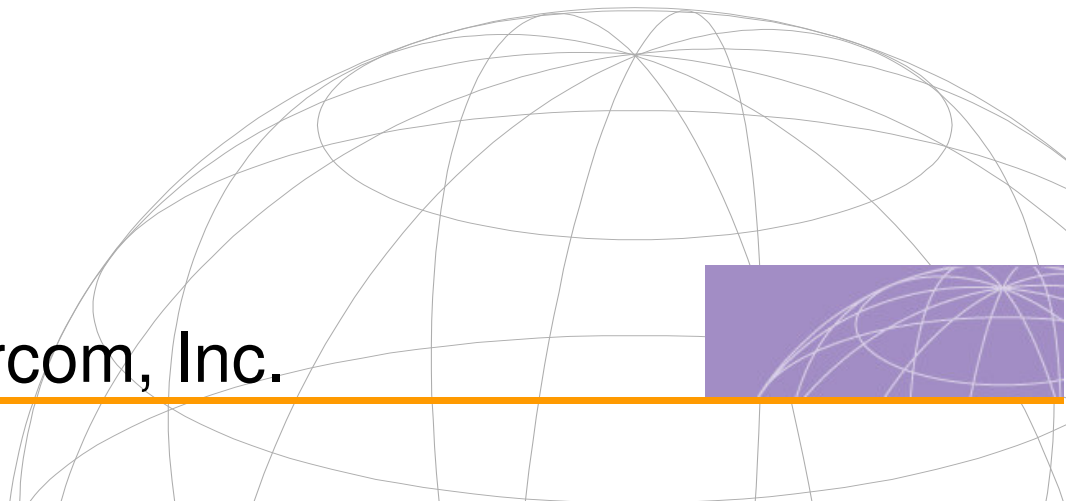




UT-300R2 ADSL2/2+Modem

USER GUIDE

UTStarcom, Inc.



Copyright © 2004 UTStarcom, Inc. All rights reserved.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without prior, express and written permission from UTStarcom, Inc.

UTStarcom, Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of UTStarcom, Inc. to provide notification of such revision or changes.

UTStarcom, Inc. provides this documentation without warranty of any kind, implied or expressed, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. UTStarcom may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in UTStarcom's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

UTStarcom, the UTStarcom logo, PAS, mSwitch, Airstar, WACOS, Netman, Total Control, and CommWorks are registered trademarks of UTStarcom, Inc. and its subsidiaries. The UTStarcom name, AN-2000, and the CommWorks logo are trademarks of UTStarcom, Inc. and its subsidiaries.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

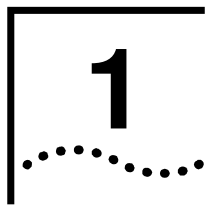
Any rights not expressly granted herein are firmly reserved.

Contents

1	Overview	1
	Device Introduction	1
	Features	2
<hr/>		
2	Installation Planning	5
	Packing List	5
	Interfaces Introduction	6
	Front Panel	6
	Rear Panel.....	7
	Cable Connections.....	7
	Connecting the ADSL Line.....	7
	Connecting the UT-300R2 to the Ethernet LAN.....	8
	Computer to UT-300R2 Connection	9
	Hub or Switch to UT-300R2 Connection.....	9
	Power on	10
<hr/>		
3	Before Configuring UT-300R2	13
	Set up TCP/IP on Your PC.....	13
	Set up Proxy Service	14
	Configure IP Settings on Your PC.....	14
	First Time Log on.....	15
<hr/>		
4	Web-based Management	17
	Summary	17
	Configuring the WAN Connection	19
	Configuring a Bridged Connection for the WAN.....	21
	Configuring a Routed/Bridged Connection for the WAN	24
	Configuring a PPP Connection for the WAN.....	26
	Dynamic IP Address for the WAN Connection.....	28

Static IP Address for WAN	30
DHCP Configuration	32
DHCP Server Settings for the LAN.....	33
Use the UT-300R2 for DHCP	34
Disabling the DHCP Server.....	34
DNS Server Setting	34
Configuring the LAN Connection.....	35
Save New Settings	37
<hr/>	
5 Advanced Configuration / Network Management.....	39
Virtual Server Configuration.....	41
Special Application Configuration	45
Configure a Filter Rule-IP Filters.....	48
Configuring a Filter Rule- MAC Filters.....	53
Configuring a Filter Rule-URL Blocking.....	56
Configuring a Filter Rule-Domain Blocking.....	59
Firewall.....	62
DMZ	64
DDNS.....	65
RIP	66
<hr/>	
6 Tools.....	67
Administrator's Settings	67
Configure System Time	68
Save UT-300R2 Configuration Settings	69
Save Configuration File to PC.....	70
Load Saved Configuration Files.....	71
Restore Factory Default Settings	72
Firmware Update	72
<hr/>	
7 UT-300R2 Status Information	75
Log	75

Traffic Statistics	76
Diagnostics	77
<hr/>	
8 Attachments	79
Technical Specifications.....	79
Glossary	82
<hr/>	



Overview

The UT-300R2 provides integrated voice and data services over ADSL (Asymmetrical Digital Subscriber Loop) WAN (Wide Area Network) connection.

Device Introduction

The UT-300R2 ADSL UT-300R2 is designed to provide a simple and cost-effective ADSL Internet connection for individual computers through the Ethernet ports, or use it to bridge your Ethernet LAN to the Internet. The UT-300R2 combines the benefits of high-speed ADSL technology and LAN IP management in one compact and convenient package. ADSL technology enables many interactive multi-media applications such as video conferencing and collaborative computing.

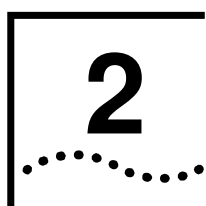
The UT-300R2 is easy to install and use. The UT-300R2 connects to computers or an Ethernet LAN via a standard Ethernet interface. The ADSL connection is made using ordinary twisted-pair telephone line with standard connectors. Multiple PCs can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address.

Figure 1 Device Appearance

Features

- Data rates up to 26 Mbps downstream
- Bridging and routing capabilities
- PPP and tunneling features
- Firewall with Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP).
- Supports ADSL, ADSL2, ADSL2+
- DSL Forum TR-048-compliant DSL CPE auto-configuration
- UPnP for seamless network interconnectivity
- Comprehensive networking protocol support includes DHCP, PPPoE, PPPoA, and RIP
- Friendly web-based graphical user interface for configuration and management

- Supports up to eight simultaneous virtual connections for a single ADSL account
- Supports T1.413 issue 2, G.dmt and G.lite standards
- Auto-handshake and rate adaptation for different ADSL flavors
- Widest range of DSLAM interoperability
- Supports bridged Ethernet over ATM (RFC 2684)
- Upgradeable firmware through web



Installation Planning

Before installing the UT-300R2, you should gather information and equipment needed to install the device, then Install the hardware as instructed, connect the cables to the device and power on the UT-300R2. Prior to accessing the web-based software built into the UT-300R2, you should check the IP settings on your computer and change them if necessary.

Packing List

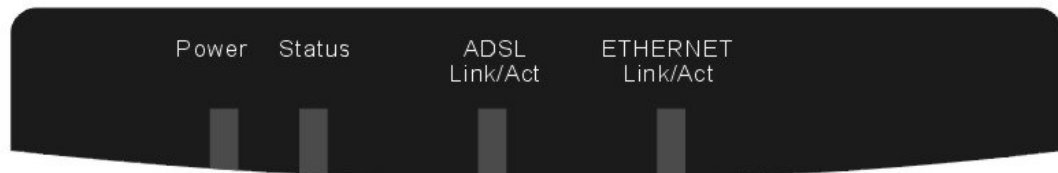
Please check the package contents by comparing them with the following list:

- One UT-300R2
- One telephone line
- One straight-through Ethernet Cable
- One Power Adapter
- One User CD-ROM
- One Splitter

Interfaces Introduction

Front Panel

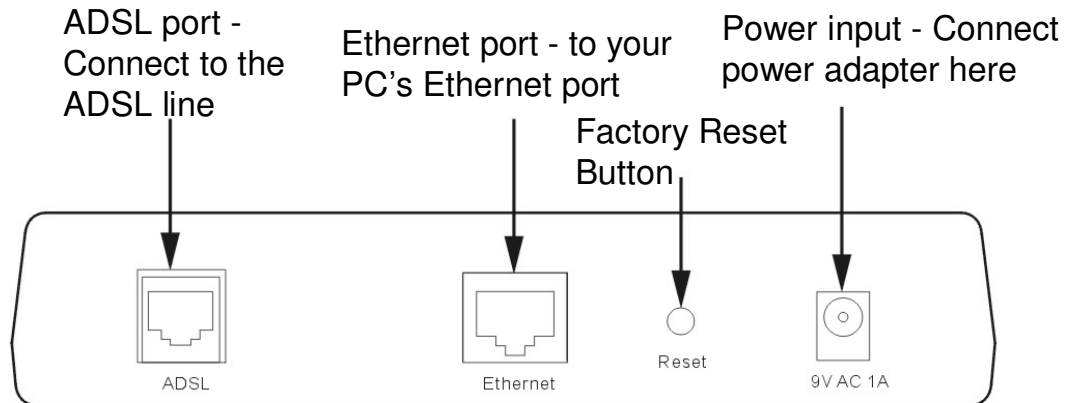
Figure 2 Front Panel



Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
Status	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
ADSL: Link/Act	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.
ETHERNET: Link/Act	A solid green light indicates a valid link on startup. This light blinks when there is activity currently passing through the Ethernet port.

Rear Panel

Figure 3 Rear Panel



Cable Connections

After verifying proper environmental conditions such as temperature, humidity and power supply, users may start the cable connections as following.

