance Protocol

Select this parameter to specify the maintenance protocol of the Frame Relay link: **T1.617/ANNEX D**, **Q.933/ANNEX A**, **LMI** or **None**. This parameter can only be configured if the Self-learn DLCI / Maintenance parameter is disabled (**OFF**).

CLLM Status

Select this parameter to specify whether CLLM frames, used for congestion indication, will be supported (**ON**) or not (**OFF**).

Polling Interval

Select this parameter to specify the number of seconds between transmission of two successive status enquiry frames.

Full Enquiry Interval

Select this parameter to specify the number of polling intervals after which a full status request frame is transmitted.

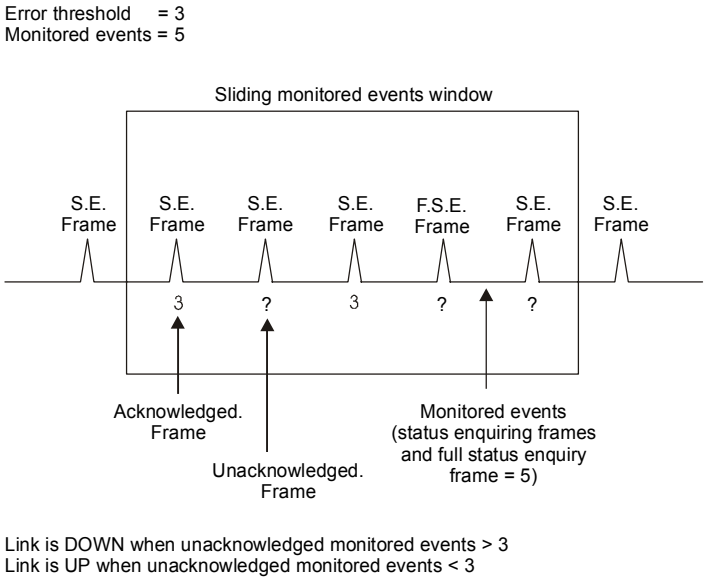


Figure 4-48. Polling Intervals

Error Threshold

Select this parameter to specify the number of unacknowledged monitored events (status enquiry frames and full status enquiry frames) that can occur in a sliding monitored events window before the link is declared DOWN.

Monitored Events

Select this parameter to specify the number of monitored events (status enquiry frames and full status enquiry frames) in a sliding monitored events window.

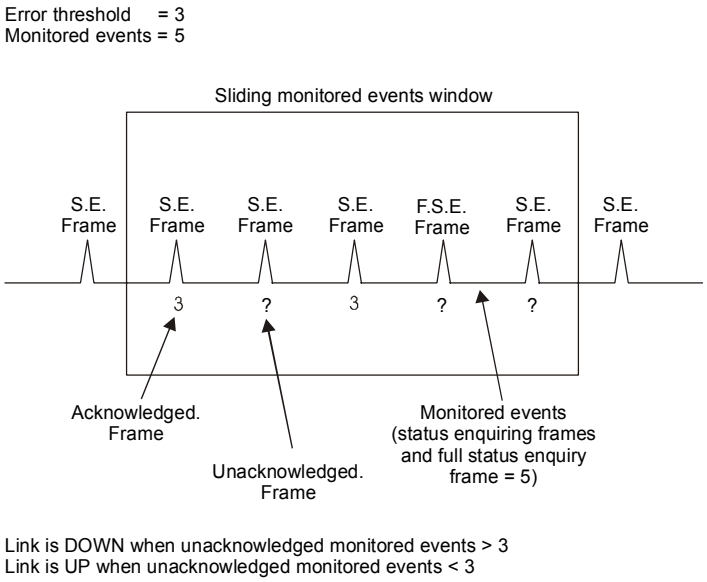


Figure 4-49. Monitored Events

After the link is declared DOWN, it can only be declared UP again when the sliding monitored events window contains only successfully monitored events, according to the parameter that was selected.

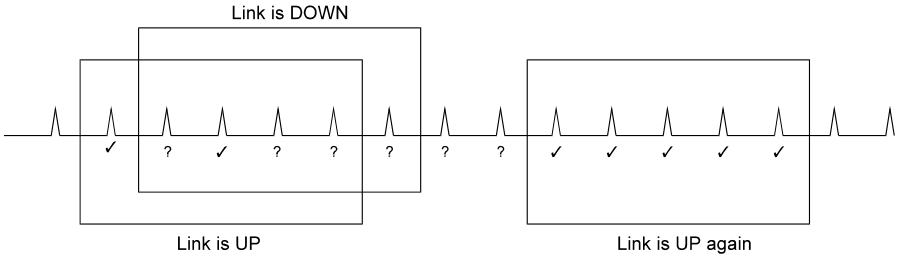


Figure 4-50. Monitored Events - Down Link

Frame Relay DLCI Parameters

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓4
Frame Relay DLCI Parameters

The parameters in the Frame Relay DLCI Parameters menu are described below.

DLCI

Select this parameter to specify the DLCI number.

State

Select this parameter to specify whether the DLCI is:

- **Enabled**
- **Disabled** (for receive/transmit).

CIR

Select this parameter to specify the maximum amount of data (in bits) which the network guarantees to transfer during the measurement interval (the measurement interval is usually one second). The value of this parameter is obtained from the Frame Relay provider.

Excess

Select this parameter to specify the maximum amount of uncommitted data bits that the network will attempt to deliver during the measurement interval. The value of this parameter should be received from the Frame Relay provider.

Throughput

Select this parameter to specify this parameter to specify the average number of data bits per second transferred by the network. When a measurement interval of one second is assigned to the CIR, the throughput value should equal the CIR value.

E1/T1 Settings

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓2
E1/T1 Settings

Select this option to configure the E1 or T1 parameters. They are described in the *T1 Setup Menu* and *E1 Setup Menu*, found later in this chapter.

WEB RANger-II with E1/T1 interfaces is an integrated router/bridge with E1/T1 and fractional E1/T1 services.

The WEB RANger-II with E1/T1 interfaces is available in five options (refer to *Figure 4-51, Figure 4-52,* and *Figure 4-53:*

- T1
- T1 with sublink
- E1
- E1 with sublink
- E1 or T1 with analog voice ports.

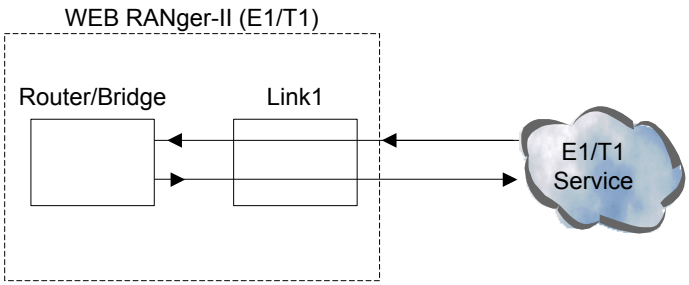


Figure 4-51. WEB RANger-II with an E1/T1 Interface

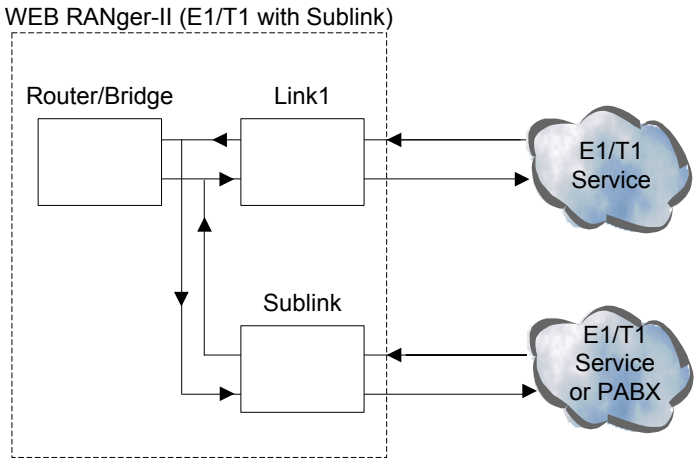


Figure 4-52. WEB RANger-II with an E1/T1 Interface and Sublink

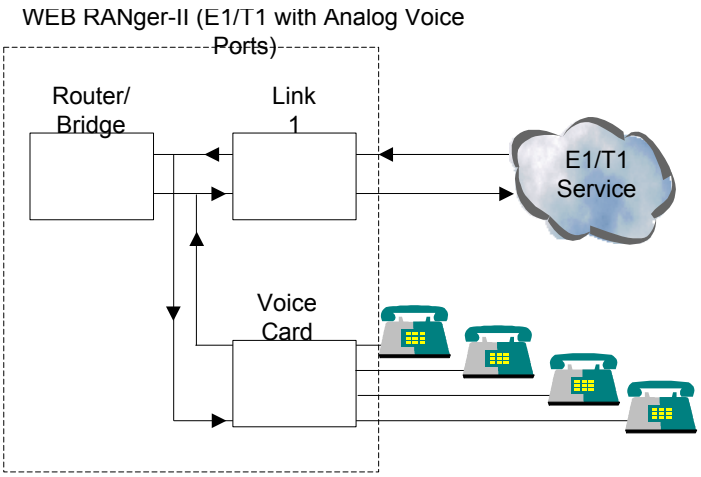


Figure 4-53. WEB RANger-II with an E1/T1 Interface and Analog Voice Ports

WEB RANger-II with sublink provides a Drop and Insert capability. The Drop and Insert capability enables multiplexing of data from the local router/bridge, and voice from the local PABX, to the E1/T1 main link.

T1 Features

- Nominal rate - 1.544 Mbps
- Data rates are multiples of 56 kbps or 64 kbps (N x 56 kbps or N x 64 kbps, N = 1 through 24)
- Time slot assignment is user selectable
- Link interface includes integral CSU/DSU depending on user configuration of the transmit level, 0 to -22.5 dB for Channel Service Unit (CSU) or 0-655 feet for Data Service Unit (DSU)
- Framing modes: Super Frame (SF (D4)) or Extended Super Frame (ESF)
- Line code: Alternate Mark Inversion (AMI)
- Zero suppression modes: B8ZS, B7ZS or transparent
- Master system clock:

  - Internal oscillator
  - Recovered from the link 1 received data
  - Recovered from the sublink received data (for WEB RANger-II with a Sublink)
- Variety of Loopback possibilities:
  - Network activated loopbacks (PLB, LLB)
  - Facility Data Link (FDL) loopbacks
  - User-configurable local or remote loopbacks
- Extended Super Frame (ESF) diagnostic for previous 24 hours collected in 15-minute intervals (according to the AT&T PUB 54016).

E1 Features:

- Nominal rate: 2.048 Mbps
- Data rates are multiples of 56 kbps or 64 kbps (N x 56 kbps or N x 64 kbps, N = 1…31)
- Time slot assignment is user-selectable
- E1 interface with or without LTU
- Interfaces: balanced or unbalanced
- Framing modes: G732N and G732S
- Optional Cyclic Redundancy Check (CRC-4)
- Line code: HDB3
- Master system clock:
  - Internal oscillator
  - Recovered from the link 1 received data
  - Recovered from the sublink received data (for WEB RANger-II with a Sublink)
- Loopback: User-configurable local or remote loopbacks
- When CRC-4 is enabled, diagnostics are available for the last 24 hours collected in 15-minute intervals (similar to the AT&T PUB 54016).

T1 Setup Menu

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓2
E1/T1 Settings

This section describes the parameters in the T1 Setup menu.

```
T1 SETUP: LINK 1  ( Device name - WEB II    )
       ----------------


   1.  Clock master : [Link 1]
   2.  Multiplier   : [64 kbps]
   3.  Time slots mapping
   4.  Loopback
   5.  T1 parameters
   6.  Alarms filter

   ESC - Return to previous menu
```

Figure 4-54. T1 Setup Menu

Clock Master

Select this parameter to set the source clock that synchronizes the whole T1 network. Timing source options are:

Internal	WEB RANger-II generates the system source clock from an internal clock oscillator.
Link 1	WEB RANger-II recovers the clock from the data received from the T1 link1.
Sublink T1	WEB RANger-II recovers the clock from the data received from the T1 sublink. (for WEB RANger-II with a Sublink)

Multiplier

Select this parameter to set the data rate of each DATA time slot. The multiplier value can be:

- **56 kbps**
- **64 kbps**.

Timeslot Mapping

Select this screen to configure the routing and the type of individual time slots for the link. *Figure 4-55* shows the type of time slots entering the multiplexer (MUX) (for WEB RANger-II with a T1 sublink). The timeslot mapping options are:

NC	Time slot not connected
DATA LINK1	Time slot used for data from the router/bridge
SUB-VOICE	Time slot used for voice from the sublink (for WEB RANger-II with a Sublink)
SUB-DATA	Time slot used for data from the sublink (for WEB RANger-II with a Sublink)

Note

For a multiplier of 64 kbps all time slots can be configured to DATA. For a multiplier of 56 kbps, a maximum of 16 time slots can be configured to DATA. For WEB RANger-II with a T1 Sublink, this limitation does not exist for time slots configured to the VOICE or DATA_SUB type.

```
T1 TIME SLOTS MAPPING :  LINK1  (device name - WEB II)
------------------

TS1   [DATA LINK1  ]                                  TS13  [NC          ]
TS2   [DATA LINK1  ]                                  TS14  [NC          ]
TS3   [DATA LINK1  ]                                  TS15  [NC          ]
TS4   [DATA LINK1  ]                                  TS16  [NC          ]
TS5   [NC          ]                                  TS17  [NC          ]
TS6   [NC          ]                                  TS18  [NC          ]
TS7   [NC          ]                                  TS19  [NC          ]
TS8   [NC          ]                                  TS20  [NC          ]
TS9   [NC          ]                                  TS21  [NC          ]
TS10  [SUB-DATA    ]                                  TS22  [NC          ]
TS11  [SUB-DATA    ]                                  TS23  [NC          ]
TS12  [SUB-VOICE   ]                                  TS24  [NC          ]


Enter time slot number (0 refer to all time slots)
Press 'Enter' - to toggle the time slot type
Press 'ESC'   - to Return to previous menu
Time slot number : 5
```

Figure 4-55. T1 Time Slots Mapping Screen

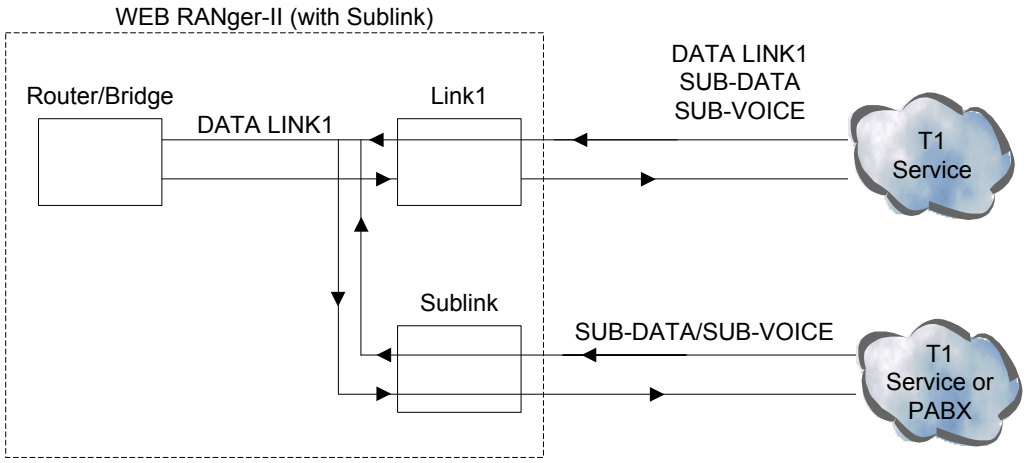


Figure 4-56. Time Slots Mapping (for WEB RANger-II with a T1 Sublink)

Loopback

Select this parameter to test the T1 interface.

Loopback options are:

Disabled

Remote Analog Loopback WEB RANger-II performs an analog loopback and transmits back the data that was received from the T1 line (see *Figure 4-57)*.

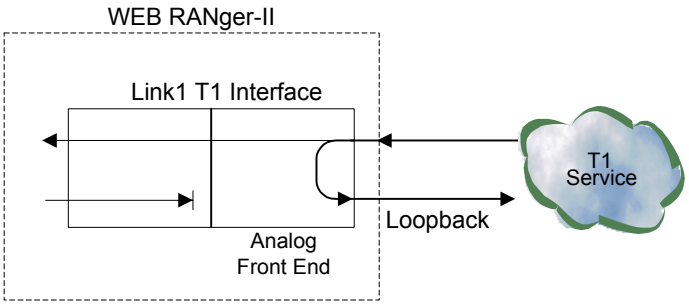


Figure 4-57. Remote Analog Loopback

Remote Analog Loopback WEB RANger-II performs an analog loopback and transmits back the data that was received from both the Link 1 T1 line and the sublink. The loopback is shown in *Figure 4-58* (for WEB RANger-II with a Sublink).

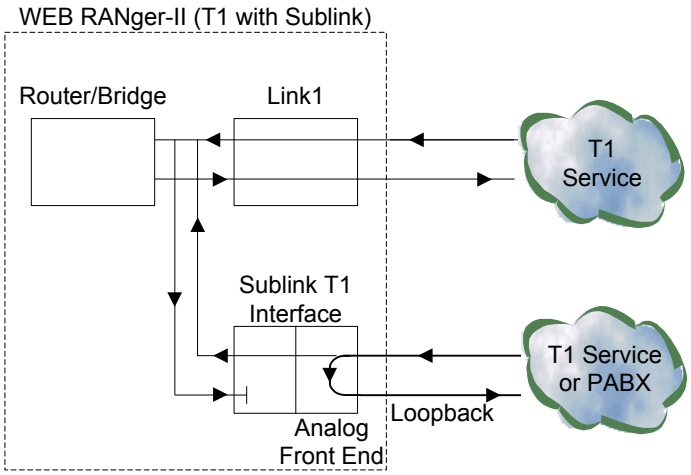


Figure 4-58. Remote Analog Loopback for T1 and Sub T1 Links

Remote Digital Loopback WEB RANger-II performs a digital loopback and transmits back the signal that was received from the T1 line. The loopback is shown in *Figure 4-59*.

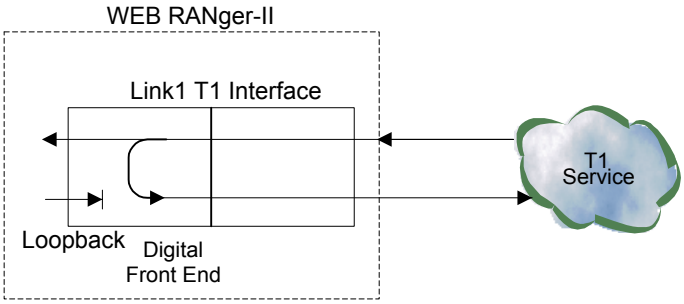


Figure 4-59. Remote Digital Loopback

Remote Digital Loopback. WEB RANger-II performs a digital loopback and transmits the signal and transmits back the signal that was received from the T1 line. The loopback is shown in *Figure 4-60* (for WEB RANger-II with a Sublink).

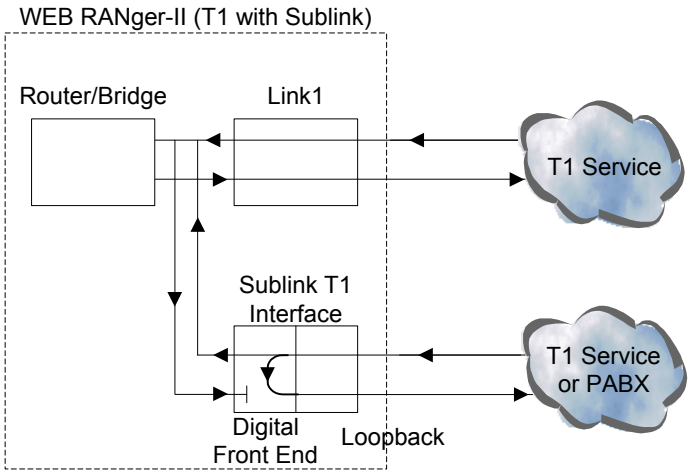


Figure 4-60. Remote Digital Loopback for T1 and Sub T1 Links

Local Analog Loopback The data transmitted from WEB RANger-II to the T1 line is sent back to the received path instead of the received data from the T1 line (see *Figure 4-61)*.

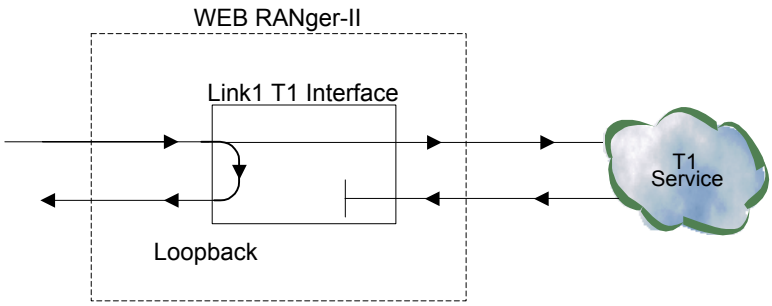


Figure 4-61. Local Analog Loopback

Local Analog Loopback Data transmitted from WEB RANger-II to the T1 line is sent back to the received path instead of the received data from the T1 line. The loopback is shown in *Figure 4-62* (for WEB RANger-II with a Sublink).

