NetPath™2000 Reference Manual

September 2005
34-00343.A

VERILINK®

FCC Requirements

Verilink products have been assembled from tested components found to comply with the limits for a 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 reference manual, may cause harmful interference to 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 the user's own expense.

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

Safety Precautions

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

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

Software License

1. General. The software, documentation and any fonts accompanying this License whether on disk, in read only memory, on any other media or in any other form (collectively the "Software") are licensed, not sold, to you by Verilink Corporation. ("Verilink") for use only under the terms of this License, and Verilink reserves all rights not expressly granted to you. The rights granted herein are limited to Verilink's intellectual property rights in the Verilink Software and do not include any other patents or intellectual property rights. You own the media on which the Verilink Software is recorded but Verilink and/or Verilink's licensor(s) retain ownership of the Software itself.

2. Permitted License Uses and Restrictions. This License allows you to use one (1) copy of the Software on within the NetPath 2000 unit. This License does not allow the Software to exist on more than one such device or computer at a time, and you may not make the Software available over a network where it could be used by multiple devices or multiple computers at the same time. Except as and only to the extent expressly permitted in this License or by applicable law, you may not copy, decompile, reverse engineer, disassemble, attempt to derive the source code of, modify, or create derivative works of the Software or any part thereof. Any attempt to do so is a violation of the rights of Verilink and its licensors of the Software. If you breach this restriction, you may be subject to prosecution and damages. THE SOFTWARE IS NOT INTENDED FOR USE IN WHICH THE FAILURE OF THE SOFTWARE COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE.

3. Transfer. You may not rent, lease, lend or sublicense the Software. You may, however, make a one-time permanent transfer of all of your license rights to the Software to another party, provided that: (a) the transfer must include all of the Software, including all its component parts, original media, printed materials and this License; (b) you do not retain any copies of the Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the Software reads and agrees to accept the terms and conditions of this License.

4. Termination. This License is effective until terminated. Your rights under this License will terminate automatically without notice from Verilink if you fail to comply with any term(s) of this License. Upon the termination of this License, you shall cease all use of the Verilink Software and destroy all copies, full or partial, of the Verilink Software.

5. Disclaimer of Warranties. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. EXCEPT FOR THE LIMITED WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS PROVIDED "AS IS", WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND DANGER AND DANGER'S LICENSORS (COLLECTIVELY REFERRED TO AS "DANGER" FOR THE PURPOSES OF SECTIONS 5 AND 6) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. DANGER DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE, THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERRORFREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY DANGER SHALL CREATE A WARRANTY. SHOULD THE SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

6. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL DANGER BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF DANGER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Verilink's total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty dollars ($50.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

7. Export Law Assurances. You may not use or otherwise export or reexport the Software except as authorized by United States law and the laws of the jurisdiction in which the Software was obtained. In particular, but without limitation, the Software may not be exported or re-exported (a) into (or to a national or resident of) any U.S. embargoed countries (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria) or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List. By using the Software, you represent and warrant that you are not located in, under control of, or a national or resident of any such country or on any such list.

8. Government End Users. The Software and related documentation are "Commercial Items", as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and

"Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

9. Controlling Law and Severability and Choice of Forum. This License will be governed by and construed in accordance with the laws of the State of Colorado, as applied to agreements entered into and to be performed entirely within Colorado between Colorado residents, that is, without giving any effect to the choice of laws provisions of the State of Colorado. This License shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect. You agree that the only courts in which you will bring lawsuits concerning the application or enforcement of this License are courts of competent jurisdiction located in the State of Colorado and you consent to the exercise of jurisdiction by any such court. This paragraph shall survive in full force and effect regardless of any termination of this License.

10. Third Party Notices and Conditions. The Software may include or utilize certain software which is owned by the Open Source Foundation, the source code of which is available under the GPL License (the "GPL"). Verilink may make modifications to this GPL Code. The license for the GPL Code is included here as Exhibit A. Those terms are fully applicable to the use of those portions of the Software that consist of or are derived from the GPL Code.

Table of Contents

Preface

Chapter 1 About NetPath 2000

Chapter 2 Installation

Chapter 3 Configuration

Appendix A Specifications

PREFACE

About this Manual

This reference guide for the NetPath 2000 describes unit features and specifications, configuration, and installation.

Manual Organization

The chapters and appendices in this manual are arranged for quick reference when you need it.

- Chapter 1, "About NetPath 2000" – This chapter describes product features and capabilities.
- Chapter 2, "Installation" – This chapter describes unit port connections and powering information.
- Chapter 3, "Configuration" – This chapter describes the menu screens and configuration parameters accessed through the Web server interface.
- Appendix A, "Specifications" – This appendix defines the specifications for the NetPath 2000.