Connecting the ADSL Line

Use the ADSL cable included with the UT-300R2 to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the UT-300R2 and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connecting the UT-300R2 to the Ethernet LAN

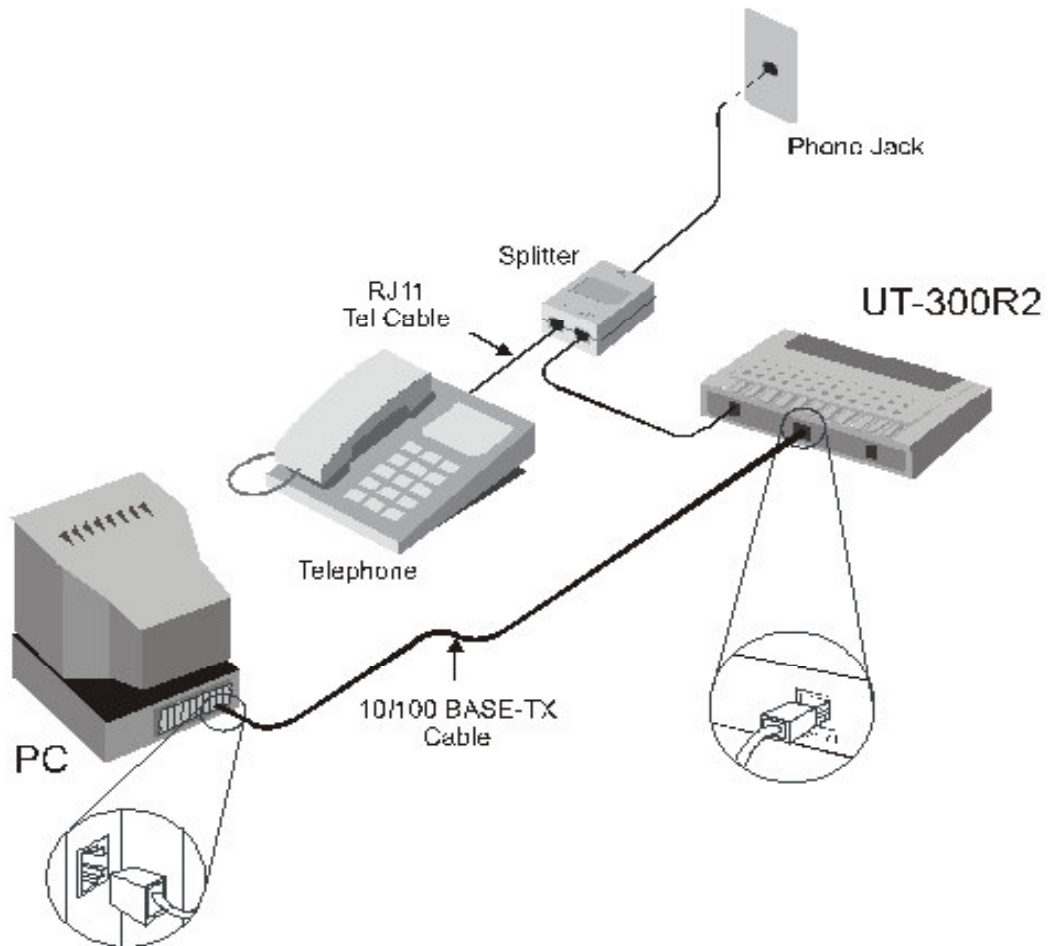
The UT-300R2 may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the UT-300R2 to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the UT-300R2 is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the UT-300R2 directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the UT-300R2 to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch.

The rules governing Ethernet cable lengths apply to the LAN to UT-300R2 connection. Be sure that the cable connecting the LAN to the UT-300R2 does not exceed 100 meters.

Computer to UT-300R2 Connection

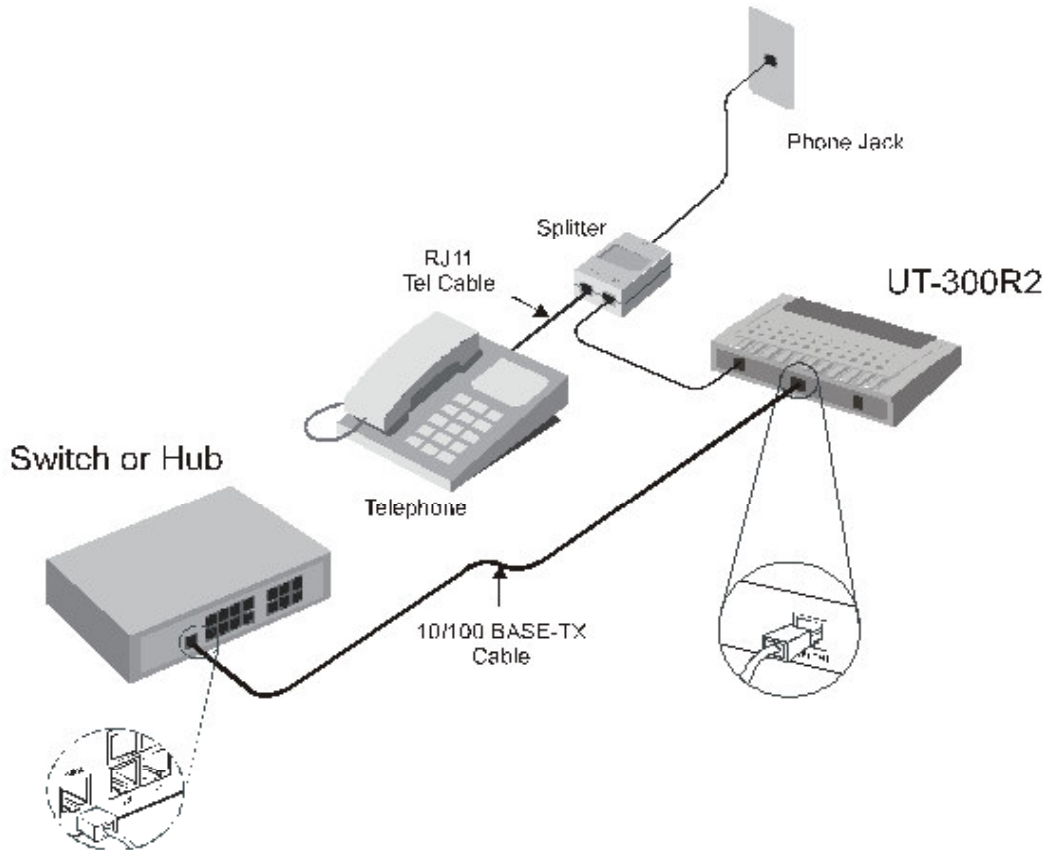
Figure 4 Computer to UT-300R2 Connection



You can connect the UT-300R2 directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided as shown in this diagram.

Hub or Switch to UT-300R2 Connection

Connect the UT-300R2 to an uplink port on an Ethernet hub or switch with a straight-through cable as shown in the diagram below:

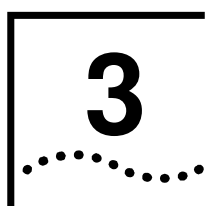
Figure 5 Hub/Switch to UT-300R2 Connection

If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

Power on

- 1 To power on the UT-300R2, please follow the steps as instructed:
- 2 Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the UT-300R2 and plug the adapter into a suitable nearby power source.

- 3 You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.



Before Configuring UT-300R2

The factory default settings of UT-300R2 optimized all functions so as to enable it to operate on most network conditions. Usually, for the users with simple network topology, the default settings can meet the basic requirements and don't need to change. In order to access the web-based software built into the UT-300R2, you should check the IP settings on your computer and change them if necessary to access web-based manager to configure the device.

Set up TCP/IP on Your PC

In order to configure your system to receive IP settings from the UT-300R2 it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. Please follow the instructions to check your IP protocol:

- 1 In Windows task bar, click the **Start** button, point to **Settings>Network and Dial-up Connection>** and click on Local Connection.
- 2 Click on **Properties>** Select Internet Protocol (TCP/IP) and then Click **Properties**.
- 3 Click on the button labeled **use the following IP address**, then you can set the IP address and Subnet mask, for example, 192.168.1.100 and 255.255.255.0.



Note: If Internet Protocol (TCP/IP) does not display as an installed component, you must install it.

Set up Proxy Service

In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

- 1 Click on the **START** button, go to **Settings** and choose **Control Panel**.
- 2 In the **Control Panel** window, double-click on the **Internet Options** icon
- 3 Click the **Connections** tab and click on the **LAN Settings** button.
- 4 Verify that the “**Use proxy server**” option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

Configure IP Settings on Your PC

To use the web-based management software, launch your web browser software and use the LAN IP address of the UT-300R2 to access the management software. The default LAN IP address of the UT-300R2 is used in the Address bar of your web browser window. Type in **http://** followed by the default IP address, **192.168.1.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.1.1**

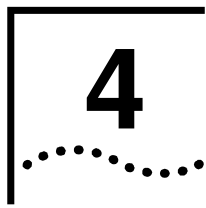
First Time Log on

After inputting the forgoing IP address on URL address bar, a new window appears prompting you for a user name and password needed to gain access the web configuration manager.

Figure 6 Log On Interface



Use the default system user name: **admin** and password: **admin** for first time set up. You can change the password once you have established the ADSL connection. The user name and password allows any computer on the same subnet as the UT-300R2 to access the web configuration manger. This password can also be used to Telnet to the device through the Ethernet or the Internet interfaces.



Web-based Management

Summary

When you successfully login the **Summary** directory button will display the UT-300R2's current connection status – both for the WAN (Internet) and LAN (your home network) connections, as shown below. You can begin the process of configuring your ADSL modem/UT-300R2 by clicking on the **WAN** button in the upper left-hand corner of the first Web page displayed.

Figure 7 Web Manager – First Page

The screenshot shows the UTStarcom Web Manager interface. The top navigation bar includes tabs for Home, Advanced, Tools, Status, and Help. The left-hand panel contains menu buttons for Summary, WAN, DHCP, DNS, LAN, and Static Route. The main content area displays the Summary page for a UT-300R2 device, showing ADSL Line Status and WAN Channel information.

Summary
Displays current configurations of UT-300R2

Model Name	UT-300R2	Firmware Version	R6.11.b1t10us
------------	----------	------------------	---------------

ADSL Line Status

ADSL State	Link Down	Data Path	
DSP Version	C.87.2.7	Operation Mode	

Upstream		DownStream	
ADSL Link Speed	0	ADSL Link Speed	0
SNR	0	SNR	0
CRC	0	CRC	0
FEC	0	FEC	0
HEC(ATM Layer)	0	HEC(ATM Layer)	0

WAN Channel

PVC Number	VPI/VCI	IP Address	Default Gateway	Subnet	Encapsulation	Status	Note
PVC0	0 / 35	---	---	---	Bridged		---
PVC1	8 / 35	---	---	---	Bridged		---
PVC2	0 / 100	---	---	---	Bridged		---
PVC3	0 / 32	---	---	---	Bridged		---
PVC4	8 / 81	---	---	---	Bridged		---
PVC5	8 / 32	---	---	---	Bridged		---
PVC6	14 / 24	---	---	---	Bridged		---

LAN Channel

MAC Address	IP Address	Subnet Mask	Speed	Duplex	Status
00:0D:88:12:31:23	192.168.1.1	255.255.255.0	100BT	Full	

Each tab displays menu buttons located in the left hand panel of the web interface. The table below lists the menus for each directory in the web manager.

Table 1 Options of Web-based page

Directory	Configuration and Read-only Menus
Home	Click the Home tab to access the Summary, WAN, DHCP, DNS, and LAN Configuration menus.
Advanced	Click the Advanced tab to access the Virtual Server, Application, Filter, Firewall, NAT, DDNS, and RIP menus.
Tools	Click the Tools tab to access the Administrator Settings (used to set the system user name and password), System Time Configuration, System Settings (load and save configuration files) and Firmware menus.
Status	Click the Status tab to view the Log, Diagnostic, and Statistics information windows.
Help	The Help menu presents links to pages that explain various functions and services provided by the UT-300R2.

Configuring the WAN Connection

To configure the UT-300R2's basic configuration settings, you can access the menus used to configure WAN, DHCP, DNS and LAN settings from the **Home** directory. To access the WAN Settings menu, click on the **WAN** link button on the upper left-hand side of the first window that appears when you successfully access the web manager.

The WAN Settings menu is also used to configure the UT-300R2 for multiple virtual connections. The next section contains information on how to configure the UT-300R2 for Multiple PVCs. Please note that most users will require only

single PVC. Select the connection type used for your account. The menu will display settings that are appropriate for the connection type you select. Follow the instruction below according to the type of connection you select in the WAN Settings menu. Your Internet Service Provider (ISP) should provide the information you need to select the proper connection type.

