AmbiCom

Wireless Access Router with 4-port switch & Wireless Presentation Gateway

User Manual

Version 1.10

Dec 15, 2002

1 Introduction

Thank you for purchasing your AmbiCom **Wireless Access Router** model ***WL1100C-AR***. The AmbiCom Wireless Access Router / Presentation Gateway is developed to be as the mediator between the different LAN interfaces, which includes Wide Area Network (WAN), Local Area Network (LAN), and Wireless Local-Area Network (WLAN). AmbiCom Wireless Access Router connects the Wide Area Network with the Local Area Network or Wireless Network and extends the service platform to multiple end points around the home or small office. The AmbiCom Wireless Access Router System is a high performance and low cost solution for home users to share an Internet connection with DHCP and NAT capabilities. Data transfer rate on WAN and LAN operates at 10/100 Mbps, and Wireless LAN operate at 11 Mbps. AmbiCom Wireless Access Router acts as the only externally known Internet Gateway on your Local-Area Network and serves as an Internet firewall against outside intruders. The Gateway can also be configured to filter internal users' access to the Internet.

The advanced **Wireless Presentation Gateway** model ***WL1100C-PG*** includes all the powerful functions of Wireless Access Router and also the capability to allow all wired or wireless clients to share one single VGA display/projector output. In the event of meeting, seminar, conference or classroom, every participant can use one single projector without the hassle to switch video cables or to setup connections. The bundled AmbiCom high performance Presentation Client Utility will efficiently deliver your screen to the Gateway (screen video over IP). With AmbiCom Wireless Presentation Gateway, wired and wireless clients can share precious resources such as Internet connection and VGA video/projector display simultaneously.

The package you have received should contain the following items:

- One AmbiCom Wireless Access Router (or Presentation Gateway)
- One AC power adapter
- User's Reference Manual
- Registration and Warranty Card

2 Features

The AmbiCom Wireless Access Router supports TCP, UDP, IP, IPX/SPX, PPPoE, ARP, SNAP, SNMP, and other protocols.

- Connects to a Broadband Cable/DSL Modem, or 10/100 Mbps Ethernet Backbone
- 4-Port 10/100 Ethernet Switch with Uplink auto-sensing
- Fast 11Mbps wireless networking, fully compatible with IEEE 802.11b standard
- Compliant with WiFi specification
- Long operating range for Wireless connection
- Standard 64-Bit or 128-Bit WEP encryption
- NAT Firewall protection from outside intruders
- Easy Installation and Management thru 'AP Configuration Wizard'
- Virtual Server support for user access public services such as: ftp server, telnet etc
- Web based configuration and management
- Support SNMP management
- Competitive fast and reliable performance
- DHCP Server for multiple LAN users to get IP Address automatically
- Advanced security management functions for Port filtering, MAC Address filtering, IP Address filtering, and DMZ hosting
- Provide multiple clients the wireless connectivity to one VGA screen or VGA Projector (WL1100C-PG model)
- Wired Ethernet clients can also be connected to the same VGA Projector (WL1100C-PG model)
- Allow displaying presentation screen on the same projector without cable plug-unplug (WL1100C-PG model)
- Free Technical Support
- 1-Year Limited Warranty

3 Before connecting the hardware

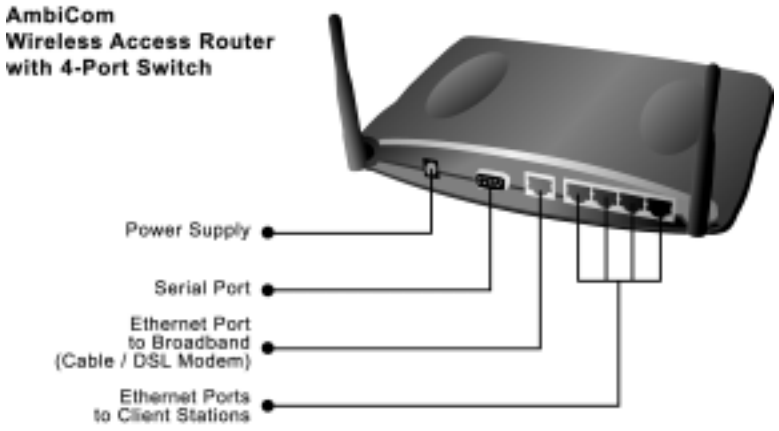
Before you connect your router and PCs, it is important that you have all information about your network settings from your ISP.