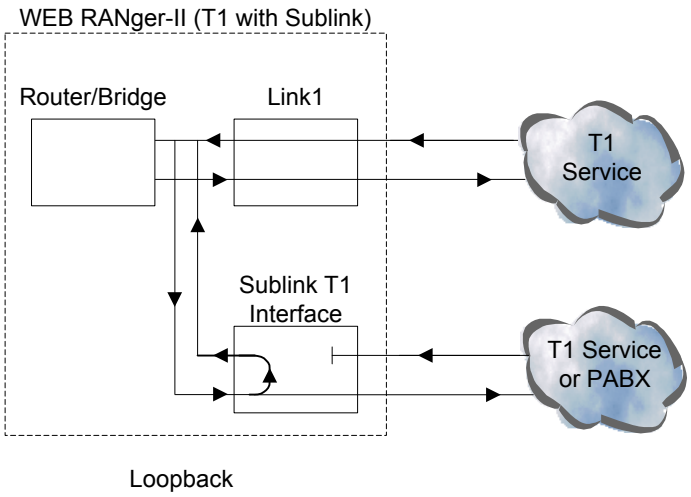


Figure 4-62. Local Analog Loopback for T1 and Sub T1 Links

T1 Link Parameters

The T1 Parameters Link1 Menu is shown in *Figure 4-63*.

```
T1 PARAMETERS: LINK 1   ( Device name - WEB II    )
    ---------------------

1.  Frame type      : [ESF]
2.  Line code       : [B8ZS]
3.  Tx line mask    : [0-133 ft / 0 dB]
4.  Sync            : [FAST]
5.  Idle code (hex) : 7C
6.  Rx gain         : [36 dB]

ESC - Return to previous menu
```

Figure 4-63. T1 Parameters Link1 Menu

Select this option to configure the following parameters:

Frame Type

Select this parameter to set the T1 framing type. Framing types are:

- **ESF** – 24 frames per multiframe
- **SF** – 12 frames per multiframe.

Line Code

Select this parameter to set the line coding method used for zero suppression. The zero suppression method is used to avoid long strings of '0', because these strings do not carry timing information. The zero suppression methods are:

- **B7ZS**
- **B8ZS**
- **Transparent**.

Tx Line Mask

Select this parameter to control the link transmit signal characteristics. Options depend on whether the link should be configured with CSU. When the link is configured without CSU, the transit signal mask is selected according to the transit line length (0-655 ft), to meet DSX-1 requirements. When the link is configured with CSU, the transit signal is attenuated by 7.5, 15, or 22.5 dB.

Sync

Select this parameter to define the time required for the link to return to normal operation after a red alarm event has terminated. Choose:

- **FAST** for one second
- **AT&T 62411** for ten seconds.

Idle Code

Select this parameter to set the value to be transmitted on the NC time slots.

Rx Gain

Select this parameter to set the maximum receive sensitivity for the T1 interface.

Remote Alarm Indication (for WEB RANger-II with a Sublink)

When configuring this parameter from the T1 Parameters menu, select this parameter to determine whether to transmit a yellow alarm indication on the T1 sublink when Link 1 is in yellow alarm state.

When configuring this parameter from the Sublink T1 Parameters menu, select this parameter to determine whether to transmit a yellow alarm indication on Link 1 when sublink T1 is in either yellow or red alarm state.

Note

When Link 1 is in red alarm state, an "all ones" indication is sent to the sublink T1.

Out-Of-Service Signaling (for WEB RANger-II with a Sublink)

Select this parameter to determine the value of the A, B signaling bits sent to Link 1 when the sublink is in the Out-Of-Service state. The C and D signaling bits are not affected.

MARK	Both A and B signaling bits are forced to '1' during out-of-service period.
SPACE	Both A and B signaling bits are forced to '0' during out-of-service period.

MARK-SPACE The A and B signaling bits are forced to '1' for 2.5 seconds, then shift to the '0' state until the out-of-service period ends.

SPACE-MARK The A and B signaling bits are forced to '0' for 2.5 seconds, then shift to the '1' state until the out-of-service period ends.

Alarm Filter

The Alarm Log File (see *Sec. 5.8*) shows all events and alarm statuses that have occurred in the E1/T1 interface. You use the Alarm Filter to mask or unmask events from the Alarm Log File.

```
T1 ALARMS FILTER  ( Device name - WEB II    )
        ----------------


     1.  Frame slip               : [Unmasked]
     2.  BPV error                : [Unmasked]
     3.  Excessive BPV            : [Unmasked]
     4.  Excessive error ratio    : [Unmasked]
     5.  Signal loss              : [Unmasked]
     6.  Yellow alarm             : [Unmasked]
     7.  Red alarm                : [Unmasked]
     8.  AIS red alarm            : [Unmasked]
     9.  AIS                      : [Unmasked]
    10.  Network loop - LLB       : [Unmasked]
    11.  Network loop - PLB       : [Unmasked]


    ESC - Return to previous menu


Choose one of the above:
```

Figure 4-64. T1 Alarms Filter Screen

E1 Setup Menu

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**3**
E1/T1 Settings

This section describes the parameters in the E1 Setup menu, shown in *Figure 4-65*.

```
E1 Setup:   LINK 1 (Device name - WEB II)
-----------------
1. Clock Master        : [Link 1]
2. Multiplier          : [964 kbps]
3. Time slots mapping
4. Loopback
5. E1 parameters
6. Alarms filter

ESC - Return to previous menu
Choose one of the above:
```

Figure 4-65. E1 Setup Menu

Clock Master

Select this parameter to set the source clock that synchronizes the whole E1 network. Timing source options are:

Internal WEB RANger-II generates the system source clock from an internal clock oscillator.

Link 1 WEB RANger-II recovers the clock from the data received from the E1 link1.

Sublink E1 WEB RANger-II recovers the clock from the data received from the E1 sublink (for WEB RANger-II with a Sublink).

Multiplier

Select this parameter to set the data rate of each DATA time slot. The multiplier value is:

- **56 kbps**
- **64 kbps**.

Timeslot Mapping

Select this parameter to configure the routing and the type of individual time slots for the link. *Figure 4-67* shows the type of time slots entering the multiplexer (MUX) (for WEB RANger-II with an E1 sublink). The timeslot mapping options are:

NC Time slot not connected.

DATA LINK1 Time slot used for data from the router/bridge.

SUB-VOICE Time slot used for voice from the sublink (for WEB RANger-II with a Sublink).

SUB-DATA Time slot used for data from the sublink (for WEB RANger-II with a Sublink).

```
E1 TIME SLOTS MAPPING :  LINK1  (device name – WEB II)
------------------

TS1   [DATA LINK1  ]                                  TS17  [NC          ]
TS2   [DATA LINK1  ]                                  TS18  [NC          ]
TS3   [DATA LINK1  ]                                  TS19  [NC          ]
TS4   [DATA LINK1  ]                                  TS20  [NC          ]
TS5   [NC          ]                                  TS21  [NC          ]
TS6   [NC          ]                                  TS22  [NC          ]
TS7   [NC          ]                                  TS23  [NC          ]
TS8   [NC          ]                                  TS24  [NC          ]
TS9   [NC          ]                                  TS25  [NC          ]
TS10  [SUB-DATA    ]                                  TS26  [NC          ]
TS11  [SUB-DATA    ]                                  TS27  [NC          ]
TS12  [SUB-DATA    ]                                  TS28  [NC          ]
TS13  [NC          ]                                  TS29  [NC          ]
TS14  [NC          ]                                  TS30  [NC          ]
TS15  [NC          ]                                  TS31  [VOICE 4     ]
TS16  [NC          ]

Enter time slot number (0 refer to all time slots)
Press 'Enter' – to toggle the time slot type
Press 'ESC'   - to Return to previous menu
Time slot number : 5
```

Figure 4-66. E1 Time Slots Mapping Screen

Note

For multiples of 64 kbps all timeslots can be configured to DATA. But, for multiples of 56 kbps, a maximum of 15 time slots can be configured to DATA.
For WEB RANger-II with an E1 Sublink, this limitation does not exist for time slots configured to the VOICE or SUB-DATA type.

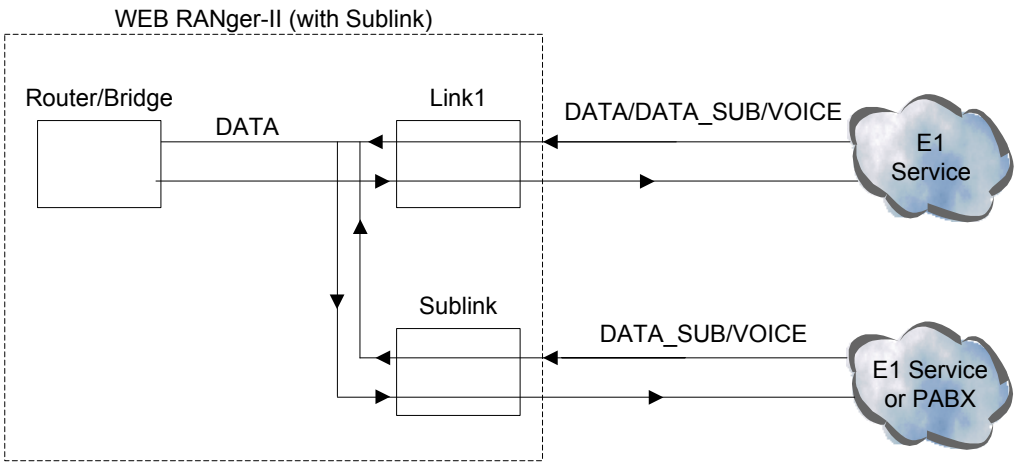


Figure 4-67. Time Slots Mapping (for WEB RANger-II with a E1 Sublink)

Loopback

Select this parameter in order to test the E1 interface.

Loopback options are:

Disabled

Remote Analog Loopback WEB RANger-II performs an analog loopback and transmits back the data that was received from the E1 line (see *Figure 4-68)*.

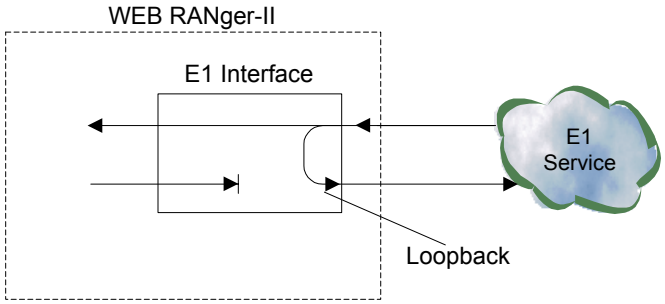


Figure 4-68. Remote Analog Loopback

Remote Analog Loopback

WEB RANger-II performs an analog loopback and transmits back the data that was received from both the Link 1 T1 line and the sublink. The loopback is shown in *Figure 4-69* (for WEB RANger-II with a Sublink).

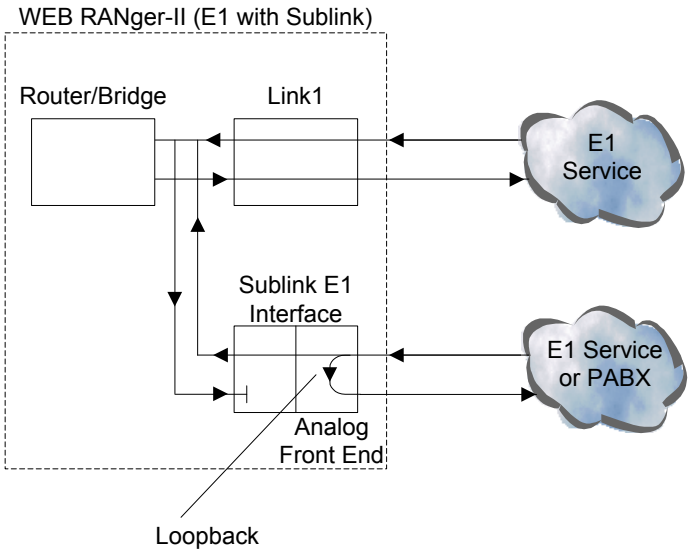


Figure 4-69. Remote Analog Loopback for E1 and Sub E1 Links

Local Analog

Data transmitted from the WEB RANger-II to the E1 line is sent back to the received path, instead of the data received from the E1 line. The loopback is shown in *Figure 4-70*.

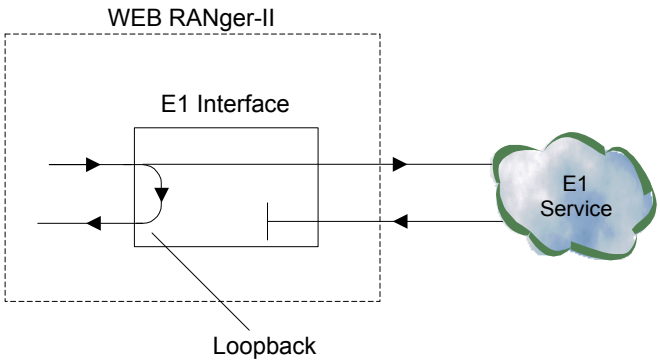


Figure 4-70. Local Analog Loopback

Local Analog Loopback

Data transmitted from WEB RANger-II to the E1 line is sent back to the received path instead of the received data from the E1 line. The loopback is shown in *Figure 4-71* (for WEB RANger-II with a Sublink).

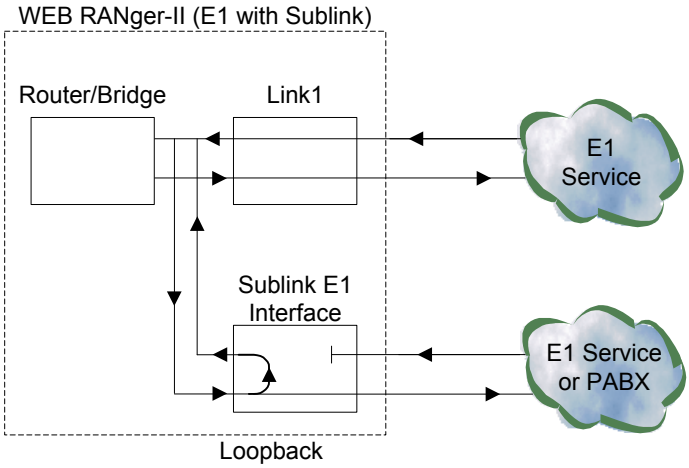


Figure 4-71. Local Analog Loopback for E1 and Sub E1 Links

E1 Link Parameters

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**3**
E1/T1 Settings

The E1 Parameters menu is shown in *Figure 4-72*.

```
E1 PARAMETERS :  LINK 1  (Device name - WEB II)


1. Frame type          : [G732S]
2. CRC-4               : [ON]
3. Sync                : [FAST]
4. Idle code (hex)     : 7C
5. Rx gain             : [30 dB]

ESC - Return to previous menu

Choose one of the above:
```

Figure 4-72. E1 Parameters

Select this option to configure the parameters that follow.

Frame Type

Select this parameter to set the E1 framing type. Framing types are:

G732N 2 frames per multiframe. Time slot 16 can be used for user data.

G732S 16 frames per multiframe. Time slot 16 is used for the Channel Associated Signaling (CAS).

CRC-4 (Cyclic Redundancy Check)

Select this parameter to enable or disable calculation of 4-bits check sum in order to detect errors in frames.

Sync

Select this parameter to define the time required for the link to return to normal operation after a red alarm event has terminated. Choose:

FAST One second

AT&T 62411 Ten seconds

CCITT 100 msec

Idle Code

Select this parameter to set the value to be transmitted on the NC time slots.

Rx Gain

Select this parameter to set the maximum receive sensitivity for the E1 interface.

Remote Alarm Indication (for WEB RANger-II with a Sublink)

When configuring this parameter from the E1 Parameters menu, select this parameter to determine whether to transmit a yellow alarm indication on the E1 sublink when Link 1 is in Yellow Alarm State.

When configuring this parameter from the Sublink E1 Parameters menu, select this parameter to determine whether to transmit a yellow alarm indication on Link 1 when sublink E1 is in either yellow or red alarm state.

Note

When Link 1 is in Red Alarm State, an "all ones" indication is sent to the sublink E1.

Out-Of-Service Signaling (for WEB RANger-II with a Sublink)

Select this parameter to determine the value of the A, B signaling bits sent to Link 1 when the sublink is in the Out-Of-Service state. The C and D signaling bits are not affected.

MARK Both A and B signaling bits are forced to '1' during out-of-service period.

SPACE Both A and B signaling bits are forced to '0' during out-of-service period.

MARK-SPACE The A and B signaling bits are forced to '1' for 2.5 seconds, then shift to the '0' state until the out-of-service period ends.

SPACE-MARK The A and B signaling bits are forced to '0' for 2.5 seconds, then shift to the '1' state until the out-of-service period ends.

Alarms Filter

Advanced Menu
↓1
Setup
↓3
Interface Parameters
↓2
E1/T1 Settings
↓

The Alarm Log File shows all events and alarm statuses that have occurred in the E1/T1 interface. However, you can use the Alarms Filter Menu to mask or unmask events from the Alarm Log File (see *Figure 4-73*).

```
E1 ALARMS FILTER (Device name - WEB II)

 1. Frame slip              :  [  Unmasked]
 2. BPV error               :  [  Unmasked]
 3. Excessive BPV           :  [  Unmasked]
 4. CRC-4 error             :  [  Unmasked]
 5. Excessive error ratio   :  [  Unmasked]
 6. Signal loss             :  [  Unmasked]
 7. Remote sync loss        :  [  Unmasked]
 8. Local sync loss         :  [  Unmasked]
 9. Local multi frame alarm :  [  Unmasked]
10. Remote multi frame alarm:  [  Unmasked]
11. AIS red alarm           :  [  Masked]
12. AIS                     :  [  Unmasked]

ESC - Return to previous menu
```

Figure 4-73. E1 Alarms Filter Screen

E1 and Voice Menu

If your WEB RANger-II supports E1 and Voice, the E1 Setup Menu appears as in *Figure 4-74*.

```
E1 SETUP: LINK 1   ( Device name - WEB II     )

   1.  Clock master : [Link 1]
   2.  Multiplier   : [64 kbps]
   3.  Time slots mapping
   4.  Loopback
   5.  E1 parameters
   6.  Voice parameters
   7.  Voice diagnostics
   8.  Alarms filter

   ESC - Return to previous menu
   Choose one of the above:
```

Figure 4-74. E1 and Voice Setup

Voice Parameters

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**2**
E1/T1 & Voice Settings
↓**6**
Voice Parameters

FXS Voice Interface

The Voice Parameters Menu for WEB RANger-II with four FXS voice channels is shown in *Figure 4-75*.

```
VOICE PARAMETERS:    ( Device name - WEB II    )

    1.  TX/RX gains
    2.  Coding law                  : [A LAW]
    3.  On/Off Hook from the E1 on  : [A bit inverted]
    4.  On/Off Hook to the E1 on    : [A bit inverted]
    5.  Default ABCD to the E1      : [0001]
    6.  Polarity                    : [Disabled]

    ESC - Return to previous menu
```

Figure 4-75. FXS Voice Interface

RX/TX Gains

Select this parameter to specify the nominal input level of the Receive and Transmit paths for each voice port. The input level range is –10 to +5 dBmm.

Coding Law

Select this parameter to specify the compounding law to be used by the voice channels. The values are:

A Law Coding E1 links

μ Law Coding T1 links

On/Off Hook *from* the T1 (E1) on

Select this parameter to specify the Receive mode for On/Off Hook signaling from T1 (E1) into FXS. The values are:

A bit

- When the received A bit signal from T1 (E1) equals *1* then *Off Hook* is indicated in the FXS interface
- When the received A bit signal from T1 (E1) equals *0* then *On Hook* is indicated in the FXS interface.

A bit inverted

- When the received A bit signal from T1 (E1) equals *1* then *On Hook* is indicated in the FXS interface
- When the received A bit signal from T1 (E1) equals *0* then *Off Hook* is indicated in the FXS interface.

B bit

- When the received B bit signal from T1 (E1) equals *1* then *Off Hook* is indicated in the FXS interface
- When the received B bit signal from T1 (E1) equals *0* then *On Hook* is indicated in the FXS interface.

B bit inverted

- When the received B bit signal from T1 (E1) equals *1* then *On Hook* is indicated in the FXS interface
- When the received B bit signal from T1 (E1) equals *0* then Off Hook is indicated in the FXS interface.

On/Off Hook *to* the T1 (E1) on

Select this parameter to specify the transmission mode for On/Off Hook signaling from FXS to T1 (E1). The values are:

A bit

- For *Off Hook* indicated in the FXS interface, the transmitted A bit signal is set to *1* towards T1 (E1)
- For *On Hook* indicated in the FXS interface, the transmitted A bit signal is set to *0* towards T1 (E1).

A bit inverted

- For *Off Hook* indicated in the FXS interface, the transmitted A bit signal is set to *0* towards T1 (E1)
- For *On Hook* indicated in the FXS interface, the transmitted A bit signal is set to *1* towards T1 (E1).

B bit

- For *Off Hook* indicated in the FXS interface, the transmitted B bit signal is set to *1* towards T1 (E1)
- For *On Hook* indicated in the FXS interface, the transmitted B bit signal is set to *0* towards T1 (E1).