Figure 8 WAN Current Settings Menu

The screenshot shows a web-based configuration interface titled "WAN Setting". It contains a table of settings for a PVC:

WAN Setting	
PVC Number	PVC-1
Wan Type	<input checked="" type="radio"/> RFC2684Bridged <input type="radio"/> RFC2684Routed <input type="radio"/> PPP
Connection Type	<input checked="" type="radio"/> Pure Bridged <input type="radio"/> Static IP <input type="radio"/> DHCP
VPI/VCI	0 / 35
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux

Below the table are four buttons: **Apply**, **Cancel**, **Add**, and **Delete**.

Select the connection type used for your account. The menu will display settings that are appropriate for the connection type you select. Follow the instruction below according to the type of connection you select in the WAN Settings menu. Your Internet Service Provider (ISP) should provide the information you need to select the proper connection type.

To change the current configuration of the UT-300R2, click the **Add** button. This will open the menu shown below. Please note that the contents of this menu will change depending upon which **Connection Type** you choose for this PVC.

Figure 9 WAN Setting – Add menu

WAN Setting	
Wan Type	<input checked="" type="radio"/> RFC2684Bridged <input type="radio"/> RFC2684Routed <input type="radio"/> PPP
Connection Type	<input checked="" type="radio"/> Pure Bridged <input type="radio"/> Static IP <input type="radio"/> DHCP
VPI/VCI	<input type="text"/> / <input type="text"/>
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux



Note: you can configure up to seven different connections on your UT-300R2 ADSL Modem/UT-300R2 by assigning a number to each configuration using the drop-down menu corresponding to the **PVC Number** heading. This could be useful if you have several ISPs and need to configure the UT-300R2 differently for each. Most users will require only single PVC, however.

Configuring a Bridged Connection for the WAN

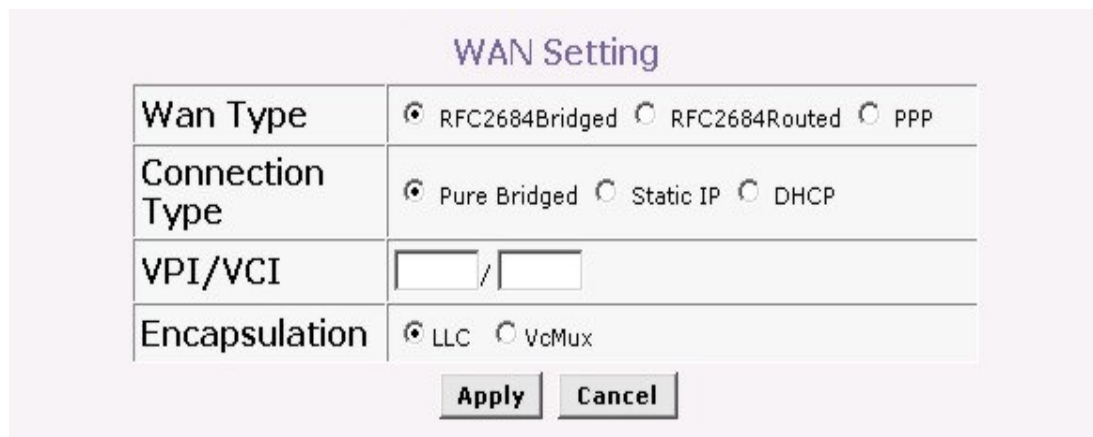
A bridged connection between your ISP and your LAN (the computers in your house or office) is the simplest type of connection possible. The UT-300R2 will simply convert the incoming and outgoing packets to the correct format for each side of the connection (Ethernet for the LAN, ATM for the WAN).

For a bridged connection it will be necessary for most users to install additional software (supplied by your ISP) on any computer that will use the UT-300R2 for Internet access. The additional software is used for the purpose of identifying and

verifying your account, and then granting Internet access to the computer requesting the connection (that is, the software supplied by your ISP will handle giving your Username and Password to the computer at your ISP that will then connect you to the Internet). The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer on the LAN, not in the UT-300R2 for a bridged connection.

Follow the instructions below to configure a Bridged connection for the WAN interface.

Figure 10 WAN Settings Menu – Pure Bridged Mode



The screenshot shows a web-based configuration interface titled "WAN Setting". It contains a table with four rows of settings, each with a label and a set of radio buttons or input fields. At the bottom of the form are two buttons: "Apply" and "Cancel".

WAN Setting	
Wan Type	<input checked="" type="radio"/> RFC2684Bridged <input type="radio"/> RFC2684Routed <input type="radio"/> PPP
Connection Type	<input checked="" type="radio"/> Pure Bridged <input type="radio"/> Static IP <input type="radio"/> DHCP
VPI/VCI	<input type="text"/> / <input type="text"/>
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux



Note: Please note that the menu shown above will change depending on which WAN Type and Connection Type you select.

- 1 Click to select the **RFC2684Bridged** radio button in the **WAN Type** options list if your ISP uses DHCP to assign you an IP address that is valid on the WAN (Internet). This is the most common type of bridged connection offered by ISPs.

- 2 Also under the **VPI/VCI**, you will need to enter two numbers, the **VCI** and **VPI** values. These numbers are used to define a unique path for your connection. Your ISP should give you the specific settings for the VPI and VCI numbers to enter. Type in the correct values assigned by your ISP.
- 3 Select the **Encapsulation** type (LLC or VcMux) radio button that corresponds to the encapsulation in use by your ISP.
- 4 When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
- 5 The new settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually save and reboot the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. On the menu that appears, click the **Save & Restart** button. The UT-300R2 will save the new settings and restart. Upon restarting the UT-300R2 will automatically establish the bridged WAN connection.



Note: *Some accounts use PPP connection software for their Internet service connection. If you have been given a CD with PPP connection software, install this now as instructed by your service provider. After the UT-300R2 has rebooted it will negotiate the ADSL connection. Use the connection software to log on to the ISP network and access the Internet.*

Configuring a Routed/Bridged Connection for the WAN

A routed bridged connection between your ISP and your LAN (the computers in your house or office) is useful if packets sent from the LAN to the WAN through the UT-300R2 must cross part of another network in your ISP's installation, before arriving at a specific computer or network device, specified by an IP address. Your ISP will need to give you the specific **IP Address**, **Subnet Mask**, and Default Gateway address that packets destined for the Internet must be sent to. The UT-300R2 will then manage both the necessary format conversion and direct the outgoing packets to the destination you specify.

For a routed/bridged connection it will be necessary for most users to install additional software (supplied by your ISP) on any computer that will use the UT-300R2 for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection (that is, the software supplied by your ISP will handle giving your Username and Password to the computer at your ISP that will then connect you to the Internet). The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer on the LAN, not in the UT-300R2 for a bridged connection.

Follow the instructions below to configure a Routed/Bridged connection for the WAN interface.

Figure 11 WAN Settings Menu – Routed/Bridged Mode

WAN Setting	
PVC Number	PVC-1 ▾
Wan Type	<input type="radio"/> RFC2684Bridged <input checked="" type="radio"/> RFC2684Routed <input type="radio"/> PPP
VPI/VCI	0 / 35
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux
IP Address
Subnet Mask	255.255.255.252 (/30) ▾
Default Gateway
Default Route	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



Note: Please note that the menu shown above will change depending on which WAN Type and Connection Type you select.

- 1 Click to select the **RFC2684Bridged** radio button in the **WAN Type** options list if your ISP uses DHCP to assign you an IP address that is valid on the WAN (Internet). This is the most common type of bridged connection offered by ISPs.
- 2 Also under the **VPI/VCI**, you will need to enter two numbers, the **VCI** and **VPI** values. These numbers are used to define a unique path for your connection. Your ISP should give you the specific settings for the VPI and VCI numbers to enter. Type in the correct values assigned by your ISP.

- 3 Select the **Encapsulation** type (LLC or VcMux) radio button that corresponds to the encapsulation in use by your ISP
- 4 Enter the IP Address, Subnet Mask, and Default Gateway address as supplied by your ISP.
- 5 When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
- 6 The new settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually save and reboot the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. On the menu that appears, click the **Save & Restart** button. The UT-300R2 will save the new settings and restart. Upon restarting the UT-300R2 will automatically establish the bridged WAN connection.



Note: *Some accounts use PPP connection software for their Internet service connection. If you have been given a CD with PPP connection software, install this now as instructed by your service provider. After the UT-300R2 has rebooted it will negotiate the ADSL connection. Use the connection software to log on to the ISP network and access the Internet.*

Configuring a PPP Connection for the WAN

Most ADSL accounts will use either the Point-to-Point Protocol over Ethernet (PPPoE) or the Point-to-Point Protocol over ATM (PPPoA) connection. Follow the instructions below to configure the UT-300R2 to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information

before you configure the WAN connection. See the table in the first section of this manual for a summary of the information you will need.

- 1 Select the **PPP** radio button to open the Point-to-Point Protocol (PPP) menu.
- 2 Click to select either the **PPPoE** or the **PPPoA** radio button in the **WAN Setting** menu under the **Connection Type** options list.
- 3 Choose the **Encapsulation** type from the options of LLC and VcMux radio buttons. If have not been provided specific information for the Connection Type setting, leave the default setting.
- 4 If you are instructed to use enable **Default Route**, this setting specifies that the UT-300R2 be used to define the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the UT-300R2 becomes the Internet gateway to the computer.
- 5 Under the **PPP** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user@isp.com.au, your ISP may assign the Password to you or you may have selected it when you set up the account with your ISP.
- 6 The **Use DNS** is enabled by default. When this is enabled, the UT-300R2 will request DNS settings from your ISP's DNS server. If your ISP has provided a specific IP address to use for DNS, you should select *Disabled* and manually configure DNS settings in the DNS menu (see **Configure DNS** below). You will not be able to access Internet web

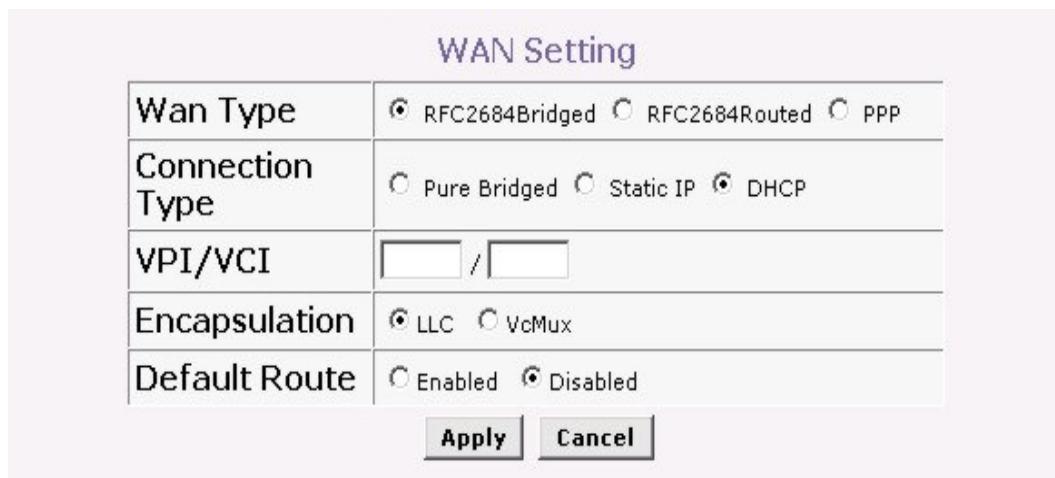
sites until the DNS settings are properly configured. Be sure to configure this before you save the new settings and restart the UT-300R2.