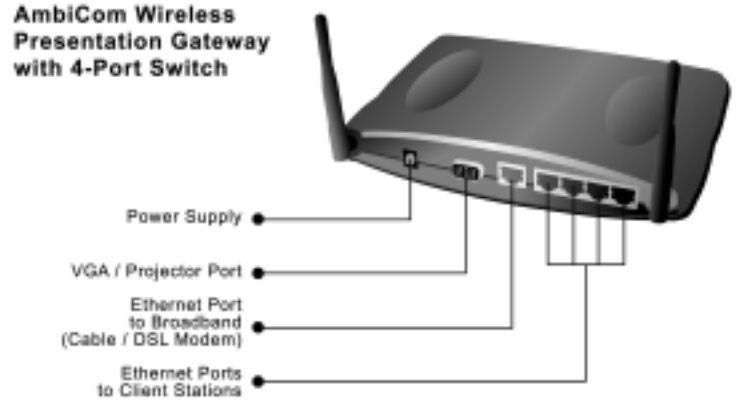
- ***IP address***: Is it dynamically assigned or Static IP connection?
- ***IP subnet mask***: If Static IP is assigned, it will be needed.
- ***DNS IP address***: If Static IP is assigned, it will be needed.
- ***Computer name***: What are the computer and group names? (required by some ISP)

If you are using the PPPoE protocol that usually can be found in most DSL modem connection, you will need to know:

- ***PPPoE Username***
- ***PPPoE Password***

If the network setting information is ready, you can start with the outlooks of the ***WL1100C-AR Access Router*** and ***WL1100C-PG Presentation Gateway***.





4 Connecting the Router

Once you have all the information you need you can start to connect your hardware together. Follow the steps:

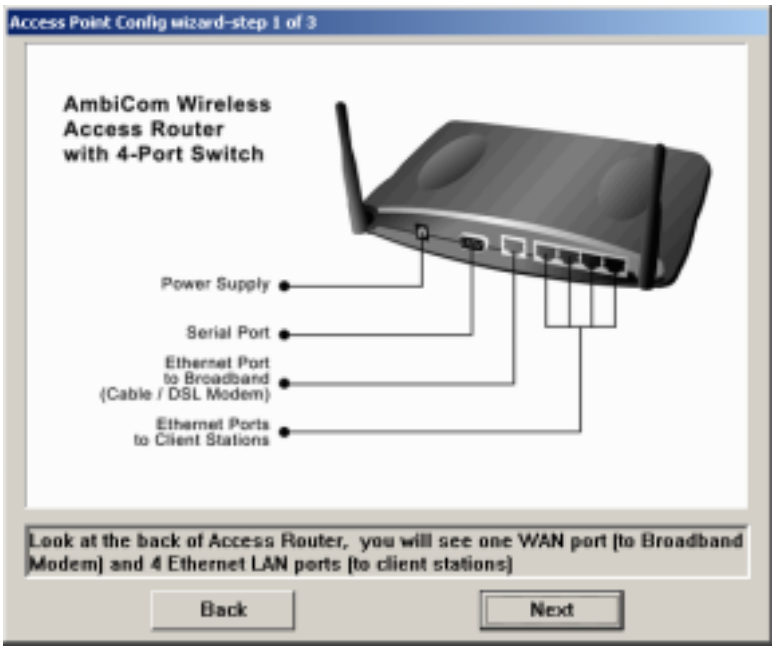
1. Turn off every system down, including your Cable/DSL modem, PCs, and Access Router.
2. Connect an Ethernet cable from your Cable/DSL modem Ethernet port to Access Router WAN port.
3. Connect another Ethernet cable from your PC Ethernet port to one of the LAN ports of Access Router.
4. If you use a Wireless LAN card, you can skip the LAN port cable connection. You can connect wirelessly without cabling later.
5. Connect the Power adapter to Access Router's Power port. The 'Diagnostic' LED will light for a few seconds while the Access Router goes through its internal diagnostic test. It will go off when the test is complete and ready.
6. Power on your Cable/DSL modem and make sure WAN 'Link' LED is on.
7. Press the reset button on the back of the Access Router and wait for the 'Diagnostic' LED goes off.
8. Power on your PC and/or your Wireless card PC.
9. The Access Router is now connected! You can insert the bundled CD and install AP Configuration Wizard on your PCs.