Typographic Conventions

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

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

Customer Service and Technical Support

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

Support from Verilink

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

Telephone

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

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

E-mail

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

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

Internet

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

http://www.verilink.com

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

Returning a Unit to Verilink

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

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

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

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

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

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

CHAPTER

1

ABOUT NETPATH 2000

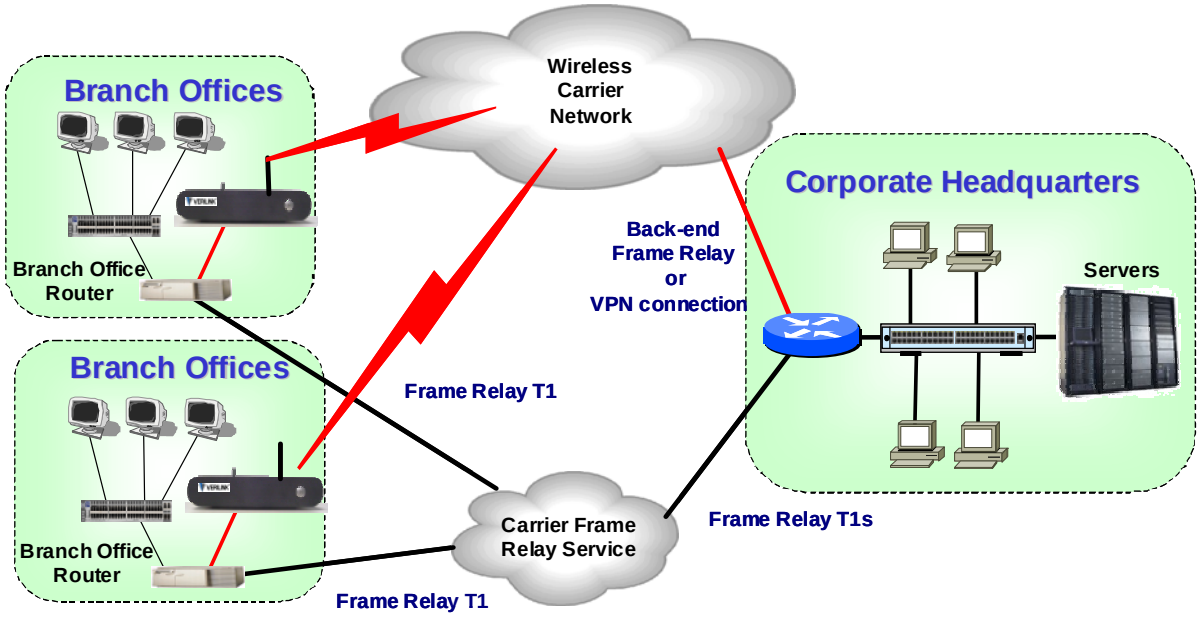
Introduction

The NetPath 2000 enables a branch office to maintain network connectivity in case of a disruption in service due to an outage of the main network connection. The NetPath 2000 uses Cingular's wireless data network as an alternate path to route mission-critical information.

NetPath 2000 Backup Operation

In a typical customer network (see Figure 1.1), the branch offices are connected to their headquarters using Cisco 17xx routers via a T1 frame relay network service to a central router located at their headquarters. The NetPath 2000 and the Cingular wireless network provide a fail-over mechanism by creating a backup connection in the event this main connection (T1 frame relay network connection) has a disruption in service. The branch office router connects to the NetPath 2000 via a cross-over Ethernet cable. Dynamic Host Configuration Protocol (DHCP) address assignment may be configured on this NetPath 2000 Ethernet port (branch router Ethernet interface).

Figure 1.1 *Typical Customer Network Configuration.*



The simplest fail-over configuration uses a static secondary default or subnet route in the branch office router via the NetPath 2000's interface. When the branch office router detects a failure of the primary default or headquarters route over the T1 frame relay network, it switches its routing to the backup Ethernet port and the NetPath 2000. The NetPath 2000 automatically connects to the Cingular wireless network and routes traffic to the corporate headquarters using the alternative wireless network.

When the main network connection is restored, the branch office router falls back to using only this Frame Relay Network and ceases sending traffic via the NetPath 2000. The NetPath 2000 continuously monitors and maintains its wireless connection via periodic keep-alive packets in the event it is required to provide network connectivity. While the main network connection is providing connectivity, the branch office router should not send any idle or keep-alive WAN traffic to the NetPath 2000 to avoid creating unnecessary wireless traffic, but it may ping the NetPath 2000 local interface.

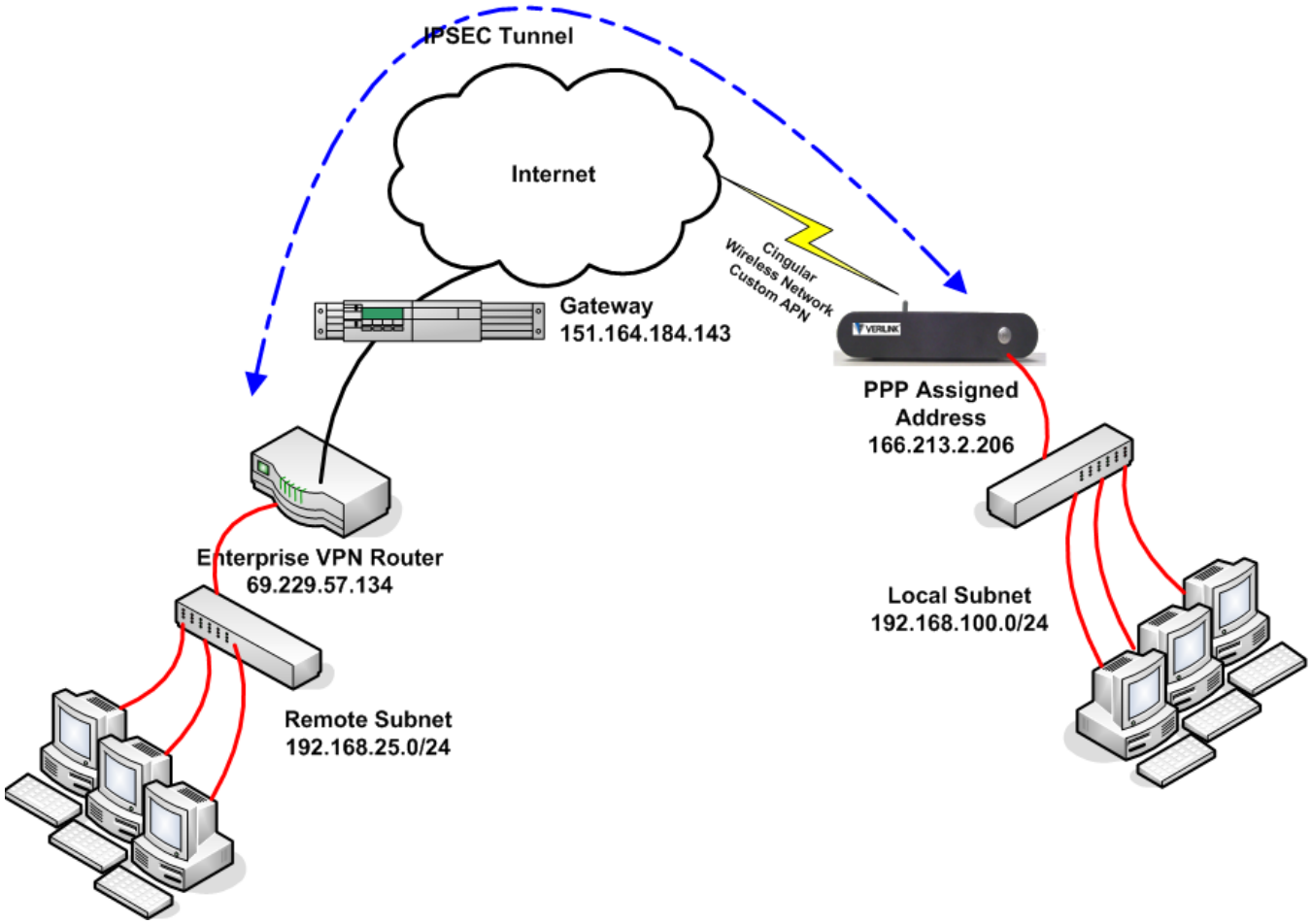
NetPath 2000 Secure Primary WAN Operation

