Wi-Fi Ethernet Client

T-316

User's Guide

Revision 1.2 February 18, 2003

www.gemtek-systems.com

Copyright

Notice

Gemtek Systems reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Gemtek Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Gemtek Systems.

Trademarks

The product described in this book is a licensed product of Gemtek Systems Holding BV.

Contents

Copyright 3
Notice 3
Trademarks........ 3

CONTENTS 4

ABOUT THIS GUIDE 5

Purpose 5
Prerequisite Skills and Knowledge 5
Conventions Used in this Document 5
Help Us to Provide Quality Documentation 5
Gemtek Systems Technical Support 5

CHAPTER 1 – INTRODUCTION 6

CHAPTER 2 – WIRELESS LAN BASICS 7

CHAPTER 3 – CONFIGURING THE WI-FI ETHERNET CLIENT 8

3.1 Overview 8
3.2 Connecting the Ethernet Client 9
3.3 Configuring the Network Connection 10
3.3.1 Information........ 11
3.3.2 Wireless Configuration........ 12
3.3.3 Security (part of the Wireless page) 13
3.3.4 Server Configuration 14
3.3.5 Stations........ 15
3.3.6 Administration 16
3.3.7 Help 17

CHAPTER 4 – TROUBLESHOOTING 18

CHAPTER 5 – TECHNICAL SPECIFICATIONS 19

CHAPTER 6 – GLOSSARY 20

About this Guide

Purpose

This document provides general product information, technical specifications and simplified installation and operational procedures of the E-810 Power-Over-Ethernet (PoE) 8-port Switch.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

!!!	Very important information. Failure to observe may result in damage.
!	Important information. Requires further user interaction.
i	Additional information. Helpful tips, but not required.
bold	Menu commands. Buttons and input fields are displayed in bold
`code`	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
`<value>`	Place holder for certain values, e.g. user inputs

Help Us to Provide Quality Documentation

If you should encounter any errors in this document or want to provide additional comments to improve the manual please send e-mail directly to: manuals@gemtek-systems.com

Gemtek Systems Technical Support

Having problems, please visit our online technical support @ http://www.gemtek-systems.com.

The site offers:

- The latest software, user documentation and product updates
- Frequently Asked Questions (FAQ)
- Direct contact to the Gemtek Systems support centers

Chapter 1 – Introduction

Thank you for purchasing the Gemtek Systems Wi-Fi Ethernet Client. This manual will assist you with the installation procedure.

The package you have received should contain the following items:

- T-316 Wi-Fi Ethernet Client
- Laptop display mounting clip
- Dual purpose cable (USB and Ethernet)
- User Guide
- CD containing the User Guide

Note: if anything is missing, please contact your vendor

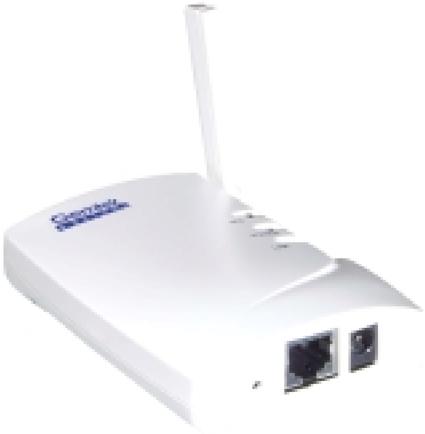


Figure 1.1 - T316 Wi-Fi Ethernet Client

Chapter 2 – Wireless LAN Basics

Wireless LAN (Local Area Networks) systems offer a great number of advantages over traditional, wired systems. Wireless LANs (WLANs) are more flexible, easier to set up and manage and often more cost effective than their wired equivalents. Using radio frequency (RF) technology, WLANs transmit and receive data using only the air as a medium, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable more mobile networks.

With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires.

Wireless LANs offer the following productivity, convenience and cost advantages over traditional wired networks:

Mobility

Wireless LAN systems can provide LAN users with access to real-time information anywhere within their organization. This mobility supports productivity and service opportunities not possible with wired networks.

Installation Speed and Simplicity

Installing a wireless LAN system can be fast and easy and eliminates the need to pull cables through walls and ceilings.