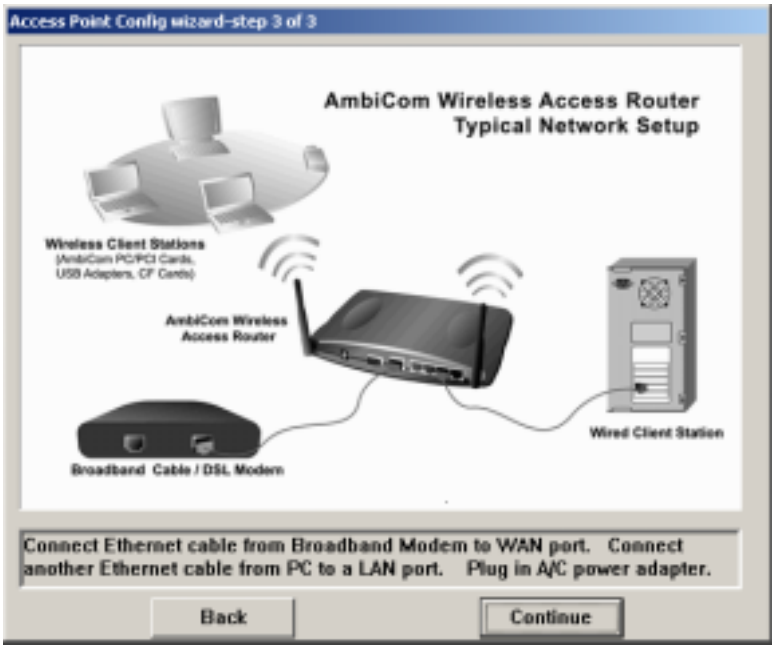
Typical setup for WL1100C-AR Access Router:

Typical setup for WL1100C-PG Presentation Gateway:

5 AP Configuration Wizard

AmbiCom WL1100C-AR and WL1100C-PG provides an AP Configuration Wizard to connect to the Access Router with ease. After WL1100C-AR(PG) utility package installed, from ***Start*** menu, click on ***WL1100C-AR (PG) Utility***, and select ***AP Configuration Wizard***. The first three screens are the step that you can follow to connect the hardware and setup the network.





If you set up the network environment according to the steps, your network should be ready. After finishing step 3, 'AP Configuration Wizard' will automatically search for the Access Router and bring up your default browser (Internet Explorer or Netscape) to connect with the Access Router and start a WEB-based configuration session.

6 WEB-based Configuration

The easiest way to connect to WL1100C-AR(PG) Wireless Access Router is to start AmbiCom "AP Configuration Wizard" which comes with the installation CD. After you install the WL1100C-AR(PG) utility, you can find the utility in: ***Start -> WL1100C-AR (PG) Utility -> AP Configuration Wizard.*** The wizard will guide you step by step the connection and cabling, then it will bring up the default browser to connect to the Access Router.

If you choose not to use the wizard, in order to connect with WL1100C-AR(PG) Wireless Access Router WEB configuration interface, you will have to know its IP address. The factory default is usually 192.168.0.1. You can start Internet Explore or Netscape and enter the URL: http://192.168.0.1 to reach WL1100C-AR(PG) WEB-based configuration interface. You will be asked for username and password in the first login screen.

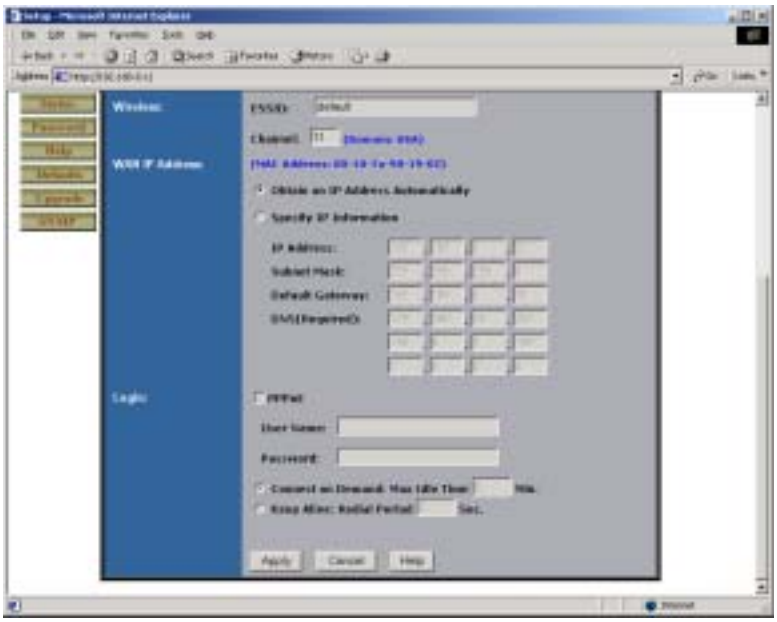
- **Login screen**

The default user name is ***admin*** and password is ***default***. You should change the password right away and keep it for administrators only.