- 7 When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.

The new settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually save and reboot the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. On the menu that appears, click the **Save & Restart** button. The UT-300R2 will save the new settings and restart. Upon restarting the UT-300R2 will automatically establish the bridged WAN connection.

Dynamic IP Address for the WAN Connection

When the UT-300R2 is configured to use Dynamic IP Address assignment for the WAN connection, a server on the ISP's network assigns the global IP address settings used for the WAN connection. This method is simply Dynamic Host Control Protocol (DHCP) for the WAN. The UT-300R2 can be configured to be a DHCP client and obtain its IP settings automatically from the DHCP server maintained by your ISP. Follow the instructions below to configure the UT-300R2 to use Dynamic IP Address assignment for the WAN connection.

Figure 12 WAN Settings - Dynamic IP Address (DHCP)

The screenshot shows a web-based configuration interface titled "WAN Setting". It contains a table with the following fields and options:

Wan Type	<input checked="" type="radio"/> RFC2684Bridged <input type="radio"/> RFC2684Routed <input type="radio"/> PPP
Connection Type	<input type="radio"/> Pure Bridged <input type="radio"/> Static IP <input checked="" type="radio"/> DHCP
VPI/VCI	<input type="text"/> / <input type="text"/>
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux
Default Route	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

At the bottom of the form are two buttons: "Apply" and "Cancel".

- 1 From the **WAN Setting** page, select the PVC you want to configure from the seven available PVCs, using the drop-down menu.
- 2 You can also specify the **VPI/VCI** numbers (assigned to this PVC by your ISP) that will be used to uniquely identify this PVC to your ISP. You can also enter or modify these two numbers later during the configuration process.
- 3 Click the **Add** button, at the bottom of the page, to add the new configuration to the list of active PVCs. This will open the **WAN Setting** configuration screen, shown above.
- 4 Click to select the **DHCP** radio button listed in the **Connection Type** options list. The menu will change to offer a different set of configuration options and will appear as shown above when DHCP is selected.
- 5 If you are instructed to use enable **Default Route** by your ISP, click the **Enabled** radio button. This setting specifies that this PVC (from the list of seven) on your UT-300R2 be used to define the default route to the Internet for your LAN.

Whenever a computer on your LAN attempts to access the Internet, the UT-300R2 will use this PVC to direct packets to the Internet, and this PVC will become the default gateway to the Internet for your LAN.

- 6 Under the **Encapsulation** heading, select either LLC or VcMux, as instructed by your ISP.
- 7 When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
- 8 The new settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually save and reboot the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. On the menu that appears, click the **Save & Restart** button. The UT-300R2 will save the new settings and restart. Upon restarting the UT-300R2 will automatically establish the bridged WAN connection.

Static IP Address for WAN

When a PVC (of the available list of seven) on the UT-300R2 is configured to use a Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection provided by this PVC. Most users will also need to configure a DNS server IP setting in the DNS Settings configuration menu (see below). Follow the instruction below to configure the UT-300R2 to use Static IP Address assignment for the WAN connection.

Figure 13 WAN Settings - Static IP

WAN Setting	
Wan Type	<input checked="" type="radio"/> RFC2684Bridged <input type="radio"/> RFC2684Routed <input type="radio"/> PPP
Connection Type	<input type="radio"/> Pure Bridged <input checked="" type="radio"/> Static IP <input type="radio"/> DHCP
VPI/VCI	<input type="text"/> / <input type="text"/>
Encapsulation	<input checked="" type="radio"/> LLC <input type="radio"/> VcMux
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask	<input type="text"/> 255.255.255.252 (/30) <input type="text"/>
Default Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Route	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 1 From the **WAN Setting** page, select the PVC you want to configure from the seven available PVCs, using the drop-down menu.
- 2 You can also specify the **VPI/VCI** numbers (assigned to this PVC by your ISP) that will be used to uniquely identify this PVC to your ISP. You can also enter or modify these two numbers later during the configuration process.
- 3 Click the **Add** button, at the bottom of the page, to add the new configuration to the list of active PVCs. This will open the **WAN Setting** configuration screen, shown above.
- 4 Click to select the **RFC2684Bridged** radio button listed in the **WAN Type** options list. The menu will change to offer a different set of configuration options, as shown above.
- 5 Select the **Connection Type** from the options to be **Static IP**, by clicking the radio button.

- 6 Enter the appropriate **IP Address**, **Subnet Mask** and **Default Gateway** address as instructed by your ISP. Your ISP should have provided these IP settings to you.
- 7 If you are instructed to use enable **Default Route** by your ISP, click the **Enabled** radio button. This setting specifies that this PVC (from the list of seven) on your UT-300R2 be used to define the default route to the Internet for your LAN. Whenever a computer on your LAN attempts to access the Internet, the UT-300R2 will use this PVC to direct packets to the Internet, and this PVC will become the default gateway to the Internet for your LAN.
- 8 When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
- 9 The new settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually save and reboot the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. On the menu that appears, click the **Save & Restart** button. The UT-300R2 will save the new settings and restart. Upon restarting the UT-300R2 will automatically establish the bridged WAN connection.

DHCP Configuration

To display the **DHCP Server** menu, click the **DHCP** button in the **Home** directory. Active DHCP Clients appear listed in the **DHCP Client Table** below the configuration menu. Information about DHCP clients includes the IP address, MAC address, host name and lease time are displayed in the list.

Figure 14 Configure DHCP server settings for the LAN

DHCP Server

The UT-300R2(A) can be setup as a DHCP Server to distribute IP addresses to the LAN network.

DHCP Server	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Starting IP Address	192 . 168 . 1 . <input type="text" value="2"/>
Ending IP Address	192 . 168 . 1 . <input type="text" value="33"/>
Lease Time	<input type="text" value="1 week"/> ▼

DHCP Client Table

Host Name	IP Address	MAC Address	Expired Time
-----------	------------	-------------	--------------

The three options for DHCP service are as follows:

- 1 You may use the UT-300R2 as a DHCP server for your LAN.
- 2 You can disable DHCP service and manually configure IP settings for all workstations.

You will use a DHCP service provided by your ISP, in which case DHCP should be disabled on the UT-300R2.

DHCP Server Settings for the LAN

The default setting of UT-300R2 's DHCP server is disabled. While you click to select the **Enabled** radio button under the **DHCP Server** option, the device will become the default gateway for DHCP clients that connected to it. When the UT-300R2 is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change

the IP address of the UT-300R2, you must change the range of IP addresses in the pool used for DHCP on the LAN.

Use the UT-300R2 for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted so that up to 253 IP addresses are available for use. The **Starting IP Address** is the lowest available IP address (default = 192.168.1.2). If you change the IP address of the UT-300R2 this will change automatically to be 1 more than the IP address of the UT-300R2. The **Ending IP Address** is the highest IP address number in the pool (default = 192.168.1.33). Select the **Lease Time** from the pull-down menu. This is the amount of time that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off. Lease time options vary from 1 hour to 1 week. DHCP client workstations on your LAN must be properly configured to use DHCP service. Be sure to save the new settings.

Disabling the DHCP Server

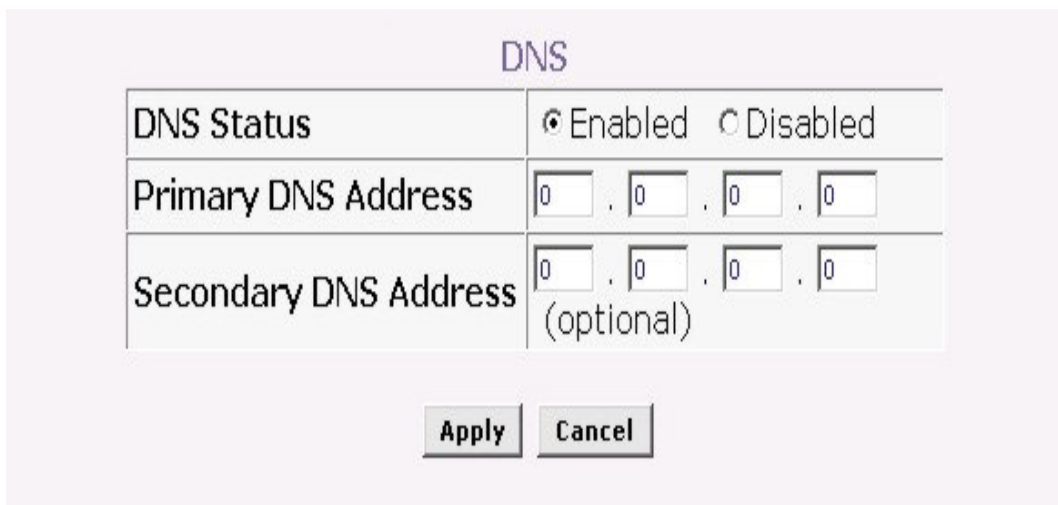
To disable DHCP, click to select the **Disabled** radio button under the **DHCP Server** option and click on the **Apply** button. Be sure to save the new settings

DNS Server Setting

The UT-300R2 is configured by default to forward the DNS server address you enter in the DNS page, shown below, to all DHCP clients on your LAN. When DNS is enabled, the DNS

clients on the LAN will automatically get DNS settings relayed from the UT-300R2 as they are entered here. Alternatively, if **DNS Status** is disabled, workstations must be configured to initiate DNS requests for each session, and therefore you must configure DNS settings for the workstations.

Figure 15 Configure DNS IP address



DNS	
DNS Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Primary DNS Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS Address (optional)	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Usually an ISP will provide you with one or two DNS server IP addresses. Enter these IP addresses in the available entry fields for the **Primary DNS Server** and the **Secondary DNS Server**.

If you do not want to use the UT-300R2 as a DNS proxy agent, change the **DNS Status** to *Disabled*.

When you have configured the DNS settings as desired, click the **Apply** button. Be sure to save the settings.

Configuring the LAN Connection

The first step in configuring your LAN is to determine the IP address scheme that the computers on your LAN will use. The

192.168.1.x (where x can range from 2 to 254) IP address range has been dedicated for home and small office use. The UT-300R2 ADSL router is configured with a default IP address of 192.168.1.1, and a subnet mask of 255.255.255.0. The next IP address available for use on a LAN is 192.168.1.2. This is why the IP address range begins with an $x = 2$, because when $x = 1$, that identifies the UT-300R2 on your LAN. The IP address where $x = 255$ has a special meaning (it is the broadcast address for your LAN). When you configure PCs on your LAN, the UT-300R2's IP address (192.168.1.1) will become the Default Gateway IP address for all PCs on your LAN.