The NetPath 2000 offers a method for secure network connectivity (see Figure 1.2). It uses Cingular's 3G wireless data network as the primary means to route mission-critical information employing internal Virtual Private Network (VPN) functionality to maintain end-to-end security.

In a typical customer network, the branch offices are connected to their headquarters through the NetPath 2000 and the Cingular wireless network. The Cingular wireless network assigns the NetPath 2000 a network IP address via a Point-to-Point Protocol (PPP) connection. The NetPath 2000, using Network Address Translation (NAT) and DHCP, provides private address

assignment to the branch office's local network over its branch office router Ethernet interface.

Figure 1.2 *NetPath 2000's Method for Secure Network Connectivity*



Front Panel

The NetPath 2000 front panel is shown in Figure 1.3.

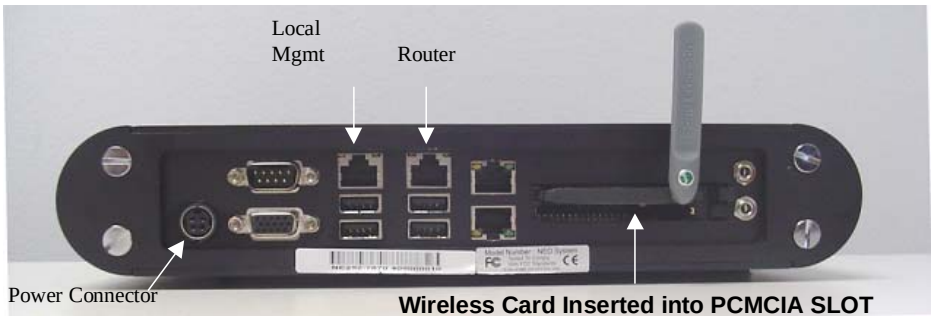
Figure 1.3 *NetPath 2000 Front Panel*

The front panel's power switch LED is illuminated with the unit is on.

Rear Panel

The NetPath 2000 rear panel is shown in Figure 1.4.

Figure 1.4 *NetPath 2000 Rear Panel*



The NetPath 2000 rear panel has three interfaces described in detail below.

NetPath 2000 Interfaces

The NetPath 2000 has the following interfaces:

Local Management Ethernet Interface

This is a direct Ethernet connection for local management and configuration. The default IP address is 192.168.100.1, and this address is configurable. DHCP can be configured ON or OFF for this interface.

Branch Router Ethernet Interface

This is a connection to the branch office router. The default IP address is 192.168.1.1, and this address is configurable. DHCP can be configured ON or OFF for this interface.

PCMCIA Slot

This connection (slot) lets you use a PCMCIA wireless card.

CHAPTER

2

INSTALLATION

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

Unpacking and Inspection

The NetPath 2000is shipped in cardboard cartons with foam inserts for shock and vibration protection. When your shipment arrives, inspect the shipping container and contents, and compare all items with those on the packing list.

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

Supplied Materials

The NetPath 2000 ships with the following standard items:

- NetPath 2000
- External Power Supply
- AC Power Cord
- Cross-over CAT5 Ethernet Cable

The contents of the shipment are shown in Figure

Figure 2.1 *Shipment Contents*

Contact Verilink Technical Support (page vi) for assistance.

Additional Requirements

The NetPath 2000 has been designed to work with one of the following wireless PCMCIA cards inserted:

- Novatel Merlin U520 UMTS
- Sony Ericsson GC83 EDGE
- Sierra Wireless AC775 EDGE

Unpacking

Remove the NetPath 2000 from the packing carton and place on a flat, stable surface.

Remove the external power supply from the packing carton and plug the 4-pin connector into the NetPath 2000 rear panel, making sure the flat portion of the cable connector is facing the top of the unit.

Plug the AC cord into the external power supply.

Plug the AC cord into a standard AC wall outlet or power strip.

Look at the NetPath 2000 front panel. If the Power switch is not lit, press the front panel Power switch once until lit.