B bit inverted

- For *Off Hook* indicated in the FXS interface, the transmitted B bit signal is set to *0* towards T1 (E1)
- For *On Hook* indicated in the FXS interface, the transmitted B bit signal is set to *1* towards T1 (E1).

Default ABCD to the T1 (E1)

Select this parameter to specify signaling bits that are not in use for the On/Off Hook or for the polarity (if enabled). Those bits will be transmitted towards T1.

Polarity (polarity reversal, also known as Wink Start Reversal)

When polarity is configured as *Enabled,* the polarity signal is received from T1 (E1) either on the B bit (while the *On/Off Hook from T1/E1* parameter is configured to *A bit* or *A bit inverted),* or on the A bit (while the *On/Off Hook from T1/E1* parameter is configured to *B bit* or *B bit inverted).*

FXO Voice Interface

The Voice Parameters Menu for WEB RANger-II with four FXO voice channels is shown in *Figure 4-76*.

```
       VOICE PARAMETERS:    ( Device name - WEB II    )

1.  TX/RX gains
2.  Coding law                 : [μ LAW]
3.  On/Off Hook from the T1 on : [A bit]
4.  Ring Detection to the T1 on: [A bit]
5.  Default ABCD to the T1     : [0000]
6.  Polarity                   : [Disabled]
7.  Signaling Feedback         : [Disabled]
8.  Out-of-Service method      : [Forced Idle]

ESC - Return to previous menu
Choose one of the above:
```

Figure 4-76. FXO Voice Interface

RX/TX Gains

Select this parameter to specify the nominal input level of the Receive and Transmit paths for each voice port. The input level range is –10 to +5 dBm.

Coding Law

Select this parameter to specify the compounding law to be used by the voice channels. The values are:

- **A Law Coding** E1 links
- **μ Law Coding** T1 links
- **On/Off Hook *from* the T1 (E1) on**

Select this parameter to specify the Receive mode for On/Off Hook signaling from T1 (E1) into FXS. The values are:

A bit

- When the received A bit signal from T1 (E1) equals *1* then *Off Hook* is indicated in the FXO interface
- When the received A bit signal from T1 (E1) equals *0* then *On Hook* is indicated in the FXO interface.

A bit inverted

- When the received A bit signal from T1 (E1) equals *1* then *On Hook* is indicated in the FXO interface
- When the received A bit signal from T1 (E1) equals *0* then Off Hook is indicated in the FXO interface.

B bit

- When the received B bit signal from T1 (E1) equals *1* then *Off Hook* is indicated in the FXO interface
- When the received B bit signal from T1 (E1) equals *0* then *On Hook* is indicated in the FXO interface.

B bit inverted

- When the received B bit signal from T1 (E1) equals *1* then *On Hook* is indicated in the FXO interface
- When the received B bit signal from T1 (E1) equals *0* then Off Hook is indicated in the FXO interface.

Ring Detection *to* T1 (E1) on

Select this parameter to specify the ring detection signaling transmission mode from FXO towards T1 (E1). The values are:

A bit

- For *ring detection* the A bit signaling is set to *1* towards T1 (E1)
- For *no ring detection* the A bit signaling is set to *0* towards T1 (E1).

A bit inverted

- For *ring detection* the A bit signaling is set to *0* towards T1 (E1)
- For *no ring detection* the A bit signaling is set to *1* towards T1 (E1).

B bit

- For *ring detection* the B bit signaling is set to *1* towards T1 (E1)
- For *no ring detection* the B bit signaling is set to *0* towards T1 (E1).

B bit inverted

- For *ring detection* the B bit signaling is set to *0* towards T1 (E1)
- For *no ring detection* the B bit signaling is set to *1* towards T1 (E1).

Default ABCD *to* the T1 (E1)

This parameter specifies the default signaling bits that are not used for ring detection or for polarity (if *Enabled*). Those bits will be transmitted towards T1.

Polarity (polarity reversal, also known as Wink Start Reversal)

When polarity is configured as *Enabled,* the polarity signal is received from T1 (E1) either on the B bit (while the *On/Off Hook from T1/E1* parameter is configured to *A bit* or *A bit inverted),* or on the A bit (while the *On/Off Hook from T1/E1* parameter is configured to *B bit* or *B bit inverted).*

Signaling Feedback

This parameter is set to:

Enabled Feedback of the *On/Off Hook signaling* that was received from T1 (E1) is transmitted back to T1 (E1)

Disabled Feedback of the *On/Off Hook signaling* that was received from T1 (E1) is not transmitted back to T1 (E1).

Out-of-Service Method

This parameter specifies the *On/Off Hook signaling* in FXO when an *Out-of-Service* condition is indicated in the T1 link. The values are:

Forced Idle Signaling is held *On Hook* for the duration of the *Out-of-Service* condition

Forced Busy Signaling is held *Off Hook* for the duration of the *Out-of-Service* condition.

E & M Voice Interface

The Voice Parameters Menu for WEB RANger-II with four E&M voice channels is shown in *Figure 4-77*.

```
       VOICE PARAMETERS:    ( Device name - WEB II    )

1.  TX/RX gains
2.  Interface type                 : [4W]
3.  E&M type                       : [A bit]
4.  Coding law                     : [μ LAW]
5.  E signal from the T1 on        : [A bit]
6.  M signal to the T1 on          : [A bit]
7.  Default ABCD to the T1         : [0000]
8.  Out-of-Service method          : [Forced Idle]

ESC - Return to previous menu
Choose one of the above:
```

Figure 4-77. E & M Voice Interface

RX/TX Gains

Select this parameter to specify the nominal input level of the Receive and Transmit paths for each voice port. The input level range is –10 to +5 dBm.

Interface Type

This parameter specifies the interface type:

2W Two-wire interface

4W Four-wire interface.

E&M Type

This parameter specifies the E&M signaling mode:

- **Type1**
- **Type2**
- **Type3**
- **Type5 –** SSDC5

Coding law

Select this parameter to specify the compounding law to be used by the voice channels. The values are:

A-Law Coding E1 links

μ-Law Coding T1 links.

E signal *from* the T1 (E1) on

Select this parameter to specify the E signal receive mode from T1 (E1) into E & M. The values are:

A bit

- When the received A bit signal from T1 (E1) equals *1* then the E signal will be activated in the E&M interface
- When the received A bit signal from T1 (E1) equals *0* then the E signal is inactivated in the E&M interface.

A bit inverted

- When the received A bit signal from T1 (E1) equals *0* then the E signal is activated in the E&M interface
- When the received A bit signal from T1 (E1) equals *1* then the E signal is inactivated in the E&M interface.

B bit

- When the received B bit signal from T1 (E1) equals *1* then the E signal is activated in the E&M interface
- When the received B bit signal from T1 (E1) equals *0* then the E signal is inactivated in the E&M interface.

B bit inverted

- When the received B bit signal from T1 (E1) equals *0* then the E signal is activated in the E&M interface
- When the received B bit signal from T1 (E1) equals *1* then the E signal is inactivated in the E&M interface.

Default ABCD to the T1 (E1)

This parameter specifies the default signaling bits that are not used for the M signal. Those bits will be transmitted towards T1.

Out-of-Service Method

This parameter specifies the *E signaling state in E & M* when an *Out-of-Service* condition is indicated in the T1 (E1) link. The values are:

Forced Idle E1 signal is held at *inactive* for the duration of the *Out-of-Service* condition

Forced Busy E1 signal is held at *active* for the duration of the *Out-of-Service* condition

Idle Busy E1 signal is held at *inactive* for 2.5 seconds, and then toggled to *active* until the *Out-of-Service* condition end

Busy Idle E1 signal is held at *active* for 2.5 seconds, and then toggled to *inactive* until the *Out-of-Service* condition end.

Timeslots for Voice Ports

Refer to Time Slot Mapping. A typical screen is shown in *Figure 4-78*.

```
T1 TIME SLOTS MAPPING :  LINK1  (device name – WEB II)

TS1   [VOICE 1     ]                                  TS13  [NC          ]
TS2   [NC          ]                                  TS14  [NC          ]
TS3   [NC          ]                                  TS15  [NC          ]
TS4   [NC          ]                                  TS16  [NC          ]
TS5   [VOICE 2     ]                                  TS17  [NC          ]
TS6   [NC          ]                                  TS18  [NC          ]
TS7   [NC          ]                                  TS19  [NC          ]
TS8   [NC          ]                                  TS20  [NC          ]
TS9   [NC          ]                                  TS21  [NC          ]
TS10  [VOICE 3     ]                                  TS22  [NC          ]
TS11  [NC          ]                                  TS23  [NC          ]
TS12  [NC          ]                                  TS24  [VOICE 4     ]



Enter time slot number (0 refer to all time slots)
Press 'Enter' – to toggle the time slot type
Press 'ESC'   - to Return to previous menu
Time slot number :
```

Figure 4-78. T1 Time Slots Mapping Link1 Screen

Voice Diagnostic Tools

Advanced Menu
↓**1**
Setup
↓**3**
Interface Parameters
↓**3**
E1/T1 & Voice Settings
↓**7**
Voice Diagnostics

There are three voice diagnostic tools that are available for WEB RANger-II. They can be set independently for each voice port:

Tone injection to the voice port	A 1 kHz signal is injected into the receive voice port path, replacing any receive signal from E1/T1.
Tone injection to the E1/T1	A 1 kHz signal is injected into the receive voice port path, replacing any receive signal from E1/T1, and injected into the E1/T1 transmit path, replacing any transmit signal to E1/T1.
Remote port loopback	The voice port signal that is received from E1/T1 is transmitted back to E1/T1.

Reset Voice Module

Advanced Menu
↓**1**
Setup
↓**2**
Device Control
↓**4**
Reset options
↓**3**
Reset interface module
↓**2**
Reset voice module

"Do you want to reset the voice module? (Y/N):'

Type **Y**.

Access Control (Security)

The Access Control mapping options are shown in *Figure 4-79*.

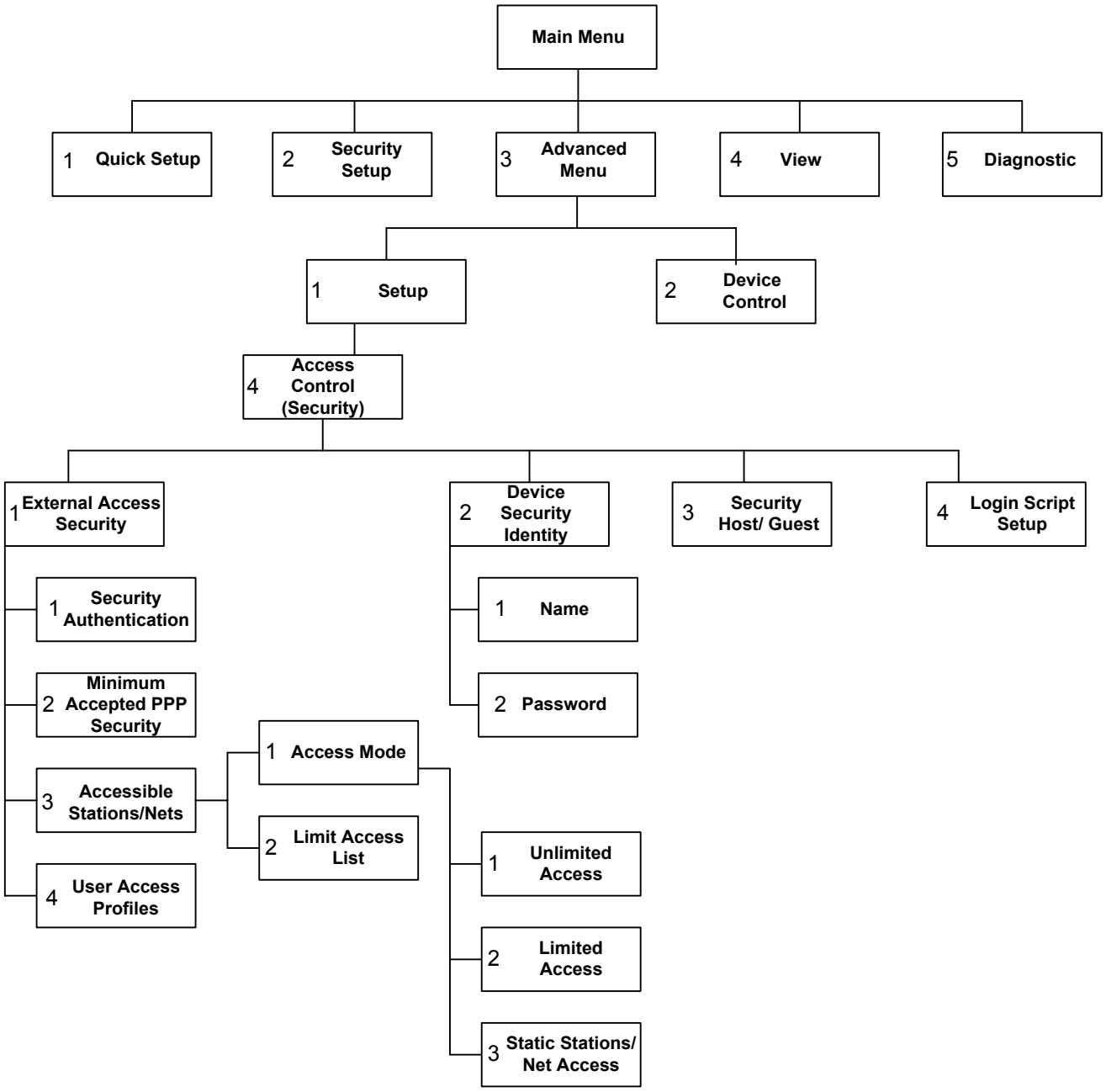


Figure 4-79. Access Control Menu Outline

➤ **To access the Access Control menu:**

1. In the Advanced Menu, press **1**.
   The Setup menu appears.
2. In the Setup menu, press **4**.
   The Access Control menu appears (see *Figure 4-80*).

```
      ACCESS CONTROL  ( Device name - WEB RANger-II  )

 1. External access security
 2. Device security identity
 3. Security Host/Guest
 4. Script Setup

  ESC - Return to previous menu

  Choose one of the above:
```

Figure 4-80. Access Control Menu

The options in the Access Control menu are described below.

External Access Security (only relevant to Link with PPP Protocol)

Advanced Menu
↓**1**
Setup
↓**4**
Access Control
↓**1**
External Access Security

Security Authentication

Select this parameter to protect your LAN against unwanted entry by outside users. Toggle between the following options:

None	Access permitted to all users.
User Access Profile	Allow/deny access according to the User Access Profile (see below).
RADIUS	Allow/deny access according to the RADIUS Authenticator.
User Access Profile +RADIUS	Access is allowed if the User Access Profile permits it OR if the User Access Profile does not have an entry for the user but the RADIUS Authenticator allows it.

Note

If you select RADIUS, configure the RADIUS Access parameters from the Host Parameters menu. Refer to RADIUS Authentication and Billing.

Accepted PPP Authentication (only relevant to Link with PPP Protocol)

PPP supports 2 types of security systems:

CHAP (Challenge Handshake Authentication Protocol)

CHAP is a type of authentication in which the authentication agent (typically a network server) sends the client program a key to be used to encrypt the username and password. This enables the username and password to be transmitted in an encrypted form to protect them against hackers.

PAP (Password Authentication Protocol)

PAP is the most basic form of authentication, in which a user's name and password are transmitted over a network and compared to a table of name-password pairs. Typically, the passwords stored in the table are encrypted. The main weakness of PAP is that both the username and password are transmitted in an unencrypted form.
Select this option for maximum and minim accepted protocol.

Accessible Stations/Nets

Select this parameter to define parameters that limit public access to the network. Access can be allowed for all stations/nets, only certain stations/nets, or only stations/nets which are static. When the access mode is 'limited', use the access list to define which stations/nets have access.

User Access Profiles (only relevant to Link with PPP Protocol)

Select this parameter to view and modify user access profiles in the access control users list. The list contains user names, security parameters and dialback options.

Device Security Identity (PPP only)

Advanced Menu
↓1
Setup
↓4
Access Control
↓2
Device Security Identity

Name

Select this parameter to assign a name to WEB RANger-II for access to the ISP's central access router. The maximum length is 30 characters.

Password

Select this parameter to assign a password to WEB RANger-II for access to the ISP's central access router. The maximum length is 30 characters.

Security Host/Guest (PPP only)

Advanced Menu
↓**1**
Setup
↓**4**
Access Control
↓**3**
Security Host/Guest

Select this parameter to define a link's security status. When a link is defined as a **Host**, users are approved according to your profile list. When the link is defined as a **Guest**, the device sends its name and password (defined above) to be approved by the host. The *Guest* mode is the default for *Originate only* links. For *Answer* and *Answer&Originate* links the default mode is *Host*.

Login Script Setup

Advanced Menu
↓**1**
Setup
↓**4**
Access Control
↓**4**
Login Script Setup

WEB RANger-II scripting tool allows you to negotiate an initial login, required by some ISPs. The initial login usually consists of a username, password and possibly some other information, which has to be entered to gain access to the ISP.

WEB RANger-II script is a sequence of commands, with a maximum of 20 commands in the script. As soon as a physical connection to the remote host is achieved (and the script is enabled), WEB RANger-II begins to forward the script. Script processing finishes when the last script command has been forwarded.

WEB RANger-II script comprises one or more command lines. Each command line consists of a *Command Code* followed by an *Argument*.

Command Code

The command codes are described in *Table 4-5*.

Table 4-5. Command Codes

Command Code	Description
waitcase *pattern*	Waits until the specified case-sensitive pattern is received from the remote host and forwards the next command. The maximum pattern length is 24 characters. Or, waits until timeout (default = 15 seconds). The link then disconnects and WEB RANger-II performs the same actions as required during authentication failure.
waitnocase *pattern*	Same as waitcase *pattern* except not case sensitive.
send *pattern*	Transmits specified pattern to remote host. The pattern can contain any recognized control symbols. The maximum pattern length is 24 characters.
sendhide *pattern*	As above. However, the pattern is displayed on the screen as asterisks. The control symbol is displayed as two asterisks when editing and as one when viewing.
timeout *number*	Changes the timeout for **waitcase**, **waitnocase** and **getip** commands. The number is the timeout value, in seconds. This value can be any number from 1 to 99 and will be used until the next timeout command.
delay *number*	The delay in seconds between sending commands. All symbols received during this time will be ignored. This value can be any number from 1 to 99.
getip *number*	This command waits for an IP address from the remote host. If the remote host returns several IP addresses in a string, the number specified by this command will determine which IP address should be used. If an IP address is received successfully from the host, and the Single IP feature is enabled, the IP address will be used on WEB RANger-II WAN interface. If an IP address is not received successfully within the specified timeout period, the link disconnects.

Argument

The argument is any string without apostrophes, quotation marks or unsigned integers (depending on the command). In addition to ASCII symbols, the argument string can include any control characters with ASCII codes from 1 to 31. While editing scripting commands, these symbols are entered in the 'control' mode i.e. each symbol is entered as "^", followed by the corresponding ASCII character from "A" to "[". The letters must be in upper case. See *Table 4-6*.

Table 4-6. Example of Argument

Code to wait/send	Control Sequence
0x0A (line feed)	^J
0x0D (carriage return)	^M
0x0B (escape)	^[

WAN Economy Menu

The WAN Economy menu options are shown in *Figure 4-81*.

