Aurorean™ Virtual Network

ANG-1100
User's Guide

Version 2.1

ENTERASYS
NETWORKS

Notice

Enterasys Networks and its licensors reserve the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made. The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS AND ITS LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF ENTERASYS NETWORKS AND ITS LICENSORS HAVE BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
35 Industrial Way
Rochester, NH 03866-5005

Part Number: 9033734-01
October 2001
Printed in the United States of America

The ENTERASYS NETWORKS logo, AUROREAN, PRESCRIPTIVE DIAGNOSTICS ENGINE, RIVERMASTER, INTELLIGENT CLIENT ROUTING, and TOLLSAVER are trademarks of Enterasys Networks.

MICROSOFT, MS, and MS-DOS are registered trademarks and Windows, Windows 95, Windows 98, Windows NT, Windows 2000 Professional and Windows Millennium are trademarks of Microsoft Corporation in the USA and other countries.

VIRTUAL NETWORK COMPUTING is a trademark of AT&T Laboratories Cambridge.

Other trademarks and trade names used in this publication belong to their respective owners.

Aurorean Virtual Network software includes the following third-party components:

> Commercial support for ActivePerl is available through PerlClinic at http://www.ActiveState.com. Peer support resources for ActivePerl issues can also be found at the ActiveState Web site under support at http://ActiveState.com/support/. The ActiveState Repository has a large collection of modules and extensions in binary packages that are easy to install and use. To view and install these packages, use the Perl Package Manager (PPM) which is included with ActivePerl. ActivePerl is the latest Perl binary distribution from ActiveState and replaces what was previously distributed as Perl for Win32. The latest release of ActivePerl as well as other professional tools for Perl developers are available from the ActiveState Web site.
>
> Gate Daemon software © 1995 The Regents of the University of Michigan. All rights reserved.
> Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.
>
> A DES implementation written by Eric Young © 1995-1997 Eric Young (eay@cryptsoft.com). All rights reserved.
>
> MD4 and MD5 implementation derived from the RSA Data Security, Inc. MD4 Message-Digest Algorithm and MD5 Message-Digest Algorithm © 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
>
> ccp.c - PPP Compression Control Protocol © 1994 The Australian National University. All rights reserved.
>
> chap.c - Crytographic Handshake Authentication Protocol © 1991 Gregory M. Christy. All rights reserved.
>
> chap_ms.c - Microsoft MS-CHAP compatible implementation © 1995 Eric Rosenquist, Strata Software Limited (www.strataware.com). All rights reserved.
>
> fsm.c - {Link, IP} Control Protocol Finite State Machine © 1989 Carnegie Mellon University. All rights reserved.
>
> Routines to compress and uncompress TCP packets (for transmission over low speed serial lines) © 1989 Regents of the University of California. All rights reserved.
>
> Portions of the Aurorean Client Software are copyrighted to ICE Engineering, Inc. and licensed through a GNU public license. For more information, including access to the source code, visit their Web site at www.ice.com.

Federal Communications Commission (FCC) Notices

The Aurorean Network Gateway-1102/1105 complies with Title 47 Part 15, Class B of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Modifications or changes made to this device, and not approved by Enterasys Networks may void the authority granted by the FCC or other such agency to operate this equipment.

There are no user-repairable components in the Aurorean Network Gateway-1102/1105.

Canadian Notices

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled “Digital Apparatus”, ICES-003 of the Department of Communications (Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques”, NMB-003 édictée par le ministre des Communications).

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

UL Notices

The Aurorean Network Gateway-1102/1105 have been tested and found to comply with the UL 1950/CSA c22.2 Revision 3/CUL regulation.

European Notices

The ANG-1102/1105 has been tested and found to comply with the CISPR 22:1997 Class B regulation.

ELECTRICAL HAZARD: Only qualified personnel should perform installation procedures.

Important Safety Instructions

1) Read these instructions carefully. Save these instructions for future reference.
2) Follow all warnings and instructions marked on the product.
3) Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
4) Do not use this product near water.
5) Do not place this product on an unstable cart, stand, or table. The product may fall, causing serious damage to the product.
6) Slots and openings in the chassis are provided for ventilation; to ensure reliable operation of the product and to protect it from overheating, these openings should not be blocked or covered. The openings should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should never be placed near or over a radiator or heat register, or in a built-in installation unless the proper ventilation is provided.
7) This product should be operated from the type of power indicated on the marking label. If you are not sure of the type of power available, consult Enterasys Networks or your local power company.
8) Do not allow anything to rest on the power cord. Do not locate this product where persons will walk on the cord.
9) If an extension cord is used with this product, make sure that the total ampere rating of the equipment plugged into the extension cord does not exceed the extension cord ampere rating. Also, make sure that the total rating of all products plugged into the wall outlet does not exceed the fuse rating.
10) Never push objects of any kind into this product through chassis slots as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.
11) Do not attempt to service this product yourself, as operating or removing covers may expose you to dangerous voltage points or other risks. Refer all servicing to qualified service personnel.
12) Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
    a) When the power cord or plug is damaged or frayed.
    b) If liquid has been spilled into the product.
    c) If the product has been exposed to rain or water.
    d) If the product does not operate normally when the operating instructions are followed. Adjust only those controls that are covered by the operating instructions since improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal condition.
    e) If the product has been dropped or the chassis has been damaged.
    f) If the product exhibits a distinct change in performance, indicating a need for service.
13) Use only the proper type of power supply cord set (provided in your accessories box) for this unit. It should be a detachable type, UL listed/CSA certified, type SPT-2, rated 7A 125V minimum, VDE approved or equivalent. Maximum length is 15 feet (4.6 meters).

Table of Contents

About This Guide

Chapter 1 – Overview

Chapter 2 – Installation

Chapter 3 – Configuring the ANG-1100 with Aurorean Web Config

Appendix A – Glossary

Appendix B – Specifications

Appendix C – Pin Assignments

Appendix D – Program License Agreement & Support

Index

About This Guide

This guide describes how to mount, connect, power-up, and maintain an Aurorean™ Network Gateway-1100 (ANG-1102 / 1105) from Enterasys Networks.

This guide is written for administrators who want to configure the ANG-1100 for their remote clients or experienced users who are knowledgeable of basic networking principles.

Contents of the Guide

Information in this guide is arranged as follows:

- ❐ *Chapter 1, Overview* highlights the key features of the Aurorean Virtual Network family of enterprise VPN products.
- ❐ *Chapter 2, Installation* describes how to physically mount, connect, and power-up Aurorean servers.
- ❐ *Chapter 3, Configuring the ANG-1100 with Aurorean Policy Manager,* details how to configure the server.
- ❐ *Appendix A, Glossary* defines terms used in this manual.
- ❐ *Appendix B, Specifications* provides essential physical and operational characteristics of the ANG-1100.
- ❐ *Appendix C, Pin Assignments* describes the pinouts of the LAN connectors.
- ❐ *Appendix D, License Agreement & Support* describes the warranty terms and support policies covering Enterasys Networks products.

Conventions Used in This Guide

The following conventions are used in this guide:

☑ **NOTE**	Notes supply additional helpful information, provide a cross-reference to the source of more information, or emphasize issues you should consider when performing an action.
⚠ **CAUTION**	Cautions contain directions that can prevent you from damaging the product or losing data.
⚠ **WARNING**	Warnings provide directions that you must follow to avoid harming yourself.
Bold	Text in boldface indicates values you type using the keyboard or select using the mouse (for example, **a:\setup**). Default settings may also appear in bold.
Italics	Text in italics indicates a variable, important new term, or the title of a manual.
SMALL CAPS	Small caps specify the keys to press on the keyboard; a plus sign (+) between keys indicates that you must press the keys simultaneously (for example, CTRL+ALT+DEL).
`Courier font`	Text in this font denotes a file name or directory.

Related Publications

The following publications are also available with the Aurorean Network Gateway-1100:

- ❒ The *ANG-1102/1105 Quick Setup* card which highlights the basic steps required to install the Aurorean Network Gateway-1100.
- ❒ The *Installation & Service Guide* which describes how to install and maintain the ANG-3000 / 7000 series, the Aurorean server which can be used to complete a VPN connection with the ANG-1100.
- ❒ A *Portable Document File (PDF)* version of this manual is available and can be downloaded from the Enterasys.com Web site. You can view this manual on-line or print a copy of it using Adobe Acrobat Reader 3.0 (or later). Acrobat Reader can be downloaded from the Enterasys web site or the Adobe web site at `www.adobe.com`.
- ❒ All Aurorean manuals, Release Notes and Quick Start Cards are stored at this URL: `http://www.enterasys.com/support/manuals`.

1

Overview

This chapter describes the key features of the Aurorean Network Gateway 1100 and how it is used.

System Description

The ANG-1100, displayed in Figure 1, provides home or small office connectivity to a corporate branch office or headquarters. It supports up to 25 tunnels.

Figure 1 ANG-1100

Figure 2 illustrates how the ANG-1100 typically connects to the corporate network.

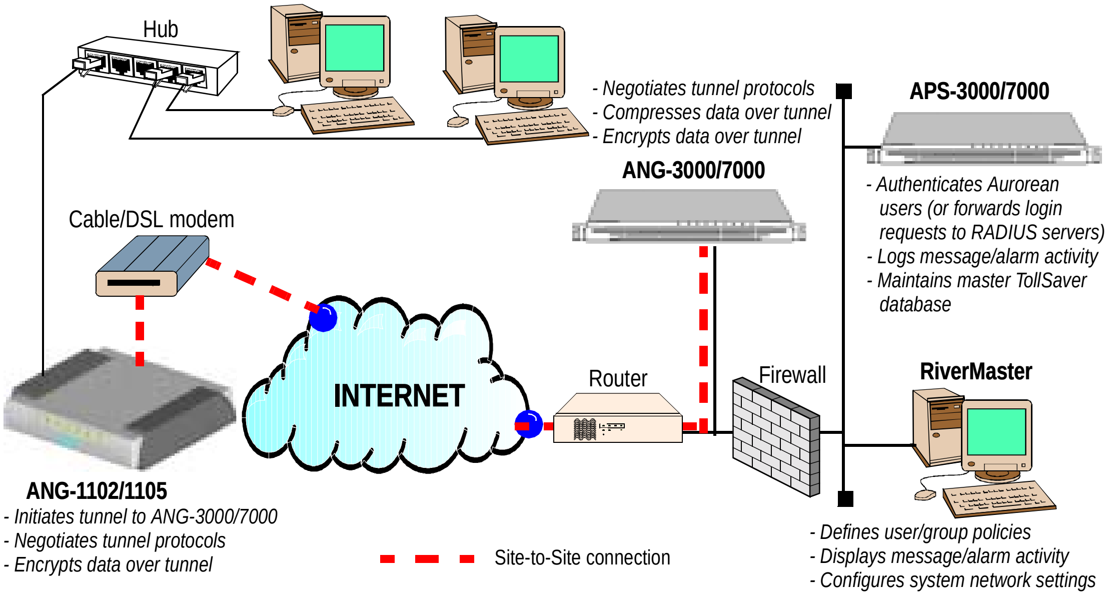

Hub
- Negotiates tunnel protocols
- Compresses data over tunnel
- Encrypts data over tunnel
ANG-3000/7000
APS-3000/7000
- Authenticates Aurorean users (or forwards login requests to RADIUS servers)
- Logs message/alarm activity
- Maintains master TollSaver database
Cable/DSL modem
INTERNET
Router
Firewall
RiverMaster
ANG-1102/1105
- Initiates tunnel to ANG-3000/7000
- Negotiates tunnel protocols
- Encrypts data over tunnel
Site-to-Site connection
- Defines user/group policies
- Displays message/alarm activity
- Configures system network settings

Figure 2 ANG-1102/1105 Topology

An ANG-1100 comes equipped with the following:

- ❒ 110-250V power supply.
- ❒ High-performance CPU: 90 MHz internal, 45 MHz external.
- ❒ Complete set of diagnostic LEDs which display the server’s operational status.
- ❒ One (ANG-1102) or four trusted (ANG-1105) 10 / 100 Base-T Ethernet ports and one external 10 Base-T port each to connect the system to the network and the Internet.
- ❒ One DB-9 port (ANG-1105) for diagnostics.

2

Installation

This chapter describes the steps required to unpack, install and connect an Aurorean Network Gateway-1102 / 1105 onto a desktop.

Unpacking the ANG-1102/1105

Remove the ANG-1102 / 1105 from the shipping box. Save the box in case the unit needs to be returned.

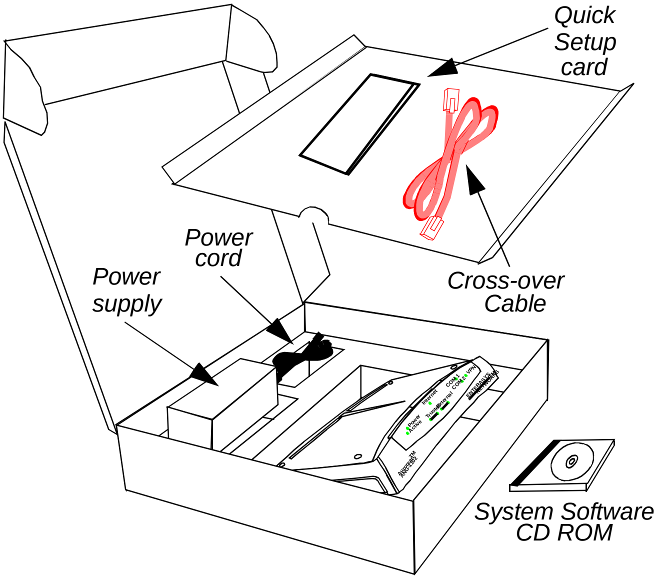


Figure 3 Removing ANG-1102/1105 from the Shipping Box

The box contains a CD ROM with this instruction manual in the Adobe PDF format, a *Quick Setup* card and accessories. See an illustration of the ANG-1105 below.

Figure 4 ANG-1105

Accessories

The ANG-1100 also is shipped with the following accessories:

- ❒ One cross-over (red) cable for a direct PC / Network Gateway connection.
- ❒ One power supply with an attached cable to connect to the ANG-1100.
- ❒ One power cord to connect the power supply to the AC outlet.