Connecting for Configuration

To configure your NetPath 2000, connect one end of the crossover CAT5 cable (supplied) to the local management interface of the NetPath 2000. Connect the other end of the CAT5 cable to a PC. The local management Ethernet interface has a default IP address of 192.168.100.1, a subnet mask of

255.255.255.0, and comes DHCP enabled. Either enable DHCP under your PC's network settings, or configure your PC to an appropriate IP address such as 192.168.100.2, subnet mask 255.255.255.0. For further information on configuring your NetPath 2000, refer to Chapter 3, *Configuration*,.

Connecting to an External Router for Wireless Backup Operation

For wireless backup, connect a straight-through CAT5 cable from the branch router Ethernet interface to the branch office router.

CHAPTER

3

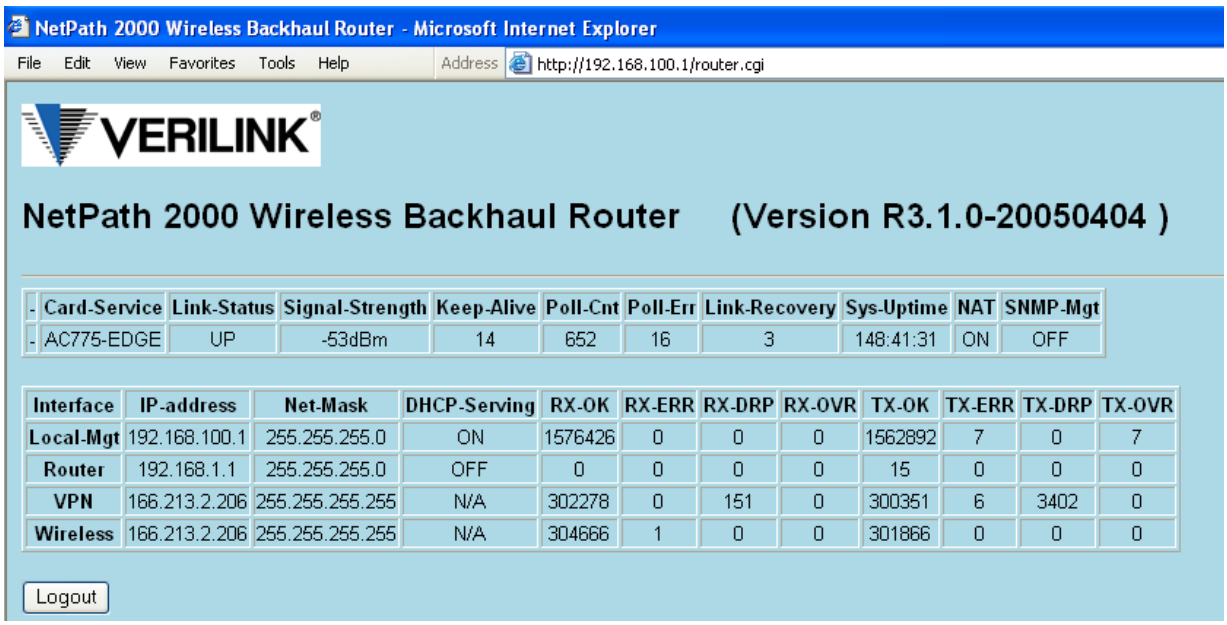
CONFIGURATION

The NetPath 2000's GUI is accessible from all three physical interfaces: the local management Ethernet port, the branch router Ethernet port, or the PCMCIA slot with card inserted. (Refer to *NetPath 2000 Interfaces* as described on page 1-4 for more information on these interfaces.)

Web Access Authentication

Access your PC's Web browser and type in the NetPath 2000's IP address, 192.168.100.1, to view the screen shown in Figure 3.1.

Figure 3.1 *NetPath 2000 Access Screen*



NOTICE: *You may need to disable personal firewalls or security programs to access this screen.*

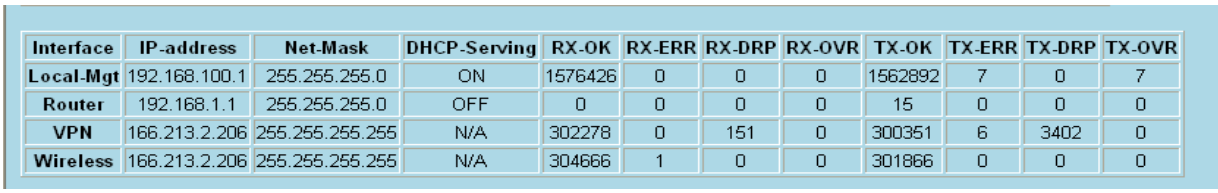
The NetPath 2000 permits two levels of access. The first provides a status-only display, and the second provides full status and configuration capability.

The default password for status-only access is “view.” This password is case-sensitive.

Status-Only Display

After you enter the password, a status screen similar to that shown in Figure 3.2 will appear.

Figure 3.2 *Sample Status Screen*



Interface	IP-address	Net-Mask	DHCP-Serving	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR
Local-Mgt	192.168.100.1	255.255.255.0	ON	1576426	0	0	0	1562892	7	0	7
Router	192.168.1.1	255.255.255.0	OFF	0	0	0	0	15	0	0	0
VPN	166.213.2.206	255.255.255.255	N/A	302278	0	151	0	300351	6	3402	0
Wireless	166.213.2.206	255.255.255.255	N/A	304666	1	0	0	301866	0	0	0

The status display headings, a description of each, and parameters, where appropriate, are listed below.

Card Service Automatically detects and displays the type of PCMCIA wireless network card inserted and type of wireless network service operation.