- **Setup**

The Basic Setup screen is the first screen you see when you access the Gateway by typing its IP address into your web browser location window. You may configure the device and get it working properly using only the settings on this screen. For most users, all you need to do is give the device a name and select the 'Obtain an IP Address Automatically' option. Some ISPs (Internet Service Providers) will require that you enter the DNS information. These settings can be obtained from your ISP if they are required. After you have configured these settings, move on with the installation by setting a password or DHCP server function of the Gateway.

- Host Name: Give your device a name. This entry is necessary for some ISPs.
- Domain Name: Specify your domain. This entry is necessary for some ISPs.
- Firmware Version: This entry shows the version of the firmware you are using.
- LAN IP Address: This is the IP Address and Subnet Mask of the Gateway to be seen by internal LAN users in your home or office. The default value is 192.168.0.1 for IP and 255.255.255.0 for Subnet Mask.
- Wireless SSID: This is the ESSID of the beacons that the Wireless LAN APwill broadcast.
- Channel: This is the channel number of WLAN AP will set. The available channels are depending on your regional location. Northern America including Canada should be from channel 1 to 11.
- WAN IP Address: This is the IP Address and Subnet Mask of the Gateway to be seen externally on the Internet. If your ISP is running a DHCP server, check the 'Obtain an IP Address Automatically' option. Your ISP will assign an IP address for you. If you have a static, or fixed IP address, Subnet Mask, and Gateway setting, check the check box in the 'Specify an IP address' option.



- DNS (Domain Name Server): Your ISP will provide you with at least on DNS IP address. Enter IP address here if you choose 'Specify an IP address' option.
- PPPoE: You will need to call your ISP to find whether PPPoE should be enabled or not. If yes, you will need to also fill both the 'User Name' and 'Password' fields that are provided by your ISP. The PPPoE connection will be disconnected if it is been idling for a period beyond the ***Max Idle Time*** setting. If you check the ***Keep Alive*** option, the AmbiCom Gateway will always try to keep the line alive.

For most users, the default values for the device should be satisfactory. The device can be used in most network scenarios without changing any of the settings. Some users will be required to enter additional information in order to connect to the Internet through an ISP or broadband (Cable/DSL modem connection) provider.

- **Wireless**

This page will lead you to change advanced parameters of Wireless LAN settings. It is strongly suggested that leave these parameters unchanged. Improper settings might leave your Wireless LAN unable to function normally. Click ‘Apply’ to save the data.

- Beacon Interval: The time interval between beacons to be generated.
- RTS Threshold: The packet size threshold to enable RTS/CTS handshaking.
- Fragmentation Threshold: The packet size threshold to split a packet into smaller ones.
- Basic Rates: The basic wireless speed rates.
- Supported Rates: The highest supported rates.
- Authentication Type: The type of authentication between the AP and a wireless client. Shared key authentication only is more restricted and secured when WEP is enabled.
- Click ‘Apply’ to save the data

- **WEP - Wireless Security Configuration**

By default, WEP encryption is disabled. Check WEP Enable to enable the wireless security. First, pick a WEP Key Length. You can then either type in an Passphrase and have the system generate a set of key for you by clicking 'Generate Key' button, or type in four keys yourself and select which key you want to use. Click 'Apply' to save the data.