Location Planning

Place the ANG-1100 on a desktop near the following:

- ❒ Ethernet wall jack, patch panel, or hub with available ports.
- ❒ Near a DSL or Cable modem.
- ❒ A grounded wall outlet or uninterruptible power supply (UPS).

Connecting Cables

Ethernet cables are used to connect the ANG-1100 to your computer or LAN and the Internet. A serial cable can be used to connect the ANG-1105 to your computer for diagnostic purposes.

All interconnections are made at the back of the ANG-1100 (refer to Figure 5). Also, a reset button is located in the rear of the unit.

CAUTION

If you press the Reset button after you have configured your ANG-1100, you will lose your entire configuration. Any settings you supplied must then be re-entered. Do **not** use the Reset button unless you want the configuration to return to factory defaults; you may want to record your settings before using the Reset button.

Ethernet Connections

The ANG-1102 is equipped with two 8-pin modular RJ-45 Ethernet ports (five ports on the ANG-1105) labeled *TRUSTED* and *EXTERNAL* as shown in Figure 5. The trusted port is connected to a computer or hub / switch with networked computers. The external port is connected to a cable or DSL modem.

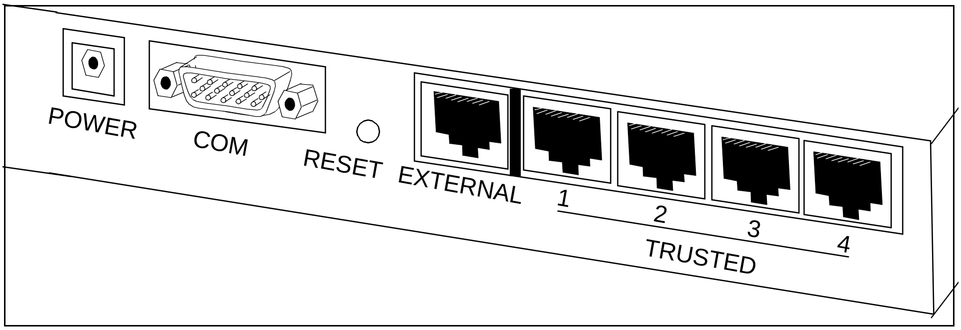


Figure 5 Location of the Serial/WAN/LAN Ports (ANG-1105 shown)

The trusted connection can be either a sole desktop computer or a hub that connects up to 25 tunnels to the network as shown in Figure 6.

Connecting an ANG-1102/1105

The ANG-1100 is typically set up in the configuration shown below.

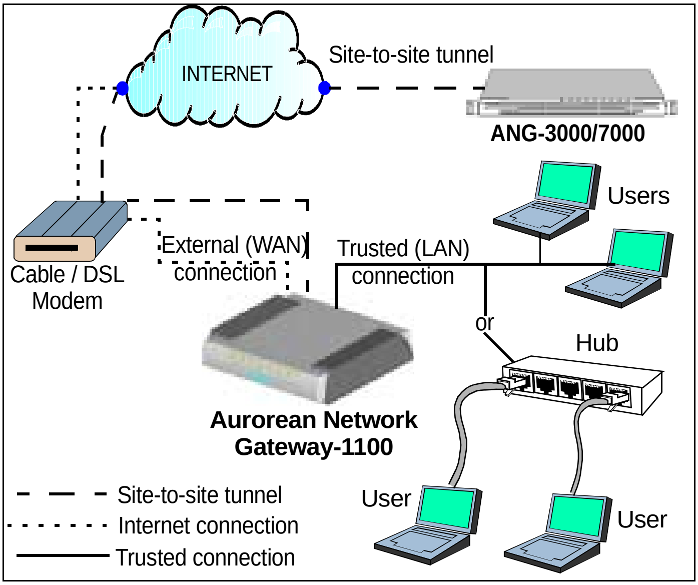


Figure 6 Connecting the ANG-1100

To connect the ANG-1100 Ethernet port, perform the following steps:

1 Do one of the following as shown in Figure 7:

– If you are connecting an ANG-1102 to a *hub*, plug one end of a straight-through Ethernet cable into the ANG's trusted port. If you are connecting an ANG-1105 to a PC, plug one end of a straight-through cable into the ANG's trusted port. If you are connecting an ANG-1105 to a hub, plug one end of the red, cross-over cable to a trusted port. Go to Step 2.

– If you are connecting the ANG-1102 directly to a *computer*, attach one end of the red, cross-over cable to a trusted port and the other end to an RJ45 connector on your computer. Skip to Step 3.

2 Plug the opposite end of the cable into a wall jack, patch panel, or hub linked to a protected network segment.

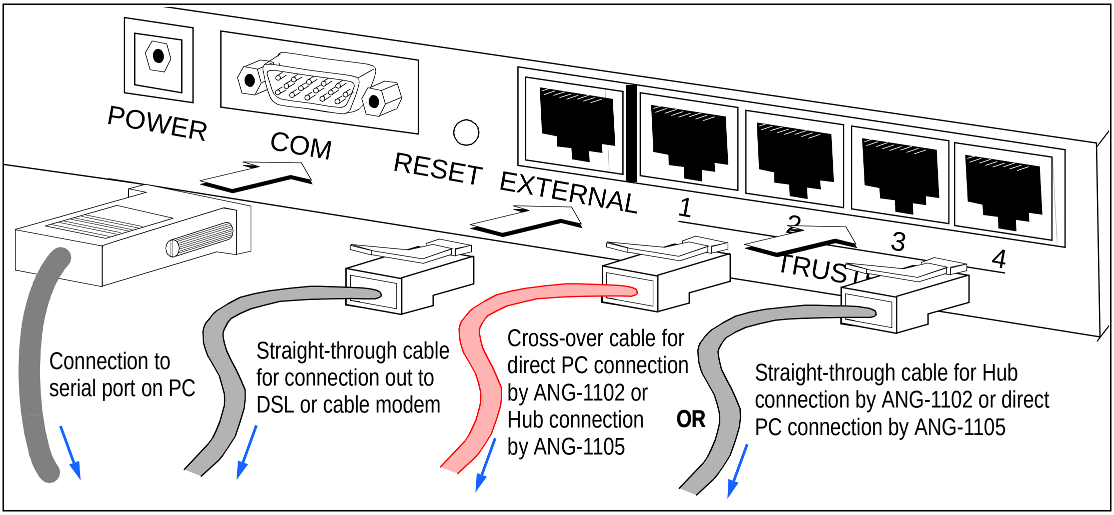

POWER
COM
RESET
EXTERNAL
1
2
3
4
TRUST
Connection to serial port on PC
Straight-through cable for connection out to DSL or cable modem
Cross-over cable for direct PC connection by ANG-1102 or Hub connection by ANG-1105
OR
Straight-through cable for Hub connection by ANG-1102 or direct PC connection by ANG-1105

Figure 7 Connecting Cables to the ANG-1100 (ANG-1105 shown)

3 Plug an Ethernet cable into the External port as shown in Figure 7.

4 Plug the opposite end of this cable into a DSL or cable modem.

NOTE

If you have a DSL modem, you will need to get an IP address from your provider and configure it. This condition may also exist for selective cable customers. Some cable internet providers require that you supply the MAC address of your computer. Refer to Chapter 3 for directions.

Serial Connection

The ANG-1105 is equipped with one 9-pin DB-9 port for use as a console port. You can then start a Hyperterminal session or establish a link using another terminal emulator.

Connecting an ANG-1105

To connect the ANG-1105 serial port, connect one end of a null modem cable (female-to-female) to the DB-9 port and another to the DB-9 port on your PC.

Connecting Power to the ANG-1102/1105

WARNING

To avoid electrical shock, connect the Aurorean system to a grounded (earthed) outlet only.

A switching power supply including a 6’ power cord and a 7’ electrical cord with an attached power supply is supplied with each system. To connect these items to an ANG-1100, perform the following steps:

1 Plug the power supply cord into the system’s power socket as shown in Figure 8.

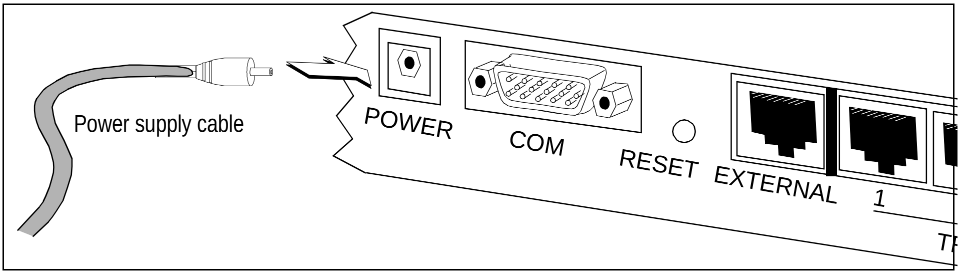


Figure 8 Connecting AC Power on the ANG-1100 (ANG-1105 shown)

2 Plug the AC power cord into the power supply and the other end into a grounded AC outlet or UPS as shown in Figure 9.

The Power LED on the ANG-1100 will light the moment you power up the unit.

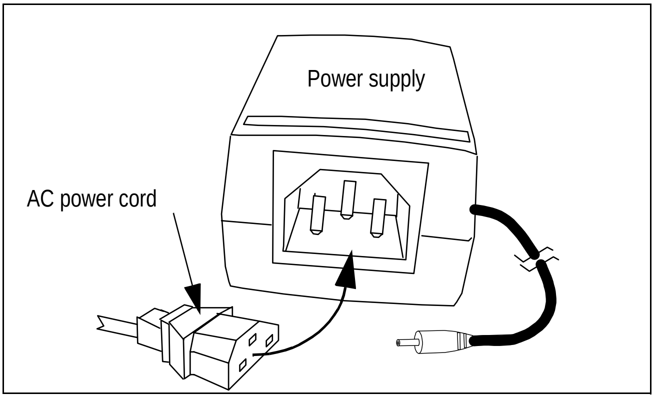


Figure 9 Connecting the Power Cable to the Power Supply

NOTE

International customers may swap the electrical cord segment shipped with the ANG-1100 for a cord that meets the proper standard for their country. A custom cord can be inserted in the power supply.

Checking ANG-1102/1105 Connections

The ANG-1100 is now connected and ready for configuration. Check the LEDS in the manner described below to confirm that the connections are working properly.

LED behavior

The LEDs behave as follows at when powered up at startup:

- ❐ Power LED stays ON for 2-3 seconds indicating boot diagnostics are running followed by boot up of the Linux kernel.
  - – If the Power LED flashes at a twice per second interval, boot diagnostics have failed.
  - – If the Power LED remains ON or OFF following the boot sequence, the kernel has failed to boot.
- ❐ Power LED blinks once per second indicating the system is operating correctly.
- ❐ LAN LEDs 1-4 either blink when active or remain ON. The ANG-1102 LAN LEDs are amber (10 Mbps); the ANG-1105 LAN LEDs are green (100 Mbps) or amber if the connected device is running at 10 Mbps.
- ❐ The WAN LED either blinks when active or remains ON.
- ❐ The VPN LED stays ON when a tunnel is connected.

The ANG-1100 is now ready for configuration. Refer to Chapter 3 for detailed instructions.

3

Configuring the ANG-1100 with Aurorean Web Config

To configure the ANG-1100, use the Internet browser on your computer and connect to the server via the Web. During the Web session, you run the Aurorean Web Config utility and configure the system. Figure 10 illustrates the process.

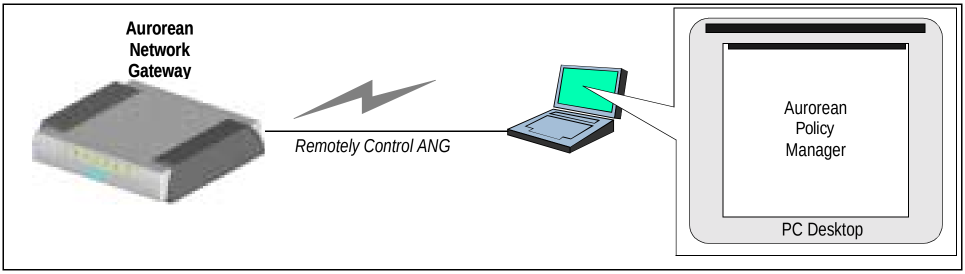


Figure 10 Configuring the ANG-1100 via Aurorean Web Config

Before You Begin

Before you begin configuration with Web Config, review the following:

- ❐ Be sure the ANG-1100 is cabled correctly as described in “Connecting an ANG-1100” in Chapter 2 of this manual.
- ❐ Ask your DSL or cable modem Internet provider and Network Administrator for any IP addresses, work group, network browsing or other information you may need to configure the ANG-1100 properly. Minimally, you will need:
  - – The IP address of the ANG-3000 / 7000 you will connect to for setting up the VPN.

- To configure your PC to include the domain of the corporate network you will connect to.

  To do so on your Windows 95/98/ME/2000 desktop: click Start, select Settings and double-click Control Panel (Win 2000: Network and Dial-up Connections). Double-click the Network icon (Win 2000: right click on Local Area Connection and click Properties), click the Protocols tab, select TCP/IP Protocol, click Properties, select the DNS tab and add the Domain Suffix in the field provided. Click OK twice to close the open windows.

❒ On your computer, release and renew the IP address for all adaptors bound to TCP/IP. Refer to the Caution on page 27 for instructions.

❒ If you have cable service, learn the MAC address of your computer as described on page 36.

❒ If your computer was supplied a static IP address and Gateway by your service provider, you *must* now accept the address from a DHCP server and remove the gateway for the ANG-1100 to find and connect with the PC.

To do so, click Start, select Settings and double-click on Control Panel. Double-click the Network icon, select the Protocols tab and TCP/IP Protocol, click on Properties and the IP Address tab. Select the Obtain an IP address from a DHCP server radio button. Click Advanced, select the Gateway, click Remove and OK. Click OK twice more to close the open windows.

❒ Web Config supports the use of Internet Explorer 5 or Netscape 4 and higher Web browsers.