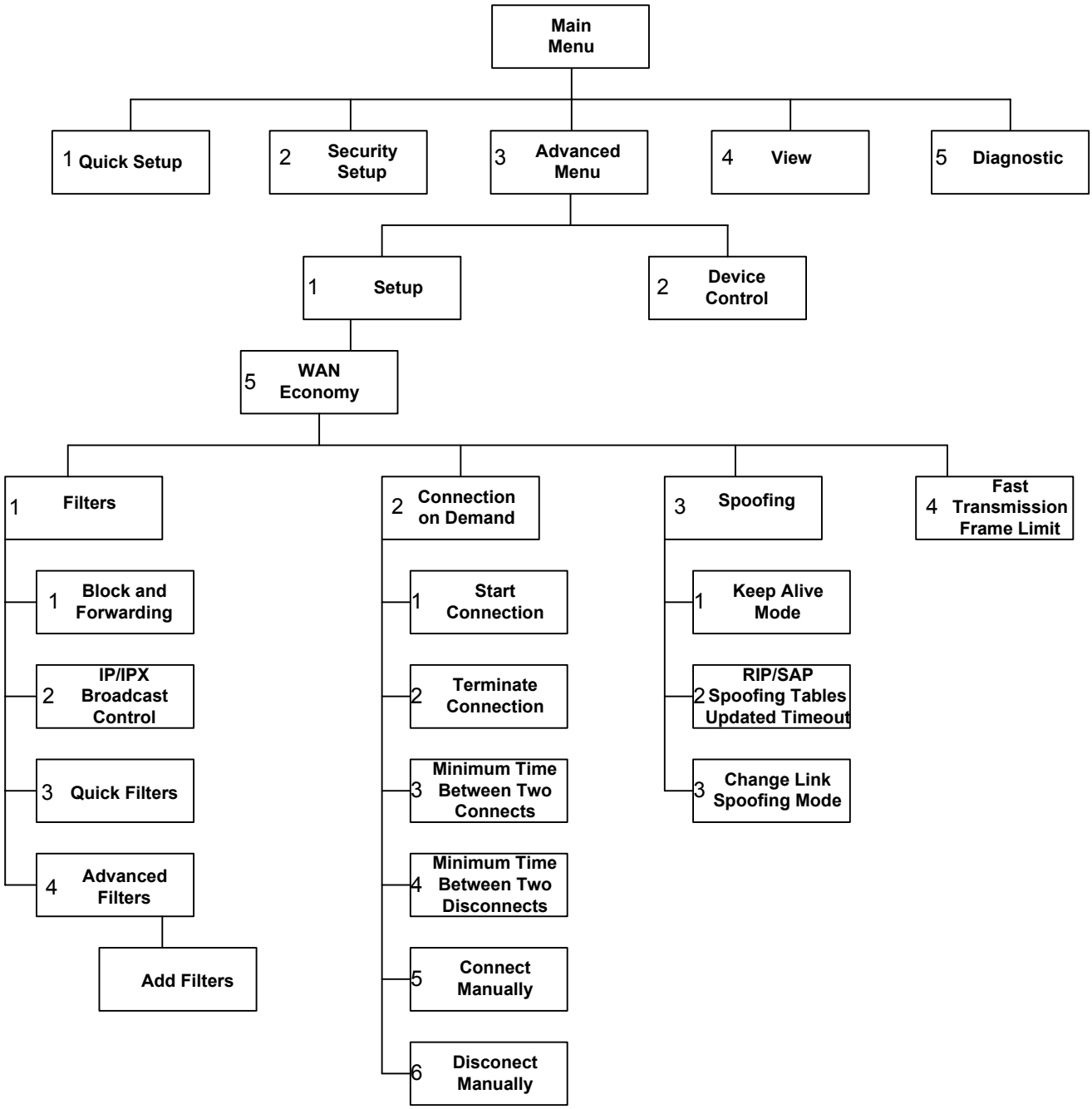


Figure 4-81. WAN Economy Menu Outline

➤ **To access the WAN Economy menu:**

1. In the Advanced Menu, press **1**.
   The Setup menu appears.
2. In the Setup menu, press **5**.
   The WAN Economy menu appears (see *Figure 4-82*).

```
      WAN ECONOMY  ( Device name - WEB RANger-II )

Use these features:
- to reduce traffic over the WAN to a minimum and increase throughput
- to keep the link up only when it is required
  1.  Filters
  2.  Connection on demand
  3.  Spoofing
  ESC - Return to previous menu
  Choose one of the above:
```

Figure 4-82. WAN Economy Menu

The options in the WAN Economy menu are described below.

Filters

Advanced Menu
↓**1**
Setup
↓**5**
WAN Economy
↓**1**
Filters

Filtering allows you to limit the amount of traffic that enters and exits the Small Office LAN via WEB RANger-II. If the WEB RANger-II is attached to more than one LAN, then select this option for each LAN interface. Filtering is used to:

- Increase security
- Reduce traffic to the link.

WEB RANger-II features two types of filters:

- Quick Filters
- Advanced Filters.

Quick Filters are used to regulate specific protocols:

- IP
- IPX
- SNA
- NetBIOS
- AppleTalk
- DECnet.

A Quick Filter can neutralize these protocols by blocking all traffic of that protocol from the LINK inwards. Refer to *Figure 4-83*.

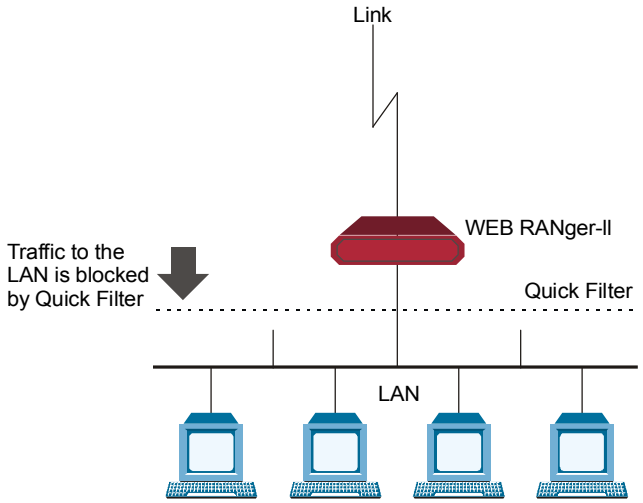


Figure 4-83. Action of a Quick Filter

Advanced Filters are used to regulate traffic in both directions. (Refer to *Figure 4-84*).

- From LAN to the Link. Using filters here will forward or block traffic from the LAN outwards.
- From Link to the LAN. Using filters here will forward or block traffic from the link inwards.

Using a variety of parameters, Advanced Filters can be used to regulate different protocols, to totally or partially block traffic, and to control traffic between links.

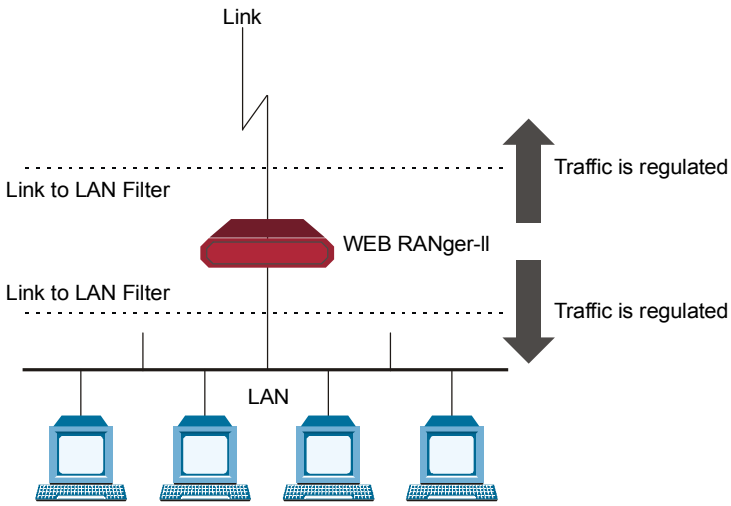


Figure 4-84. Action of an Advanced Filter

There are two modes through which filtering can be implemented: **blocking** and **forwarding**.

Blocking

The block command causes WEB RANger-II to test every packet of data that is sent to or from the LAN. If the packet passes the test, passage is denied.

Example:

You want to ensure that IP/UDP packets do not go on to the link in the direction of the Internet/Intranet. Thus, you design a filter that tests each packet to see if it is an IP/UDP packet. If the packet tests positive, it is automatically blocked.

Forwarding

The forward command works in the same way as the block command. However, with forwarding, if the packet passes the test, the packet is allowed to pass to or from the LAN.

Example:

To allow a certain user on the Small Office LAN to access the Internet for FTP purposes, create a filter to test each packet for the IP host address of the specified user and the FTP socket of the packet. If the packet passes the test, the packet is forwarded to the Internet/Intranet.

Multiple Filters

Up to 18 filters can be defined. If there are two filters that have contradictory operations, forwarding takes precedence over blocking.

Example:

You want to allow **only** one particular user on the Small Office LAN to access the Internet for FTP purposes. To insure that no one else is able to access the Internet, create a blocking filter for all traffic going to the link. To do this, from the Blocking and Forwarding menu enter **Block all traffic for Link1**. In addition, create a filter to test each packet for the IP host address of the specified user and the FTP socket of the packet. *Since forwarding takes precedence over blocking*, that user's frames are forwarded.

Definition of Filter Tests

You need to define the filter test that will be applied to every packet that is transmitted. Use any combination of the following parameters to define the filter test:

- Protocol
- Operation (block, forward, etc.)
- Interface (LAN, Link)
- Destination and/or source IP address of the packet
- Destination and/or source MAC address of the packet (layer 2)
- IP socket (upper and lower level)
- IP packet type (broadcast, multicast).

Note *Up to 18 filters can be defined. To avoid reducing WEB RANger-II performance, minimize the number of active filters.*

Defining Filters

Filters can be defined through the control port, TELNET or SNMP. First decide on the mode and conditions for a filter, then follow the instructions below to set filter parameters.

```
 FILTERS  ( Device name - WEB RANger-II  )

1. Block and Forwarding
2. IP / IPX broadcast control - [Full Propagation]
3. Quick filters
4. Advanced filters

Esc - Return to main menu

Choose one of the above:
```

Figure 4-85. Filters Menu

➤ **To configure the operation:**

1. From the Filters menu, choose **Block and Forwarding**.
2. Toggle between **Block** and **Forward**.

➤ **To configure the broadcast control:**

The broadcast control filter manages special frames, normally not propagated throughout the network. The frames managed are:

- IP - Local broadcast propagation
- IPX - Zero destination propagation, IPX Type 20 frames propagation
- NETBIOS over IP - IP frames with TCP/UDP ports 137, 138, 139 propagation.
- From the Filters menu, press **2** to toggle between Full Propagation and Block Propagation.

Factory default: Block Propagation.

Quick Filters are defined per protocol. Configure each protocol that you want to block or forward.

➤ **To configure the Quick Filter parameters:**

1. From the Filters menu, choose **Quick Filters**.

   The Quick Filters menu appears (see *Figure 4-86*).

Quick Filters Menu

Advanced Menu
↓**1**
Setup
↓**5**
WAN Economy
↓**1**
Filters
↓**3**
Quick Filters

There are 4 steps in defining a Quick Filter:

1. From the Advanced Setup menu, choose: **Set up** → **WAN Economy** → **Filters**.
2. Configure the operation.
3. Configure the broadcast control.
4. Configure the Quick Filter parameters.

To toggle between Forward/Block, press the number of the protocol that you want to filter.

Note *Remember that forwarding takes precedence over blocking. If you combine filters that contain both operations, the frame will be forwarded.*

```
QUICK  FILTERS  ( Device name - WEB RANger-II )

Choose the protocols you want to block or forward!!:
(The Blocking or forwarding is to interface LAN 1 only)

1. IP          NO FILTERS
2. IPX         NO FILTERS
3. SNA         NO FILTERS
4. NetBIOS     NO FILTERS
5. AppleTalk   NO FILTERS
6. DECnet      NO FILTERS
7. Others      NO FILTERS

ESC - Return to previous menu
Choose one of the above:
```

Figure 4-86. Quick Filters Menu

Note *In WEB RANger-II 2 LANs configuration:*
For LAN1, use Quick Filters
For LAN2, use Advanced Filter.

Advanced Filters

Advanced Menu
↓**1**
Setup
↓**5**
WAN Economy
↓**1**
Filters
↓**4**
Advanced Filter

There are 4 steps in defining an Advanced Filter:

1. From the Advanced Setup menu, choose:
   Set up → **WAN Economy** → **Filters**.
2. Choose Advanced Filter.
3. If you are defining a new filter, choose **Add**.
   If you are editing a filter, choose **Edit** and enter the filter number.
4. Define the desired parameters.

Advanced Filter Concepts

When defining an advanced filter the following parameters must be determined:

- Filter ID – A selection number used to view, edit or delete a particular file. To work with any filter, the Filter ID number must be entered (as in *Figure 4-87*).
- Protocol – The protocol on which the filter operates
- Operation – Defines the action of the filter
- Interface – Determines the filter interface
- Source Address – Defines the source address of passing frames
- Destination Address – Defined the destination address of passing frames
- High level (IP only) – Includes or exclude high level protocols
- Source / Destination Port – Defines the port source / destination address of an application
- Source / Destination Socket – Defines the socket source / destination address of an application
- Low Level – Includes or exclude the low level protocols
- Mask – Defines a mask filter
- Status – Defines the filter's status.

```
   ADD  FILTERS ( Device name - WEB RANger-II )

     Enter     -  Enter data
     T         -  Toggle (parameters inside [] )
     N         -  Next line (skip this one)
     SPACE     -  Move right
     BACKSPACE -  Move left
     ESC       -  Return to previous menu

Filter Id -  1
```

Figure 4-87. Add Filters Menu

True-False Menus

Many of the Advanced Filter parameters can be configured so that:

- Frames *with* that parameter pass (true)
- Frames *without* that parameter pass (false).

For example, if you choose BroadCast - True, any frame which *is* BroadCast will pass. If you choose BroadCast - False, any frame which *is not* BroadCast will pass.

Advanced Filter Parameters

- Filter ID - The system automatically assigns a new number to each filter
- Protocol - The protocol on which the filter operates
- Operation - The action which the filter applies to a frame that passes:
  - **Forward**
  - **Block**
  - **Connect**
  - **Disconnect**.

The operations are listed in their order of priority. For example if the connect and disconnect commands are applied to a frame, the connect command takes precedence.

Note *Connect and disconnect are only relevant to Connection on Demand. When accessed through the Filter menu, only they appear.*

- Interface – The area where the filters will act. If you want to filter traffic going to the LAN, choose **LAN**. If you want to filter traffic going to the link, choose **Link**.

- Source Address – Toggle to the desired address type (**MAC** or **NET**). The address format (hexadecimal or binary) appears. Type in the complete source address.
  If you want to include a group of addresses, type **<x>** to indicate "Don't care". For example, a filter with the MAC source address the 4020.D2FE.xxxx will pass any address beginning with 4020.D2FE. You select **IP RANGE** to filter a group of sequential IP addresses.
- Destination Address – Toggle to the desired address type (**MAC**, **NET**, **All**, **BroadCast**, **MultiCast**). The address format (hexadecimal or binary) appears. Type in the complete destination address. Choose **True** or **False**.
- Normally, a frame has a particular destination, as specified in the destination address field of the frame. Such frames are referred to as "All" frames. "BroadCast" frames are intended for all stations. If you specify "BroadCast" do not specify a mask pattern. Select **IP RANGE** to filter a group of sequential IP addresses.
- High Level – When you choose this parameter, 2 choices appear:
  - **Yes**

    When **Yes** is chosen, a list of High Level protocols appear:
    - **FTP**
    - **WWW**
    - **TELNET**
    - **E-MAIL**
    - **TFTP**
    - **SNMP**
    - **DNS**
    - **RIP**.
  - **No**.
    Select the protocols you want to filter. Choose **True** or **False**.
- Source/Destination Sockets - This parameter differs for IP and IPX:
  - IP: The Destination Port is enabled when no High Level protocol is specified. If you define a port number in decimal numbers, define the low-level protocol as **UTP** or **TCP**. If no port number is defined, define the low-level protocol as **UTP**, **TCP**, or **ICMP**. Choose **True** or **False**.
  - IPX: If a socket address or low-level protocol is not defined, a socket number may be specified. Choose **True** or **False**.
- Low Level (IP protocol) - Toggle to the required low level protocol for the filter. If the port number is defined in decimal format, specify the low-level protocol as **UTP** or **TCP**. If no port number is defined, specify the low-level protocol as **UTP**, **TCP**, or **ICMP**. Choose **True** or **False**.

- Low Level (IPX protocol) - Toggle to the required low level protocol for the filter. If a socket is defined in the destination address, a low-level protocol or socket number may not be specified. Conversely, if a socket address or low level is not defined, a socket number may be specified.
- Mask - A mask is a test pattern that is used to allow certain frame patterns only. You define a code against which the frame is compared.
  To create a mask, toggle to **Yes**. Three pairs of codes and offsets must be created. The offset defines the point in the frame at which the comparison is made. For example, an offset of 8 means that the 8th byte is compared to the code. The offset can be from the 7th byte onwards.
  The frame is made of 3 different portions:
  - MAC: at the beginning of the frame
  - LLC: after the source address in the frame
  - DATA: after the LLC section in the frame.

  For each code-offset pair, select the code format:
  - **Binary:** specify 48 address bits to be either 0,1, or X (unspecified).
  - **Hexadecimal:** specify 12 hex digits to be 0-F or X (unspecified).

  For each code-offset pair, choose **True** or **False**.

  Every frame, at the designated offsets, is compared to the 3 codes in the mask. If all 3 codes and the True-False condition match the code written in the frame, the frame passes.

Note *Only 1 mask can be defined.*

- Status - Toggle between:
  - **Active**
  - **Not Active** - Not active allows you to define filters which can be stored and used at a later time.

Saving Filter Parameters

All filters are stored in the Flash Memory, thereby preserving them if the power goes down. When filtering is selected, all of the filters are copied into the RAM. The RAM copy is then used to activate the software filtering process. Any filter which is modified, (by clearing all, deleting one, or changing a parameter) goes into effect immediately. The previous filter also remains in effect until the system is rebooted.

To exit filtering and return to the main Setup menu, press **<Esc>**. The following prompt appears: **'up' (Y/N)?**

Press **Y** to save changes in the Flash Memory. Press **N** to cancel your changes. The system loads the previous set of masks the next time the system is rebooted.

Connection on Demand

To save money, you may want to limit the time that a link is kept open. COD allows you to determine the traffic conditions that open and close the link. Using COD, a line is opened only when traffic conditions fulfill specified conditions. When there is no need for a connection, the line is automatically terminated.

COD is only effective if:

- The line is connected to a modem or ISDN (a dialup link)
- The link is asynchronous
- The connection type is *originate* or *answer&originate*.

If the connection type is *answer only*, the line connection is started when the unit is turned on in order to receive calls. If the connection type is *originate only* or *answer&originate* the connection starts when a telephone number is defined.

You need to configure:

- Start Connection
- Terminate Connection.

Start Connection

Start Connection is used to determine under which conditions is a line established. To use this function, the line *must not* be designated as *answer only*. After a physical connection is made, data is transferred.

Start Connection has 4 options:

- **Upon Power Up** - The line is established when the unit is turned on. Upon Power Up is recommended for leased lines only.
- **Any Frame to Forward** - The line is established when any frame that is directed to the link arrives.
- **Specific Frame to Forward** - The line is established only when specific types of frames directed to the link arrives. To determine which frames are establish a line, filters are used to specify the type of frame.
  Any number of filters can be used. Filters work as a Boolean "OR"; by specifying a filter for frame type A and filter for frame type B , you establish a line for Frame type A or Frame type B.
  Choosing this option automatically opens the Advanced Filter menu, with *Connect Operation* selected.
- **Never** - The line is permanently cutoff. In this case, you manually decide when to activate a line.

Terminate Connection

Terminate Connection is used to determine under which conditions does a link terminates. Termination takes place only after a physical connection is made.

Terminate Connection has 4 options:

- **Never** - The line is never terminated. **Never** is usually used when **Upon Power Up** is used.
- **No Frame to Forward** - The line is terminated after a specified time passes without a frame passing through the line. You specify the time in which a frame must pass. The default is 60 seconds.
- **Upon Time Out** - The line is terminated after a fixed period of time regardless of the traffic. The default is 60 seconds.
- **No Specific Frame to Forward** - The line is terminated if traffic of a specific type of frame falls below a certain rate over a period of time. You determine the number of frames and the time period in which they must pass. Using filters, you specify which type of frames are counted. If frames other than those specified pass through, they are not counted.
  Choosing this option automatically opens the Advanced Filter menu.

COD includes 4 other options which can be used to regulate line time.

- **Minimum Time Between 2 Connections** - This option determines how much time there must be between a line being terminated and then reactivated. This option is only used when *upon power up* is chosen in *start connection*. All other options are determined by the frame traffic.
- **Minimum Time Between 2 Disconnections** - This option determines the minimum time between two disconnections. Using this option allows you to determine a minimum time-up. This option overrides other *terminate connection* options.
- **Connect Manually** - This option activates a line immediately. This option overrides any other connection option, including *minimum time between 2 connections*.
- **Disconnect Manually** - This option terminates a line immediately. This option overrides any other terminate option, *including minimum time between 2 disconnections*.

The following examples demonstrate how COD can be used.

Example 1:

A company needs their WEB RANger-II to be connected to the Internet 24 hours a day. Therefore the following must be defined:

- Start connection is *upon power up*
- Terminate Connection is *never* (see *Figure 4-88*).

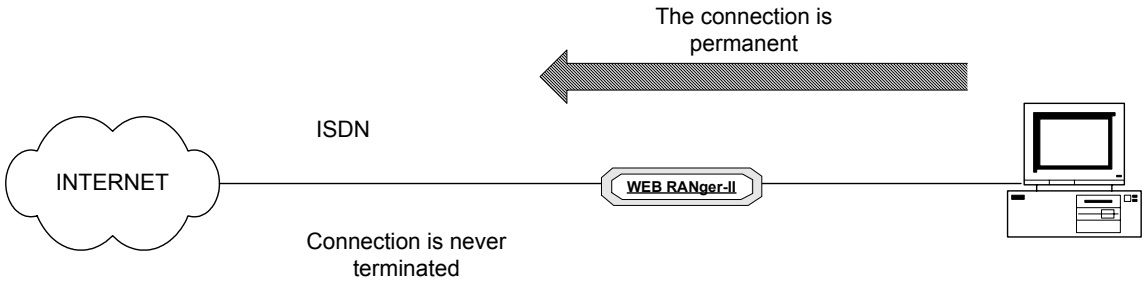


Figure 4-88. Permanent Connection

Example 2:

To lower expenses, WEB RANger-II is configured so that a line to the Internet is activated when there is a need to connect to the Internet and terminates when no frames are transmitted for 60 seconds. Therefore the following must be defined:

- Start Connection is *any frame to forward*
- Terminate Connection is *no frame to forward* for 60 seconds (see *Figure 4-89*).