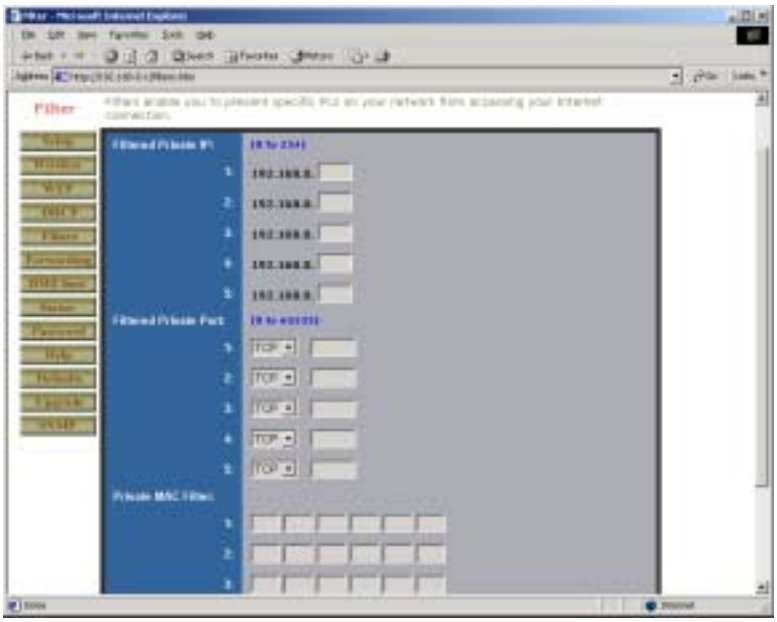
- **DHCP Setting**

The Gateway can be setup to be used as a DHCP (Dynamic Host Configuration Protocol) server on your network. A DHCP server assigns an available IP address to each computer on your network automatically. You must configure all the PCs on your LAN to connect to a DHCP server. Consult your operating system's documentation to learn how to do this.

If you do not want to use the Gateway's DHCP server function, you have to carefully configure the IP address, IP mask, and DNS setting on every computer on your network. Be careful not to assign the same IP Address to different computers.

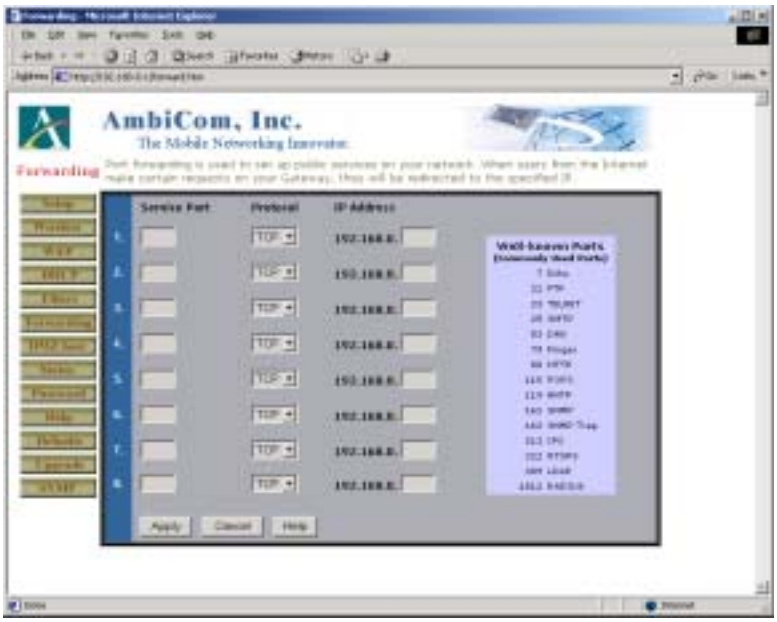
- ♦ Beginning IP Address: Enter a numerical value for the DHCP server to begin assigning addresses.
- ♦ Number of DHCP users: Enter the maximum number of computers that you want the DHCP server to assign IP addresses to.
- ♦ Click 'Apply' to save the data

- **Filters**



- By using the Filters screen, you can configure the Gateway to block specific internal users from accessing the Internet. You can setup different filters for different users based on their IP addresses or their network Port number.
- Enter the IP address that you want to filter into the 'Filtered Private IP' fields. User with an IP address you filtered will not be able to access the Internet.
- You can filter users by entering their network port number. Select the protocols and enter the port numbers into the 'Filtered Private Port' fields. User with a port number you filtered will not be able to access the Internet.
- You can also filter users by entering their physical address. Enter MAC addresses that you want to filter into the 'Private MAC Filter' fields. User with the MAC address you filtered will not be able to access the Internet.
- Click 'Apply' button to save any change

- **Forwarding**



Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the router can forward those requests to specific computers that are equipped to handle the requests. For example, if you set the port number 80 (HTTP) to be forwarded to the IP address 192.168.0.2, the all HTTP requests from outside users will be forwarded to 192.168.0.2.

You may use this function to establish a Web Server or FTP Server via an IP Gateway for Internet users to access. Be sure that you enter a valid IP Address; you may need to establish static IP address with your Internet provider in order to properly run an Internet Server. For added security, Internet users will be able to communicate with server, but they will not actually be connected. The packets will simply be forwarded through the router.

- Enter the port numbers and select the protocol used by the server as well as the IP address of the server that you want to Internet users to be able to access.
- Configure as many entries as you would like until all of the link entries are filled.
- Click 'Apply' button to save the settings
- To disable the forwarded path to a server, just delete the port number and IP Address from the fields.
- Click 'Apply' button to save the settings

- **DMZ Host**

The DMZ Host setting can allow one local user to be exposed to the Internet. It's for local user who needs to setup special-purpose server such as Internet game or video-conferencing. To enable the DMZ Host setting, enter the IP address and click 'Apply' button. Make sure you need this option before you enable this setting. Any firewall protection of the local DMZ host will be disabled.