❒ If your Web browser has Proxy settings, you must do the following:

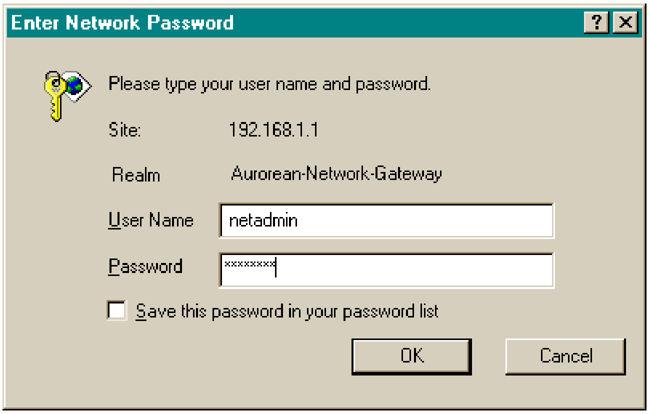
- For Internet Explorer users, under Tools/Internet Options/Connections/LAN Settings, **uncheck** “Automatically detect settings” and “Use automatic configuration script” boxes. Also **check** the “Use a proxy server” and “Bypass proxy server for local addresses” boxes and ask your network administrator for the IP Address, Port number and any Advanced settings.
- For Netscape users, under Edit/Preferences/Advanced/Proxies, **uncheck** any proxy radio buttons and **check** the “Direct connection to the Internet” button. No bypass option is available.

Logging into Web Config

To log into Web Config, perform the steps below.

1. Point your Web browser at the default trusted IP address of the ANG-1100. In the browser's Location field at the top of the window, type: **http://192.168.1.1** and click OK.

   The Login window appears as shown in Figure 11.



Please type your user name and password.

Site: 192.168.1.1

Realm Aurorean-Network-Gateway

User Name netadmin

Password ********

□ Save this password in your password list

Figure 11 Login Window

2. Type **netadmin** in the User Name and Password fields as shown in Figure 11.

3. Click the checkbox to save your password if you desire and click OK.

   The VPN Status window appears as shown in Figure 13.

Setting Your Password

Because the default password is readily available through all ANG-1100 documentation, we strongly recommend that you ensure security by configuring a new password to replace the default password *netadmin*.

NOTE

If you forget your password after changing it from the factory default, you can return to using *netadmin* by pressing the Reset button and reinstate all factory default values.

Change the Password by performing the following steps:

1 Click the Set Password menu option.

The Set Password window appears as shown in Figure 12.

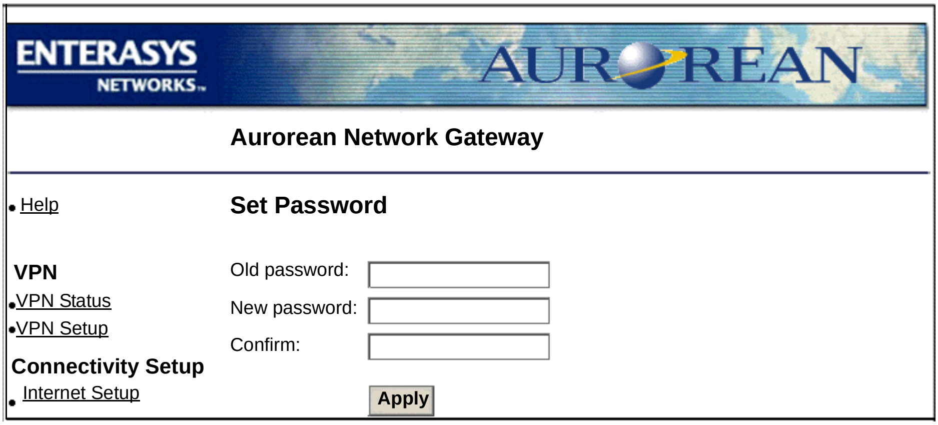


Figure 12 Set Password Window

2 Type the old Password in the field provided.

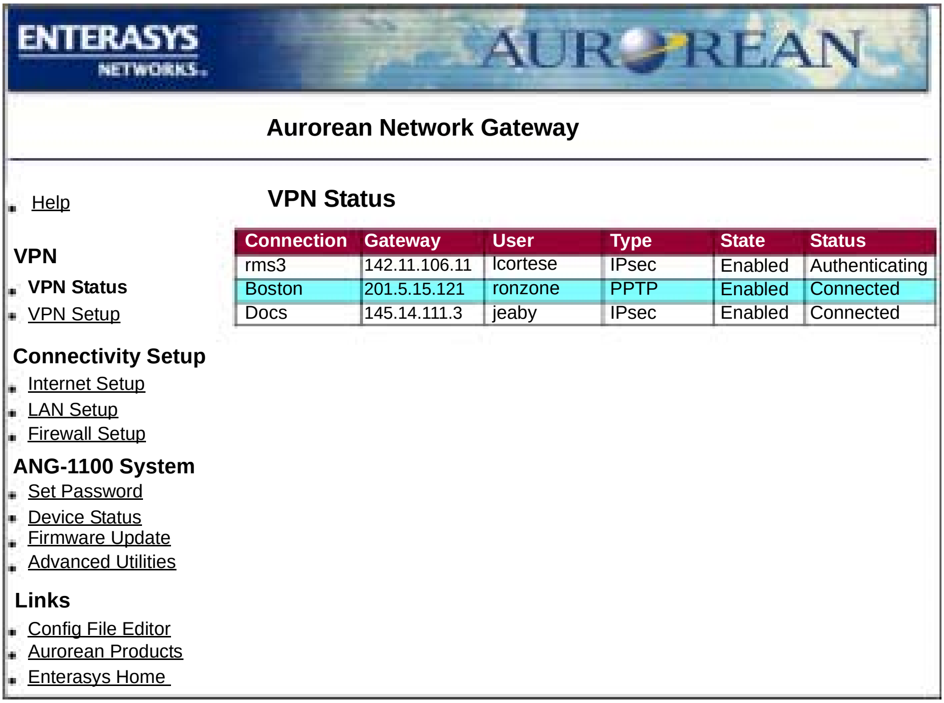
3 Type a new Password in the field provided.

4 Confirm the new password in the field provided.

5 Click Apply.

Viewing VPN Status

The VPN Status window is the first screen to appear after logging in. At this point, you have just begun configuration so the VPN Status window appears empty. Later, after you have configured a VPN connection to an ANG-3000/7000, the window will display information similar to the data shown in Figure 13.



Aurorean Network Gateway

VPN Status

Connection	Gateway	User	Type	State	Status
rms3	142.11.106.11	lcortese	IPsec	Enabled	Authenticating
Boston	201.5.15.121	ronzone	PPTP	Enabled	Connected
Docs	145.14.111.3	jeaby	IPsec	Enabled	Connected

Figure 13 VPN Status Window

1 Click the Setting Up the VPN menu option and go to the next page.

Setting Up the VPN

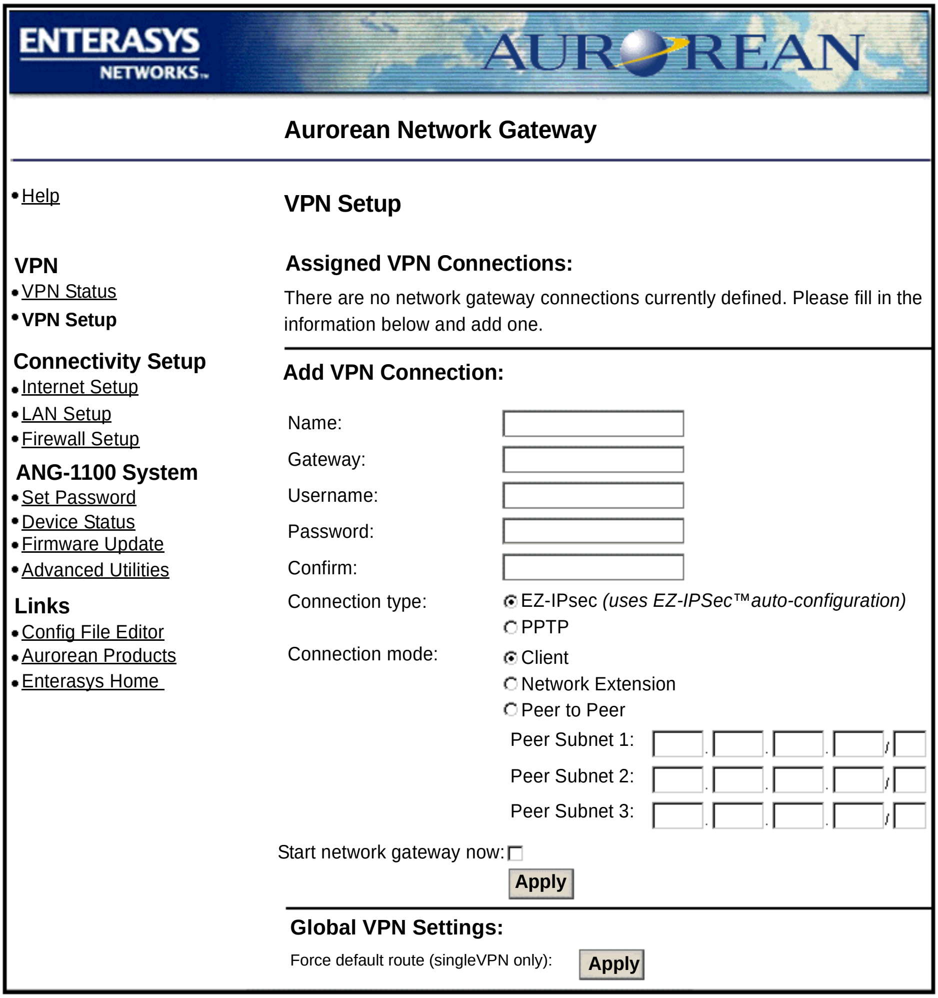
The VPN configuration created on the ANG-1100 completes a link with the ANG-3000/7000 on the remote end of this connection. If your network administrator has already set up the ANG-3000/7000 with appropriate User, Password and Group information, after setting up the VPN you will build the site-to-site tunnel connection and be up and running on the corporate LAN.

Before you start VPN configuration, be sure that your network administrator has supplied any IP addresses and masks required

Begin VPN Setup by performing the following steps:

1 Click the VPN Setup menu option.

The VPN Setup window appears as shown in Figure 14.



VPN Setup

Assigned VPN Connections:

There are no network gateway connections currently defined. Please fill in the information below and add one.

Add VPN Connection:

Name:

Gateway:

Username:

Password:

Confirm:

Connection type: ● EZ-IPsec *(uses EZ-IPSec™auto-configuration)* ○ PPTP

Connection mode: ● Client ○ Network Extension ○ Peer to Peer

Peer Subnet 1: . . . /

Peer Subnet 2: . . . /

Peer Subnet 3: . . . /

Start network gateway now: □

Global VPN Settings:

Force default route (singleVPN only):

Figure 14 VPN Setup Window

2 Enter the Name of the remote ANG-3000/7000 you are connecting to.

3 Enter the Gateway IP address of the remote ANG-3000/7000.

4 Enter the Username on the remote ANG-3000/7000.

CAUTION

When using PPTP, which selects MS-CHAPv2 authentication as a default, a Username cannot contain a plugin selector (e.g., *user@domain*). For example, if Windows 2000's IAS is being used to authenticate PPTP tunnels via a RADIUS plugin, the plugin must be the *authorization's* default plugin.

5 Enter the Password on the remote ANG-3000/7000.

6 Confirm the password on the remote ANG-3000/7000.

7 Select the Connection type: either EZ-IPsec or PPTP.

The EZ-IPsec feature provides one-button configuration for standard IPSec with IKE tunnels connecting to an ANG-3000/7000.

8 Select one of the following Connection modes:

- Client - standard site-to-site connectivity.
- Network Extension - expanded connectivity to devices on the trusted network behind the ANG-1100.

CAUTION

Choosing Network Extension mode requires that you configure, in the LAN Setup window, the IP address and mask with unique values supplied by your Network Administrator. You cannot select NEM and enable the ANG-1100 without your administrator's approval.

- Peer to Peer - connectivity for devices on remote networks over tunnels between two ANG-1100 servers, or interoperability between an ANG-1100 and a Cisco, Nortel or Nokia/Checkpoint VPN gateway. This option requires adding the IP address and Subnet Mask of up to 3 remote peers.

NOTE

Choosing Peer to Peer mode requires that you configure one or more IP addresses and subnet masks of connected peers with values supplied by your Network Administrator.

9 *Optional*. Check the Start network gateway now checkbox and click Apply to create instant access or wait until the other end of the connection is created.

10 *Optional*. Click Force default route under Global VPN Settings.

Force default route disables the ANG-1100's Intelligent Client Routing (ICR) feature which allows users to browse the Internet outside the tunnel. Be aware that with Force Default enabled, the ANG-1100 transmits all traffic through the tunnel which may cause Web browsing problems. This feature works with only one tunnel up and running; it is disabled if you create more than one tunnel.

11 Click Apply.

After applying your changes, a VPN Setup update window appears displaying configuration revisions.

✓ NOTE

Now that you have set up a site-to-site connection, configuration is complete unless you want to change the default Internet, LAN, Firewall, Password default values or your service is a Digital Subscriber Line (DSL) which requires that you configure a PPPoE connection (refer to "Setting Up the Internet Connection" on page 20). Some cable internet providers also require that you specify a MAC address (refer to "Using Advanced Utilities" on page 35 for more information).

✓ NOTE

If you press the Reset button after configuring your ANG-1100, you will lose your entire configuration. Any settings you supplied must then be re-entered. Do not use the Reset button unless you want the configuration to return to factory defaults. Also, you may want to record your settings.