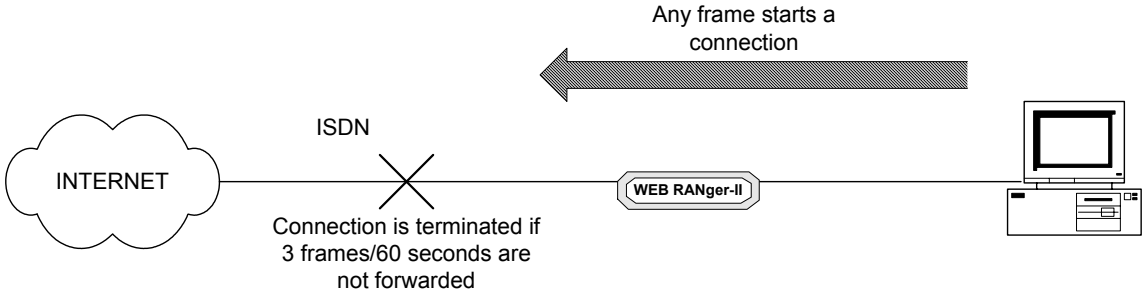


Figure 4-89. Any Frame Starts a Connection

Example 3:

The company management wants to allow the PC with the IP address 1.2.3.4 only access to the Internet. In addition, the connection to the Internet is to be terminated if 3 frames every 60 seconds are not transmitted from this PC.

Therefore the following must be defined:

- Start connection must be *specific frame to forward*. A filter which allows only frames from the 1.2.3.4 IP address must be defined.
- Terminate connection must be *no specific frame to forward*. A filter which counts only frames from the 1.2.3.4 IP address must be defined. In addition the rate must be defined at 3 frames/60 seconds (see *Figure 4-90*).

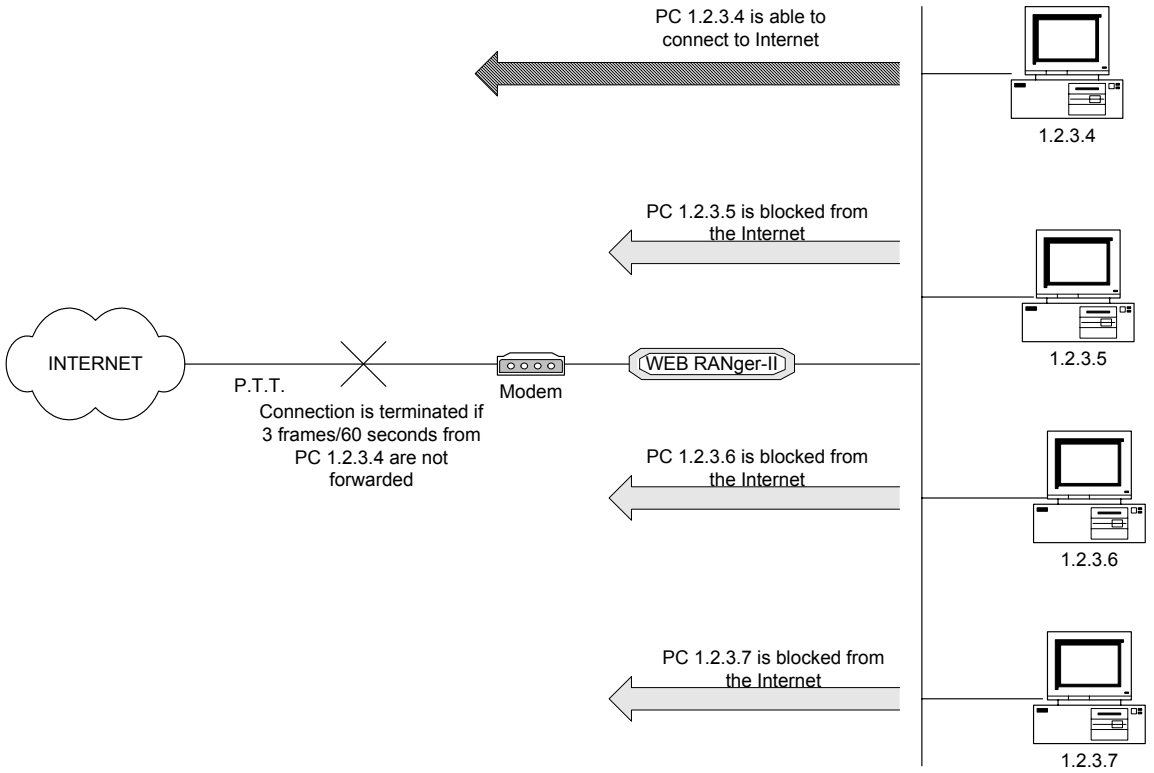


Figure 4-90. Limiting Access to a Specific PC

Example 4:

A company uses a phone line which uses a phone and modem to connect to the Internet. The only time that the employees may connect to the Internet is if they need to upload or download files to a FTP site. Any connection to the Internet is to be done manually. After the file has been uploaded or downloaded the connection is to be terminated automatically. Therefore the following must be defined:

- Start connection must be *never*. Any time someone wants to connect, the user must connect manually.
- Terminate connection must be *upon time out*. The time is set to 30 seconds.
- Set filter to *FTP only forwarded* (see *Figure 4-91*).

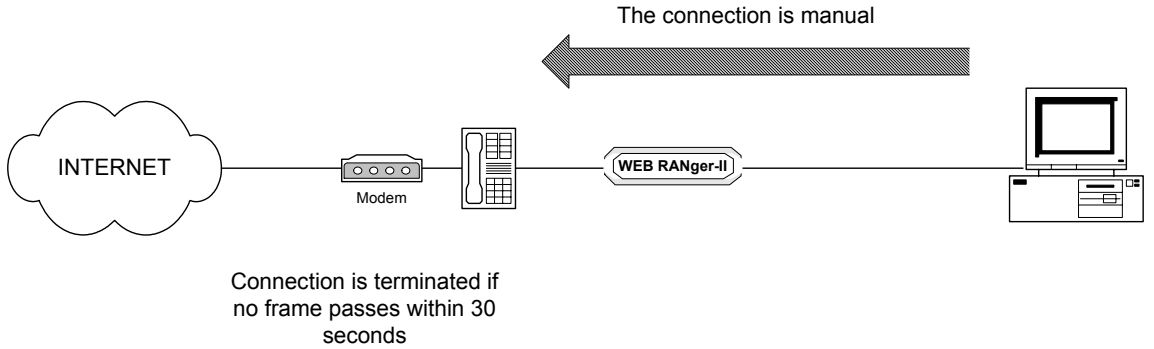


Figure 4-91. Manual Connection

IP/IPX Spoofing

Spoofing is a technique used to reduce network overhead, especially in wide area networks (WAN). Some network protocols send frequent packets for management purposes. These can be routing updates or keep-alive messages. In a WAN this can introduce significant overhead, due to the typically smaller bandwidth of WAN connections.

Spoofing reduces the required bandwidth by having devices, such as bridges or routers, answer for the remote devices. This fools (spoofs) the LAN device into thinking that the remote LAN is still connected, even though it is not. The spoofing saves the WAN bandwidth, because no packet is ever sent out on the WAN.

Figure 4-92 shows the IP/IPX Spoofing menu.

```
 IP/IPX SPOOFING  ( Device name - ET - 8D  )


Keep Alive (IPX)

1.  Keep Alive mode: [Disabled]
2.  Timeout - PC-LAN bridge links (minutes): 120

RIP / SAP spoofing (IP/IPX)

3.  RIP/SAP spoofing tables updated timeout (minutes): 30
4.  Change link spoofing mode

Link 1 spoofing mode: Disabled
Link 2 spoofing mode: Disabled
ESC - Return to previous menu

 Choose one of the above:
```

Figure 4-92. IP/IPX Spoofing Menu

The parameters in the Spoofing menu are:

- Keep Alive (IPX)
- RIP/SAP Spoofing (IP/IPX).

Keep Alive (IPX)

Keep Alive Mode

Select this parameter to **Enable**/**Disable** the Keep Alive mode. Keep Alive mode allows the remote user to remain on the local server station list for a specified period of time during link disconnection.

Timeout

The amount of time inactive PC to LAN links are kept open when WEB RANger-II is configured as a bridge.

Note *SPX spoofing is not supported.*

RIP/SAP Spoofing (IP/IPX)

Spoofing is a technique used to reduce network overhead, especially in a WAN. Some network protocols send frequent packets for management purposes. These can be routing updates or keep-alive messages. In a WAN this can introduce significant overhead, due to the typically smaller bandwidth of WAN connections.

Select this parameter to determine the length of time (in minutes) between exchange of RIP and IPX SAP tables over the WAN. This parameter is applicable unless spoofing mode is set to "Upon Change" only.

Change Link Spoofing Mode

This parameter can have the following values:

- **Disabled** (default) - When disabled, RIP/SAP updates are sent:
  - After a defined time (default time is 30 seconds IP, 60 seconds IPX RIP and SAP);
  - **AND** when there is a change in the network topology; for example an interface goes up or down, or a routing entry aged.
- **Enabled -** When enabled, RIP/SAP updates are sent:
  - After a defined time;
  - When there is a change in the network topology;
  - After a defined time and a change in network topology.
- **Enabled COD -** When this parameter is set to Enabled COD, updates are sent according to:
  - The disabled parameter when the line is up.
  - The enabled parameter when the line down.

Fast Transmission Frame Limit

This option allows you to insert the maximum number of acknowledge frames in the buffer to prevent unnecessary retransmissions on the WAN.

Factory Default Options

The Factory Default menu allows you to change all configuration parameters, returning configuration parameters back to their factory defaults.

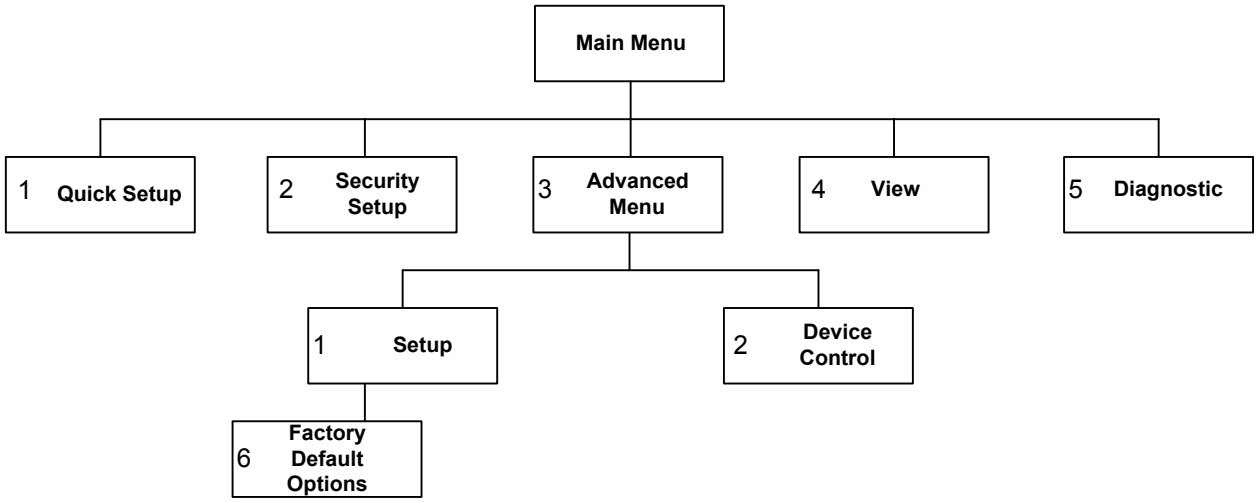


Figure 4-93. Factory Default Menu Outline

➤ **To access the Factory Default menu**

1. In the Advanced Setup menu, press **1**.
   The Setup menu appears. :
2. From the Setup menu, press **6**.
   A string of text appears, prompting you to reset certain parameters.
3. Press **Y** to reset the parameters to the factory default, or **N** to avoid reset.
   The next string of text appears.

Figure 4-94 displays all the parameters that can be reset.

```
Reset MONITOR parameters to factory default?          (Y/N): Y
Reset DEVICE ID parameters to factory default?        (Y/N): Y
Reset MASKS parameters to factory default?            (Y/N): Y
Reset FORWARDING parameters to factory default?       (Y/N): Y
Reset SPOOFING parameters to factory default?         (Y/N): Y
Reset SNMP parameters to factory default?             (Y/N): Y
Reset LINKS parameters to factory default?            (Y/N): Y
Reset DOWNLOAD parameters to factory default?         (Y/N): Y
Reset COD parameters to factory default?              (Y/N): Y
Reset MODEMS parameters to factory default?           (Y/N): Y
Reset FRAME RELAY parameters to factory default?      (Y/N): Y
Reset PPP parameters to factory default?              (Y/N): Y
Reset HOST IP parameters to factory default?          (Y/N): Y
Reset TELNET parameters to factory default?           (Y/N): Y
Reset RADIUS parameters to factory default?           (Y/N): Y
Reset SECURITY parameters to factory default?         (Y/N): Y
```

Figure 4-94. Factory Default Screen

4.6 Device Control Menu

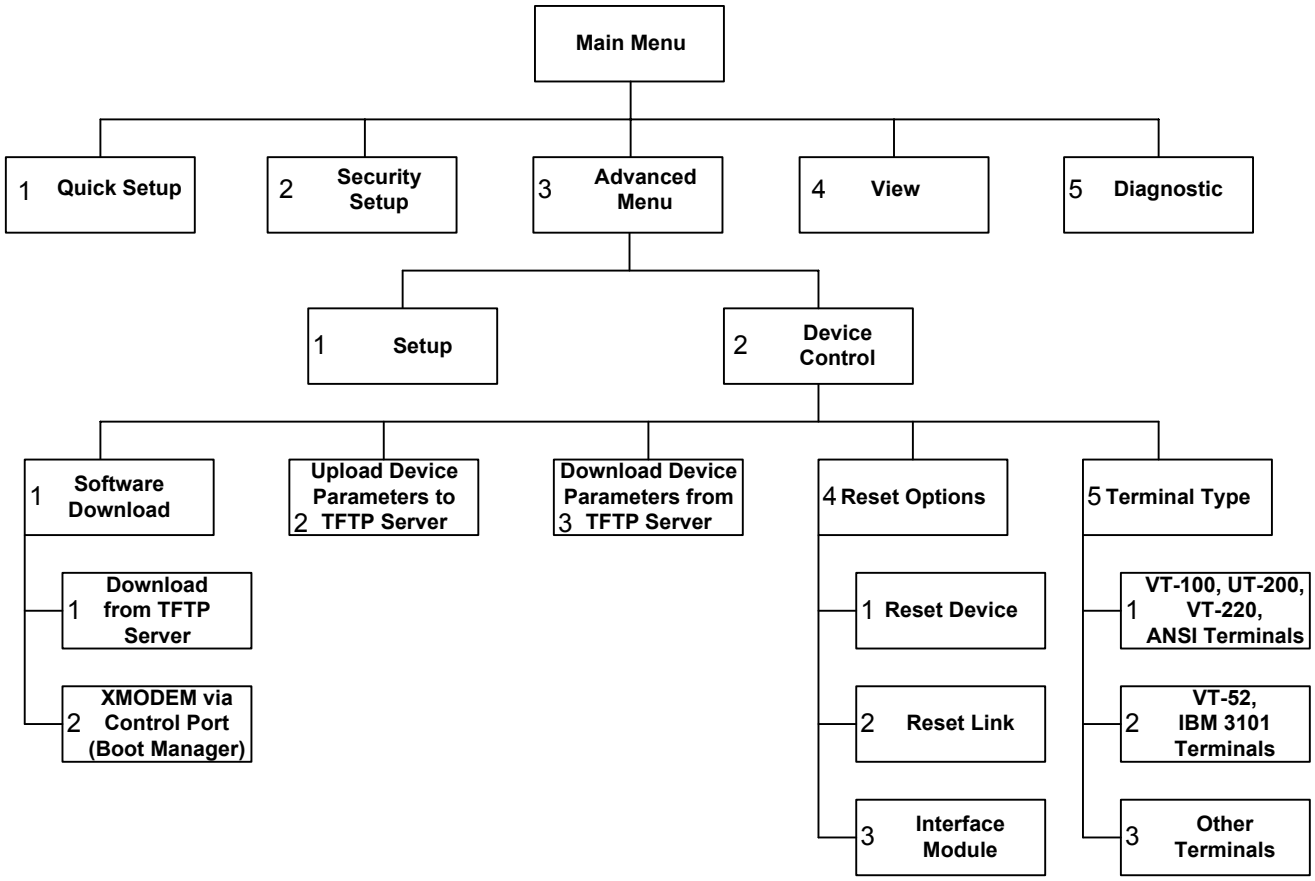


Figure 4-95. Device Control Menu Outline

➤ **To access the Device Control menu:**

1. In the Advanced Menu, press **2**.

   The Device Control menu appears (see *Figure 4-96*).

```
     DEVICE CONTROL  ( Device name - WEB RANger-II  )

  1.  Software download
  2.  Upload device parameters to TFTP server
  3.  Download device parameters from TFTP server
  4.  Reset options
  5.  Terminal type

  ESC - Return to previous menu
  Choose one of the above:
```

Figure 4-96. Device Control Menu

The options in the Device Control menu are described below.

Software Download

Advanced Menu
↓2
Device Control
↓1
Software Download

Select this option to download a new software version.

```
SOFTWARE PARAMETERS IN THE DOWNLOAD (Device name-WEB II )

1.  The parameters in the download from TFTP Server
2.  The parameters in the MODEM via control port (BOOT Manager)
3.  The parameters in the download software to ISDN module

ESC - Return to previous menu
Choose one of the above :
```

Figure 4-97. Software Download Menu

WEB RANger-II includes a Dual Image Flash, capable of storing two different versions of software in two different partitions.

Upon reset (or boot, refer to *Appendix* B), WEB RANger-II automatically runs the program stored in the **active** partition.

New software versions are loaded into the **backup** partition. If loading succeeds, the **backup** partition becomes **active** and reset is automatically performed, running the new software version. If loading fails, however, the device will still be capable of working, since the Flash partition storing the old version is still **active**. Refer to *Figure 4-98*.

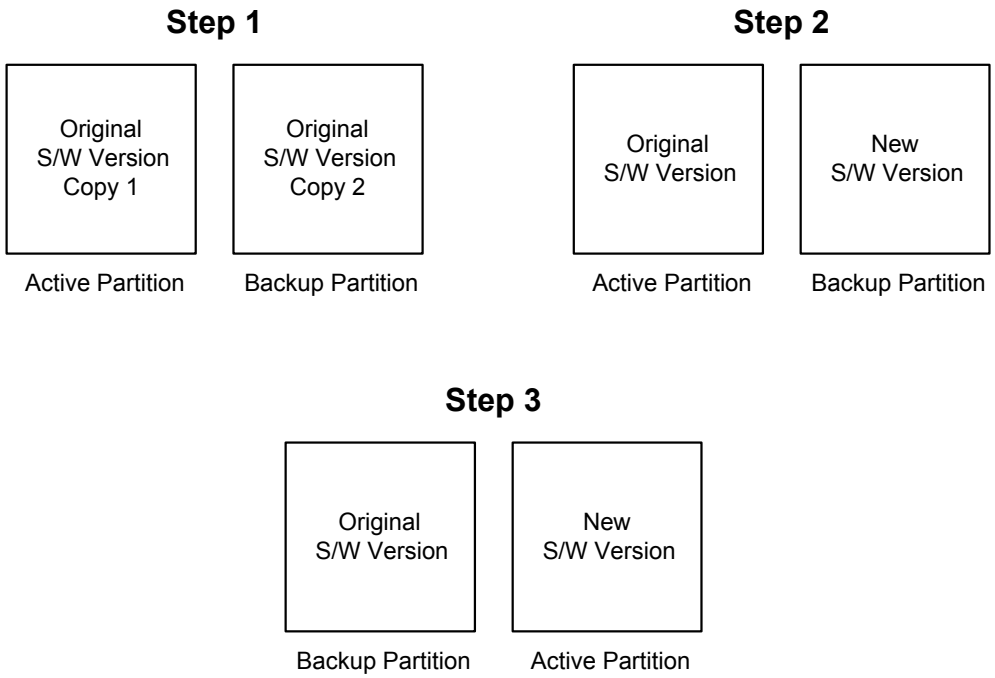


Figure 4-98. Using the Dual Image Flash

Control Dual Image Flash by the BOOT Manager. You use the BOOT Manager to manually define active and backup partition, run backup partition, erase some or all information from Flash, etc. The BOOT Manager is accessible via the above menu or immediately after resetting the hardware. Refer to *Appendix B* for a detailed description of the BOOT Manager.

The options in the Software Download menu are described below.

Download from TFTP Server

Advanced Menu
↓2
Device Control
↓1
Software Download
↓1
Download from TFTP Server

TFTP is an IP/UDP client-server application. The unit is a TFTP client. Operating opposite the client, you need a TFTP server connected to the LAN or WAN interface via an IP network.