- **Status**

This screen provides the current status of the device. All of the information provided is read-only.

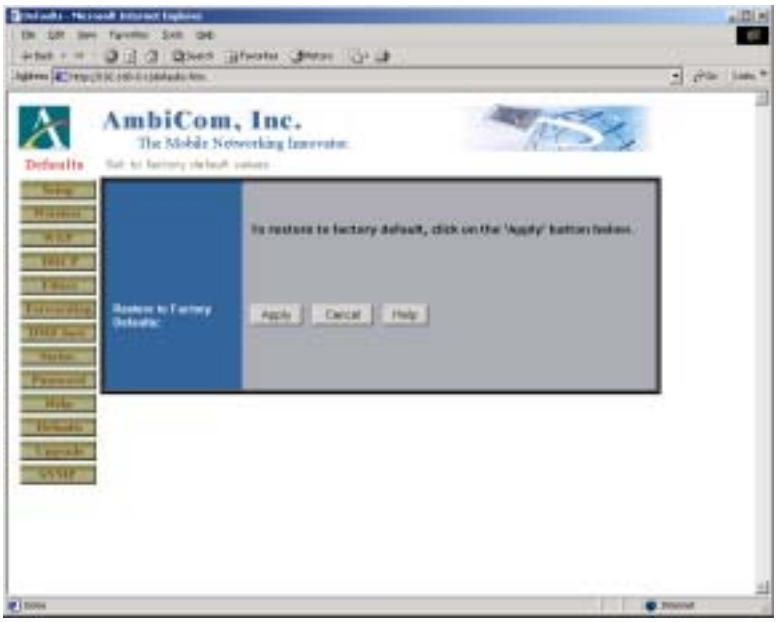
- Firmware Version: Shows the version of the firmware installed
- LAN MAC Address: Shows the MAC address.
- LAN IP Address: Shows the current IP address (seen by users on your internal home or office network).
- WAN MAC Address: Shows the MAC Address of the router (seen by external users on the Internet).
- WAN IP Address: Shows the IP Address of the router (seen by external users on the Internet).
- WAN Subnet Mask: Shows the Network Mask of the router (seen by external users on the Internet).
- WAN Default Gateway: Shows the default gateway of the Gateway system (seen by external users on the Internet).
- DNS IP Address: Shows the current IP Address of the Domain Name Server.

- **Password**

It is strongly recommended that you change the password for the router. When a password is set, users who try to access the router will be prompted to enter the router's password.

- ♦ Enter New Password: Enter a password. Your password must be less than 32 characters, and it cannot contain any spaces.
- ♦ Re-enter to Confirm: Re-enter the password for confirmation.
- ♦ Click 'Apply' to save the data.

- **Set to factory default**



Restore everything to factory default. After you click 'Apply' button, the system will be reset to the factory setting.

- **Upgrade**

WL1100C-AR(PG) provides an easy and safe way to upgrade your firmware. Click on the 'Browse' button will help you locate the firmware file. Once you find the file, click on 'Apply' to upload to firmware file to WL1100C-AR(PG). The whole process will take usually around 30 seconds. Once it's done, you will be asked to reset and restart the system.

- **SNMP**

AmbiCom WL1100C-AR and WL1100C-PG provides the advanced SNMP management option. By default it is disabled. You can enable it by click on the 'SNMP Agent Enable' check box.

- Get Community: Community string for GET operations.
- Set Community: Community string for SET operations.
- Trap Community: Community string for SNMP Trap operations.
- Trap Target: To specify where the SNMP Trap to be sent.
- System Name: A unique name for this system.
- System Location: Location information about this system.
- System Contact: Contact information about this system.

7 Wireless Presentation Gateway Client Utility

The Wireless Presentation Gateway comes with a client utility to be installed on each wired or wireless client that would like to share the video display/projector. The client utility will deliver your computer screen over IP protocol to the Presentation Gateway. The utility can be invoked from ***Start*** menu, click on ***WL1100C-AR (PG) Utility***, and select ***WL1100C-PG Presentation Client Utility.***

The first screen will display selectable menu items. Click on the 'Settings' to open the Presentation Gateway parameter settings.