You can configure the UT-300R2's LAN IP address to any IP addressing scheme that meets the needs of your LAN. Many users will find it convenient to use the default settings together with the DHCP service to manage the IP settings for their LANs. The IP address of the UT-300R2 is the base address used for DHCP. In order to use the UT-300R2 for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the UT-300R2. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the UT-300R2. See the next section for information on DHCP setup, as described below.

So, if you want to use an IP addressing scheme that is different from the 192.168.1.x/255.255.255.0 scheme, you will need to give the UT-300R2 ADSL router a new IP address. This is done on the **LAN Settings** page, as shown below.

To access the **LAN Settings** menu, click the **LAN** button in the **Home** directory.

Figure 16 Configure LAN IP settings

LAN Settings	
The IP address of the ADSL Router	
IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/> ▾
Local Domain Name	<input type="text"/> (optional)

To change the **LAN IP Address** or **Subnet Mask**, type in the desired values and click the **Apply** button. The new IP settings must be saved and the UT-300R2 must be restarted for the settings to go into effect. To manually **Save & Restart** the UT-300R2, click on the **Tools** directory tab and then click the **System** menu button. Then click the **Save&Restart** button. The UT-300R2 will save the new IP settings and restart. Your web browser should automatically be redirected to the new IP address.

Save New Settings

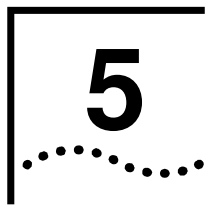
Most changes that require updating the UT-300R2's non-volatile RAM will automatically trigger a save and reboot procedure. Any changes you have made that you want to be saved to the UT-300R2's memory can be saved using the **System Setting** page, as shown below. To save settings you need to access the **System** menu. Click on the **Tools** directory tab then click the **System** menu button to view the menu pictured below.

Figure 17 Save Settings and Restart the UT-300R2

The screenshot shows a web-based management interface titled "System Setting". It contains several sections with buttons for configuration:

- Save Settings To Local Hard Drive** with a **Save** button.
- Load Settings From Local Hard Drive** with a text input field, a **Browse...** button, and a **Load** button.
- Restore To Factory Default Settings** with a **Restore** button.
- Save and Restart Device** with a **Save&Restart** button.
- A **Help** button is located at the bottom center.

To save the new settings, click the **Save& Restart** button. It will take about two minutes for the whole process to be completed. Do not turn off the power while the UT-300R2 is saving and restarting.



Advanced Configuration / Network Management

This chapter introduces and describes the management features that have not been presented in the previous chapter. These include the more advanced features used for network management and security as well as administrative tools to manage the UT-300R2, view statistics and other information used to examine performance and for troubleshooting.

Use your mouse to click the directory tabs and menu buttons in order to display the various configuration and read-only menus discussed below. The table below summarizes again the directories and menus available in the management web interface. In this chapter you will find descriptions for the menus located in the Advanced, Tools and Status directories.

Figure 18 Advanced configuration menus

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Status: Enabled Disabled

Name:

Private IP: . . .

Protocol Type:

Private Port:

Public Port:

Schedule: Always

From: time : AM to : AM

day to

Virtual Servers List

Name	Private IP	Protocol Type	Schedule	
<input type="checkbox"/> Virtual Server FTP	0.0.0.0	TCP 21/21	Always	
<input type="checkbox"/> Virtual Server HTTP	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/> Virtual Server HTTPS	0.0.0.0	TCP 443/443	Always	
<input type="checkbox"/> Virtual Server DNS	0.0.0.0	UDP 53/53	Always	
<input type="checkbox"/> Virtual Server SMTP	0.0.0.0	TCP 25/25	Always	
<input type="checkbox"/> Virtual Server POP3	0.0.0.0	TCP 110/110	Always	
<input type="checkbox"/> Virtual Server Telnet	0.0.0.0	TCP 23/23	Always	
<input type="checkbox"/> IPSec	0.0.0.0	UDP 500/500	Always	
<input type="checkbox"/> PPTP	0.0.0.0	TCP 1723/1723	Always	
<input type="checkbox"/> NetMeeting	0.0.0.0	TCP 1720/1720	Always	
<input type="checkbox"/> DCS-1000	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/> DCS-2000	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/> DVC-1000	0.0.0.0	TCP 1720/1720	Always	

Directory	Configuration and Read-only Menus
Virtual server	This page allows you to configure the UT-300R2 ADSL router to allow remote users to assess service such as web or FIP service through a public IP address.

Directory	Configuration and Read-only Menus
Application	This page allows you to configure the UT-300R2 ADSL router to allow applications that require multiple connections such as Internet gaming, video conferencing, Internet telephony, and others that are unable to work through Network Address Translation (NAT)
Filter	Filters are used to deny or allow access to the Internet for various PCs on your LAN. The UT-300R2 can refuse PCs on your LAN access to the Internet based upon their IP or MAC address, or it can restrict access to specific web sites.
DMZ	If your computer cannot run Internet applications properly with the device, then you can enable this option to allow the computer accessing the unrestricted Internet. Enter the IP address of the computer as a DMZ (Demilitarized Zone) host. Adding the computer to the DMZ may expose it under insecurity risk; thus suggest not use this option unless no other alternatives.
DDNS	This page allows you to configure the UT-300R2 to use the DYNAMIC Domain Name Service (Dynamic DNS), if you have a previously established account.
RIP	This allows you to enable or disable the Routing Information Protocol (RIP) on PVC's that allow routing.

Virtual Server Configuration

A Virtual Server can allow remote users to access services to PCs on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The UT-300R2 will accept remote requests for these services at your Global IP Address (the one assigned to your account by your ISP), using the specified TCP or UDP protocol and port number, and then redirect these requests to

the server on your LAN with the Private IP address you specify. Remember that the Private IP Address must be within the range specified for your LAN.

The Virtual Server feature employs UDP/TCP port redirection to direct traffic through the WAN port to specified servers on your private network. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the UT-300R2 to direct HTTP packets to a designated HTTP server in the DMZ. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each instruction set or rule is indexed and can be modified or deleted later as needed.

Virtual server configuration sets can be used together with complimentary features such as Firewall Rules, and Filters to improve efficiency and security. Consider how these other functions will effect the virtual server sets you have configured and enabled.

The table below describes the configuration settings presented in the Virtual Server menu.

Figure 19 Virtual Server Menu and List

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Name	<input type="text"/>	<input type="button" value="Clear"/>
Private IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Protocol Type	TCP ▾	
Private Port	<input type="text"/>	
Public Port	<input type="text"/>	
Schedule	<input checked="" type="radio"/> Always	
	<input type="radio"/> From	time <input type="text"/> : <input type="text"/> <input type="text"/> AM to <input type="text"/> : <input type="text"/> <input type="text"/> AM
		day <input type="text"/> to <input type="text"/>

Virtual Servers List

	Name	Private IP	Protocol Type	Schedule	
<input type="checkbox"/>	Virtual Server FTP	0.0.0.0	TCP 21/21	Always	
<input type="checkbox"/>	Virtual Server HTTP	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/>	Virtual Server HTTPS	0.0.0.0	TCP 443/443	Always	
<input type="checkbox"/>	Virtual Server DNS	0.0.0.0	UDP 53/53	Always	
<input type="checkbox"/>	Virtual Server SMTP	0.0.0.0	TCP 25/25	Always	
<input type="checkbox"/>	Virtual Server POP3	0.0.0.0	TCP 110/110	Always	
<input type="checkbox"/>	Virtual Server Telnet	0.0.0.0	TCP 23/23	Always	
<input type="checkbox"/>	IPSec	0.0.0.0	UDP 500/500	Always	
<input type="checkbox"/>	PPTP	0.0.0.0	TCP 1723/1723	Always	
<input type="checkbox"/>	NetMeeting	0.0.0.0	TCP 1720/1720	Always	
<input type="checkbox"/>	DCS-1000	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/>	DCS-2000	0.0.0.0	TCP 80/80	Always	
<input type="checkbox"/>	DVC-1000	0.0.0.0	TCP 1720/1720	Always	

To modify virtual server settings for any previously created virtual server set listed, click on the note pad icon in the right hand column of the **Virtual Servers List** for the set you want to configure. The set will appear highlighted in the list and the parameters that have been configured appear in the settings fields above the list. Adjust the settings as desired and click the **Apply** button to put them into effect.

To configure a virtual server set, define the following settings in the Virtual Server configuration menu located in the top half of the browser window.

Directory	Configuration and Read-only Menus
Status	This allows you to enable or disable any of the Virtual servers entered into the Virtual Servers List
Name	You can assign a name to a Virtual server entry for easier identification.
Private IP	This is the IP address of the server on your LAN that will provide the service to remote users. This Private IP address is used to direct the service to a specific computer on your private network such as an FTP, Email or public web server. Type in the address of the server used for the service being configured here.
Protocol Type	You can select the transport protocol (TCP or UDP) that the application on the virtual server will use for its connections. Select redirect TCP, UDP or Both (All) types of packets from the pull –down menu. The choice of this protocol is dependent on the application that is providing the service. If you do not know which protocol to choose, check your application’s document.
Private Port	<p>This is the TCP/UDP port on LAN (Private) interface. Keep in mind that if you use a non-standard port number for an application with a reserved UDP/TCP port, some additional configuration may be required for the servers or workstations using the application on the LAN side.</p> <p>Port redirection must be used with a specified server or computer on the LAN (identified by the Private IP address)</p>

Directory	Configuration and Read-only Menus
Public Port	The Public Port is the TCP/UDP port on the WAN interface. Select one of the following options from the pull-down menu to define a Single Port, Range of Port, Any port or Safe Ports (port above 1024). If you are redirecting a single standard TCP/UDP port from the WAN to the LAN, select the Single Port option and use the standard port number here (such as port 23 for Telnet or port 25 for SMTP.) If choose the Any Port option, all TCP/UDP traffic will be directed as specified.
Schedule	This allows you to select between Always or a timed basis for the Virtual server entry to be enabled.

Click the **Apply** button to put the new virtual server configuration set or modification into effect. Any server sets configured in the menu will appear in the Virtual Server List with the new settings. The UT-300R2 must save the new settings and reboot before the new virtual server configurations are applied.

To remove any configuration set from the Virtual Server List, click on the trashcan icon for set you want to delete.

Special Application Configuration

Some applications (programs on your PCs) require multiple TCP/UDP connections to the Internet. Internet games, video conferencing, and Internet telephony are examples of such applications. These type of applications can not work with Network Address Translation (NAT). If you want to use such applications on your LAN, you will need to make an entry for

that application in the Special Applications List on your UT-300R2 ADSL router.

Figure 20 Special Applications Menu

Special Application

Special Application is used to run applications that require multiple connections.