Values: AC775GC82/U520
EDGE/UMTS

Link Status Displays the communication state of the inserted PCMCIA wireless network card. “Down” indicates the card is searching to find the specific wireless service. “Up” indicates the card and network are in service. “Restarting” indicates the NetPath 2000 is attempting to recover from a communication error with the card. “Unknown” indicates the NetPath 2000 cannot communicate with the wireless network card.

Values: Down, Up, Restarting, Unknown

Signal Strength Displays the RSSI in dBm’s if the Link Status indicates anything other than UP. Locate the NetPath 2000 where a signal is available. When the Link Status indicates UP, the Signal Strength will display N/A.

Values: Dbm or N/A

Keep-Alive Displays the numbers of minutes between Keep-Alive transmissions.

Values: 1–60 min

Poll-Cnt Displays the number of polls.

Poll-Err Displays the number of polling errors.

Link-Recovery Displays the number of times the PCMCIA card has lost connection and the NetPath 2000 has had to reestablish connection to the wireless network.

Sys-Uptime Displays the time since reboot or power cycle. This is router operational time, not wireless connection time.

NOTICE: *Sys-Uptime indicates router operational time, not wireless connection time.*

NAT Indicates whether NAT is enabled on the Branch Router interface.

Values: ON, OFF

SNMP-Mgt Indicates whether the NetPath 2000 can be configured and monitored from the wireless network.

Values: ON, OFF

Interface Lists the NetPath 2000 interfaces.

Values: Local-Mgt, Router, VPN, Wireless

IP-address Displays the IP address of each interface.

Net-Mask Displays the net mask address of each interface.

DHCP-Serving Displays the current DHCP setting for the two Ethernet interfaces.

Values: ON, OFF, N/A

RX-OK Displays the number of receive packets without errors.

RX-ERR Displays the number of receive packets with errors.

RX-DRP Displays the number of receive packets missing.

RX-OVR Displays the number of receive overruns.

TX-OK Displays the number of transmit packets without errors.

TX-ERR Displays the number of transmit packets with errors.

TX-DRP Displays the number of transmit packets missing.

TX-OVR Displays the number of transmit overruns.

Administration-Level Status and Configuration Display

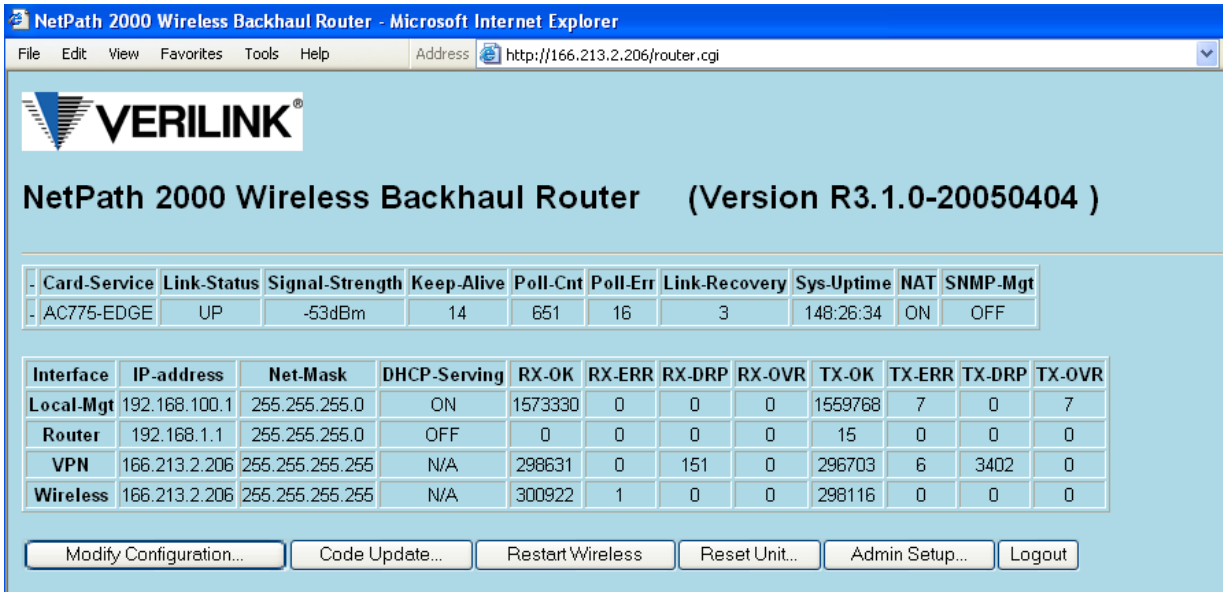
Configuration control is permitted only at the administration-access level. The default administration password is “admin.” This password is case sensitive.

After you enter the password, a screen similar to that shown in Figure 3.3 will appear.

The configuration information contained in this chapter assumes the use of the local management Ethernet port.

NOTICE: *The configuration information shown in the menus below assumes the use of the local management Ethernet port.*

Figure 3.3 *Sample Administration-Level Status and Configuration Screen*



-	Card-Service	Link-Status	Signal-Strength	Keep-Alive	Poll-Cnt	Poll-Err	Link-Recovery	Sys-Uptime	NAT	SNMP-Mgt
-	AC775-EDGE	UP	-53dBm	14	651	16	3	148:26:34	ON	OFF