Setting Up the Internet Connection

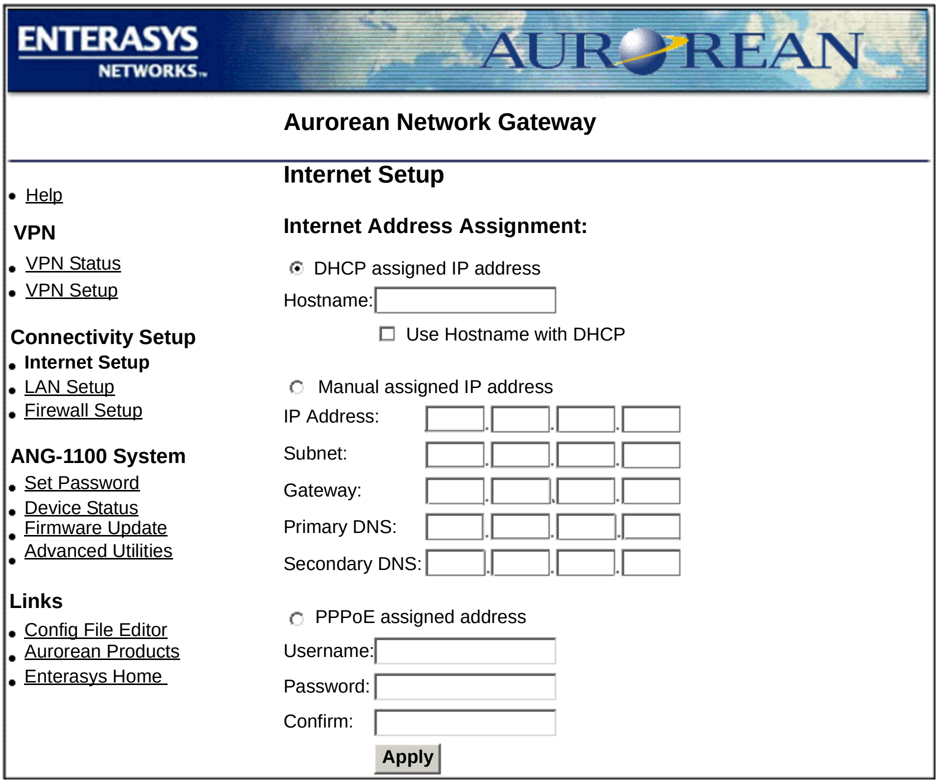
Internet configuration of the External side of the ANG-1100 involves choosing the type of IP address assignment the ANG-1100 will accept. The ANG can accept one of the following:

- ❐ A DHCP-assigned IP address - your network automatically sets the ANG's IP address via the DHCP (Dynamic Host Configuration Protocol) server. This is the factory default setting.
- ❐ A Manual-assigned IP address - you or your network administrator set the ANG's IP address and associated Subnet, Gateway, and DNS values. Consult with your Network Administrator for required values.
- ❐ A PPPoE (PPP over Ethernet) assigned IP address - your DSL provider transparently sets the IP address via the use of a Username and Password. Obtain this information from your service provider before you enter this data.

Begin Internet Setup by performing the following steps:

1 Click the Internet Setup menu option.

The Internet Setup window appears as shown in Figure 15.



Aurorean Network Gateway

- Help

VPN

- VPN Status
- VPN Setup

Connectivity Setup

- **Internet Setup**
- LAN Setup
- Firewall Setup

ANG-1100 System

- Set Password
- Device Status
- Firmware Update
- Advanced Utilities

Links

- Config File Editor
- Aurorean Products
- Enterasys Home

Internet Setup

Internet Address Assignment:

● DHCP assigned IP address

Hostname:

□ Use Hostname with DHCP

○ Manual assigned IP address

IP Address: . . .

Subnet: . . .

Gateway: . . .

Primary DNS: . . .

Secondary DNS: . . .

○ PPPoE assigned address

Username:

Password:

Confirm:

Figure 15 Internet Setup Window

2 Do one of the following:

❐ Click the DHCP radio button and perform the following steps:

– Enter a Hostname for the system.

– *Optionally*, check the Use hostname with DHCP checkbox.

– Click Apply.

❐ Click the Manual assigned IP address radio button and perform the following steps:

– Specify the ANG-1100’s IP address.

– Set the Subnet mask.

– Enter the Gateway IP address.

– Specify the Primary DNS IP address.

- Set the Secondary DNS IP address.
- Click Apply.

❒ Click the PPPoE assigned IP address radio button and perform the following steps:

- Specify a Username supplied by your cable / DSL provider.
- Enter a Password.
- Type the password again in the Confirm field.
- Click Apply.

3 If you chose the Manual or PPPoE options, a window appears detailing the reconfiguration changes and prompting you to reboot the ANG-1100. Click Reboot Now.

After a few moments when an IP address has been received for the external port, the Internet LED will turn on. If a static IP address was configured, the Internet LED will shine immediately.

NOTE

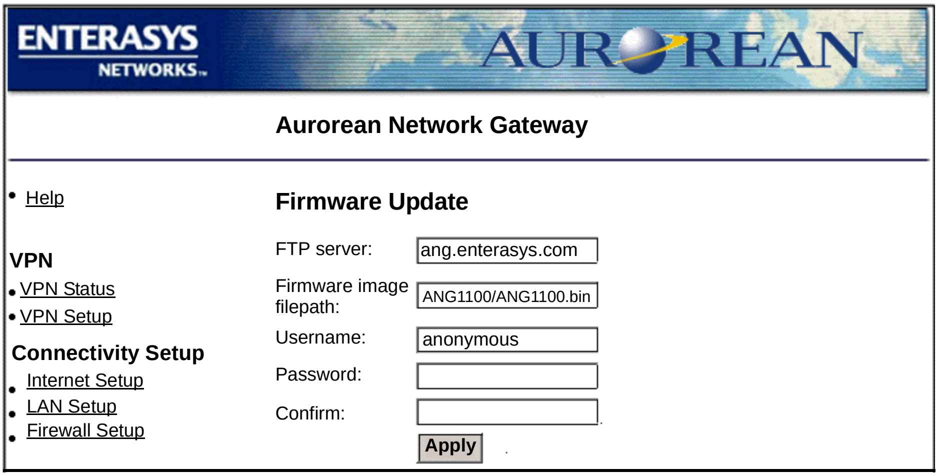
If you press the Reset button after configuring your ANG-1100, you will lose your entire configuration. Any settings you supplied must then be re-entered. Do not use the Reset button unless you want the configuration to return to factory defaults. Also, you may want to record your configuration settings.

Downloading the Latest Firmware

After logging in, download the latest firmware image to the ANG-1100's flash memory (provided the MAC address is set for cable service users - refer to page 36) by accessing the FTP server where it is stored. As new firmware becomes available, you can update it again. Begin updating your firmware by performing the following steps:

1 Click the Firmware Upgrade menu option.

The Firmware Upgrade window appears as shown in Figure 16.



Firmware Update

FTP server: ang.enterasys.com

Firmware image filepath: ANG1100/ANG1100.bin

Username: anonymous

Password:

Confirm:

Figure 16 Firmware Update Window

2 In the FTP server field, enter the name of the FTP server where the new ANG image is stored: **ang.enterasys.com**

3 Type the full path of the location of the Firmware image: **`/ANG1100/ANG1100.bin`**

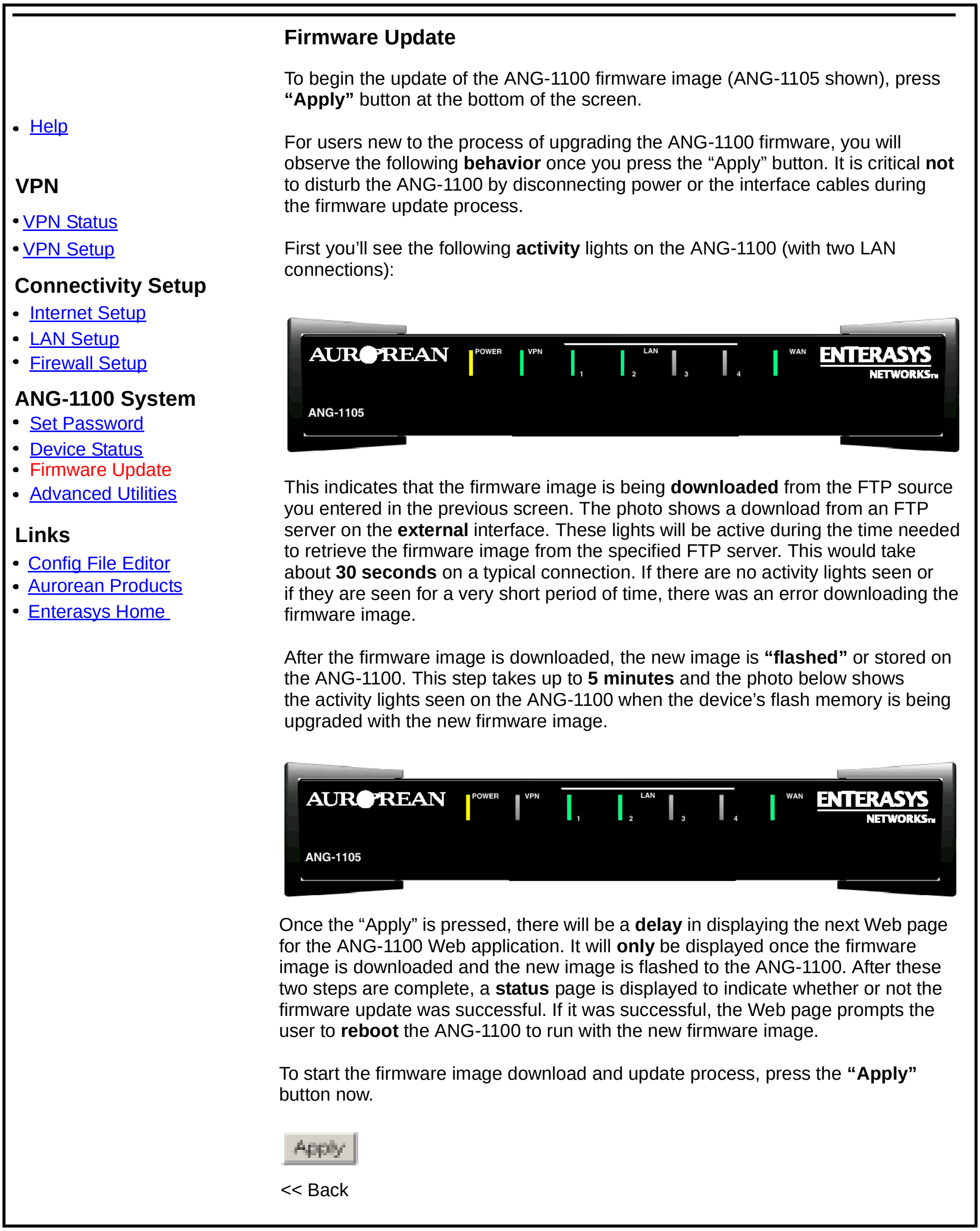
4 Enter the Username **anonymous**

5 Enter **netadmin** in the Password and Confirm fields and click Apply.

The Firmware Update window appears as shown in Figure 17.

6 Click Apply.

Depending on your network connection, the image (nearly 2 MB) downloads for 20-30 seconds and loads in flash memory for 2-3 minutes more. Note that the Power and VPN LEDs blink very quickly together during this interval and then turn off. The WAN LED blinks as well. Meanwhile, the ANG Web Config screen appears blank.



- Help

VPN

- VPN Status
- VPN Setup

Connectivity Setup

- Internet Setup
- LAN Setup
- Firewall Setup

ANG-1100 System

- Set Password
- Device Status
- Firmware Update
- Advanced Utilities

Links

- Config File Editor
- Aurorean Products
- Enterasys Home

Firmware Update

To begin the update of the ANG-1100 firmware image (ANG-1105 shown), press **“Apply”** button at the bottom of the screen.

For users new to the process of upgrading the ANG-1100 firmware, you will observe the following **behavior** once you press the “Apply” button. It is critical **not** to disturb the ANG-1100 by disconnecting power or the interface cables during the firmware update process.

First you’ll see the following **activity** lights on the ANG-1100 (with two LAN connections):

This indicates that the firmware image is being **downloaded** from the FTP source you entered in the previous screen. The photo shows a download from an FTP server on the **external** interface. These lights will be active during the time needed to retrieve the firmware image from the specified FTP server. This would take about **30 seconds** on a typical connection. If there are no activity lights seen or if they are seen for a very short period of time, there was an error downloading the firmware image.

After the firmware image is downloaded, the new image is **“flashed”** or stored on the ANG-1100. This step takes up to **5 minutes** and the photo below shows the activity lights seen on the ANG-1100 when the device’s flash memory is being upgraded with the new firmware image.

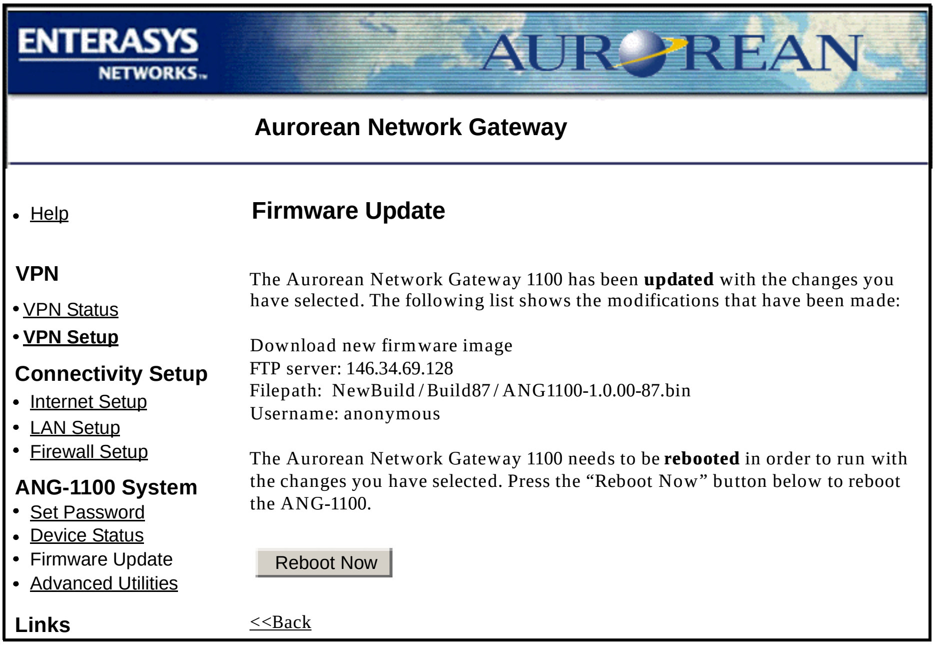
Once the “Apply” is pressed, there will be a **delay** in displaying the next Web page for the ANG-1100 Web application. It will **only** be displayed once the firmware image is downloaded and the new image is flashed to the ANG-1100. After these two steps are complete, a **status** page is displayed to indicate whether or not the firmware update was successful. If it was successful, the Web page prompts the user to **reboot** the ANG-1100 to run with the new firmware image.