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Name	<input type="text"/>	<input type="button" value="Clear"/>
Trigger Port	<input type="text" value="0"/> - <input type="text" value="0"/>	
Trigger Type	TCP <input type="button" value="v"/>	
Public Port	<input type="text" value="0"/>	
Public Type	TCP <input type="button" value="v"/>	

Special Applications List

	Name	Trigger Port	Public Port	
<input type="checkbox"/>	Battle.net	6112-6112	6112	
<input type="checkbox"/>	Dialpad	7175-7175	51200-51201,51210	
<input type="checkbox"/>	ICU II	2019-2019	2000-2038,2050-2051,2069,2085,3010-3030	
<input type="checkbox"/>	MSN Gaming Zone	47624-47624	2300-2400,28800-29000	
<input type="checkbox"/>	PC-to-Phone	12053-12053	12120,12122,24150-24220	
<input type="checkbox"/>	Quick Time 4	554-554	6970-6999	

To configure a Special Applications List entry, define the following settings in the Virtual Server configuration menu located in the top half of the browser window.

Directory	Configuration and Read-only Menus
Status	This allows you to enable or disable any of the Special Applications entered into the Special Applications List.
Name	You can assign a name to a Special Applications entry for easier identification.

Directory	Configuration and Read-only Menus
Trigger Port	This is the TCP or UDP port number that will be used to initiate a connection from the LAN to the WAN (internet) from a PC on your LAN that is running this application. The entry can be either a single port number or a range of port numbers. Consult your application documentation to determine the port numbers that should be included.
Trigger Type	This is either the TCP or UDP protocol, that the application uses to establish connections between PCs.
Public Port	This is the port number on the WAN (internet) that will be used to access to this application. This can be either a single port number or a range of port numbers. Use a comma to add multiple ports or port ranges.
Public Type	This is the TCP or UDP port number that will be used to initiate a connection from the WAN (internet) to a PC on your LAN that is running this application. The entry can be either a single port number or a range of port numbers. Consult your application documentation to determine the port numbers that should be included.

Click the **Apply** button to put the new virtual server configuration set or modification into effect. Any Special Application configured in the menu will appear in the Special Applications List with the new settings. The UT-300R2 must save the new settings and reboot before the new Special Applications configurations are applied.

To remove any configuration set from the Special Applications List, click on the trashcan icon for set you want to delete.

Configure a Filter Rule-IP Filters

You can limit access to the WAN from PCs on your LAN, or limit access from the WAN to your LAN using filter rules that can be configured on your UT-300R2 ADSL router. The UT-300R2 router will examine incoming and outgoing packets to determine if they meet the requirements you specify in the Filter rule, and then either **Allow** or **Deny** access based upon the rule you have configured. These rules can be based on IP addresses, MAC addresses, URLs, Domain names, and TCP/UDP port numbers. In addition, you can specify a rule to apply to packets from your LAN to the WAN (Internet), from the WAN to your LAN, or both.

To configure a filter rule, click on the **Filter** button under the **Advanced** tab. This will open the **Filters** page, as shown below.

Figure 21 Filters Configuration Menu – IP Filters

Filters


Filters are used to allow or deny LAN users from accessing the Internet.

<input checked="" type="radio"/> IP Filters	<input type="radio"/> URL Blocking
<input type="radio"/> MAC Filters	<input type="radio"/> Domain Blocking

Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Name	<input type="text"/> <input type="button" value="Clear"/>
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	LAN	<input type="text"/>	<input type="text"/>	TCP	0 - 0
Destination	LAN	<input type="text"/>	<input type="text"/>		
Schedule	<input checked="" type="radio"/> Always				
	<input type="radio"/> From	time 01 : 00 AM to 01 :			
		00 AM day Sun to Sun			

IP Filters List

	Action	Name	Source	Destination	Protocol	
<input checked="" type="checkbox"/>	Allow	Allow to Ping WAN Port	WAN, 0.0.0.0-255.255.255.255	LAN, 192.168.1.1-192.168.1.1	ICMP 8-8	
<input checked="" type="checkbox"/>	Allow	Default Allow	LAN, 0.0.0.0-255.255.255.255	Both, 0.0.0.0-255.255.255.255	Any 0-65535	
<input checked="" type="checkbox"/>	Deny	Default Deny	Both, 0.0.0.0-255.255.255.255	LAN, 0.0.0.0-255.255.255.255	Any 0-65535	

The first page allows you to enter an IP address, or range of IP addresses to form the basis of a filter rule for the UT-300R2 router. The **Filters** page will change when you select on of the other radio buttons (**MAC Filters**, **URL Blocking**, or **Domain Blocking**) to allow you to enter the appropriate information for other filter rule types, as shown below.

Previously entered or default IP filter rules are listed in the **IP Filters List** at the bottom of the page. When you configure an

additional IP filter rule and click the **Apply** button, the new rule will be added to this list.

The first step in configuring an IP filter rule is to determine if you want to **Allow** or **Deny** access. Click the appropriate radio button under the **Action** field. You can also turn the IP filter rule on or off using the **Enabled** or **Disabled** radio buttons under the **Status** field. For easy reference, you can enter an alphanumeric name in the **Name** field.

You can then specify the **Source for** packets to be filtered from the drop-down menu. If the source is selected as **LAN**, then this rule will apply to packets that are sent from PCs on your LAN to the WAN (Internet). If the source is selected as **WAN**, then this rule will apply to packets that are sent from PCs on the WAN. If **both** are selected, then this rule will apply to packets that are sent from PCs on both the WAN and your LAN.

A similar situation applies to the **Destination** drop-down menu. If the destination is selected as **LAN**, then this rule will apply to packets that are to be sent to PCs on your LAN. If the destination is selected as **WAN**, this rule will apply to packets that are to be sent to PCs on the WAN. If **Both** is selected, then this rule will apply to packets that are to be sent to PCs on both the WAN and your LAN.

Next, you must enter either a single IP address or a range of IP addresses in the **IP Range Start** and **IP Range End** fields. Remember that IP addresses are in the form x.x.x.x – where x varies from 0 to 255 – and that an IP address range must be contiguous.

From the **Protocol** drop-down menu, select the protocol that you want this rule to apply to. You can select from the **TCP**, **UDP**, **ICMP**, or **Any** protocols. If **Any** is selected, this rule will apply to any packets that has one of the specified IP addresses as its source or destination.

You can also specify a range of TCP or UDP ports for this rule to apply to in the **Port Range** fields.

The **Schedule** field allows you to specify when the UT-300R2 router will enable this rule. Click **always** if you want this rule to be enabled at all times. Otherwise, click the **from** radio button and enter the time and day of the week you want this rule to be enabled.

Click the **Apply** button to enter the rule into the **IP Filters List** and restart the router.

Directory	Configuration and Read-only Menus
IP Filters	This radio button selects the IP address filter rule entry page, which will be displayed when you click on it.
MAC Filters	This radio button selects the MAC address filter rule entry page, which will be displayed when you click on it.
URL Blocking	This radio button selects the URL filter rule entry page, which will be displayed when you click on it.
Domain Blocking	This radio button selects the Domain name filter rule entry page, which will be displayed when you click on it.
Status	This set of radio buttons allows you to enable or disable this rule.
Name	You can enter a name for the rule, for easier identification later.

Directory	Configuration and Read-only Menus
Action	Select Allow to permit packets to pass through the UT-300R2 if they meet the criteria of this rule, and Deny dropping packets that meet the criteria of this rule.
Source	<p>When LAN is specified in the Interface drop-down menu, this filter will apply to packets that have one of the specified IP addresses as their source, and are sent from a PC on your LAN.</p> <p>When WAN is specified in the Interface drop-down menu, this filter will apply to packets that have one of the specified IP addresses as their source, and are sent from a PC on the WAN (Internet).</p> <p>If Both is selected, then this rule will apply to packets that are sent from PCs on both the WAN and your LAN.</p>
Destination	<p>When LAN is specified in the Interface drop-down menu, this filter will apply to packets that have one of the specified IP addresses as their destination, and are being sent to a PC on your LAN.</p> <p>When WAN is specified in the Interface drop-down menu, this filter will apply to packets that have one of the specified IP addresses as their destination, and are being sent to a PC on the WAN (Internet).</p> <p>If Both is selected, then this rule will apply to packets that are being sent to PCs on both the WAN and your LAN.</p>
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN
Protocol	Select the transport protocol (TCP, UDP, ICMP, or All) that will be used for the filter rule.

To remove any rule from the **IP Filters List**, click on the trashcan icon for set you want to delete.

To edit any previously entered IP filter rule, click on the Note pad icon.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Outbound or Inbound Filters List with the new settings. The UT-300R2 must save the new settings and reboot before the new rules are applied.

Configuring a Filter Rule- MAC Filters

Select the other radio buttons **MAC Filters** to enter the page of MAC Filters. This is to deny LAN computers to access the Internet. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the unit.

Figure 22 Filters Configuration Menu – MAC Filters

Filters

Filters are used to allow or deny LAN users from accessing the Internet.

<input type="radio"/> IP Filters	<input type="radio"/> URL Blocking
<input checked="" type="radio"/> MAC Filters	<input type="radio"/> Domain Blocking

MAC Filters

Use MAC address to allow or deny computers access to the network.

<input type="radio"/> Enabled MAC Filters	
<input checked="" type="radio"/> Disabled MAC Filters	
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Name	<input style="width: 80%;" type="text"/> <input type="button" value="Clear"/>
MAC Address	<input style="width: 15%;" type="text"/> : <input style="width: 15%;" type="text"/> : <input style="width: 15%;" type="text"/> : <input style="width: 15%;" type="text"/> : <input style="width: 15%;" type="text"/> : <input style="width: 15%;" type="text"/>
DHCP Client	<input style="width: 80%;" type="text" value="No any DHCP Client entry yet"/> <input type="button" value="Clone"/>

MAC Filters List

Name	MAC Address

Previously entered or default MAC filter rules are listed in the **MAC Filters List** at the bottom of the page. When you configure an additional MAC filter rule and click the **Apply** button, the new rule will be added to this list.

Select to enable or disable IP filter in Status option, the default is “Enabled”. Then enter a name for the rule in the Name blank, for easier identification later. Click **Clear** button to delete the entered name. Next enter the MAC address of the computer on the LAN (Local Area Network) side.

You may read the DHCP client's host name and MAC address listed from DHCP Client drop-down menu. Select the client computer, which you want to add on the MAC filter list and then

click Apply button. Or you may click **Clone** to automatically add computer's MAC address to the MAC Address section.

Click the **Apply** button to enter the rule into the **MAC Filters List** and restart the router.

Directory	Configuration and Read-only Menus
IP Filters	This radio button selects the IP address filter rule entry page, which will be displayed when you click on it.
MAC Filters	This radio button selects the MAC address filter rule entry page, which will be displayed when you click on it.
URL Blocking	This radio button selects the URL filter rule entry page, which will be displayed when you click on it.
Domain Blocking	This radio button selects the Domain name filter rule entry page, which will be displayed when you click on it.
Status	This set of radio buttons allows you to enable or disable this rule.
URL Address	You can enter a group of keywords that if found in any Universal Resource Locator (URL), this rule will apply and access to the web site will be denied.

To remove any rule from the **MAC Filters List**, click on the trashcan icon for set you want to delete.

To edit any previously entered MAC filter rule, click on the Note pad icon.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Outbound or Inbound Filters List with the new settings. The UT-300R2 must

save the new settings and reboot before the new rules are applied.