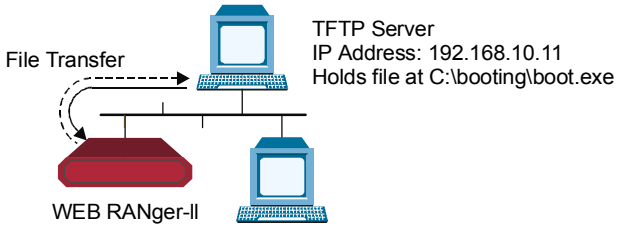


Figure 4-99. Downloading from a TFTP Server

➤ **To download a new software version via TFTP server:**

1. Select option **1** from the Software Download menu.

```
Do you want to download new software version? (y/n): Y

TFTP server IP address: 192.168.182.34
New software file name: webeb.mbi

Download process will erase the program code
in the second partition of the device.

Upon completion of the download,
the device will be reset automatically.

Press 'S' to start the download process
or
ESC to return to previous menu:
```

Figure 4-100. Software Download Menu

2. Confirm that the Do You Want To Download New Software Version field is set to **Yes**.
3. In the TFTP Server IP Address field**,** type the IP address of the TFTP server.
4. In the New Software File Name field, type the path and file name of the new software version.
5. Press **S** to start the download process.

During the process, the new program code is downloaded to the Flash **backup** partition, thus erasing its previous contents.
Upon completion, the newly downloaded Flash partition becomes active, while the old version's partition becomes backup. The device automatically resets, running the new program stored in the active partition.
During the download process, a counter shows the number of packets that have passed. Downloading can be interrupted at any time by pressing the **<Esc>** key.

XMODEM via Control Port (BOOT Manager)

Advanced Menu
↓**2**
Device Control
↓**1**
Software Download
↓**2**
XMODEM

Use this option to access the BOOT Manager via the control port. Refer to *Appendix B* for more information on the Boot Manager.

Upload Device Parameters to TFTP Server

Advanced Menu
↓**2**
Device Control
↓**2**
Upload Device Parameters

Select this parameter to save device configuration parameters into a file by uploading to the TFTP server. This operation sends all unit parameters to the TFTP server and will be saved under a filename that you specify.

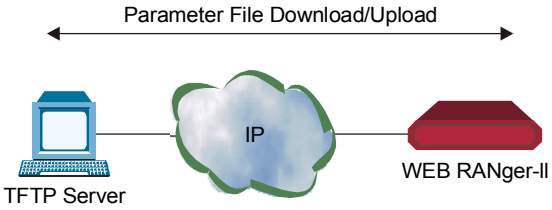


Figure 4-101. Downloading/Uploading Parameters

➤ **To upload device parameters:**

1. Activate the TFTP server application connected to the unit via an IP network.
2. Configure the following IP parameters: IP address, IP mask and IP default gateway.
3. Select the TFTP upload option.
4. Enter the TFTP server IP address.
5. Assign a name to the configuration file you want to save on the server, for example V35 file.
6. Press **S** to start the upload process.

Download Device Parameters from TFTP Server

Advanced Menu
↓2
Device Control
↓3
Download Device Parameters

Select this option to load device configuration parameters from a file by downloading from the TFTP server.

➤ **To download device parameters:**

1. Activate the TFTP server application connected to the unit via an IP network.
2. Configure the following IP parameters: IP address, IP mask and IP default gateway.
3. Select the TFTP download option.
4. Enter the TFTP server IP address.
5. Enter the name of the configuration file you want to download from the server, for example V35 file.
6. Press **S** to start the download process.

Note *Upon completion of the download process, the unit performs reset. The new parameters only come into effect after resetting.*

Reset Options

Advanced Menu
↓2
Device Control
↓4
Reset Options

Select this option for resetting:

- Device
- Link
- Interface module.

Terminal Type

Advanced Menu
↓2
Device Control
↓5
Terminal Type

Use this option to choose a terminal type:

- Select **1** for VT-100, UT-200, VT-220 ANSI Terminals
- Select **2** for VT-52, IBM 3101 Terminals
- Select **3** for other terminals.

Since each terminal type uses different ASCII control codes for cursor control, WEB RANger-II requires this information to display the screens clearly. This setting affects the Statistics screen display only.

Chapter 5

Troubleshooting and Diagnostics

Topics covered in this chapter include:

- View Configuration screen
- View Interface Connections screen
- View Routing Tables screen
- Viewing Statistics
- Viewing E1/T1 Diagnostics
- Viewing Frame Relay DLCIs
- Viewing E1/T1 Alarms Log File
- Diagnostic Tools
- Common Faults.

5.1 View Menu

Use the View menu options to see information on interface connections, routing tables, statistics, diagnostics, and alarms. *Figure 5-1* shows the View Menu options.

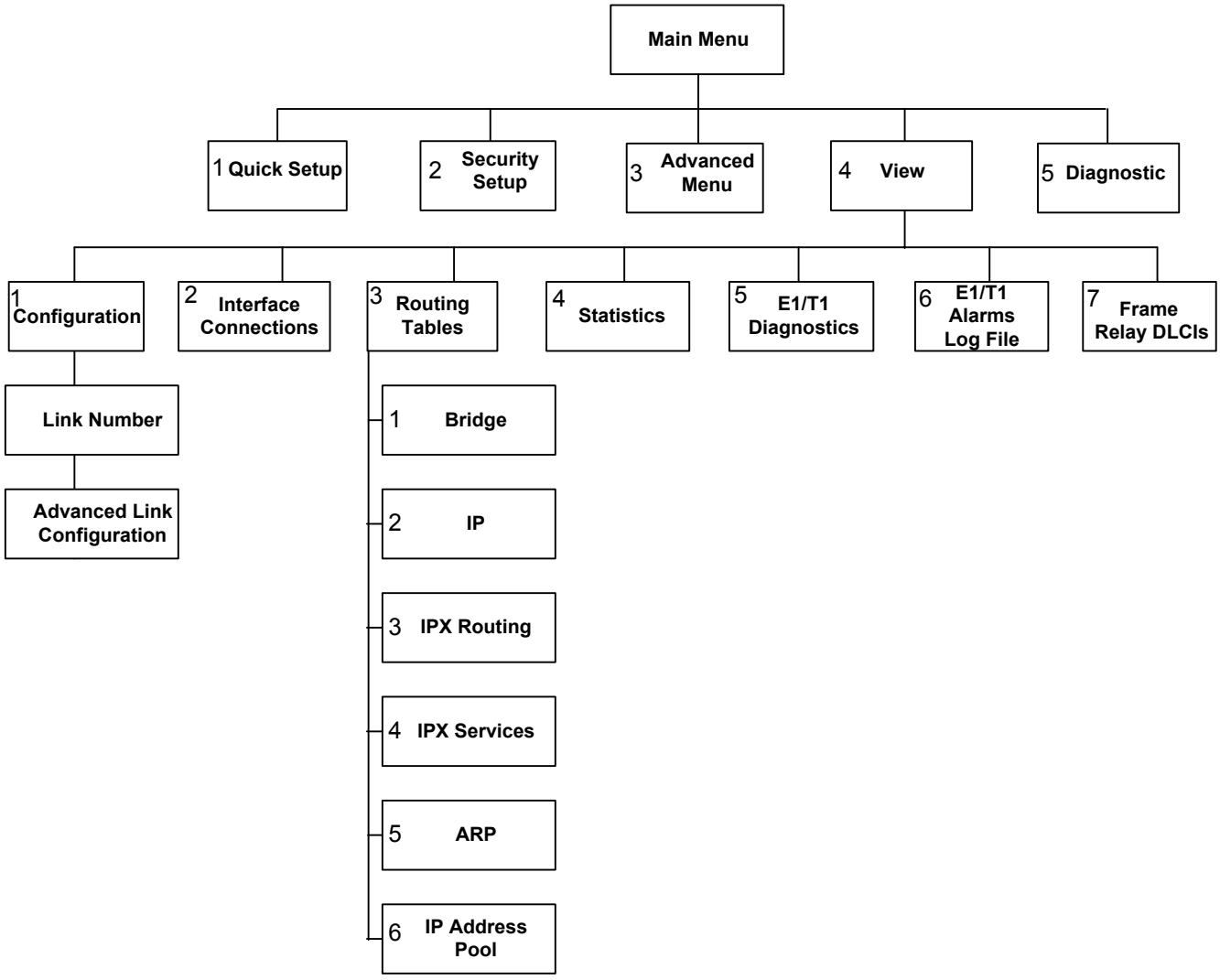


Figure 5-1. View Menu Outline

➤ **To access the View Menu:**

1. In the Main Menu, press **4**.

   The View Menu appears (see *Figure 5-2*).

```
      VIEW  MENU  ( Device name - WEB II  )

1.  Configuration
2.  Interface Connections
3.  Routing Tables
4.  Statistics
5.  E1/T1 Diagnostics
6.  E1/T1 alarms log file
7.  Frame relay DLCIs


Press number to select or ESC to return to the previous menu:
```

Figure 5-2. View Menu

The options in the View Menu are described in this chapter.

Configuration

View Menu
↓1
Configuration

Select this option to view the configuration parameters for the device and link that were entered through the Setup menu. The Advanced Link Configuration screen displays configuration parameters for a specific link. Since these screens are "display-only" you cannot use them to adjust parameters. *Figure 5-3* displays configuration for WEB RANger-II WAN interfaces.

```
      VIEW CONFIGURATION  ( Device name - WEB II    )

 Device type       :  WEB II
 Contact person    : name of contact person
 System location   : the location of this device
 Hardware version                : 1.0   ( 1997-11-17 )
 Software version                : 4.00 A2 ( 1999-11-01 )
 Burned-In MAC address           : 0020 D216 AD87  ( active )
 Local Administered MAC address  : 4020 D216 AD87
 IP address                      : 10.10.90.1
    Link  Interface   Type              Clock(Kbps)       Status     Mode
    ----- ----------  ----------------  -----------       ------     ----
 1) 1     T1+FXS      Synchronous       Ext Link1/ 1280   Enabled    Router
 ESC - Return to previous menu
 For advanced link configuration information - enter link number:
```

Figure 5-3. View Configuration Screen

Interface Connections

View Menu

↓2

Interface Connections

This screen displays connection status for all WEB RANger-II WAN interfaces.

Figure 5-4 displays the connection status for all WEB RANger-II WAN interfaces. Each DLCI status is displayed for Frame Relay links, in addition to the Frame Relay status itself.

```
INTERFACE CONNECTIONS    (Device name – WEB II)

               ROUTING     DEVICE         CONNECTED      CONNECTION
INTRFACE        TYPE         NAME          USER NAME        STATUS
-------------------------------------------------------------------
LINK1          IP PPP                                     LCP+IP/VJ


R – Refresh
ESC – Return to previous menu
```

Figure 5-4. Interface Connections Screen

Routing Tables

View Menu

↓3

Routing Tables

Select this option to display different routing tables (see *Figure 5-5*).

```
ROUTING TABLES  ( Device name - WEB RANger-II  )
   1.  Bridge
   2.  IP
   3.  IPX Routing
   4.  IPX Services
   5.  ARP
   6.  IP Address Pool


   ESC - Return to previous screen
```

Figure 5-5. Routing Tables Menu

The options in the Routing Tables menu are described below.

Bridge

View Menu
↓3
Routing Tables
↓1
Bridge

Select this option to display a table that contains information on Bridge MAC addresses (see *Figure 5-6*).

```
    BRIDGE TABLE  (Page-1) ( Device name - WEB RANger-II  )

   MAC ADDRESS          TYPE                  INTERFACE

   0020D2FD5153         Static or Dynamic     LAN

   ESC - Return to previous menu
\
```

Figure 5-6. Bridge Table

IP

View Menu
↓3
Routing Tables
↓2
IP

Select this option to display a table that contains information on IP routing (see *Figure 5-7*).

```
       IP TABLE  (Page-1) ( Device name - WEB RANger-II  )

  IP ADDRESS        IP MASK        TYPE  COST     NEXT HOP      AGEING  INTRF

Default gateway                                 ---------------          LINK1
001.000.000.000  255.000.000.000  INTRF    0   001.001.001.001 00:00:00 LAN1
001.001.001.001  255.255.255.255  INTRF    0   --------------- 00:00:00 LAN1
002.000.000.000  255.000.000.000  INTRF    0   002.002.002.002 00:00:00 LAN2
002.002.002.002  255.255.255.255  INTRF    0   --------------- 00:00:00 LAN2

ESC - Return to previous menu
```

Figure 5-7. IP Table

IPX Routing

View Menu
↓3
Routing Tables
↓3
IPX Routing

Select this option to display information on IPX routing.

```
        IPX ROUTING TABLE (Page-1) ( Device name - WEB RANger-II  )

IPX NET     IPX NODE        TYPE     HOPS  TICKS   AGEING   INTERFACE

0000000A  0000C0F5D899  NET (RIP)     1      2   00:00:50  LAN
0000001B  0000C0F5D899  NET (RIP)     4      5   00:00:50  LAN
0000001C  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000001D  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000001E  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000001F  0000C0F5D899  NET (RIP)     1      2   00:00:50  LAN
0000001G  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000001H  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000002I  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000002J  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000003K  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000006L  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000009M  0000C0F5D899  NET (RIP)     2      3   00:00:50  LAN
0000012N  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000067O  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN
0000083P  0000C0F5D899  NET (RIP)     3      4   00:00:50  LAN

ESC - Return to previous menu
```

Figure 5-8. IPX Routing Table

IPX Services

View Menu
↓3
Routing Tables
↓4
IPX Services

Select this option to display a table that contains information on IPX services (SAP table). Refer to *Figure 5-9*.

```
    IPX SERVICES TABLE  (Page-1) ( Device name - WEB RANger-II  )

SERVER   NAME           TYPE       PX NET      HOPS   INTERFACE

ACCESS                  0004     3381AFCA     2        LAN
ACCOUNT_RAD             0004     0000AAAB     2        LAN
BACKUP                  0004     0001267C     2        LAN
ENG                     0004     ACE1111D     3        LAN
EXPORT                  0004     00AA110E     2        LAN
FDD_EYE                 0004     0032142F     1        LAN

  ESC - Return to previous menu, N - next screen
```

Figure 5-9. IPX Services Table

ARP Table

View Menu
↓3
Routing Tables
↓5
ARP Table

Select this option to display the correlation between the IP address and the MAC address of each station on the LAN (see *Figure 5-10*).

```
      ARP TABLE  (Page-1) ( Device name - WEB RANger-II )

   IP ADDRESS      MAC ADDRESS    AGEING

 192.168.1.33    0020D2FD9F16   00:00:00
 192.168.1.35    0000B431CBD6   00:00:50
 192.168.1.36    0000B471B335   00:02:15
 192.168.1.38    0020D2FD51F0   00:02:15

 ESC - Return to previous menu
```

Figure 5-10. ARP Table

IP Address Pool

View Menu
↓3
Routing Tables
↓6
IP Address Pool

Select this option to display the IP address pool (see *Figure 5-11*).

```
   IP ADDRESS POOL (Page-1) ( Device name - WEB II    )

                                        300 sec. to ready DHCP server
   IP ADDRESS        IP MASK          MAC       LEASE   STATUS   INTERFACE
---------------  ---------------  ------------  -----  --------  ----------
001.001.001.001  255.255.255.000                   0   DECLINED
001.001.001.002  255.255.255.000                   0   FREE
001.001.001.003  255.255.255.000                   0   FREE
001.001.001.004  255.255.255.000                   0   FREE
001.001.001.005  255.255.255.000                   0   FREE

   ESC - Return to previous menu
```

Figure 5-11. IP Address Pool Table

Statistics

View Menu
↓4
Statistics

Select this option to display information on the traffic between the networks connected by WEB RANger-II. The statistics enable you to view network performance.

```
        STATISTICS FOR THE LAST  00:03:47  ( Device name - WEB II    )

       LAN 1  STATISTICS (per second) CURRENT       MAX        AVG
       ------------------
1) Total network frames                 00000       00000       00000
2) Received good frames                 00000       00000       00000
3) Received good broadcast/multicast    00000       00000       00000
4) Received masked frames               00000       00000       00000
5) Transmitted frames                   00000       00000       00000
6) Memory overflow errors               00000       00000       00000
7) LAN errors                           00000       00000       00000
8) Received missed frames errors        00000       00000       00000
9) LAN buffers overflow                 00000       00000       00000

C - Clear statistics, U - Update average,
L - LAN, Link Number
ESC - Return to previous menu
```

Figure 5-12. LAN Statistics

E1/T1 Diagnostics

View Menu
↓5
E1/T1 Diagnostics

Select this option to display error information for the E1/T1 link. This information enables you to evaluate the line quality. The errors are accumulated in 15-minute intervals. WEB RANger-II keeps up to 96 intervals (for 24 hours).

In addition, there is a rolling 24-hour total of each error parameter. The rolling total is displayed for the interval parameter called TOTAL. The interval parameter called CURRENT is the open interval, which did not yet reach 15 minutes. The errors counted in the CURRENT interval are not included in the TOTAL interval. The amount of time that has elapsed is displayed on the right of the CURRENT parameter line. T1 diagnostics are available only when frame mode is ESF. E1 diagnostics are available only when CRC-4 is enabled.

Figure 5-13 illustrates the T1 Diagnostics screen and *Figure 5-14* illustrates the E1 Diagnostics screen.

```
T1 DIAGNOSTICS - LINK 1   ( Device name - WEB II    )

 INTERVAL    ES      UAS     SES     BES    LOFC     CSS     DM
 --------   -----   -----   -----   -----   -----   -----   -----
 CURRENT       0     546     556       0       0       0          09.16 min
     1         0     890     900       0       0       0
     2         0     890     900       0       0       0
     3         0     890     900       0       0       0
     4         0     890     900       0       0       0
     5         0     890     900       0       0       0
     6         0     890     900       0       0       0
     7         0     890     900       0       0       0
     8         0     890     900       0       0       0
     9         0     890     900       0       0       0
    10         1     890     900       1       1       1
  TOTAL        1    8900    9000       1       1       1       0

 ESC - previous menu  |  R - Refresh  |  C - Clear diagnostics
```

Figure 5-13. T1 Diagnostics

```
E1 DIAGNOSTICS - LINK 1 ( Device name - WEB II )

INTERVAL     ES     UAS     SES     BES    LOFC     CSS
CURRENT       0     548     558       0       1       0    09.18 min

ESC - previous menu  |  R - Refresh  |   C - Clear diagnostics
```

Figure 5-14. E1 Diagnostics

Interval Parameters

Current Errored Seconds (ES)

An errored second is any second containing one or more CRC error events, or one or more OOF events, or one or more controlled slip events.

Unavailable Seconds Out-Of-Frame (UAS)

An unavailable second out-of-frame is any second in which a failed signal state exists. A failed signal state is declared when 10 consecutive severely errored seconds (SES) occur, and is cleared after 10 consecutive seconds of data are processed without a SES.

Severely Errored Seconds (SES)

A SES is a second with 832 or more CRC error events, or one or more OOF events.

Bursty Errored Seconds Out-Of-Frame (BES)

A BES is a second with 2 to 831 CRC error events.

Current Loss of Frame Counter (LOFC)

The loss of frame (LOF) counter counts the loss of frame alignment events.

Current Slip Second Counter (CSS)

A CSS is a second with one or more controlled slip events.

Degraded Minutes (DM)

The total number of degraded minutes in the current 24-hour interval. A degraded minute is a minute in which the bit error rate (BER) exceeded $1x10^{-6}$. This number is updated every minute.

E1/T1 Alarms Log File

View Menu
↓6
E1/T1 Alarms Log File

Figure 5-15 and *Figure 5-17* illustrate the Alarms screen.

```
E1/T1 ALARMS     ( Device name - WEB II)   time from start - 00:00:09:26

INTERFACE           TYPE          STATUS     DAYS     HOURS     MIN     SEC
---------         -----------     ------     ----     -----     ---     ---

Link 1 E1       Local sync loss    ON         0        0         0       2


ESC - previous menu  |  R - Refresh  |   C - Clear diagnostics
```

Figure 5-15. E1 Alarms Screen

Frame Relay DLCIs

View Menu
↓7
E1/T1 Diagnostics

Select this option to display frame relay DLCI settings (see *Figure 5-16*).

```
FRAME RELAY DLCI SETTINGS ( Device name - WEB RANger-II  )

 LINK   DLCI   STATE    CIR   EXCESS  THROUGHPUT STATUS

LINK-1   16    Enabled   0    64000       0 UP
LINK-1   17    Enabled   0    64000       0 UP
LINK-1   18    Enabled   0    64000       0 UP

ESC - Return to previous menu
```

Figure 5-16. Frame Relay DLCI Settings

```
E1/T1 ALARMS   ( Device name - WEB II    )   time from start - 00:02:39:39

    INTERFACE             TYPE          STATUS   DAYS    HOURS    MIN     SEC
  -------------   ------------------   ------   -----   -----   -----   -----
  Link 1 T1        Red alarm              ON      0        0       0       2
  Link 1 T1        Frame slip                     0        0       0       1

  ESC - previous menu  |  R - Refresh  |  C - Clear alarms
```

Figure 5-17. T1 Alarms Screen

5.2 Diagnostic Tools

This section provides information on using the diagnostic tools of WEB RANger-II.