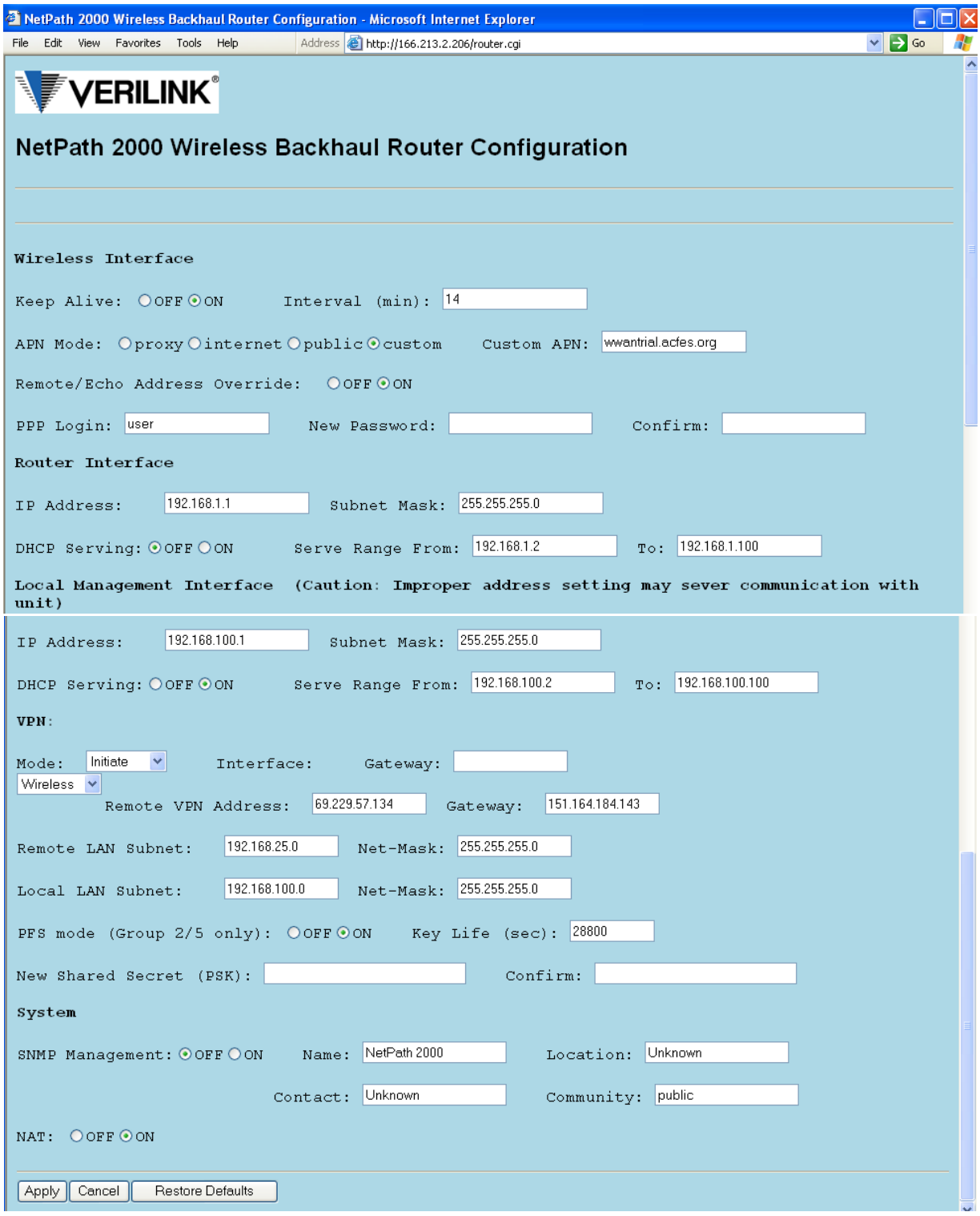
Interface	IP-address	Net-Mask	DHCP-Serving	RX-OK	RX-ERR	RX-DRP	RX-OVR	TX-OK	TX-ERR	TX-DRP	TX-OVR
Local-Mgt	192.168.100.1	255.255.255.0	ON	1573330	0	0	0	1559768	7	0	7
Router	192.168.1.1	255.255.255.0	OFF	0	0	0	0	15	0	0	0
VPN	166.213.2.206	255.255.255.255	N/A	298631	0	151	0	296703	6	3402	0
Wireless	166.213.2.206	255.255.255.255	N/A	300922	1	0	0	298116	0	0	0

This screen is identical to the Status-Only access screen except for the configuration buttons at the bottom of the screen. These buttons let you change the NetPath 2000's configuration, software, and passwords. Each of these buttons is described below.

Modify Configuration

The "Modify Configuration" button displays the screen shown in Figure 3.4 and lets you change the NetPath 2000's configuration.

Figure 3.4 *Modify Configuration Screen*



Wireless Network Interface

The wireless network interface settings are described below.

Keep Alive Select OFF or ON for packet transmissions and select a range from 1–60 minutes. Suggested value is 14 minutes.

APN Mode Four APNs are available: proxy, internet, public, and custom. Use "Custom" to custom-name an APN. (For detailed APN information, please refer to *Access Point Names (APNs)* as described on page 3-10).

Remote/Echo Address Override Select OFF or ON. When ON, this feature overrides a remote/echo address to prevent illegal PPP termination addresses on the service provider's network. This may be required if the NetPath 2000 cannot communicate with the network termination.

Values: OFF, ON

Login/Password/ Confirm Password Not all networks require a user name and password. Your service provider will provide these to you if necessary.

Router Interface

The branch router interface settings are described below.

IP Address Sets the IP address of the NetPath 2000's Ethernet interface. The factory-default setting is 192.168.1.1.

Subnet Mask Sets the address mask that delineates local subnet range. In most cases, the factory-default range of 255.255.255.0 will suffice.

DHCP Serving Enables DHCP. If enabled, the user must enter an IP address range to be served.

Values: OFF, ON

Serve Range From Sets the first address of the connected equipment served.

To Sets the last address of the connected equipment served. When combined with "Serve Range From," determines the number of addresses served.

Local Management Interface

Use this interface to connect a PC directly to the NetPath 2000 to configure and/or check status. Settings are described below.