To start the firmware image download and update process, press the **“Apply”** button now.

<< Back

Figure 17 Second Firmware Update Window

7 After downloading and “flashing” are complete, a status page displays as shown in Figure 18 indicating the process was successful and displays the FTP server IP address and new build filepath.



Firmware Update

The Aurorean Network Gateway 1100 has been **updated** with the changes you have selected. The following list shows the modifications that have been made:

Download new firmware image
FTP server: 146.34.69.128
Filepath: NewBuild/Build87/ANG1100-1.0.00-87.bin
Username: anonymous

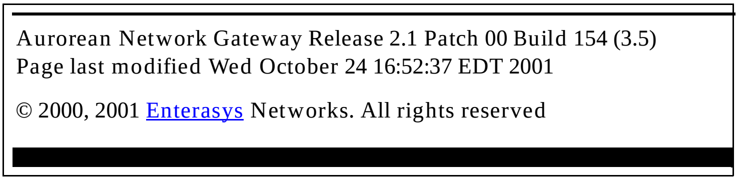
The Aurorean Network Gateway 1100 needs to be **rebooted** in order to run with the changes you have selected. Press the “Reboot Now” button below to reboot the ANG-1100.

Figure 18 Successful Firmware Update Window

8 Reboot the ANG by clicking Reboot Now.

Power and VPN LEDs turn off; then the Power LED turns on for about 4 seconds. Once the kernel is up, the Power LED blinks every half-second. The VPN LED then turns on when the tunnel comes up.

9 To ensure that the image was updated, compare the date last modified, Release, Build and Patch numbers in the lower left corner of the VPN Status window as shown in Figure 19 with the previous release information. The Device Status window also lists this data.



Aurorean Network Gateway Release 2.1 Patch 00 Build 154 (3.5)
Page last modified Wed October 24 16:52:37 EDT 2001

© 2000, 2001 Enterasys Networks. All rights reserved

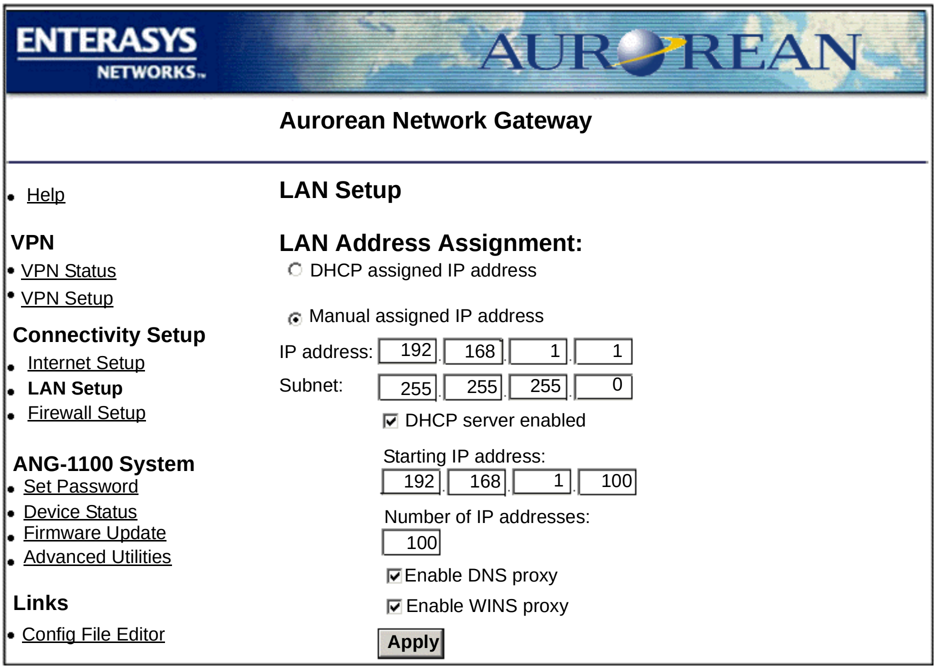
Figure 19 Image Date and Build Information

Setting Up the LAN

LAN configuration of the Trusted side of the ANG-1100 involves choosing either to manually set an IP address and subnet for the ANG-1100 or dynamically assign its IP address via your network's DHCP server. The factory default LAN setting configures the ANG as a DHCP server on the trusted LAN and automatically assign IP addresses to local PCs. Usually, this setting need not be modified. Begin LAN Setup by performing the following steps:

1. Click the LAN Setup menu option.

   The LAN Setup window appears as shown in Figure 20.



LAN Setup

LAN Address Assignment:

○ DHCP assigned IP address

● Manual assigned IP address

IP address: 192 . 168 . 1 . 1

Subnet: 255 . 255 . 255 . 0

☑ DHCP server enabled

Starting IP address: 192 . 168 . 1 . 100

Number of IP addresses: 100

☑ Enable DNS proxy

☑ Enable WINS proxy

Figure 20 LAN Setup Window

2. Do one of the following:

   ❒ Click the DHCP assigned IP address radio button and perform the following steps:

   – Click Apply.

❒ Click the Manual assigned IP address radio button and perform the following steps:

– Set the ANG-1100's IP address.

CAUTION

If you chose NetWork Extension mode (in the VPN Setup window), you must manually configure the IP and Starting IP address of the ANG with values supplied by your Network Administrator. This trusted subnet is routed to the central Intranet so it must have a distinct IP address. By default, the ANG-1100 uses 192.168.1.0/24 as the trusted network subnet so it must be changed to a unique subnet not in use on the network.

– Set the Subnet mask.
– *Optional*. Click the DHCP server enabled box if the server is up and running.
– Set the Starting IP address of the range of consecutive IP addresses you will create for this ANG-1100.
– Set the total Number of IP addresses the ANG-1100 can distribute.
– *Optional*. Keep Enable DNS proxy checked so that the ANG-1100 will act as a DNS server for all its tunnels. DNS proxy resolves host names and IP addresses because the domain server is non-routable, forcing attached hosts to request these values. If your hosts know the DNS address they are seeking, you can disable this feature. This option is on by default.
– *Optional*. Keep Enable WINS proxy checked so that PCs on the LAN can be notified of WINS servers discovered during tunnel setup. WINS proxy notifies local PCs of the remote WINS servers without manual intervention. This option can be disabled if local PCs already know remote WINS server IP addresses. This option is on by default.
– Click Apply.

CAUTION

If you change the default LAN Setup and reboot the ANG-1100, you must release and renew the IP address for all adaptors bound to TCP/IP on your connected computer(s) in order to reconnect with the ANG-1100 and make future changes. Perform the following steps:

- On your desktop, click Start. and Run.
- For Windows 95/98/ME systems, type: `winipcfg,` click OK, click

Release and click OK. Then click Renew All and click OK.

- For Windows NT/2000 systems, type `ipconfig /release` and press ENTER. Then type `ipconfig /renew` and press ENTER.
- For Macintosh systems, check the TCP-IP control panel.

3 If you chose the DHCP option or changed the DNS or WINS default entries, a window appears detailing the reconfiguration changes and prompting you to reboot the ANG-1100. Click Reboot Now.

NOTE

If you press the Reset button after configuring your ANG-1100, you will lose your entire configuration. Any settings you supplied must then be re-entered. We strongly recommend that you do not use the Reset button unless you want the configuration to return to factory defaults.

Setting Up the Firewall

Firewall security is established in a *one-way, outbound* configuration by default on the ANG-1100's External interface. A strong combination of firewall and NAT security is achieved to allow users *out* from their ANGs but disallow any others *in* from the Internet. The firewall also provides the following optional choices to control management of the ANG-1100 via HTTP and/or Telnet:

❒ Enable/disable HTTP/Telnet from the Trusted network

❒ Enable/disable HTTP/Telnet over the VPN tunnels

❒ Enable/disable HTTP/Telnet in the clear from the Internet

Enabling any of these options allows ANG-1100 management via the Web or Telnet. We recommend that you accept the factory default settings which allow Web and Telnet management access on the Trusted LAN connection but disable these permissions on the Internet and VPN Gateway connections.

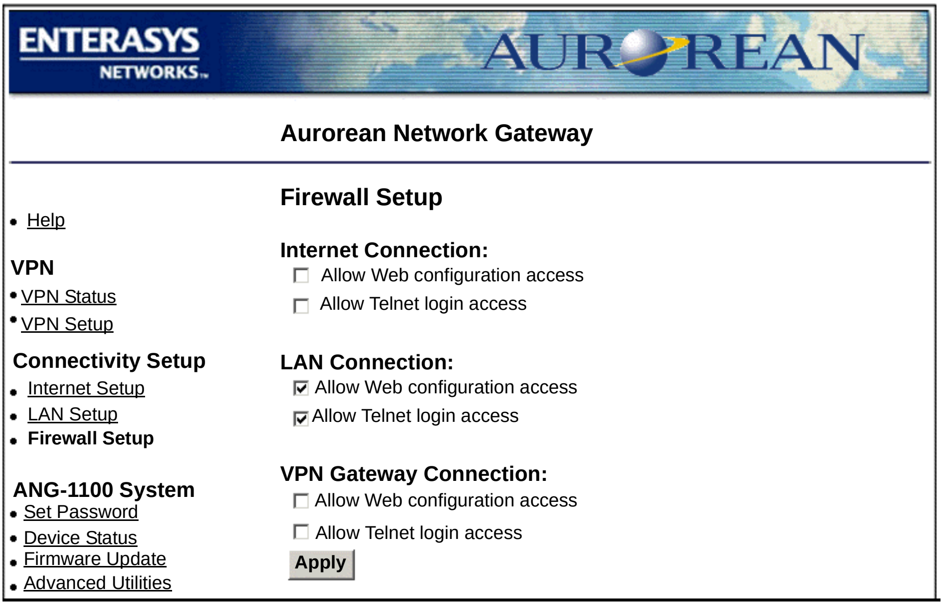
WARNING

DO NOT LEAVE ALL THREE CONNECTIONS DISABLED. If you do so, you will be UNABLE TO CONFIGURE THE ANG-1100 without resetting the system and returning to the factory default configuration.

Begin Firewall Setup by performing the following steps:

1 Click the Firewall Setup menu option.

The Firewall Setup window appears as shown in Figure 21.



Firewall Setup

Internet Connection:
□ Allow Web configuration access
□ Allow Telnet login access

LAN Connection:
☑ Allow Web configuration access
☑ Allow Telnet login access

VPN Gateway Connection:
□ Allow Web configuration access
□ Allow Telnet login access

Figure 21 Firewall Setup Window

2 Enable the option of your choice and click Apply.

NOTE

Experienced administrators can fine tune firewall functionality by editing the *ipfwadm* file in the Configuration Editor. For more detailed information, check the following IPFWADM Web sites:
- `www.xos.nl/linux/ipfwadm/paper/`
- `www.fwtk.org/ipfwadm/faq/ipfwadm-faq.html`

✓ NOTE

If you press the Reset button after you have configured your ANG-1100, you will lose your entire configuration. Any settings you have changed from factory defaults, such as firewall rules, will be removed. We recommend that you save these settings to a Notepad file which you then can reference if you are compelled to use the Reset button.

Setting Your Password

Because the default password is readily available through all ANG-1100 documentation, we strongly recommend that you ensure security by configuring a new password to replace the default password *netadmin*.

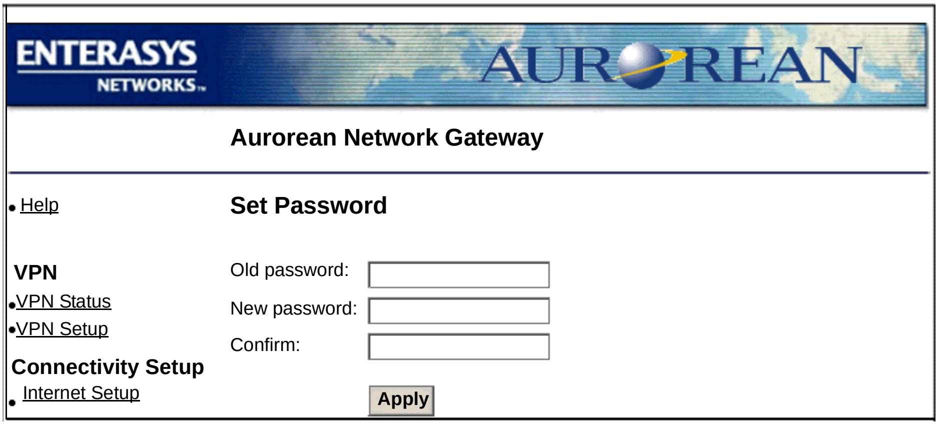
✓ NOTE

If you forget your password after changing it from the factory default, you can return to using netadmin by pressing the Reset button and return to all factory default values.

Change the Password by performing the following steps:

1 Click the Set Password menu option.

The Set Password window appears as shown in Figure 22.



Aurorean Network Gateway

- Help

VPN

- VPN Status
- VPN Setup

Connectivity Setup

- Internet Setup

Set Password

Old password:

New password:

Confirm:

Figure 22 Set Password Window

2 Type the old Password in the field provided.

3 Type a new Password in the field provided.

4 Confirm the new password in the field provided.

5 Click Apply.

Checking Device Status

The Device Status window provides a host of important data to ensure the ANG-1100 is connected properly and to permit troubleshooting as problems occur. When consulting Enterasys Customer Support, you will be asked to display this window.