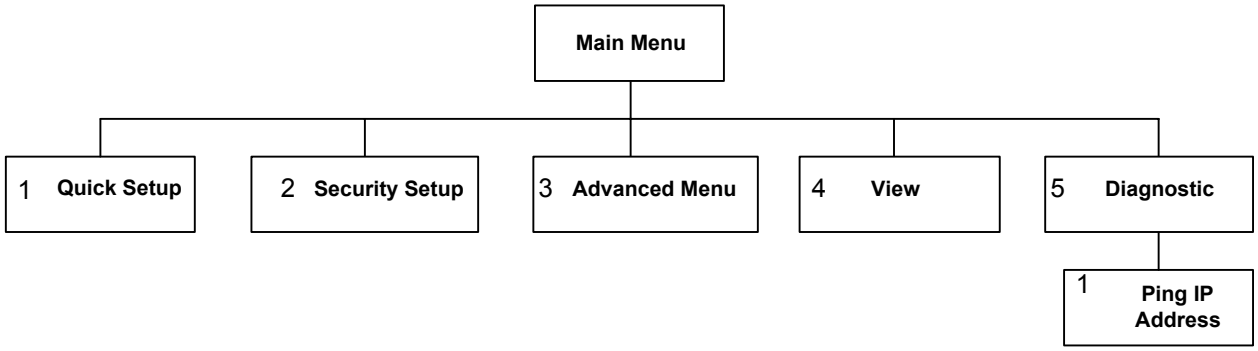


Figure 5-18. Diagnostic Tools Menu Outline

➤ **To access the Diagnostic Tools menu:**

1. In the Main Menu, select option **5**.
   The Diagnostic Tools menu appears (see *Figure 5-19*).

```
     DIAGNOSTIC TOOLS  ( Device name - WEB II )

1.  Ping terminal
 ESC - Return to previous menu
  Choose one of the above:
```

Figure 5-19. Diagnostic Tools Menu

The Diagnostic Tools menu has a Ping option. The Ping option allows you to confirm IP connectivity by 'pinging' (dialing) other IP hosts. If there is a reply from the remote IP host, connectivity is confirmed (see *Figure 5-20*).

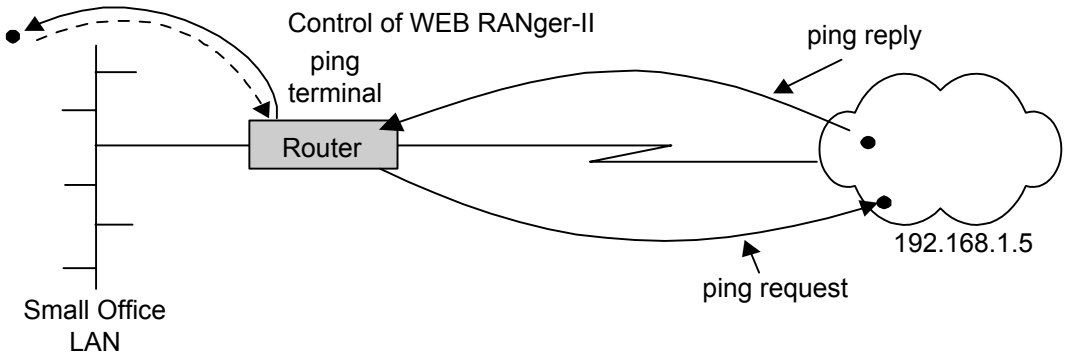


Figure 5-20. Pinging an IP Host

➤ **To ping another host:**

1. From the Main Menu, select option **4**.
   The Diagnostic Tools menu appears.
2. From the Diagnostic Tools menu, select option **1**.
   You are prompted to enter the IP address of the host.
3. Enter the host's IP address. WEB RANger-II pings the destination host.
   A message appears showing the result of the request (see *Figure 5-21*). WEB RANger-II continues pinging the host until you press **<Esc>.**

```
     PING TERMINAL  ( Device name - WEB II  )

Insert the target IP address in the format : xxx.xxx.xxx.xxx
ESC - Return to previous menu
Ping IP address: 10.10.10.10

Pinging 10.10.10.10

Reply from 10.10.10.10:   time = 0.100 sec
Reply from 10.10.10.10:   time = 0.050 sec
Reply from 10.10.10.10:   time = 0.050 sec
Reply from 10.10.10.10:   time = 0.050 sec

ESC - Return to previous menu
```

Figure 5-21. Ping Terminal Screen

5.3 Common Faults

Some general faults and their solutions are listed in *Table 5-1*. If a persistent fault condition occurs, confirm that the WEB RANger-II is configured properly. Link errors are sometimes caused by loose contact between connectors and lack of cable continuity. Check that all connectors are plugged in properly and that cable quality is good. *Table 5-2* lists faults specific to E1/T1/Voice. *Table 5-3* lists faults specific to routing problems.

Table 5-1. General Faults and Solutions

Symptom	Possible Cause	Course of Action
All front panel indicators are OFF	Unit not receiving power.	Check that power is supplied to the unit. Check fuse and replace it if necessary (by qualified technician only)
READY LED is OFF	There are fewer than two UP interfaces	Check VIEW interface connnection status

E1/T1/Voice Troubleshooting

Table 5-2. E1/T1/Voice Faults and Solutions

Symptom	Possible Cause	Course of Action
Local SYNC LOSS (for E1) or RED alarm (for T1) is ON in main link	External problem	Check E1/T1 cable
Local SYNC LOSS (for E1) or RED alarm (for T1) is ON in sublink	External problem	Check E1/T1 cable

Router Troubleshooting

LAN and Wan can connect the IP router to other IP networks. Operating the Ping terminal that sends Ping frames to the IP Host indicates the availability of the connection in the IP level. When the Ping terminal continuously receives a response from the IP Host, the IP Connection is UP.

➤ **If the IP connection to the LAN is DOWN:**

1. Check the LAN indicators on the front panel.
2. Select the View menu.
3. From the View menu,
   - Select Interface Configuration
     or
   - Select Routing Tables, then IP Routing.

Table 5-3. Router Faults and Solutions

Symptom	Possible Cause	Course of Action
Red LAN ERROR indicator ON	LAN status set to DISABLE	Check VIEW interface connection status
	Problem with LAN cable or hub	Check LAN cable and hub
Red LAN ERROR indicator blinking	Problem with LAN cable or hub	Check LAN cable and hub
Physical connection OK but no IP connection	IP configuration problem	Look for mistakes in IP routing table, HOST IP addreses, default gateway

➤ **If the IP connection to the WAN is down:**

1. Check the WAN indicators on the front panel.
2. Select the View menu.
3. From the View menu,
   - Select Interface Configuration
     or
   - Select Routing Tables, then IP Routing.

Table 5-4. WAN Faults and Solutions

Symptom	Possible Cause	Course of Action
Red WAN ERROR indicator is ON or Connection Status shows SYNC NOT OBTAIN	In Synchronous Link receive clock (RCLK) is 0 kbps	Check VIEW configuration status – Baud Rate 0 kbps indicates a physical problem with the line
	Physical problem with WAN line	Check WAN cable and modem
Red WAN ERROR indicator is ON or Connection Status shows SYNC NOT OBTAIN	Physical problem with WAN line	Check WAN cable and modem
E1/T1 alarm indicators On or blinking, or Connection Status shows E1/T1 alarms	Physical problem with E1/T	See *Table 5-2*
PPP – Connection Status shows SYNC NOT OBTAIN	Physical connection OK, but no PPP connection	1. Check if opposite unit is ON 2. Check PPP configuration of WEB RANger-II and opposite unit

Table 5-4. WAN Faults and Solutions (Cont.)

Symptom	Possible Cause	Course of Action
PPP – Connection Status shows LCP	PPP connection established but no IPCP connection	Check PPP configuration of WEB RANger-II and opposite unit
Frame Relay: Connection shows "PORT DOWN"	Physical connection exists but no frame relay port UP	1. Check connection between modem and frame relay switch 2. Check WEB RANger-II and switch configuration
Frame Relay: Link connectiom shwos "PRT UP" and DCLI connection shows "DCLI DOWN"	UP physical connection exists and frame relay port UP but specific DLCI is down	1. Check if unit opposite DLCI is ON 2. Check WEB RANger-II, frame relay switch, and configuration of opposite unit
Physical and logical connection OK, but no IP connection	Problem with IP configuration	Look for mistakes in IP routing table, HOST IP addresses, and default gateway

Appendix A

Interface Specifications and Cable Diagrams

A.1 Interface Signal List (Female Connectors)

Table A-1. Interface Signal List (Female Connectors)

	Signal Function	Source	V.24/ RS-232 DB-25 Female	V.35** 34-PIN (Female)		EIA-530 DB-25 (Female)		V.36/ RS-449** DB-37 (Female)		X.21* DB-15 (Female)		Description
				Pin	Circuit	Pin	Circuit	Pin	Circuit	Pin	Circuit [Function]	
Ground	Protective Ground	Common	1	A Frame	101	1		1		1	– [Shield]	Chassis ground. May be isolated from Signal Ground.
	Signal Ground	Common	7	B Signal GND	102	7	AB	19	SG	8	– [GND]	Common Signal and DC power supply ground.
Data	Transmitted Data	DTE	2	S TD(B) P TD(A)	103 103	2 14	BA (A) BA (B)	4 22	SD(A) SD(B)	2 9	T(A) T(B) [Transmit]	Serial data output from WEB RANger-II. The data transitions occur on the rising edge of the clock.
	Received Data	DCE	3	R RD(A) T RD(B)	104 104	3 16	BB(A) BB(B)	6 24	RD(A) RD(B)	4 11	R(A) R(B) [Receive]	Serial data input to the WEB RANger-II. The data transitions occur on the rising edge of the clock.

Table A-1. Interface Signal List (Female Connectors) (Cont.)

	Signal Function	Source	V.24/ RS-232 DB-25 Female	V.35** 34-PIN (Female) Pin Circuit	EIA-530 DB-25 (Female) Pin Circuit	V.36/ RS-449** DB-37 (Female) Pin Circuit	X.21* DB-15 (Female) Pin Circuit [Function]	Description
Control	Request to Send	DTE	4	C RTS 105	4 CA(A) 19 CA(B)	7 RS(A) 25 RS(B)	3 C(A) 10 C(B) [Control]	ON from the unit upon completion of Self-Test.
	Clear To Send	DCE	5	D CTS 106	5 CB(A) 13 CB(B)	9 CS(A) 27 CS(B)-	– –	WEB RANger-II expects CTS ON.
	Data Set Ready	DCE	6	E DSR 107	6 CC(A) 22 CC(B)	11 DM(A) 29 DM(B)	– –	Not used.
	Data Terminal Ready	DTE	20	H DTR 108	20 CD(A) 23 CD(A)	12 TR(A) 30 TR(B)	– –	ON when WEB RANger-II is ready to transmit or receive data.
	Carrier Detect	DCE	8	F DCD 109	8 CF(A) 10 CF(B)	13 RR(A) 31 RR(B)	5 I(A) 12 I(B) [Indication]	Unit expects DCD ON
Timing	Transmit Clock	DCE	15	Y SCT(A) 114 A SCT(B) 114	15 DB(A) 12 DB(B)	5 ST(A) 23 ST(B)	6 S(A) 13 S(B) [Signal Timing]	WEB RANger-II requires clock for synchronization (in synchronous mode).
	Receive Clock	DCE	17	X SCR(B) 115 V SCR(A) 115	17 DD(A) 9 DD(B)	8 RT(A) 26 RT(B)	– –	WEB RANger-II requires clock for synchronization (in synchronous mode).

*The X.21 connection is made by an RS-530 to X.21 conversion cable supplied with the RS-530 model.

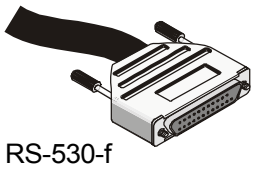
**The V.36/RS-449 connection is made by an RS-530 to V.36 conversion cable supplied with the RS-530 model.

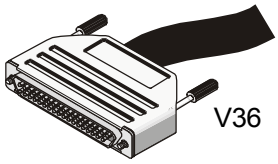
***The V.35 connection is made via an adapter cable (DB-25 connector to V.35-34 pin connector) for MBE 10-8D and MBE10-1D.

A.2 Cable Diagrams

RS-530			X.21 / 15-pin	
Shield	1	→	1	Shield
Signal GND	7	→	8	Signal GND
RTS-a	4	→	3	C-a
RTS-b	19	→	10	C-b
CTS-a	5	←		
CTS-b	13	←		
DCD-a	8	←	5	I-a
DCD-b	10	←	12	I-b
TC-a	15	←	6	S-a
TC-b	12	←	13	S-b
RC-a	17	←		
RC-b	9	←		
TD-a	2	→	2	T-a
TD-b	14	→	9	T-b
RD-a	3	←	4	R-a
RD-b	16	←	11	R-b

Figure A-1. Cable Supplied for X.21 Interface





RS-530			RS-449/V.36-37 pin
Shield	1	1	Shield
TD-a	2	4	SD-a
TD-b	14	22	SD-b
RD-a	3	6	RD-a
RD-b	16	24	RD-b
RTS-a	4	7	RS-a
RTS-b	19	25	RS-b
CTS-a	5	9	CS-a
CTS-b	13	27	CS-b
DSR-a	6	11	DM-a
DSR-b	22	29	DM-b
DTR-a	20	12	TR-a
DTR-b	23	30	TR-b
Sig. GND	7	19,20,37	SG
DCD-a	8	13	RR-a
DCD-b	10	31	RR-b
TC-a	15	5	ST-a
TC-b	12	23	ST-b
RC-a	17	8	RT-a
RC-b	9	26	RT-b
LL	18	10	LL
RL	21	14	RL
EXT-CK-a	24	17	TT-a
EXT-CK-b	11	35	TT-b
TM	25	18	TM

Figure A-2. Cable Supplied for V.36 interface

A.3 E1/T1 Connectors

The unbalanced interface of the E1 and SUB E1 links are terminated in two BNC connectors. The connectors are designated RX-IN and TX-OUT. The balanced interface of the E1, SUB E1, T1 and SUB T1 are terminated in an eight-pin RJ-45 connector, wired in accordance with *Table A-2*.

Table A-2. E1/T1 and SUB E1/T1 Link Connectors, Pin Allocation

Pin	Designation	Direction	Function
1	RD(T)	Input	Receive data (tip)
2	RD(R)	Input	Receive data (ring)
3	FG	↔	Frame ground
4	TD(T)	Output	Transmit data (tip)
5	TD(R)	Output	Transmit data (ring)
6	FG	↔	Frame ground
7,8			Not connected

Note

Use a cross cable to connect PABX to the SUB E1/T1 link.

Table A-3. ISDN "S" Interface Pin Assignments

Pin Number	Signal Name
3	Tx+
4	Rx+
5	Rx-
6	Tx-

Table A-4. Control Cable RJ-45 to DB-25 Connection (DCE)

RJ-45		DB-25	
Pin 4	GND	Pin 7	GND
Pin 5	TX	Pin 3	RX
Pin 6	RX	Pin 2	TX
Pin 7	RTS	Pin 5	CTS
Pin 8	CTS	Pin 4	RTS

Table A-5. ISDN "S" Interface Pin Assignment

Pin Number	Signal Name
3	TX+
4	RX+
5	RX–
6	TX–

A.4 E&M, FXS and FXO Interface Connectors

E&M Connector

The E&M interface of WEB RANger-II terminates in an 8-pin RJ-45 connector wired in accordance with *Table A-6*.

Table A-6. E&M Connector Pinout

Pin	Designation	Function
1	SB	Signaling battery
2	M	M lead input
3	R1-OUT	Voice output (4-wire) Voice input/output (2-wire)
4	R-IN	Voice input (4-wire)
5	T-IN	Voice input (4-wire)
6	T1-OUT	Voice output (4-wire) Voice input/output (2-wire)
7	SG	Function depends on signaling mode: • RS-464 Type I, III: Direct connection to signal ground • RS-464 Type V, SSDC5: Connection to signal ground through 1.1 kΩ resistor • RS-464 Type II: SG lead
8	E	E lead output

FXO/FXS Connector

The FXS and FXO interfaces of WEB RANger-II terminate in 6-pin RJ-11 connectors wired in accordance with *Table A-7*.

Table A-7. FXO/FXS Connector Pinout

Pin	Function
1, 2	Not connected
3	Ring
4	Tip
5, 6	Not connected

Appendix B
BOOT Manager

B.1 Introduction

WEB RANger-II includes a Dual Image Flash, capable of storing two different versions of software in two different partitions.

Upon reset, WEB RANger-II automatically runs the program stored in the **active** partition.

New software versions are loaded into the **backup** partition. If loading succeeds, the **backup** partition becomes the **active** partition and WEB RANger-II is reset automatically, running the new software version. If loading fails, the device is still capable of working, since the Flash partition storing the old version remains active.

The BOOT Manager can control dual Image Flash. Use the BOOT Manager to:

- Download new software
- Manually define the active and backup partitions
- Run the backup partition
- Erase some or all information from Flash.

B.2 Accessing BOOT Manager

There are several ways to access BOOT Manager:

- Via option **2** in the Software Download menu
- Via the **Rescue** option.

Access via Software Download Menu

➤ **To access BOOT Manager from the Software Download Menu:**

1. In the Advanced Menu, press **3.**

   The Device Control menu appears (see *Figure B-1*).

```
      DEVICE CONTROL  ( Device name - WEB II )

1.  Software download
2.  Upload device parameters to TFTP server
3.  Download device parameters from TFTP server
4.  Reset options
5.  Terminal type

ESC - Return to previous menu
Choose one of the above:
```

Figure B-1. Device Control Menu

2. Press **1**.

   The Software Download menu appears (see *Figure B-2*).

```
    SOFTWARE DOWNLOAD (Device name - WEB RANger-II)

1.  Download from TFTP Server
2.  XMODEM via control port (BOOT Manager)
3.  Download software to ISDN module

ESC - Return to previous menu
Choose one of the above:
```

Figure B-2. Software Download Menu

3. Press **2.**

   The BOOT Manager menu appears (see *Figure B-3*).

Rescue

If WEB RANger-II does not respond properly, try the Rescue option:

➤ **To access BOOT Manager from the Rescue option:**

1. Connect to the terminal emulator.
2. Switch on WEB RANger-II and immediately press **R**.

   The BOOT Manager menu appears (see *Figure B-3*).

B.3 The BOOT Manager Menu

The BOOT Manager Menu is shown in *Figure B-3*.

```
BOOT 360 Version 1.05 (Feb 23 1998)

Active: 1999 Oct 13 13:55 MBE360.X     VER 4.00
Backup: 1999 Aug 16 14:56 MBE360.X     VER 4.00

1) Load new software
2) Partitions status
3) Run backup partition
4) Reactivate backup partition
5) Duplicate active partition
6) Erase configuration
7) Erase all FLASH
8) Set baud rate

0) Exit

Choose one of the above:
```

Figure B-3. BOOT Manager Menu

The options in the BOOT Manager menu are described below.

Load New Software

Select this option to download new software via the control port using the XMODEM protocol. During the download process, the new program code is downloaded to the Flash **backup** partition, thus erasing its previous contents.

Upon completion, the newly downloaded Flash partition becomes the **active** partition, while the old version's partition becomes the **backup** partition. The device automatically resets, running the new program stored in the **active** partition. For more information refer to *Figure B-4*.

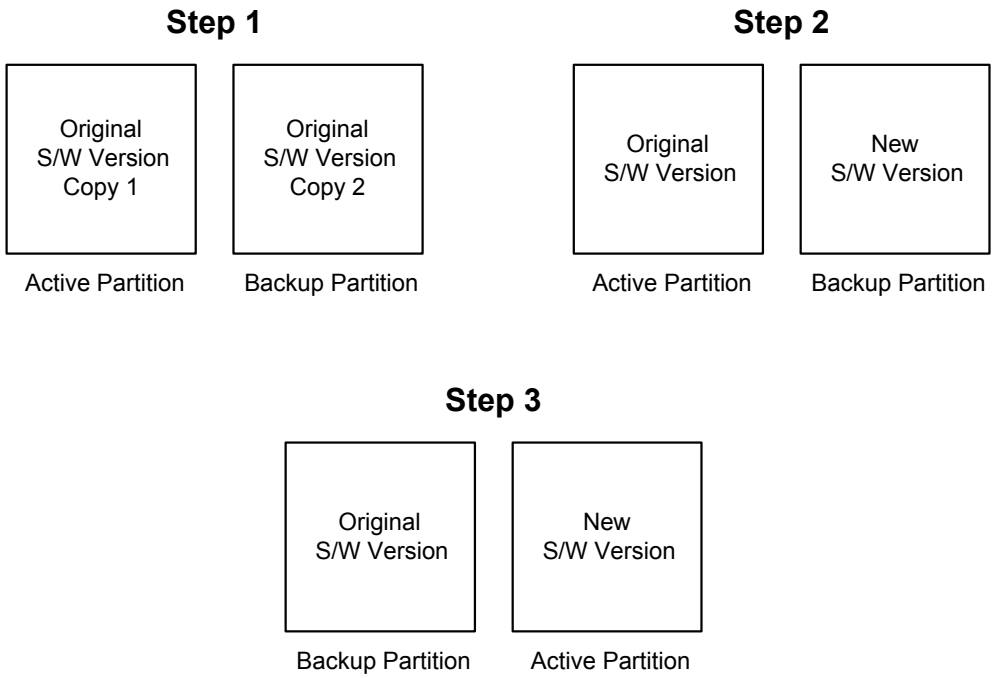


Figure B-4. Dual Image Flash

Note *The terminal emulator of Windows 95 (HyperTerminal) has the following bug. After changing baud rate the status line presents the new value, but this value does not come into effect unless you perform the disconnect and connect commands immediately after the change.*

Partitions Status

Select this option to display information about the status of the **active** and the **backup** flash partitions. Note that the BOOT Manager menu also displays a partial status at its upper part:

```
Active : 1998 Apr 16 14:56 WEBEB.X
Backup : 1998 Apr 16 14:56 WEBEB.X
```

Figure B-5. Status of Flash Partitions

Run Backup Partition

Select this option to run the program stored in the **backup** partition of the Flash memory. Normally that program is the previous software version.