Configuring a Filter Rule-URL Blocking

You can limit access to the WAN from PCs on your LAN, or limit access from the WAN to your LAN using filter rules that can be configured on your UT-300R2 ADSL router. The UT-300R2 router will examine incoming and outgoing packets to determine if they meet the requirements you specify in the Filter rule, and then either **Allow** or **Deny** access based upon the rule you have configured. These rules can be based on IP addresses, MAC addresses, URLs, Domain names, and TCP/UDP port numbers. In addition, you can specify a rule to apply to packets from your LAN to the WAN (Internet), from the WAN to your LAN, or both.

To configure a filter rule, click on the **Filter** button under the **Advanced** tab. This will open the **Filters** page, as shown below.

Figure 23 Filters Configuration Menu – URL Blocking

The screenshot shows a web interface for configuring filters. At the top, the title is "Filters" with a subtitle "Filters are used to allow or deny LAN users from accessing the Internet." Below this is a table with four radio button options: IP Filters, MAC Filters, URL Blocking (selected), and Domain Blocking. Underneath is a section titled "URL Blocking" with the instruction "Block those URLs which contain keywords listed below." This section contains a "Status" field with "Enabled" (selected) and "Disabled" options, and a "URL Address" input field. At the bottom of this section are "Apply", "Cancel", and "Help" buttons. The final section is titled "URLs Blocking List" and contains a table with a header "URL Address" and an empty cell.

Filters	
Filters are used to allow or deny LAN users from accessing the Internet.	
<input type="radio"/> IP Filters	<input checked="" type="radio"/> URL Blocking
<input type="radio"/> MAC Filters	<input type="radio"/> Domain Blocking

URL Blocking
Block those URLs which contain keywords listed below.

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
URL Address	<input type="text"/>

URLs Blocking List

URL Address

The first page allows you to enter an IP address, or range of IP addresses to form the basis of a filter rule for the UT-300R2 router. The **Filters** page will change when you select one of the other radio buttons (**MAC Filters**, **URL Blocking**, or **Domain Blocking**) to allow you to enter the appropriate information for other filter rule types, as shown below.

Previously entered or default URL Blocking rules are listed in the **URLs Blocking List** at the bottom of the page. When you configure an additional URL blocking rule and click the **Apply** button, the new rule will be added to this list.

Click the **Apply** button to enter the rule into the **URLs Blocking List** and restart the router.

Directory	Configuration and Read-only Menus
IP Filters	This radio button selects the IP address filter rule entry page, which will be displayed when you click on it.
MAC Filters	This radio button selects the MAC address filter rule entry page, which will be displayed when you click on it.
URL Blocking	This radio button selects the URL filter rule entry page, which will be displayed when you click on it.
Domain Blocking	This radio button selects the Domain name filter rule entry page, which will be displayed when you click on it.
Status	This set of radio buttons allows you to enable or disable this rule.
URL Address	You can enter a group of keywords that if found in any Universal Resource Locator (URL), this rule will apply and access to the web site will be denied.

To remove any rule from the **URLs Blocking List**, click on the trashcan icon for set you want to delete.

To edit any previously entered URL blocking rule, click on the Note pad icon.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Outbound or Inbound Filters List with the new settings. The UT-300R2 must save the new settings and reboot before the new rules are applied.

Configuring a Filter Rule-Domain Blocking

You can limit access to the WAN from PCs on your LAN, or limit access from the WAN to your LAN using filter rules that can be configured on your UT-300R2 ADSL router. The UT-300R2 router will examine incoming and outgoing packets to determine if they meet the requirements you specify in the Filter rule, and then either **Allow** or **Deny** access based upon the rule you have configured. These rules can be based on IP addresses, MAC addresses, URLs, Domain names, and TCP/UDP port numbers. In addition, you can specify a rule to apply to packets from your LAN to the WAN (Internet), from the WAN to your LAN, or both.

To configure a filter rule, click on the **Filter** button under the **Advanced** tab. This will open the **Filters** page, as shown below.

Figure 24 Filters Configuration Menu – Domain Blocking

Filters

Filters are used to allow or deny LAN users from accessing the Internet.

<input type="radio"/> IP Filters	<input type="radio"/> URL Blocking
<input type="radio"/> MAC Filters	<input checked="" type="radio"/> Domain Blocking

Domain Blocking

Disabled Domain Blocking

Allow users to access all domains except "Blocked Domains"

Deny users to access all domains except "Permitted Domains"

Domain Name Permitted Blocked

Permitted Domains List

Domain Name	
-------------	--

Blocked Domains List

Domain Name	
-------------	--

The first page allows you to enter an IP address, or range of IP addresses to form the basis of a filter rule for the UT-300R2 router. The **Filters** page will change when you select one of the other radio buttons (**MAC Filters**, **URL Blocking**, or **Domain Blocking**) to allow you to enter the appropriate information for other filter rule types, as shown below.

Previously entered or default Domain Blocking rules are listed in the **Permitted Domains List** or the **Blocked Domains List** at the bottom of the page. When you configure an additional Domain blocking rule and click the **Apply** button, the new rule will be added to this list.

Click the **Apply** button to enter the rule into the appropriate list and restart the router.

Directory	Configuration and Read-only Menus
IP Filters	This radio button selects the IP address filter rule entry page, which will be displayed when you click on it.
MAC Filters	This radio button selects the MAC address filter rule entry page, which will be displayed when you click on it.
URL Blocking	This radio button selects the URL filter rule entry page, which will be displayed when you click on it.
Domain Blocking	This radio button selects the Domain name filter rule entry page, which will be displayed when you click on it.
Disabled Domain Blocking	This set of radio buttons allows you to disable this rule.
Allow	Click this radio button to allow access all domains except the Blocked Domains.
Deny	Click this radio button to allow access all domains except the Permitted Domains.
Domain Name	Enter the Domain name you want this rule to apply to here. Click the Permitted radio button if you want to allow access to this domain. Click the Blocked radio button if you want to deny access to this domain.

To remove any rule from the corresponding list, click on the trashcan icon for set you want to delete.

To edit any previously entered Domain blocking rule, click on the Note pad icon.

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Outbound or

Inbound Filters List with the new settings. The UT-300R2 must save the new settings and reboot before the new rules are applied.

Firewall

The Firewall Configuration menu allows the UT-300R2 to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection that can be enabled on the UT-300R2, as well as filtering for specific packet types sometimes used by hackers.

Figure 25 Firewall Configuration Menu

Firewall Configuration	
Black List Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Duration	<input type="text" value="10"/> Minute
Use Attack Protection	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Use Dos Protection	<input type="radio"/> Allow <input checked="" type="radio"/> Deny
Max Tcp Open Handshaking Count	<input type="text" value="100"/>
Max ICMP Count	<input type="text" value="100"/>
Max Host Count	<input type="text" value="30"/>

Under **Black List Status** you can choose to **Enable** or **Disable** protection against a basket of attack and scan types included as **Attack Protection**. When Attack Protection is enabled, it will

create a firewall policy to protect your network against the following attack types and port scans:

Attacks	Port Scans	
Ping of Death Attack	Fragmentation Scan	Null Scan
Tear Drop Attack	UDP Scan	RST Scan
IP Spoofing Attack	ICMP Scan	SYNACK Scan
Smurf Attack	TCP Session Scan	FIN Scan
Land Attack	Xmas Scan	ACK Scan

You can also choose to **Enable** or **Disable** protection against various denial-of-service type attacks with the **DOS Protection** option.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.

The Service Filtering options allow you to block FTP, Telnet or response to Pings from the external network. Check the category you want to block to enable filtering of that type of packet.

When you have selected the desired Firewall policies, click the **Apply** button to enforce the policies. Remember to save any configuration changes.

DMZ

Click on the DMZ menu button to display the DMZ menu. If your computer cannot run Internet applications properly with the device, then you can enable this option to allow the computer accessing the unrestricted Internet. Enter the IP address of the computer as a DMZ (Demilitarized Zone) host. Adding the computer to the DMZ may expose it under insecurity risk; thus suggest not using this option unless no other alternatives.

User can select to enable or disable the UPNP Settings and VPN Pass-Through in this page; the default settings are both Enabled.

Figure 26 DMZ menu

The screenshot shows a configuration page with three main sections: DMZ, UPNP Settings, and VPN Pass-Through. Each section has a table for configuration options.

DMZ	
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IP Address	192 . 168 . 1 . <input type="text" value="0"/>

UPNP Settings	
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

VPN Pass-Through
Allows VPN connections to work through the ADSL Router.

PPTP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPSec	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

At the bottom of the page are three buttons: **Apply**, **Cancel**, and **Help**.

DDNS

The UT-300R2 supports Dynamic DNS used to share your IP address that is assigned by your ISP, dynamically. Since your ISP assigns an IP address that changes, if you want PCs from the WAN (Internet) to be able to find servers on your LAN, you can establish an account with a DDNS service provider. The Dynamic DNS service updates your IP address – as it is changed and assigned by your ISP – and then updates a link between your new IP address and an existing URL. In this way, if a user on the Internet types in your URL, then that user's PC will still be able to find your web site, even though your IP address has changed.

Figure 27 DDNS menu

DDNS	
Enabled DDNS	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Service Provider	www.dyndns.org ▼
Host Name	UTStarCom
User Name	admin
Password	•••••


You must establish an account with one of the supported DDNS service providers to use this feature.

RIP

Figure 28 RIP menu

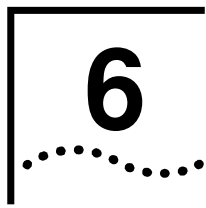
RIP

Interface Name	rfc1483-0
RIP 1 Received	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RIP 1 Send	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RIP 2 Received	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RIP 2 Send	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Send MultiCast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Interface Name	RIP 1 Received	RIP 1 Send	RIP 2 Received	RIP 2 Send	Send MultiCast	Edit
rfc1483-0	Disabled	Disabled	Disabled	Disabled	Disabled	

RIP can be enabled on any existing WAN or LAN interfaces. It may be specified to receive RIP requests and reply to them, it can be specified to send RIP queries, or to both receive and send RIP packets. Furthermore, the RIP version can be specified. The table below lists the parameters that can be specified for the pull-down RIP menus. Click the **Apply** button to setup RIP as specified.

Current RIP configurations cannot be edited. To remove a RIP configuration, click on the trashcan icon for the set. Remember to save the configuration changes.



Tools

Click the **Tools** tab to reveal the menu buttons for various functions located in this directory. These menus are used to change the system password used to access the web manager, to save or load UT-300R2 configuration settings, upgrade the device firmware, save current configuration settings, restore default settings, and to perform miscellaneous actions such as performing Ping tests. These menus are described below.

Administrator's Settings

Click the Administrator of Tools to set the administrator's setting. Administrator has read/write ability on the web page and can make some changes. You can change the Admin account password here for personal security. To change the password used to access the UT-300R2's web manager, Type the a new password and confirm the password to be certain you have typed it correctly. Click the **Apply** button to activate the new password.

Figure 29 Administrator Settings Menu

Administrator Settings

Please change the administrator account password for personal security and privacy. You may change it by entering a new password.