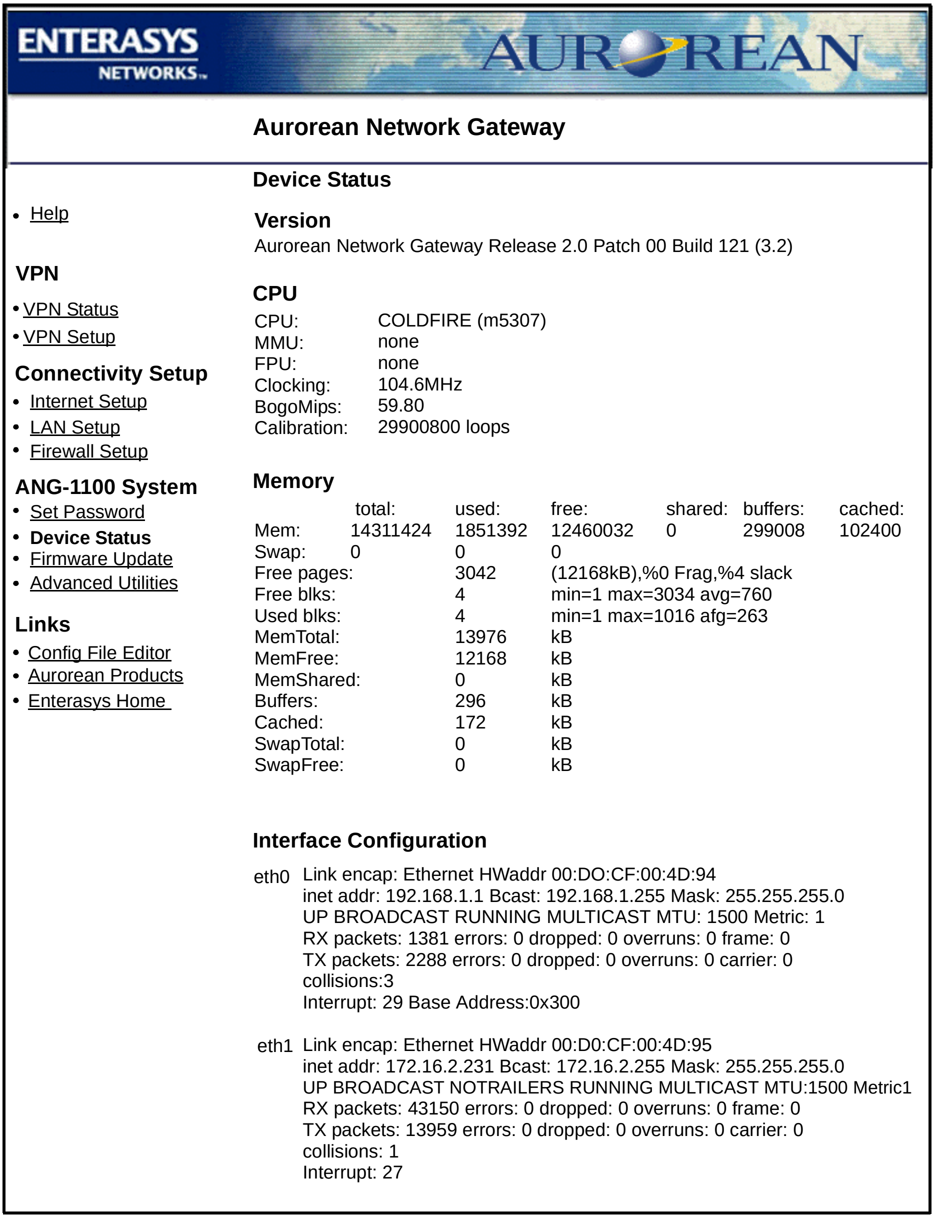
The following categories are detailed in the Device Status window:

- ❒ *Version* lists the Release, Patch and Build numbers, and internal name of the ANG-1100's firmware.
- ❒ *CPU* itemizes Motorola Coldfire chip specifications.
- ❒ *Memory* enumerates ANG-1100 memory values including Total, Used, Free, Shared, Cached, Buffered and Swapped bytes.
- ❒ *Interface Configuration* describes Trusted (eth0), External (eth1), IPsec (eth1:0-24), PPTP (ppp0-24) and Local Loopback (lo) port data including IP and MAC addresses, netmasks, Receive and Transmit errors and other information. Note that the ppp0 interface is the Internet, not WAN interface, if the Internet is configured for PPPoE.
- ❒ *Network Devices* tabulates interface Receive and Transmit errors.
- ❒ *Route Table* entries detail connected networks, gateways, their associated IP addresses, netmasks and other data.
- ❒ *Interrupts* lists the hardware interrupts supported on the ANG-1100 as well as their vectors and interrupt counters. The two SMC9194 items listed are the Ethernet Trusted and External port interrupts.
- ❒ *System Log* categorizes ANG-1100 functions / malfunctions including routing connections / disconnections.

Check Device Status by performing the following step:

1 Click the Device Status menu option.

The Device Status window appears as shown in Figure 23.



Aurorean Network Gateway

Device Status

Version

Aurorean Network Gateway Release 2.0 Patch 00 Build 121 (3.2)

CPU

```
CPU:          COLDFIRE (m5307)
MMU:          none
FPU:          none
Clocking:     104.6MHz
BogoMips:     59.80
Calibration:  29900800 loops
```

Memory

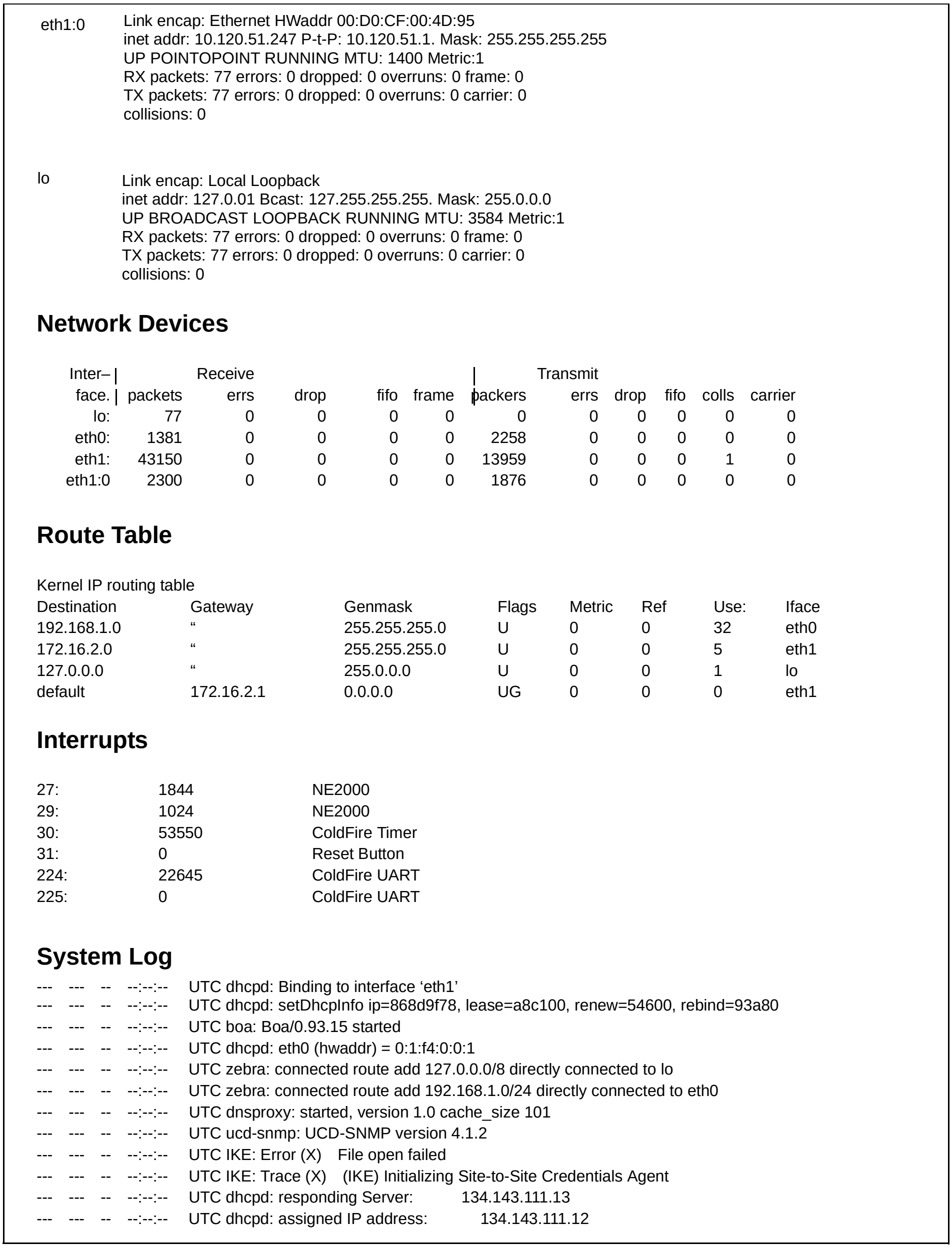
```
              total:     used:     free:        shared:  buffers:   cached:
Mem:        14311424   1851392   12460032       0        299008     102400
Swap:       0          0         0
Free pages:            3042      (12168kB),%0 Frag,%4 slack
Free blks:             4         min=1 max=3034 avg=760
Used blks:             4         min=1 max=1016 afg=263
MemTotal:              13976     kB
MemFree:               12168     kB
MemShared:             0         kB
Buffers:               296       kB
Cached:                172       kB
SwapTotal:             0         kB
SwapFree:              0         kB
```

Interface Configuration

```
eth0  Link encap: Ethernet HWaddr 00:DO:CF:00:4D:94
      inet addr: 192.168.1.1 Bcast: 192.168.1.255 Mask: 255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1
      RX packets: 1381 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 2288 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions:3
      Interrupt: 29 Base Address:0x300

eth1  Link encap: Ethernet HWaddr 00:D0:CF:00:4D:95
      inet addr: 172.16.2.231 Bcast: 172.16.2.255 Mask: 255.255.255.0
      UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric1
      RX packets: 43150 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 13959 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 1
      Interrupt: 27
```

Figure 23 Device Status Window



```
eth1:0      Link encap: Ethernet HWaddr 00:D0:CF:00:4D:95
            inet addr: 10.120.51.247 P-t-P: 10.120.51.1. Mask: 255.255.255.255
            UP POINTOPOINT RUNNING MTU: 1400 Metric:1
            RX packets: 77 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 77 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0


lo          Link encap: Local Loopback
            inet addr: 127.0.01 Bcast: 127.255.255.255. Mask: 255.0.0.0
            UP BROADCAST LOOPBACK RUNNING MTU: 3584 Metric:1
            RX packets: 77 errors: 0 dropped: 0 overruns: 0 frame: 0
            TX packets: 77 errors: 0 dropped: 0 overruns: 0 carrier: 0
            collisions: 0
```

Network Devices

```
 Inter–|           Receive                         |          Transmit
  face.| packets     errs     drop     fifo  frame |packers     errs  drop  fifo  colls  carrier
    lo:       77        0        0        0      0       0        0     0     0      0        0
  eth0:     1381        0        0        0      0    2258        0     0     0      0        0
  eth1:    43150        0        0        0      0   13959        0     0     0      1        0
 eth1:0     2300        0        0        0      0    1876        0     0     0      0        0
```

Route Table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric  Ref     Use:    Iface
192.168.1.0     “               255.255.255.0   U       0       0       32      eth0
172.16.2.0      “               255.255.255.0   U       0       0       5       eth1
127.0.0.0       “               255.0.0.0       U       0       0       1       lo
default         172.16.2.1      0.0.0.0         UG      0       0       0       eth1
```

Interrupts