Installation Flexibility

Wireless technology allows the network to go where wires cannot go.

Reduced Cost-of-Ownership

While the initial investment required for wireless LAN hardware might be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs will be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, additions, and changes.

Scalability

Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer to full infrastructure networks, and also allow roaming over a broad area.

Chapter 3 – Configuring the Wi-Fi Ethernet Client

The following section will assist in installing the wireless LAN Adapter successfully. You will connect the T-316 Ethernet Client to your system, then set the appropriate networking parameters. The Gemtek Systems Ethernet Client eliminates the need to install drivers and for setting the network properties. It looks to the system like a normal wired connection to an Ethernet network.

3.1 Overview

Here are the steps you will be required to perform to establish your wireless network connection:

- Install the Access Point. An AP is required for Infrastructure (BSS – Basic Service Set) network mode.
- Connect the Ethernet Client (T-316).
- Set up the network connection, including WEP security.

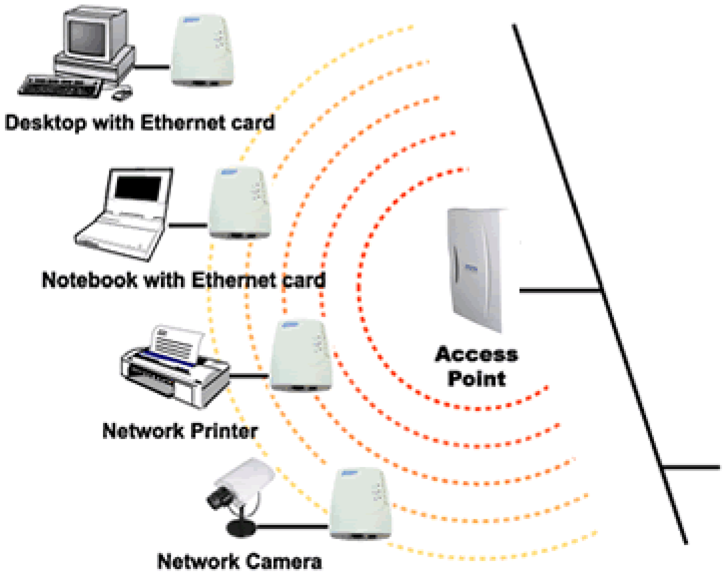


Figure 3.1 – Network Application Scheme

3.2 Connecting the Ethernet Client

1. (Optional) Mount T-316 Wi-Fi Ethernet Client to your laptop display using the enclosed mounting clip.
2. Insert the circular power and Ethernet plugs into the appropriate connectors on the T-316
3. Connect the power connector into a (powered) USB port.
4. Plug the Ethernet cable into the Ethernet connector (RJ45) on your system's Ethernet port.

There are three LED indicators on the front of the T-316: Activity (ACT), Power (POWER) and Link Status (LINK). The Power indicator should be on continuously (green), the Link Status (yellow) and Activity (green) will blink indicating activity on the wired and wireless networks respectively.

Reset the T-316

!	If you press the reset button for more than four seconds, the Wireless Ethernet Client will be reset to the default factory settings. All changes you made to the configuration will be lost.

1. Insert the end of a paper clip into the hole next to the Ethernet connector to press the reset button, and hold it for at least four seconds. LINK LED will blink during this process.

2. Release the reset button after the ACT LED goes off. All settings will be cleared and set to the defaults. You can refer to this manual and reconfigure the Wireless Ethernet Client by yourself.

3.3 Configuring the Network Connection

!	The T-316 has a default IP Address of 192.168.5.99 with a subnet mask of 255.255.255.0. The computer that you are using for initial configuration must have its IP Address set within the same range, i.e., 192.168.5.xxx, where xxx is any number between 001 and 254, excluding 099.

The Ethernet Client is a ready-to-use device. It is delivered with default settings that allow you to access to it with any JavaScript-enabled web-browser such as Internet Explorer 4.0 (or higher), or Netscape Navigator 4.0 (or higher). To get to the configuration and status information, enter into the address line http://192.168.5.99, the default address of the Ethernet Client.