NOTICE: *You will lose communication if the NetPath 2000's IP address is not configured correctly or if the IP address is unknown.*

IP Address Sets the IP address of the NetPath 2000'a Ethernet interface. The factory-default setting is 192.168.100.1.

Subnet Mask Sets the address mask that delineates local subnet range. In most cases, the factory-default range of 255.255.255.0 will suffice.

DHCP Serving Enables DHCP. If enabled, the user must enter an IP address range to be served.

Values: OFF, ON

Serve Range From Sets the first address of the connected equipment served.

To Sets the last address of the connected equipment served. When combined with "Serve Range From," determines the number of addresses served.

VPN

The VPN settings are described below.

Mode Enables VPN to initiate or respond automatically upon usage (Normal) or force responder mode (Listen) or initiate a tunnel (Initiate).

Values: Disabled, Normal, Listen, Initiate

Interface Selects which interface supports VPN tunneling. Set to Wireless, unless in Test Mode.

Values: Wireless, Local-Mgt, Router

Gateway Sets Gateway address. Leave blank when using the wireless interface since, in this case, the Gateway is provided through the PPP link.

Remote VPN Address Sets the address of the remote VPN unit. This address must match the remote VPN termination device.

Gateway Sets the IP address of the routable Gateway to the remote terminating VPN device.

Remote LAN Subnet Sets the remote subnet address on the unencrypted remote side of the tunnel.

Net-Mask Sets the remote LAN net-mask to narrow the range of remote network clients contacted.

Local LAN Subnet Sets the local subnet address on the unencrypted local LAN side of the tunnel. This address must match the router interface address described above.

Local LAN Net-Mask Sets the local LAN net-mask to narrow the range of local network clients connected to the tunnel.

PFS Mode Enables or disables the Perfect Forward Secrecy (PFS) mode.

Values: OFF, ON

Key Life Sets the PFS Key Life update period in seconds. The default is 28800 seconds.

New Shared Secret (PSK) Sets the shared secret password for authentication. This password is case sensitive.

Confirm Confirms the previously set shared-secret password. This character string is case sensitive and must match the previously set shared secret.

System

The system-level configuration lets you modify the system-level networking capabilities, including remote management via SNMP and NAT between the Ethernet and wireless ports.

SNMP Management Enables SNMP.

Values: OFF, ON

Name Sets SNMP name.

Location Sets SNMP location.

Contact Sets SNMP contact name.

Community Sets SNMP community delimiter.

NAT Enables NAT between the wireless network interface and the branch router and local management interfaces.

Values: OFF, ON

Applying Configuration Changes

The following buttons appear at the bottom of the Configuration screen.

Apply This button applies the configuration changes. You must apply the changes before they will take effect. After selecting "Apply," the changes are made and the browser will revert to the Status Display screen.

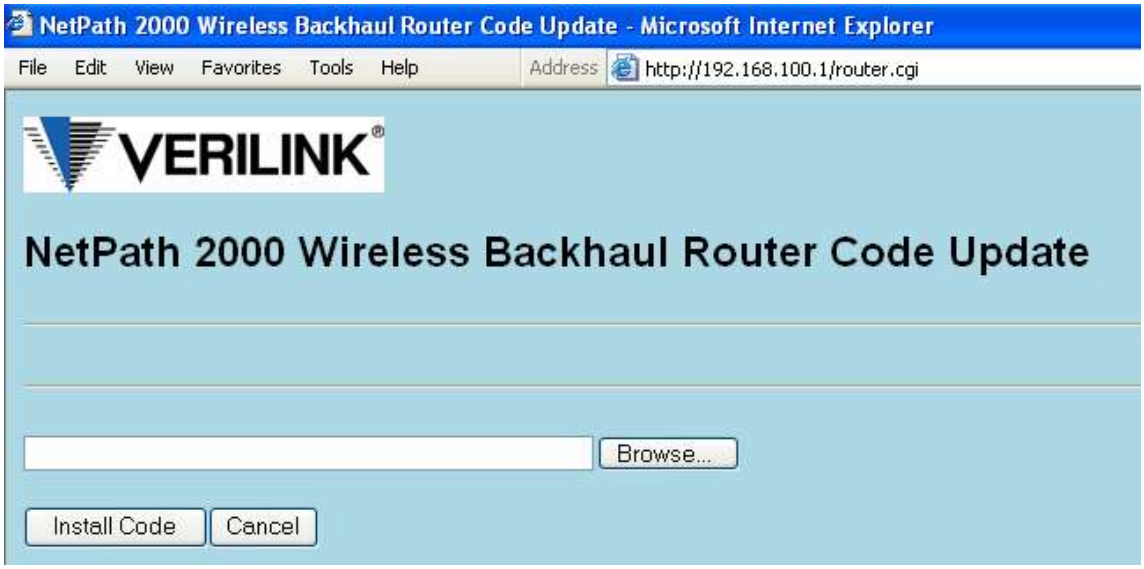
Cancel This button cancels any configuration changes. After selecting "Cancel," all changes are canceled and the browser will show the Status Display screen.

Restore Defaults This button will restore all configurable entries to the factory default settings. Select "Apply" to complete this action.

Code Update

To update the NetPath 2000's operating software, select the "Code Update button. The NetPath 2000 will display the screen shown in Figure 3.5.

Figure 3.5 *Code Update Screen*



Type the file location or select the “Browse” button to find the location of the file that contains the code update. Select your file and press “OK.”

Select “Install Code” to initiate the file transfer and update the code, or select the “Cancel” button to cancel the update.