Enter the IP address of Presentation Gateway (by default, it's 192.168.0.1). Enter the password if it had been set on the Presentation Gateway side. Enter the interval (in seconds) that the utility should deliver your computer screen to the Presentation Gateway. So for every that amount of time, the VGA port on the Presentation Gateway will refresh with your computer screen. Click on 'OK' to continue.

After setting up the parameters, click on 'Start!' button to start delivering your computer screen to the Presentation Gateway. Click on 'Stop!' to stop it.

8 Terminology

DHCP

DHCP stands for Dynamic Host Configuration Protocol. It is designed to ease configuration management of large networks by allowing the AmbiCom Gateway System to collect all the IP host configuration information. This includes IP address, name, gateway, and default servers. DHCP is a "client/server" protocol, meaning that machine with the DHCP database "serves" requests from DHCP clients. The clients typically initiate the transaction by requesting an IP address and perhaps other information from the server. The server looks up the client in its database, usually by the client's media address, and assigns the requested fields

NAT

NAT stands for Network Address Translation. NAT allows client IP hosts on a stub network connected to the Internet to access Internet hosts without having to obtain and assign "real" IP addresses for each host. It works by modifying the IP headers IP addresses and selected fields in upper layer protocol headers so that the hidden internal IP addresses are replaced with a "real" assigned IP address, which can safely traverse the Internet. Once the NAT Router is assigned at least 1 "real" IP address, up to 64 thousand IP client machines can share this address to simultaneously to access Internet hosts. This technology is based on Internet standards. NAT is described by RFC1631.

FILTER

AmbiCom Wireless Access Router supports Address and Protocol Filters. Address Filter supports MAC, IP, and Port Address Filter Manger. You can block any network traffics or packets by specifying physical MAC address, or logical IP or Port address. The Protocol filter help reduce the traffic based on functionality or protocol. For example, you may want to eliminate all Internet Control Message Protocol (ICMP) traffic, Domain Naming System (DNS) traffic, Open Shortest Path First (OSPF) traffic, Novell NetWare traffic, or Non-TCP/IP traffics.

DMZ

This is a feature that is included on AmbiCom routers. A DMZ allows a single computer on your LAN to expose ALL of its ports to the Internet. When doing this, the exposed computer is no longer 'behind' the firewall. The DMZ sits between the Internet and an internal network's line of defense, usually some combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web HTTP servers, FTP servers, SMTP (e-mail) servers and DNS servers.

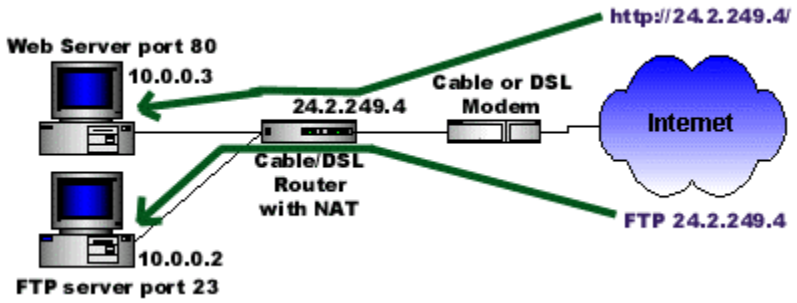
Ports

Applications running on TCP/IP open connections to other computers using something called ports. Ports allow multiple applications to reside on a single

computer - all talking TCP/IP. Ports are another set of numbers AFTER the standard IP address. Applications often hide these port numbers to reduce the complexity of TCP/IP. Example: web services (HTTP) reside on port 80 by default. To reach a web site, you could type http://www.sitename.com:80 into your browser. The number 80 is the default port number for the HTTP protocol so typing it is not necessary. There are 65535 available ports.

Port Forwarding

A broadband router or other NAT application (like ICS) creates a firewall between your internal network and the Internet. A firewall keeps unwanted traffic from the Internet away from your LAN computers. A 'tunnel' can be created through your firewall so that the computers on the Internet can communicate to one of the computers on your LAN on a single port. This is handy for running web servers, game servers, ftp servers, or even video conferencing. This is called port forwarding. One of your computers could run a web server (port 80) while another computer could run an FTP server (port 23) - both on the same IP address. Most applications work fine without configuration when making an outgoing connection. All applications need some kind of port forwarding when you need to act as a server to take incoming connections.



Port Forwarding vs. DMZ

A DMZ is far easier to set up than port forwarding but exposes your entire computer to the Internet. Sometimes TCP/IP applications require very specialized IP configurations that are difficult to set up or are not supported by your router. In this case, placing your computer in the DMZ is the only way to get the application working. Placing a computer in the DMZ should be considered 'temporary' because your firewall is no longer able to provide any security to it.