```
27:         1844        NE2000
29:         1024        NE2000
30:         53550       ColdFire Timer
31:         0           Reset Button
224:        22645       ColdFire UART
225:        0           ColdFire UART
```

System Log

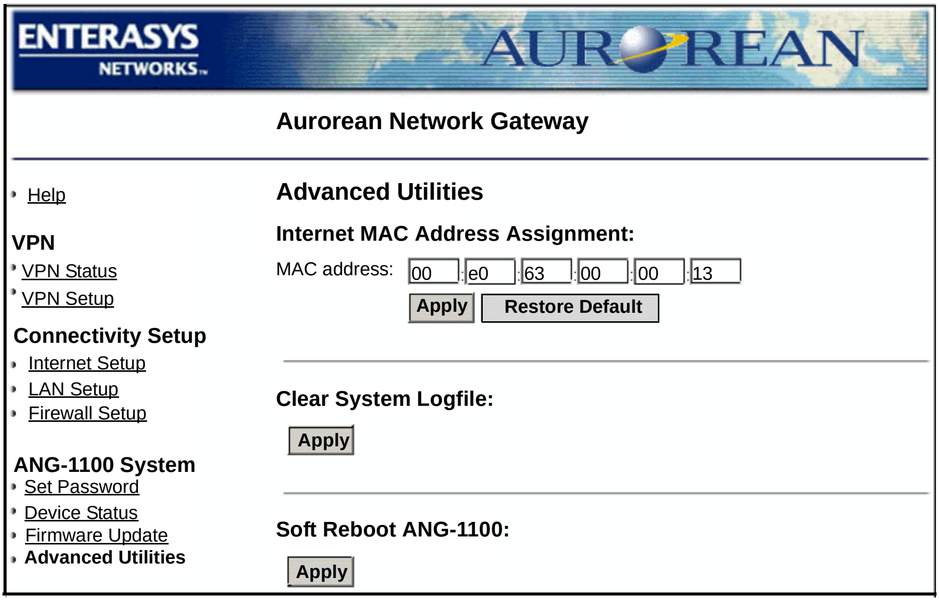
```
---  ---  --  --:--:--  UTC dhcpd: Binding to interface ‘eth1’
---  ---  --  --:--:--  UTC dhcpd: setDhcpInfo ip=868d9f78, lease=a8c100, renew=54600, rebind=93a80
---  ---  --  --:--:--  UTC boa: Boa/0.93.15 started
---  ---  --  --:--:--  UTC dhcpd: eth0 (hwaddr) = 0:1:f4:0:0:1
---  ---  --  --:--:--  UTC zebra: connected route add 127.0.0.0/8 directly connected to lo
---  ---  --  --:--:--  UTC zebra: connected route add 192.168.1.0/24 directly connected to eth0
---  ---  --  --:--:--  UTC dnsproxy: started, version 1.0 cache_size 101
---  ---  --  --:--:--  UTC ucd-snmp: UCD-SNMP version 4.1.2
---  ---  --  --:--:--  UTC IKE: Error (X)   File open failed
---  ---  --  --:--:--  UTC IKE: Trace (X)   (IKE) Initializing Site-to-Site Credentials Agent
---  ---  --  --:--:--  UTC dhcpd: responding Server:         134.143.111.13
---  ---  --  --:--:--  UTC dhcpd: assigned IP address:          134.143.111.12
```

Figure 24 Device Status Window (continued)

Using Advanced Utilities

Advanced Utilities provided by the ANG-1100 include:

- Setting the MAC Address of a newly attached ANG-1100 when you want to quickly connect to a cable service provider. MAC addresses are used by service providers to identify supported users. The ANG-1100 can proxy your computer's MAC address to the ISP but your provider may require that you change the default value reported by the ANG-1100 to reflect the PC's actual MAC address.
- Clearing the System Logfile - shown in the Device Status window - when you want to erase old and display updated information.
- Soft Rebooting to reset the ANG-1100 without recycling power. This function is similar to pressing CTRL-ALT-DELETE on your computer.



Aurorean Network Gateway

Advanced Utilities

Internet MAC Address Assignment:

MAC address: 00 : e0 : 63 : 00 : 00 : 13

Clear System Logfile:

Soft Reboot ANG-1100:

Figure 25 Advanced Utilities Window

1 Click the Advanced Utilities menu option.

The Advanced Utilities window appears as shown in Figure 25.

2 Do one of the following:

- To change the ANG-1100's MAC address to reflect your computer's MAC address, first find the computer's address by issuing the proper command at a DOS prompt. For Windows 95/98/ME systems, type `winipcfg`; for Windows NT/2000 systems, type `ipconfig /all`; for Macintosh systems, check the TCP-IP control panel.

  In the command output, look for the *Physical* or *Adapter Address* value. For example:

  ```
  c:>ipconfig /all
  Ethernet adapter E190x1:

  Description . . : 3Com 3C90x Ethernet Adapter
  Physical Address : 00-10-4B-9D-18-17
  ```

  Enter the value in the **Internet MAC Address Assignment** fields.

  Click Apply and Reboot Now when prompted to save the change.

- Select Clear System Logfile and click Apply.
- Select Soft Reboot ANG-1100 and click Apply.

NOTE

ANG-1100 connections broken during a reboot will be lost after service returns. Idling the traffic stream (Telnet, e.g.) for a couple minutes before re-initiating the connection resolves the problem.

Using the Configuration Editor

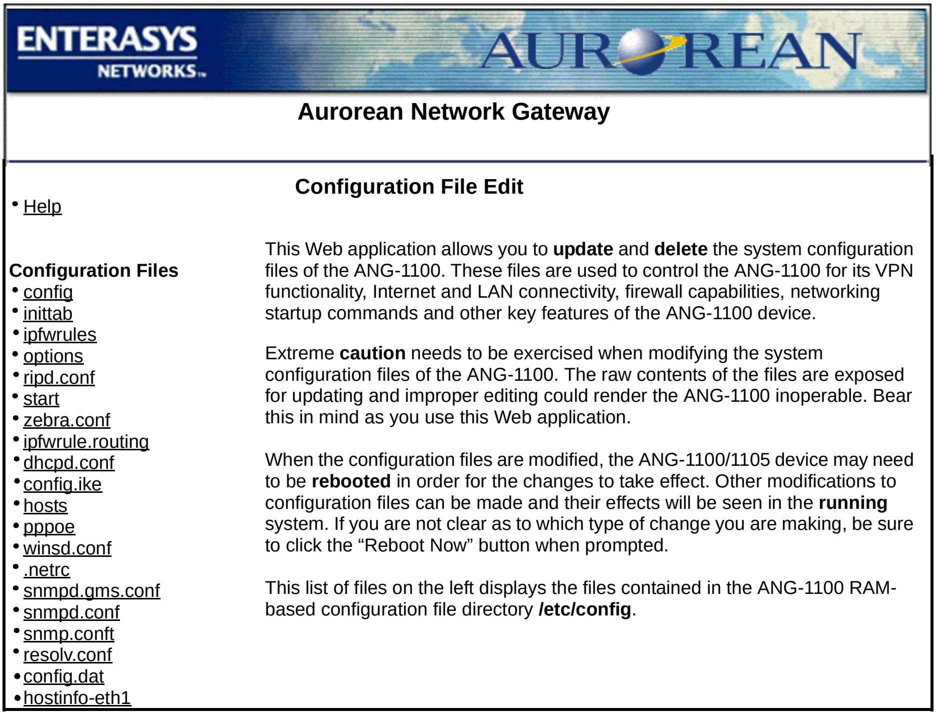
Knowledgeable network administrators can use the Configuration Editor to modify the ANG-1100's LINUX 2.0 operating system configuration files.

CAUTION

Inexperienced users or those unfamiliar with LINUX attempting to use this editor may disable the system. We recommend only expert users, in conjunction with Enterasys Customer Support, use this editor.

1 Click the Configuration Edit menu option.

The Configuration Edit window appears as shown in Figure 26.



Aurorean Network Gateway

Configuration File Edit

- Help

Configuration Files

- config
- inittab
- ipfwrules
- options
- ripd.conf
- start
- zebra.conf
- ipfwrule.routing
- dhcpd.conf
- config.ike
- hosts
- pppoe
- winsd.conf
- .netrc
- snmpd.gms.conf
- snmpd.conf
- snmp.conft
- resolv.conf
- config.dat
- hostinfo-eth1

This Web application allows you to **update** and **delete** the system configuration files of the ANG-1100. These files are used to control the ANG-1100 for its VPN functionality, Internet and LAN connectivity, firewall capabilities, networking startup commands and other key features of the ANG-1100 device.

Extreme **caution** needs to be exercised when modifying the system configuration files of the ANG-1100. The raw contents of the files are exposed for updating and improper editing could render the ANG-1100 inoperable. Bear this in mind as you use this Web application.

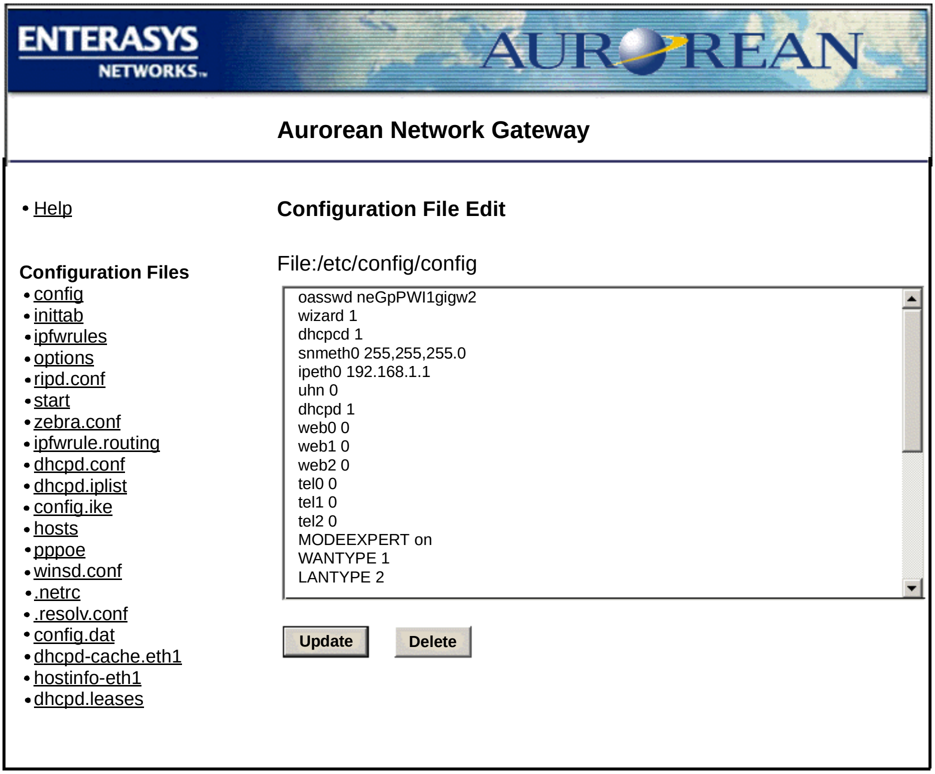
When the configuration files are modified, the ANG-1100/1105 device may need to be **rebooted** in order for the changes to take effect. Other modifications to configuration files can be made and their effects will be seen in the **running** system. If you are not clear as to which type of change you are making, be sure to click the “Reboot Now” button when prompted.

This list of files on the left displays the files contained in the ANG-1100 RAM-based configuration file directory **/etc/config**.

Figure 26 Configuration Edit Window

2 Click on the configuration file of your choice.

3 The arguments of the configuration file you selected are displayed in the Configuration File Edit window, as shown in Figure 27.



File:/etc/config/config

```
oasswd neGpPWI1gigw2
wizard 1
dhcpcd 1
snmeth0 255,255,255.0
ipeth0 192.168.1.1
uhn 0
dhcpd 1
web0 0
web1 0
web2 0
tel0 0
tel1 0
tel2 0
MODEEXPERT on
WANTYPE 1
LANTYPE 2
```

Figure 27 Configuration File Edit Window

4 Edit the UNIX configuration file and click Update or Delete.

NOTE

You can remove the Configuration Editor (along with the Advanced Utilities option) from the main menu by selecting *config*, deleting the **MODEEXPERT on** argument and clicking Update.

NOTE

If you press the Reset button after configuring your ANG-1100, you will lose your entire configuration. Any settings you have changed from factory defaults, such as firewall rules, will be removed. We recommend that you save these settings to a Notepad file which you then can reference if you are compelled to use the Reset button.

Configuring IP Port Forwarding

ANG-1100’s support of IP Port Forwarding permits you to make servers on the trusted network of the ANG-1100 available to the rest of the VPN. In contrast to Network Address Translation (NAT), which allows access to external-side servers initiated by *internal-side* hosts, Port Forwarding permits access to internal-side servers initiated by external-side hosts.

This is accomplished by rewriting the headers of all packets bound for the ANG-1100 and forwarding them to another host on the trusted-side of the network, depending on their destination port (port numbers corresponding to standard, well-known protocols). The IP addresses are re-written so that incoming IP (TCP and UDP) packets are forwarded to their intended destinations, and the reply packets are re-written to appear to be coming from the ANG-1100.

This process requires static, known values for the following:

❒ The *IP address assigned to ANG-1100* by the VPN. This address is in RiverMaster in the ANG-1100's user account and may not be assigned dynamically via pools or virtual subnets.

❒ The *IP address of the server* on the ANG-1100 trusted network (one server per protocol). This may not be dynamically assigned by the ANG-1100 via DHCP.

❒ The *protocol* (TCP or UDP) and the *protocol port number.*

IP Port Forwarding is configured by editing the *ipportfw* command in the *ipfwrules* configuration file in the Config Editor tool of the Web Config. The ipportfw commands should be entered at the end of the ipfwrules file.

Refer to the tables below for command usage, switches, arguments, and definitions.

Usage		
ipportfw -A -[t | u] l.l.l.l/lport -R a.a.a.a/rport		add entry
ipportfw -D -[t | u] l.l.l.l/lport		delete entry
	l.l.l.l is the address of the VPN interface receiving packets to be forwarded	
	a.a.a.a is the server address on the LAN	
	lport is the port being redirected	
	rport is the port being redirected to	

Switch	**<arg>**	**Definition**
-t	VPN address/port	Forward TCP traffic
-u	VPN address/port	Forward UDP traffic
-A	None	Add the IP port forwarding table entry
-C	None	Clear the IP port forwarding table
-D	None	Delete the IP port forwarding table entry
-R	IP address/port	Define the server IP address
-L	None	List the IP port forwarding table

Follow the steps below to configure IP port forwarding.

1 Login to Web Config.

2 Click on the Config File Editor menu option.

3 Click on the ipfwrules Configuration File.

4 In the Configuration File Edit window, scroll to the end of the file.

5 Under **Expert-Config**, type the following rules:

- ipportfw -C
- ipportfw -A <-t or -u> <VPN address/local port> -R <local server IP address/remote port>

6 Click Update and Reboot Now when prompted to save the change.

Refer to the table below for a sample IP port forwarding configuration:

Example