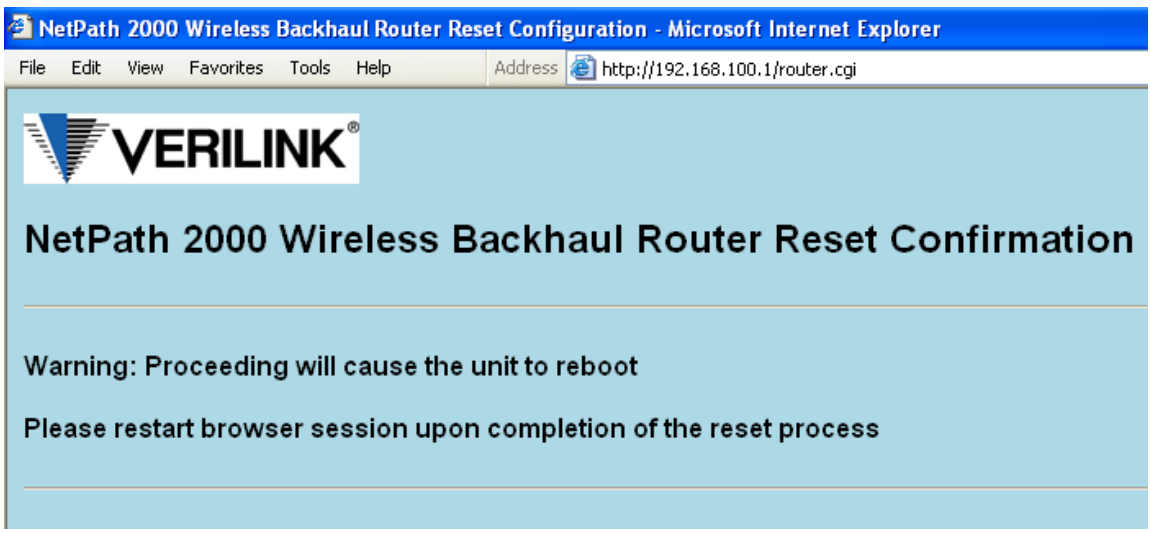
Restart Wireless

Select the “Restart Wireless” button to restart the PCMCIA wireless network card. This immediately disconnects any existing wireless link, clears the card services statistics, and restarts the wireless card acquisition process.

Reset Unit

Select the “Reset Unit” button to display the screen shown in Figure 3.6.

Figure 3.6 *Reset Confirmation Screen*



Select the “Proceed” button to reset the NetPath 2000 unit. The unit will reboot. Select the “Cancel” button to abort the reset and return to the Display Status screen.

Access Point Names (APNs)

APNs are a mechanism for the wireless service provider to specify what IP address options are available, how the wireless device links with external networks, what fixed-end connections are available, and any other services the wireless device may permit. APNs are defined as part of a wireless carrier’s subscriber account and are provisioned by the carrier. Some are general-purpose APNs such as public and proxy, while others are custom. All IP addresses are dynamically assigned to the NetPath 2000 wireless interface based on the APN type and capabilities as provisioned by the wireless service.

The NetPath 2000 offers four basic types of APN services: Proxy, Internet, Public, and Custom. Each of these options is described in the table below.

APN Type	IP Address	Service Provider Network
Proxy	Private	Default APN. Network performs NAT. Supports only mobile-originated IP-based communications to the Internet. Does not allow communication with customer-dedicated, fixed-end connections. *Note: there are other options for mobile-terminated communications, including Wireless Application Protocol (WAP) push mechanisms and Short Message Service.*
Internet	Public	No NAT performed, nor required. Supports only mobile-originated, IP-based communications to the Internet. Communication with customer-dedicated, fixed-end connections permitted.
Public	Public	No NAT performed, nor required. Supports only mobile-originated, IP-based communications to the Internet. Does not allow communication with customer-dedicated, fixed-end connections.
Custom	Usually Public (Private Available under special circumstances.	Used with dedicated-customer, fixed-end connections. Provides routing and security options. Enables mobile-terminated applications if desired.

APPENDIX

A

SPECIFICATIONS

Routing

- Routes IP packets between wireless network card and branch router Ethernet interface.
- DHCP server optional for all Ethernet interfaces.

VPN

- IPSEC tunnel mode
- VPN server or client, initiate, listen, or normal modes
- IKE auto-keying
- Main mode negotiation
- Pre-shared keys (PSK/shared secrets)
- ESP 3DES encryption
- ESP HMAC-MD-5 or HMAC-SHA1 authentication
- PFS group 2/5
- Configurable session keylife in seconds

Management

- Web GUI
- Local management
- Ethernet port
- Optional remote management through wireless network card
- Command line interface
- Local management
- Local management Ethernet interface – SSH and SCP
- Optional remote management through wireless network card – SSH and SCP
- SNMP monitoring
- RFC1213 MIB2
- SSH access

Hardware Interfaces

- Local management Ethernet interface – management interface: RJ-45
- Branch router Ethernet interface – branch router interface: RJ-45
- Serial port – DB-9, 9600/8/n/1

Wireless Network Interface

- Novatel Merlin U520 UMTS
- Sony Ericsson GC82/GC83 EDGE
- Sierra Wireless AC775 EDGE

Power

Voltage:	120 VAC
Frequency:	50–60 Hz
Dissipation:	60 W

Mechanical

Mounting:	Standalone
Dimensions:	Width 10.7 in. (??? cm)
	Height 2 in. (??? cm)
	Depth 6.7 in. (??? cm)
Weight:	??? pounds (??? kg)

Environmental

Operating Temp:	32 to 1104 °F (0 to 40 °C)
Storage Temp:	–13 to 140 °F (–25 to 60 °C)
Humidity:	90 % maximum (non-condensing)

Industry Listings

EMI:	FCC Part 15, Class A