The "backup" program runs **once**. The next hardware reset or Boot will run the program stored in the **active** partition.

Reactivate Backup Partition

Select this option to turn the **backup** partition into the **active** partition (and vice versa). In this way you can return to the previous software version permanently.

This command may be executed up to 16 times, after which downloading of the new software will be required. Therefore avoid using this option for a one-time run of the old version (use the **Run Backup Partition** option for that purpose).

Duplicate Active Partition

Select this option to duplicate the program stored in the **active** partition into the **backup** partition.

Erase Configuration

Select this option to erase the device configuration parameters. The device configuration parameters are also stored in the flash memory. Sometimes these configuration parameters are needed after downloading a new version of Boot Manager. When the new version's parameter set is not fully compatible with the previous version's parameters, then you need to erase the previous version's parameters. You can also use this command to set the device to the default settings. The Erase Configuration command is also useful if you forget the password.

Erase All FLASH

Select this option to erase the device configuration parameters, and the programs stored in both partitions. Remember to download new software before attempting to operate the device.

Set Baud Rate

Select this option to set the device's baud rate to either **9.6, 19.2, 38.4, 57.6** or **115.2** kbps. For software download, it is recommended to use the highest rate possible, i.e. 115.2 kbps (the baud rate must be higher than 9.6 kbps to enable downloading).

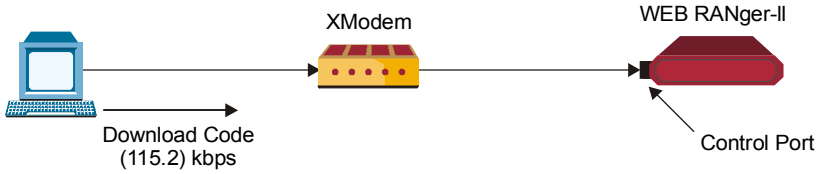


Figure B-6. Setting the Baud Rate

Change your terminal baud rate and press Enter several times to ensure that the device identifies the new value.

Note

The terminal emulator of Windows 95 - HyperTerminal has the following bug. After changing baud rate the status line presents the new value, but this value does not come into effect unless you perform the disconnect and connect commands immediately after performing the change.

Exit

Select this option to exit the BOOT Manager menu and perform BOOT/RESET WEB RANger-II.

If the BOOT Manager is idle for more the two minutes, exit is performed automatically.

Appendix C

SNMP Management

This appendix provides specific information required for managing WEB RANger-II with the Simple Network Management Protocol (SNMP).

C.1 SNMP Environment

General

The SNMP management functions of the WEB RANger-II are provided by an internal SNMP agent, which can use inband and out-of-band communication.

The SNMP management communication uses the User Datagram Protocol (UDP). UDP is a connectionless-mode transport protocol, part of the suite of protocols of the Internet Protocol (IP).

Note

Telnet management uses the TCP protocol over IP for management communication. After a Telnet session is started, the management interface is similar to that used for the supervision terminal,

This section covers the information related to the SNMP environment. For a description of the IP environment, refer to the *IP Environment* section below.

SNMP Principles

The SNMP management protocol is an asynchronous command/response polling protocol. All of the management traffic is initiated by the SNMP-based network management station, which addresses the managed entities in its management domain. Only the addressed managed entity answers the polling of the management station, except for trap messages.

The managed entities include a function called an “SNMP agent”, which is responsible for interpretation and handling of the management station requests to the managed entity, and the generation of properly-formatted responses to the management station.

SNMP Operations

The SNMP protocol includes four types of operations:

- **getRequest** - Command for retrieving specific management information from the managed entity. The managed entity responds with a **getResponse** message.

- **getNextRequest** – Command for retrieving sequentially specific management information from the managed entity. The managed entity responds with a **getResponse** message.
- **setRequest** – Command for manipulating specific management information within the managed entity. The managed entity responds with a **getResponse** message.
- **trap** – Management message carrying unsolicited information on extraordinary events (that is, events which occurred not in response to a management operation) reported by the managed entity.

The Management Information Base

The management information base (MIB) includes a collection of ***managed objects***. A managed object is defined as a parameter that can be managed, such as a performance statistics value.

The MIB includes the definitions of relevant managed objects. Various MIBs can be defined for various management purposes, types of equipment, etc.

An object's definition includes the range of values (also called “instances”) and the “access” rights:

- **Read-only** – Instances of that object can be read, but cannot be set
- **Read-write** – Instances of that object can be read or set
- **Write-only** – Instances of that object can be set, but cannot be read
- **Not accessible** – Instances of that object cannot be read nor set.

MIB Structure

The MIB has an inverted tree-like structure, with each definition of a managed object forming one leaf, located at the end of a branch of that tree. Each “leaf” in the MIB is reached by a unique path. By numbering the branching points from the top down, each leaf can be uniquely defined by a sequence of numbers. The formal description of the managed objects and the MIB structure is provided in a special standardized format, called Abstract Syntax Notation 1 (ASN.1).

Since the general collection of MIBs can also be organized in a similar structure, under the supervision of the Internet Activities Board (IAB), any parameter included in a MIB that is recognized by the IAB is uniquely defined.

MIBs are classified in various classes (branches): the experimental branch, and the group of private (enterprise-specific) branch. This is to provide the flexibility necessary in a global structure. Under the private enterprise-specific branch of MIBs, each enterprise (manufacturer) can be assigned a number, which is its enterprise number. The assigned number designates the top of an enterprise-specific sub-tree of non-standard MIBs. Within this context, RAD has been assigned the enterprise number 164. Therefore, enterprise MIBs published by RAD can be found under 1.3.6.1.4.1.164.

MIBs of general interest are published by the IAB in the form of a Request for Comment (RFC) document. In addition, MIBs are also often assigned informal names that reflect their primary purpose. Enterprise-specific MIBs are published and distributed by their originator, which is responsible for their contents.

MIBs Supported by the WEB RANger-II SNMP Agent

The interpretation of the relevant MIBs is a function of the SNMP agent of each managed entity. The general MIBs supported by the WEB RANger-II SNMP agent are as follows:

- RFC 1158 (standard MIB-II)
- RFC 1406 (standard IP/IP MIB).

In addition, the WEB RANger-II SNMP agent supports the RAD-private (enterprise-specific) MIB identified as (read the following as a continuous string):

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).
rad(164).radGen(6).systems(1).radSysWAN(3).radFcdIP(30).
```

Enterprise-specific MIBs supported by RAD equipment, including those for the WEB RANger-II, are available in ASN.1 format from the RAD Technical Support Department.

Management Domains Under SNMP

SNMP enables, in principle, each management station that knows the MIBs supported by a device to perform all the management operations available on that device. However, this is not desirable in practical situations, so it is necessary to provide a means to delimit management domains.

SNMP Communities

To enable the delimitation of management domains, SNMP uses “communities”. Each community is identified by a name, which is an alphanumeric string of up to 255 characters defined by the user.

Any SNMP entity (this term includes both managed entities and management stations) is assigned by its user a community name. In parallel, the user defines for each SNMP entity a list of the communities, which are authorized to communicate with it, and the access rights associated with each community (this is the SNMP community name table of the entity).

In general, SNMP agents support two types of access rights:

- **Read-only –** the SNMP agent accepts and processes only SNMP **getRequest** and **getNextRequest** commands from management stations which have a read-only community name.
- **Read-write –** the SNMP agent accepts and processes all the SNMP commands received from a management station with a read-write community name. SNMP agents are usually configured to send traps to management stations having read-write communities.

Authentication

In accordance with the SNMP protocol, the SNMP community of the originating entity is sent in each message.

When an SNMP message is received by the addressed entity, first it checks the originator's community: messages with community names not included in the SNMP community names table of the recipient are discarded (SNMP agents of managed entities usually report this event by means of an authentication failure trap).

The SNMP agents of managed entities evaluate messages originated by communities appearing in the agent's SNMP community names table in accordance with the access rights, as explained above. Thus a **setRequest** for a MIB object with read-write access rights will nevertheless be rejected if it comes from a management station whose community has read-only rights with respect to that particular agent.

C.2 IP Environment

General

The SNMP agent of the WEB RANger-II can communicate either out-of-band or inband:

- Out-of-band communication is performed via the CONTROL DCE port. The communication uses the Serial Link Internet Protocol (SLIP).
- Inband communication uses a proprietary protocol. You can select the way inband management traffic is carried: by the FDL, which supports a data rate of 4 kbps, or in a dedicated time slot of each link. When a dedicated time slot is used, the data rate is selectable (8, 16, 32, or 64kbps), but the sub link supports only 8 kbps.

Note

The FDL option can be used only when ESF framing is used.

You can separately enable the use of out-of-band communication, and of inband communication on each link (main and/or sub).

IP Environment

The SNMP agent of the WEB RANger-II uses either the UDP or the TCP transport protocol, part of the suite of IP protocols.

IP Address Structure

Under the IP protocol, each IP network element (SNMP agents, network management stations, etc.) is called an IP host and must be assigned an IP address. An IP address is a 32-bit number, usually represented as four 8-bit bytes. Each byte represents a decimal number in the range of 0 through 255.

The address is given in decimal format, with the bytes separated by decimal points, e.g., 164.90.70.47. This format is called ***dotted quad notation***.

An IP address is logically divided into two main portions:

- **Network Portion –** The network portion is assigned by the Internet Assigned Numbers Authority (IANA). There are five IP address classes: A, B, C, D, and E. However, only the classes A, B and C are used for IP addressing. Consult your network manager with respect to the class of IP addresses used on your network.

  The network portion of an IP address can be one, two or three bytes long, in accordance with the IP address class. *Table C-1* illustrates this arrangement.

Table C-1. Arrangement of Network Portion of IP Address

	IP ADDRESS			
	Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Class A	Network Portion	Host Portion		
Class B	Network Portion		Host Portion	
Class C	Network Portion			Host Portion

The class of each IP address can be determined from its leftmost byte, in accordance with *Table C-2*.

Table C-2. IP Address Class Determination

Address	First Byte	Address Range
Class A	0 through 127	0.H.H.H through 127.H.H.H
Class B	128 through 191	128.N.H.H through 191.N.H.H
Class C	192 through 223	192.N.N.H through 223.N.N.H

N – indicates bytes that are part of the network portion
H – indicates bytes that are part of the host portion

- **Host Portion –** The host portion is used to identify an individual host connected to the network. The host identifier is assigned by the using organization, in accordance with its specific needs.

Note

The all-zero host identifier is always interpreted as a network identifier, and must not be assigned to an actual host.

Often, the host portion is further subdivided into two portions:

- **Subnet number**. For example, subnet numbers can be used to identify departmental subnetworks. The subnet number follows the network identifier.
- **Host number** – the last bits of the IP address.

Automatic Routing of IP Traffic

The SNMP agent of the WEB RANger-II units includes a proprietary IP router function that is used to route management messages automatically.

The proprietary IP router operates both on the inband, as well as on the out-of-band traffic, depending on the communication methods that have been enabled.

The router of each SNMP agent collects information on the other SNMP agents whose messages pass through by monitoring the IP source and destination addresses of the IP messages, and combining this information with the information on the direction to the management station. This automatic learning capability enables using any network topology, including topologies with closed loops.

C.3 SNMP Traps

The SNMP agent of the WEB RANger-II supports the standard MIB-II traps. In addition, each WEB RANger-II alarm is sent as a specific trap to the management station.

Appendix D
Glossary

10BaseT - 10BaseT is a LAN protocol that allows stations to be attached via twisted pair cable.

ARP (Address Resolution Protocol) - ARP is a method for finding a host's Ethernet address from its Internet address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for the second host to send back its Ethernet address.
ARP is defined in RFC 826.

Bandwidth - Bandwidth is the rate at which data passes through the link. The greater the bandwidth, the more information can be sent through the link at a particular time.

Bridging - Bridging is the forwarding of traffic between network segments based on data link layer information. These segments have a common network layer address.

Broadcast - Broadcast is a transmission to multiple, unspecified recipients. On an Ethernet network, a broadcast packet is a special type of multicast packet which all nodes on the network are always willing to receive.

Default Gateway - Default Gateway is a routing table entry that is used to direct packets addressed to hosts or networks not explicitly listed in the routing table.

DLCI (Data Link Control Identifier) - DLCI is a channel number that is attached to data frames to tell the network how to route the data in Frame Relay Networks.

DNS (Domain Name System) - DNS is a general-purpose distributed, replicated, data query service chiefly used on Internet for translating hostnames into Internet IP addresses.
DNS is defined in STD 13, RFCs 1034 and 1035.

Dynamic Station - A dynamic station is a host that is added automatically to an ARP or LAN table.

E1/T1 - E1/T1 services provide high-speed connections. E1/T1 supports Frame Relay, PPP and HDLC, providing the flexibility to support high-performance point-to-point or point-to-multipoint topologies.

Firewall - A firewall system controls access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

Frame Relay - Frame Relay is a packet-switching protocol for connecting devices on a WAN. Frame Relay networks support data rates up to 1.544Mbps.

IP Address - The IP Address is a 32-bit host address. It is usually represented in dotted decimal notation, e.g. 128.121.4.5. The address can be split into a network number (or network address) and a host number unique to each host on the network and sometimes also a subnet address.
IP Address is defined in RFC 791.

IP Mask - The IP mask is a unique 4 byte (32 bit) value that allows the recipient of IP packets to distinguish between different host IDs.

IP/IPX Routing - IP/IPX Routing is the process, performed by a router, of selecting the correct interface and next hop for a packet being forwarded. Routing is done in order to send a packet to a specific destination.

IPX (Internetwork Packet Exchange) - IPX is a network layer protocol used in Novell NetWare file server operating systems.
A router with IPX routing can interconnect LANs so that Netware clients and servers can communicate.

Leased Lines - A leased line is a private telephone circuit permanently connecting two points, normally provided on a lease by a local PTT.

MAC (Media Access Control) - MAC is the lower sublayer of the data link layer. MAC is the interface between a node's Logical Link Control and the network's physical layer. The MAC differs for various physical media.

MAC Address - The MAC Address is the hardware address of a device connected to a shared network medium.

Mask - A mask is a filtering aid that is used to define classes of addresses. By defining classes, any packet can be judged as to whether it should pass the filter or not.

MTU (Maximum Transmit Unit) - The Maximum Transmission Unit is the largest frame length which may be sent on a physical medium.

Multicast - Multicast is an Ethernet addressing scheme used to send packets to devices of a certain type or for broadcasting to all nodes.

NCP (NetWare Core Protocol) - NCP is a Novell trademark for the protocol used to access Novell NetWare file and print service functions. NCP uses an underlying IPX or IP transport protocol.

NetBEUI (NetBIOS Extended User Interface) - NetBEUI is the network transport protocol used by all of Microsoft network systems and IBM LAN Server based systems.

Parity - Parity is an extra bit added to a byte or word to reveal errors in storage (in RAM or disk) or transmission. Even/odd parity means that the parity bit is set so that there are an even/odd number of one bits in the word, including the parity bit. Odd parity means that the parity bit is set so that there are an odd number of one bits in the word, including the parity bit.

PPP (Point-to-Point Protocol) - PPP is the protocol defined in RFC 1661, the Internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links.
PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.,It can configure connections to a remote network

dynamically, and test that the link is usable. PPP can be configured to encapsulate different network layer protocols (such as IP, IPX, or AppleTalk) by using the appropriate network.

Protocol - A protocol is a set of formal rules describing how to transmit data across a network. Low level protocols define the electrical and physical standards to be observed, bit- and byte-ordering, and the transmission, error detection and correction of the bit stream. High level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, sequencing of messages etc.

PSTN (Public Switched Telephone Network) - PSTN is the collection of interconnected systems operated by the various telephone companies and administrations (PTTs) around the world.

RFC (Request for Comment) - RFC is a numbered Internet informational documents and standards widely followed by commercial software and freeware in the Internet and UNIX communities.

RIP (Routing Information Protocol) - RIP is the companion protocol to IPX for exchange of routing information in a Novell network. It is not related to the Internet protocol of the same name.

SAP - SAP is the OSI term for the component of a network address which identifies the individual application on a host which is sending or receiving a packet.

SNMP (Simple Network Management Protocol) - SNMP is the Internet standard protocol, defined in STD 15, RFC 1157, developed to manage nodes on an IP network.

SOCKS - SOCKS is a security package that allows a host behind a firewall to use Finger, FTP, Telnet, Gopher, and Mosaic to access resources outside the firewall while maintaining the security requirements.

Spoofing - Spoofing is a technique used to reduce network overhead, especially in a WAN. Some network protocols send frequent packets for management purposes. These can be routing updates or keep-alive messages. In a WAN this can introduce significant overhead, due to the typically smaller bandwidth of WAN connections.
Spoofing reduces the required bandwidth by having devices, such as bridges or routers, answer for the remote devices. This fools (spoofs) the LAN device into thinking the remote LAN is still connected, even though it's not. The spoofing saves the WAN bandwidth, because no packet is ever sent out on the WAN.

SPX (Sequenced Packet Exchange) - SPX is a transport layer protocol built on top of IPX. SPX is used in Novell NetWare systems for communications in client/server application programs, e.g. BTRIEVE (ISAM manager).

Static Station - A static station is a host that is added manually to an ARP or LAN table.

Stop Bit - Stop Bits mark the end of a unit of transmission (normally a byte or character). In serial communications, where each bit of the message is transmitted in sequence, stop bits are extra "1" bits which follow the data and any parity bit.

Synchronous Transmission - Synchronous transmission is when data bits are transmitted at a fixed rate. The sender and the receiver are synchronized.

TCP (Transmission Control Protocol) - TCP is the most common transport layer protocol used on Ethernet and the Internet.
TCP is built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication, flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections.
TCP is defined in STD 7, RFC 793.

TCP/IP stack (Transmission Control Protocol over Internet Protocol) -TCP/IP stack is the standard Ethernet protocols incorporated into 4.2BSD UNIX. While TCP and IP specify two protocols at specific layers, TCP/IP is often used to refer to the entire DoD protocol suite based upon these, including Telnet, FTP, UDP and RDP.

TFTP (Trivial File Transfer Protocol)- TFTP is a simple file transfer protocol used for downloading boot code to diskless workstations.

Throughput - Throughput is the amount of data a communications channel can carry, usually in bytes per second.

UDP (User Datagram Protocol) - UDP is an Internet standard network layer, transport layer and session layer protocols which provide simple but unreliable datagram services. It adds a checksum and additional process-to-process addressing information. UDP is a connectionless protocol which, like TCP, is layered on top of IP.
UDP is defined in STD 6, RFC 768.

WAN (Wide Area Network) - A WAN is a network, usually constructed with serial lines, extending over distances greater than one kilometer.

Index

24 Raoul Wallenberg St., Tel Aviv 69719, Israel
Tel: +972-3-6458181, Fax: +972-3-6483331, +972-3-6498250
E-mail: erika_y@rad.com, Web site: www.rad.com

Customer Response Form

RAD Data Communications would like your help in improving its product documentation. Please complete and return this form by mail or by fax or send us an e-mail with your comments.

Thank you for your assistance!

Manual Name: WEB RANger-II

Publication Number: 766-201-03/04

Please grade the manual according to the following factors:

	Excellent	*Good*	*Fair*	*Poor*	*Very Poor*
Installation instructions	❒	❒	❒	❒	❒
Operating instructions	❒	❒	❒	❒	❒
Manual organization	❒	❒	❒	❒	❒
Illustrations	❒	❒	❒	❒	❒
The manual as a whole	❒	❒	❒	❒	❒

What did you like about the manual?

_____

_____

_____

_____

_____

Error Report

Type of Error(s) or Problem(s):

- ❒ Incompatibility with product
- ❒ Difficulty in understanding text
- ❒ Regulatory information (Safety, Compliance, Warnings, etc.)
- ❒ Difficulty in finding needed information
- ❒ Missing information
- ❒ Illogical flow of information
- ❒ Style (spelling, grammar, references, etc.)
- ❒ Appearance
- ❒ Other _____

Please list the exact page numbers with the error(s), detail the errors you found (information missing, unclear or inadequately explained, etc.) and attach the page to your fax, if necessary.

_____

_____

_____

_____

Please add any comments or suggestions you may have.

_____

_____

_____

You are:

- ❒ Distributor
- ❒ End user
- ❒ VAR
- ❒ Other _____

Who is your distributor? _____

Your name and company: _____

Job title: _____

Address: _____

Direct telephone number and extension: _____

Fax number: _____

E-mail: _____

data communications

www.rad.com

INTERNATIONAL HEADQUARTERS:

24 Raoul Wallenberg Street, Tel Aviv 69719, Israel, Tel: 972-3-6458181
Fax: 972-3-6498250, 972-3-6474436, Email: market@rad.com

U.S. HEADQUARTERS:

900 Corporate Drive, Mahwah, N.J. 07430, Tel: (201) 529-1100
Toll Free: 1-800-444-7234, Fax: (201) 529-5777, Email: market@radusa.com

Publication No. 766-201-03/04