```
ipportfw -C
ipportfw -A -t10.120.50.215/23 -R 192.168.0.1/23
ipportfw -A -t10.120.50.215/21 -R 192.168.0.1/21
ipportfw -A -t10.120.50.215/6000 -R 192.168.0.2/6000
```

The above sample configuration performs the following tasks:

- Clears the IP port forwarding table
- Maps telnet (TCP port 23) from the VPN address (10.120.50.215) to port 23 on the internal server 192.168.0.1
- Maps FTP from the VPN address to the same 192.168.0.1 server
- Maps X windows (TCP port 6000) to a different server, 192.168.0.2

A

Glossary

Aurorean Network Gateway

An Enterasys Networks device that creates a secure virtual private circuit over the Internet between itself and a remote user's computer. The Aurorean Network Gateway encapsulates data packets using IPSec and encrypts data to prevent third-parties from intercepting and examining it. There are three types of Aurorean Network Gateways:

- ❒ Aurorean Network Gateway-7000 - a tunnel server that can accommodate up to 5000 remote users
- ❒ Aurorean Network Gateway-3000 - a tunnel server that can accommodate up to 500 remote users
- ❒ Aurorean Network Gateway-1102/1105 - a tunnel server that establishes a site-to-site tunnel between itself and an ANG-7000/3000 server. It can accommodate up to 25 tunnels.

Aurorean Web Config

Aurorean Web Config is the utility used to configure the Aurorean Network Gateway-1102/1105. It is Web based and is accessed through the use of a Web browser.

Aurorean Policy Server

An Enterasys Networks device that manages Aurorean Network Gateways. Network administrators configure Aurorean Policy Servers from a RiverMaster computer. The network administrator can create a remote user database on the Aurorean Policy Server or instruct the Aurorean Policy Server to authenticate remote users against an external authentication server (such as a RADIUS or SecurID server). When the network administrator changes tunnel connection parameters, the Aurorean Policy Server provide updated configuration files to Aurorean Network Gateways on request.

DHCP

Dynamic Host Configuration Protocol (DHCP) servers are used to assign IP addresses. The Aurorean Network Gateway-1102/1105 is capable of assigning IP addresses.

DSL

Refers to Digital Subscriber Lines. DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. Usually the maximum distance between the home or office and the switching station has to be around one mile.

Ethernet

The Ethernet originated in 1974 by Xerox to connect many office machines together to allow communications between them. Coax cable was originally used. today twisted pair wire can be used and the speeds can be up to 10 megabits per second.

Firewall

A combination of hardware and software which limits the exposure of a corporate network to outside attack by enforcing a boundary between the network and the Internet. Firewalls normally fall into one of two categories: application-level or network-level (often referred to as a packet filter). An application-level firewall examines traffic at the application level, and only passes packets that are sent by approved applications (such as FTP, E-mail, or Telnet). This type of firewall often readdresses outgoing traffic so that it appears to have originated at the firewall rather than an internal host, thereby concealing the address of the internal host. A network-level firewall examines traffic at the network packet level, and filters packets based on the destination and/or source address.

Generic Routing Encapsulation (GRE)

Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link over the Internet. For PPTP, GRE is used to encapsulate PPP data packets within an IP packet (IP packet headers contain address information necessary for routing, while PPP packets do not).

Internet Service Provider (ISP)

A vendor who provides direct access to the Internet. ISPs bill users for the amount of time they are connected, and may also offer additional services such as Web site hosting, E-mail, or news group readers. Remote users reach the ISP by dialing into an ISP POP with a computer, modem, and phone line, or over a dedicated circuit (such as a cable modem connection).

IP

Abbreviation of *Internet Protocol*, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called *Transport Control Protocol (TCP/IP)*, which establishes a virtual connection between a destination and a source.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 172.16.4.14 could be an IP address.

IP Security Protocol (IPSec)

Short for *IPSecurity*, a set of protocols developed to support secure exchange of packets at the IP layer.

LAN

Locan Area Network (LAN) connects computers and peripherals together in an office or a campus to allow the computers to access each other and other common peripherals.

LEDs

Abbreviation of *light emitting diode*, an electronic device that lights up when electricity is passed through it. LEDs are usually red, but the ANG-1102/1105 uses green LEDs. The LEDs are used to indicators.

Mac Address

Short for *Media Access Control address*, a hardware address that uniquely identifies each node on a network.

Network Address Translation (NAT)

Described by Whatis.com as the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This provides security since each outgoing or incoming request must undergo a translation process that also offers the chance to qualify or authenticate the request or match it with a previous request. NAT also conserves the number of global IP addresses that a company uses and permits the use of a single IP address to interface with the world.

Network Administrator

The person responsible for installing and maintaining a company's network equipment, and also insuring that network resources (such as servers and the applications running on them) are consistently available and performing well. In terms of Enterasys Networks products, this person physically installs Aurorean Policy Servers and Aurorean Network Gateways, distributes Aurorean Client Software to remote users, and runs RiverMaster software on his/her computer to manage the entire VPN.

Point of Presence (POP)

In Internet terms, the physical site that contains an ISP's network equipment. Remote users dial into the POP, authenticate against the ISP's customer database, and then gain access to the Internet. ISPs typically have POPs scattered throughout their service area, so that can customers can dial a local phone call and avoid paying long- distance charges when accessing the Internet.

Point-to-Point Protocol (PPP)

The Internet standard for sending network traffic over serial lines, such as dial-up phone lines. Unlike its predecessor SLIP (Serial Line Internet Protocol), PPP provides error detection and compression capabilities.

Point-to-Point Tunneling Protocol (PPTP)

A network protocol for linking remote locations over the Internet rather than over costly long-distance or leased lines. To accomplish this, PPTP encapsulates other network protocols (such as TCP/IP, IPX, and NetBEUI) and uses encryption to secure the data sent over the Internet. PPTP was developed jointly by Microsoft and U.S. Robotics (3Com).

PPPoE

The *Point-to-Point over Ethernet* protocol provides a connection to the Internet through a DSL provider. It is also identified as *PPPoE*.

RiverMaster

A management application running on a Windows NT 4.0 Workstation computer which communicates with Aurorean Policy Servers and Aurorean Network Gateways. Using RiverMaster, a network administrator creates user databases, sets policies for user groups, views activity logs, and generates usage reports.

Routers

Devices which direct network traffic among LANs or WANs until the data reaches its destination. To do this, routers communicate with one another using dedicated protocols such as IGRP (Interior Gateway Routing Protocol) and BGP (Border Gateway Protocol) to transfer information on network addressing, status, and configuration.

TCP/IP

Abbreviation for *Transmission Control Protocol/Internet Protocol.* The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

Tunneling

Technology that lets a network transport protocol carry information for other protocols within its own packets. For example, by encapsulating NetBEUI packets, IP can route them across the Internet, which is not normally possible.

Virtual Private Network (VPN)

An extension of a company’s private network that uses the resources of the public Internet. While most private networks use dedicated lines and equipment that are company property, a virtual private network “borrows” resources from the Internet on an as-needed basis.

B

Specifications

This appendix details the specifications of the ANG-1100.

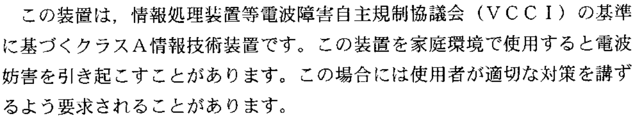
Table 1 ANG-1100 Specifications

Category		Parameters
Chassis	Depth	6” (16 cm)
	Width	10” (25 cm)
	Height	1.5” (4 cm)
	Weight	1 lb. (.5 kg)
Environment	Operating Temperature	0° to 40° C (32° to 104° F)
	Storage Temperature	-20° to +70° C (-4° to +158° F)
	Humidity	0 to 95%, non-condensing
Power Supply	Power Adapter	External universal, auto switching: 110-250 VAC Regulated UL Listed Class 2 power supply must be used.
		Output: 5V, 4.0 Amp
CPU	Processor	Motorola© Coldfire XCF5307 at 90 Mhz internal, 45 MHz external
	Memory	16 MB Micron SRAM with clock speed of 45MHz
Storage Devices	Hard Drive	4 MB Intel Flash

Table 1 ANG-1100 Specifications (Continued)

Category		**Parameters**
Performance	Server Capacity	> 25 concurrent tunnels
	Tunnel Performance	Up to 3 Mbps with IPSec
	Hardware acceleration	SafeNet 1140 CryptoCore chip on ANG-1105
Protocols & Standards	Tunnel Protocols	IP Security Protocol (IPSec) as defined in RFC 2401 and 2409 Point-to-Point Tunneling Protocol (PPTP) as defined in RFC 1234 Generic Routing Encapsulation (GRE) as defined in RFC 1701 and 1702 Internet Key Exchange (IKE) PPP over Ethernet (PPPOE)
	Encapsulated LAN Protocols	IP
	Routing Protocols	RIP V1, V2 Support for dynamic Virtual Network addressing, local network addressing, or static routes
	Authentication	HMAC SHA1 and MD5 Challenge Handshake Authentication Protocol (CHAP) MS-CHAP (Microsoft proprietary version of CHAP)
	Encryption	MPPE, 40- and 128-bit configurable keys (RC4-compatible) IPSec, 40- and 128-bit configurable keys (RC-4 compatible) DES (56-bit) or Triple-DES (168-bit) with IPSec only
	Compression	Microsoft Point-to-Point Compression (MPPC)
	Firewall support	Port filtering and packet inspection firewall
		NAT Gateway to mask internal device addresses
	Other	DHCP Server
Operating System	Type	Version of Linux (uClinux 2.04)

Table 1 ANG-1100 Specifications (Continued)

Category		**Parameters**
Ethernet	Number of Ports	Two (ANG-1102) or five (ANG-1105)
	Data Transfer Rate	10 Mbps on the ANG-1102, 100 Mbps on the ANG-1105
	Connector	8-position modular jack (RJ-45)
Serial	Number of Ports	One DB-9 jack on the ANG-1105 as a console interface
Safety Regulations	US/Canada/ Europe	UL 1950, CSA c22.2 No.950, 73/23/EEC, EN60950, and IEC950
EMCI	US, Canada, Europe, Japan, Australia, New Zealand, Taiwan, Russia, International	FCC Part 15 Class B; CSA C108.8, 89/336/EEC, EN55022, EN61000-3-2; EN61000-3-3; EN55024; AS/NZS 3548, and VCCI V3.  この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

C

Pin Assignments

This appendix describes pin assignments for the Ethernet connectors on the ANG-1100. Additionally, the ANG-1105 provides a serial connector.

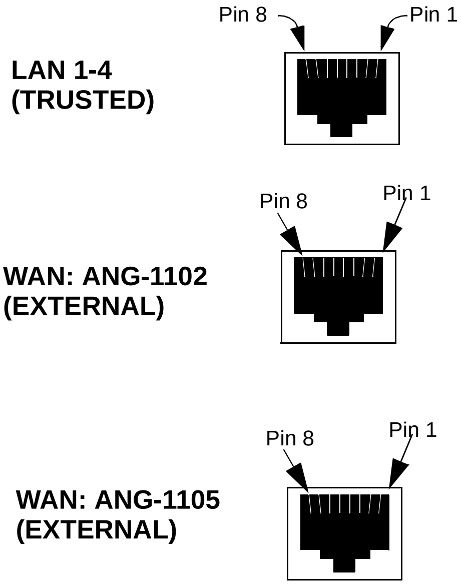
ANG-1100 servers are equipped with either two or five Ethernet ports located at the rear of the chassis, supporting full-duplex 10Base-T transmission. Connections from your PC to the ANG-1105 require the use of a straight-through cable (not supplied); PC connections to the ANG-1102 require a crossover cable or a straight-through cable if using a hub.

Both Ethernet port types conform to IEEE 802.3 standards with 8-pin modular RJ-45 connectors. Figure 1 shows the pin assignments for ANG-1100 server Ethernet ports.

Replacement Ethernet cables must meet the following requirements:

❒ Category 3, 4, or 5 unshielded twisted-pair (UTP) wiring

❒ Length cannot exceed 328 feet (100 meters)

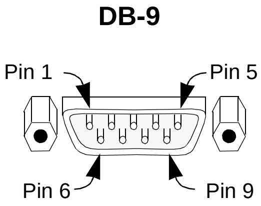


Pin	Signal
1	Transmit +
2	Transmit -
3	Receive +
4	*Return*
5	*Return*
6	Receive -
7	*Return*
8	*Return*

Pin	Signal
1	Transmit -
2	Transmit +
3	Receive -
4	*Return*
5	*Return*
6	Receive+
7	*Return*
8	*Return*

Figure 1 Ethernet Port Pin Assignments

The ANG-1105 is equipped with a single serial port for debugging purposes. An industry-standard serial cable can be used to connect to the male DB-9 connector. See Figure 2 for serial port pin assignments.



Pin	Signal
1	Carrier Detect (CD)
2	Receive Data (RX)
3	Transmit Data (TX)
4	Data Term Ready (DTR)
5	Ground (GND)
6	No Carrier (NC)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	No Carrier (NC)

Figure 2 Serial Port Pin Assignments

D

Program License Agreement & Support

This appendix describes the terms and conditions that govern the use of Aurorean Virtual Network 1100 products and provides contact information for obtaining technical support from Enterasys Networks.

Enterasys Networks, Inc. Program License Agreement

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. ("Enterasys") that sets forth your rights and obligations with respect to the Enterasys software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT Enterasys Networks:

(603) 332-9400. Attn: Legal Department.

License

You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Enterasys.

Other Restrictions

You may not reverse engineer, decompile, or disassemble the Program.

Applicable Law

This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

Export Requirements

You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

United States Government Restricted Rights

The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

Exclusion of Warranty

Except as may be specifically provided by Enterasys in writing, Enterasys makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

ENTERASYS DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY Enterasys IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

No Liability for Consequential Damages

IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS ENTERASYS PRODUCT, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

Technical Support

Enterasys Networks provides easy access to technical support information through a variety of services.

Support from Enterasys Networks

Enterasys Networks offers two ways of contacting customer support personnel.

On-line Services

To receive answers to technical questions on Aurorean Virtual Network products, send E-mail to:

`support@enterasys.com`

Please include your name, title, company, and phone number in all correspondence.

Phone Support

Enterasys Networks customer support personnel are available by calling **1-800-872-8440**. When you call, please call from a position where you can operate the RiverMaster management application or view the server's LEDs, and make sure you have the following information ready:

- ❒ State of the LEDs on both the front and rear panels of the server(s)
- ❒ A list of the error messages appearing in the RiverMaster message/alarm display
- ❒ Details about any recent configuration changes, if applicable

Enterasys Networks also recommends that you have the *RiverMaster Administrator's Guide* on hand when you call.

Returning Products for Repair

After discussing the problem with Enterasys Networks Customer Support or your authorized Enterasys Networks reseller, you may be asked to return the APS-3000/7000 or ANG-1102/1105/3000/7000 for repairs. You will receive a Return Material Authorization (RMA) number for the server. Ship the server, with the RMA number clearly visible on the outside of the package, to the following address:

Enterasys Networks
35 Industrial Way
Rochester, NH 03866

Enterasys Networks recommends that you reuse the original shipping box or equivalent packaging to protect the server during shipment.

NOTE

Products sent to Enterasys Networks without an RMA number will be returned to the sender unopened, at the sender's expense.

Index