Port forwarding can sometimes be difficult to configure, but provides a relatively safe way of running a server from behind a firewall. Since only a single port (or small series of ports) is exposed to the Internet, the computer is easier to secure. Additionally, port forwarding allows you to run multiple kinds of servers from different computers on your LAN.

Many broadband routers have special port forwarding configuration screens for standard applications (FTP, WWW, Mail, etc) and special screens for custom applications.

Packet Inspection

To accomplish its connected sharing task, NAT routers do something called Packet Inspection. Part of this inspection process involves blocking unwanted and un-requested packets trying to reach your LAN computers. It can also involve forwarding 'wanted' packets to servers you might have running on 1your LAN.

Stateful Packet Inspection (SPI)

SPI is a little different than ordinary 'packet inspection'. The basic interpretation of SPI is that a router/firewall with SPI will protect you from more attacks than a router without SPI. SPI means that the router will look at a packet of information, examine it in some way, and determine what to do with it (beyond simple routing). SPI routers not only understand TCP/IP, they understand the kind of applications that are running on the protocol. This understanding allows the router to filter out advanced forms of attacks on the Internet like Denial of Service attacks.

Local IP settings

Allows user to modify the local IP settings. Most routers come configured to set your LAN up in the 192.168.0.x range. Routers that let you change at least the last two octets (192.168.x.x) are much more useful as your network becomes more complex. There is also a security benefit to changing your local IP settings from the default.

Virtual Private Network (VPN)

A VPN allows secure communication between computers or networks over a public network like the Internet.

9 Specifications

- **Product Name**:
  Wireless Access Router and 4-Port Switch,
  Wireless Presentation Gateway with Access Router and 4-Port Switch
- **Model Number**: WL1100C-AR, WL1100C-PG
- **WL1100C-PG VGA Port**: 1024 x 768 @ 256 color (60Hz)
- **Configuration Wizard OS support**: Windows 98/ME/2K/XP with a working wired/wireless network adapter and TCP/IP protocol installed
- **Standards**: IEEE 802.3u (10/100BaseTX), IEEE 802.11b (Wireless)
- **Protocol**: CSMA/CD, CSMA/CA
- **WAN Port**: One 10/100Mbps RJ-45 for Cable/DSL Modem Ethernet port
- **LAN Ports**: Four 10/100Mbps RJ-45 Switched Ports, Uplink auto-detect
- **Cabling Type**: UTP CAT 5 or better
- **RF Output Power**: 23 dBm – FCC, 20 dBm - CE
- **Wireless LAN Operating Range**:
  11 Mbps – 300m (980 ft.)/450m (1470 ft.)
  5.5 Mbps – 400m (1300 ft.)/600m (1960 ft.)
  2 Mbps – 500m (1640 ft.)/750m (2460 ft.)
  1 Mbps – 800m (2620 ft.)/1200m (3930 ft.)
- **LED**: Power, Status, WLAN Activity, 10/100 Link Speed, 10/100 Link/Activity
- **Dimensions**: 220 mm x 155 mm x 35 mm (8.6” x 6.1” x 1.4”)
- **Weight**: 0.6 kg (20.56 oz.)
- **Power**: External, 5V DC, 3A
- **Power Consumption**: 1.5A
- **Certification**: FCC, CE, WiFi Compliance
- **Operating Temp**: 0^{o}C to 40^{o}C (32^{0}F to 104^{o}F)
- **Storage Temp**: -20^{o}C to 70^{o}C (-4^{0}F to 158^{o}F)
- **Operating Humidity**: 10% to 85%, non-condensing
- **Storage Humidity**: 5% to 90%, non-condensing
- **Warranty**: 1-year Limited

]

Notice : The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

IMPORTANT NOTE: To comply with the FCC RF exposure compliance requirements, no change to the antenna or the device is permitted. Any change to the antenna or the device could result in the device exceeding the RF exposure requirements and void user's authority to operate the device. The antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other transmitter.

The Federal Communication Commission Radio Frequency Interference Statement includes the following paragraph:

The equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communication. However, there is no grantee that interference will not occur in a particular installation. If this equipment dose cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on , the user is encouraged to try to correct the interference by one or more of the following measures:

--Reorient or relocate the receiving antenna.
--Increase the separation between the equipment and receiver.
--Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
--Consult the dealer or an experienced radio/TV technician for help.

The user should not modify or change this equipment without written approval Form A m b e o n . Modification could void authority to use this equipment.