New Password	<input type="password" value="••••••••"/>
Confirm Password	<input type="password" value="••••••••"/>

Block WAN Ping

When you 'Block WAN Ping', you are causing the public WAN IP address on the ADSL Router to not respond to ping commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Discard PING from WAN side	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
-----------------------------------	---

Remote Management

Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
IP Address	<input type="text" value="*"/>
Port	8080 <input type="button" value="v"/>

Configure System Time

Use the Time menu to configure the UT-300R2's system time manually or from an SNTP server or your computer's system clock.

Figure 30 Time Settings Menu

Time	
Set the UT-300R2 system time.	
Date	2002/01/01
Time	00:53:17
Time Mode	<input type="radio"/> Use NTP Server <input checked="" type="radio"/> Set time Manually <input type="radio"/> Use PC Time
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
Default NTP Server	62 , 119 , 40 , 99
Set the Time	Year 2002 Month Jan Day 01
	Hour 00 Minute 00 Second 00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

If you opt to use the Automatic option you must have an IP address of an available SNTP server. Date settings use the format Year/Month/Date, Time settings use the format Hour (24 hour clock)/ Minute/ Second.

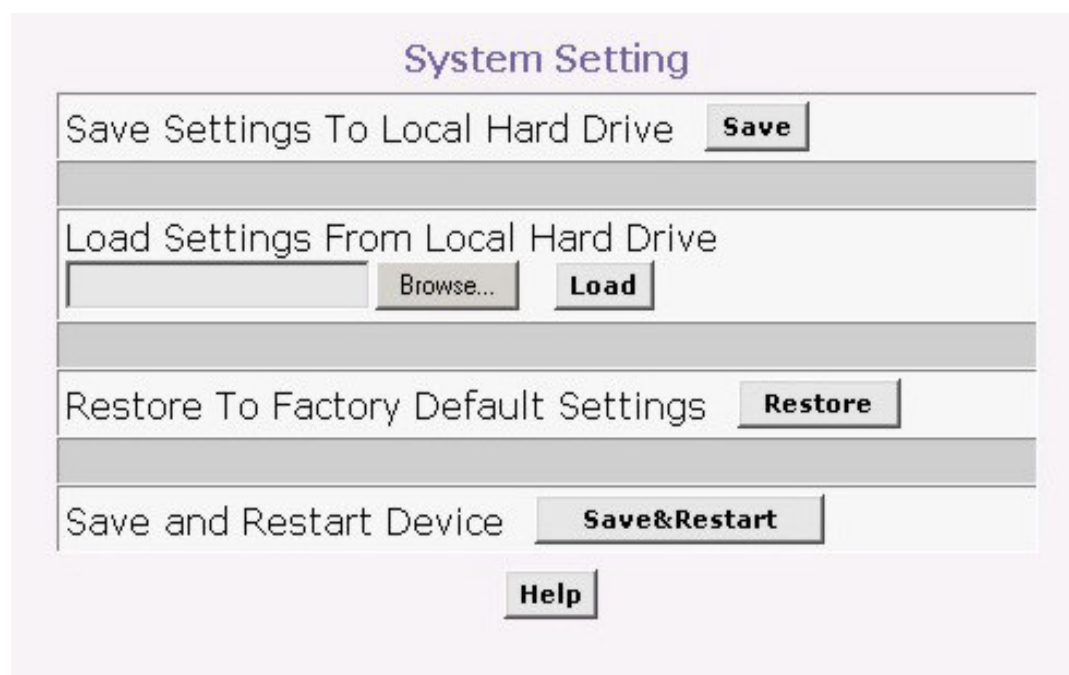
Click the **Apply** to set the Date and Time settings.

Save UT-300R2 Configuration Settings

When you have completed configuration of the UT-300R2, make sure you save the current configuration settings to flash memory or risk losing the settings. To save the current configuration settings, click the **Misc.** menu button to view the **Miscellaneous Configuration** menu and click the **Save and Reboot** button. The current settings will be saved to NV-RAM and the system will restart. Do not turn off the UT-300R2 during

this process. It should take about two minutes to complete. After restarting, it is a good idea to backup the UT-300R2 configuration file to your computer. See the instructions below to save configuration files to your PC.

Figure 31 Miscellaneous Configuration Menu



Other functions available in this menu are a Ping test and IGMP enable/disable.

Save Configuration File to PC

Once you have configured the UT-300R2 to your satisfaction, it is a good idea to back up the configuration file to your computer. Use the System Setting menu to save the existing configuration file to the hard drive of the system you are using to access the web manager. To save the system configuration file to your computer, click the **Save** button. You will be prompted to select

a location on your computer to put the file. The file type is .cfg and may be named anything you wish.

Load Saved Configuration Files

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Or type the full path and file name of the .cfg file in the space provided. Click the **Load** button to begin transferring and loading the .cfg file to the UT-300R2. Confirm that you want to load the file when prompted and the process is completed automatically. The UT-300R2 will reboot and begin operating with the configuration settings that have just been loaded.

Figure 32 System Settings

The screenshot displays a web-based interface titled "System Setting". It contains four main sections, each with a button:

- Save Settings To Local Hard Drive** with a **Save** button.
- Load Settings From Local Hard Drive** with a text input field, a **Browse...** button, and a **Load** button.
- Restore To Factory Default Settings** with a **Restore** button.
- Save and Restart Device** with a **Save&Restart** button.

A **Help** button is located at the bottom center of the interface.

Restore Factory Default Settings

To reset the UT-300R2 to its factory default settings, click the **Restore** button. You will be prompted to confirm your decision to reset the UT-300R2. The UT-300R2 will reboot with the factory default settings including IP settings.

Firmware Update

Note: Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the UT-300R2's configuration settings before upgrading the firmware.

Use the Firmware Upgrade menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System Settings menu described above.

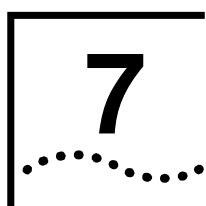
Use the Firmware Upgrade menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System Settings menu described above.

Figure 33 Firmware Upgrade

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the UT-300R2 automatically.

Please note that firmware version will be changed depend on different

Software and it shows on Figure 33.



UT-300R2 Status Information

Use the various read-only menus to view system information and monitor performance.

Log

The log file keeps record of the events and activities occurring on the device. It can display up to 256 events. The latest activities will overwrite the outdated ones. When the device is rebooted, the logs are automatically cleared.

Figure 34 View Log



The log menu buttons in this function as follow:

First Page	Display the first page of the log.
Last Page	Display the last page of the log.
Previous	Moves back one log page.
Next	Moves forward one log page.
Clear Log	Clears the logs completely.
Save Log	Save log file to your hard drive.

Traffic Statistics

The device keeps statistic of the data traffic that it handles. You are able to read the amount of Receive and Transmit packets that pass through the device on the ADSL interface or Ethernet interface. Click the **Refresh** button to update the counters and the **Reset** button to clear the counters. The traffic counter will reset when the device is rebooted.

Figure 35 Traffic Statistics

Traffic Statistics
Traffic Statistics display Receive and Transmit packets passing through the ADSL Router

	Receive	Transmit
ADSL	19691 Packets	19691 Packets
LAN	19691 Packets	816 Packets

[Refresh](#) [Reset](#) [Help](#)

Diagnostics

The UT-300R2 has a diagnostic feature that allows you to determine the relative quality of the link between your LAN and the WAN. Click on the Submit button to conduct this test.

Figure 36 Diagnostics

Diagnostics

This page performs system Diagnostics on UT-300R2

PVC Number

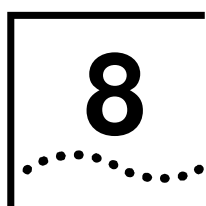
Modem Connection Test	
Testing Ethernet connection	PASS
Testing ADSL line for sync	UNKNOW
Testing Ethernet connection to ATM	UNKNOW

ATM Connection Test	
Testing ATM OAM segment ping	UNKNOW
Testing_ATM OAM end to end ping	UNKNOW

Ping Test

Ping Test is used to send 'Ping' packets to test if a computer is on the internet.

Host Name or IP address	<input type="text"/>	<input type="button" value="Ping"/>
Ping Result		



Attachments

Technical Specifications

Hardware	
One ADSL port	RJ-11, inner pair (pin 2,3)
Standard Compliance	ADSL Standards: ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) AnnexA ITU G.992.2 (G.lite) Annex A ITU G.994.1 (G.hs)
	ADSL2 Standards: ITU G.992.3 (G.dmt.bis) Annex A ITU G.992.4 (G.lite.bis) Annex A
	ADSL2+ Standards: ITU G.992.5 Annex A
Performance	Pass DSL Forum TR-048 Performance Criteria.
Fast Ethernet Switch port	RJ-45, 10/100Mbps, MDI
Standard Compliance	IEEE802.3, IEEE802.3u
External Linear Power Adapter	Input: per region requirement. Output: 9V AC, 1A
Reset Button	Reset to factory default

Safety and Environmental	
CSA International Mark	Including CSA950, UL1950, IEC60950, EN60950
EMC Certification	FCC part15 class B
PTT Test	FCC part68
Operating Temperature	0 °C to 40 °C
Storage Temperature	-20 °C to 70 °C
Operating Humidity Range	5% to 95% Non-condensing
Software Feature	Description
Transparent bridging	
Spanning Tree	IEEE 802.1d
Dynamic Learning	Up to 1000 MAC addresses
Encapsulation	Bridged/Routed Ethernet over ATM (RFC1483/2684)
	Classical IP over ATM (RFC1577)
IPv4	TCP/UDP ARP RARP ICMP
IP Routing	RIP v1 (RFC 1058), RIP v2 (RFC 1389)
IP Static Routing	
DHCP	DHCP Server (RFC2131)
	DHCP Client (RFC2131)
Multiple PVC	Support 8 PVCs

ATM Cell format	ITU-T Rec. I.361
OAM support	F4/F5 Loopback
ATM QoS (Traffic Shaping)	UBR, CBR, VBR-rt, VBR-nrt
Point-to-Point Protocol	RFC1661
PPP over ATM	RFC2364
PPP over Ethernet	RFC2516
User Authentication	PAP (RFC 1334), CHAP (RFC 1994)
VPN Pass Through	IPSec/L2TP/PPTP pass through
IP Filtering	IP Filtering
	MAC Filtering
	URL Filtering
	Domain Blocking
SPI	Detection of Known Attacks
Administration	Username/Password control for Telnet, WEB configuration
HTTP Server	For WEB-based management
Telnet	Through LAN with user name/password
TFTP	For firmware upgrade
SNMP v.1 and v.2c	MIB II (RFC 1213)
Remote Management	Management from WAN

Glossary

ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DSLAM	Digital Subscriber Line Access Multiplexer
IEEE	Institute of Electrical and Electronics Engineering
LAN	Local Area Network
MAC	Media Access Control
OAM	Operation, Administration, and maintenance
POTS	Plain Old Telephone Service
PPPoE	PPP over Ethernet
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection
QoS	Quality of Service
SSID	Service Set Identifier
VoIP	Voice over Internet Protocol

- WAN** Wide Area Network
- WEP** Wired Equivalent Privacy
- WLAN** Wireless Local Area Network



UTStarcom, Inc. USA
1275 Harbor Bay Parkway Alameda, CA 94502, USA
Tel: 510-864-8800 Fax: 510-864-8802
<http://www.utstar.com>