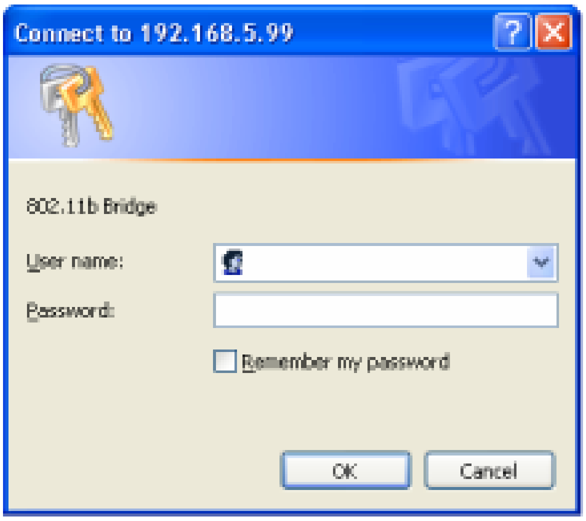


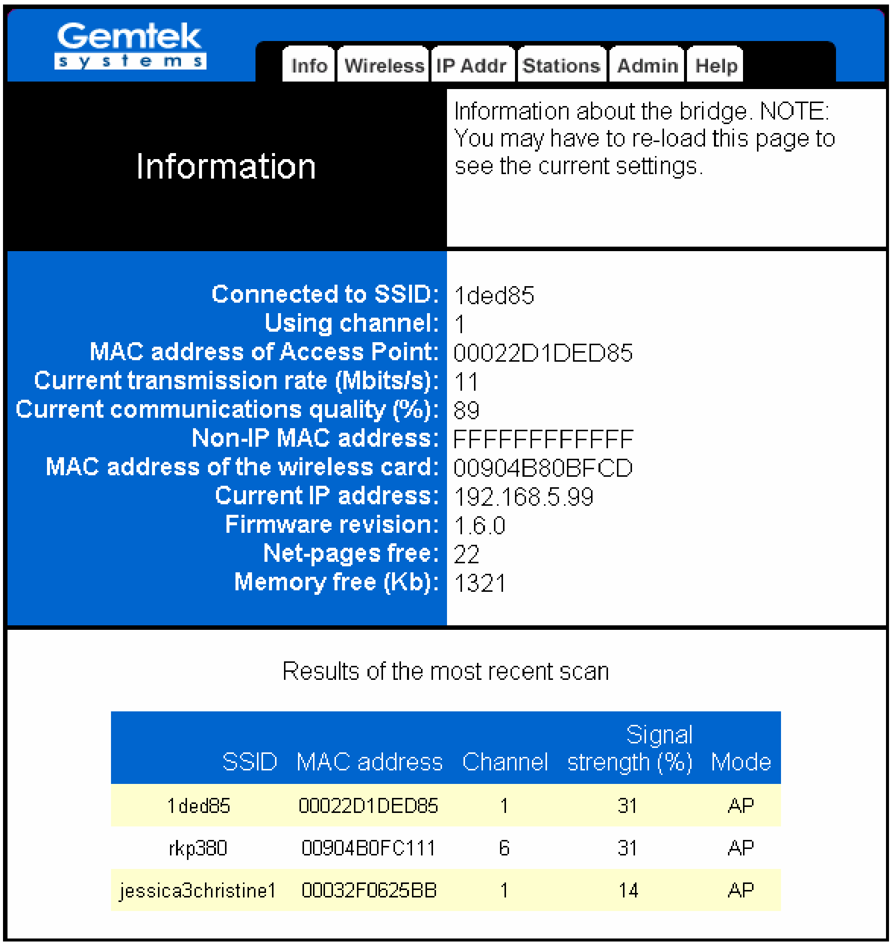
Figure 3.2 – Login window

Click **OK**. No **User name** or **Password** is required.

Factory Default Settings for the Wireless Ethernet Client	
SSID	Blank
Channel	6
Transmission rates	Auto
WEP enable	No
IP Address mode	Static
IP Address	192.168.5.99
Subnet mask	255.255.255.0
User Name	Blank
Administrator or password	Blank (no password needed)

3.3.1 Information

The Information window displays the current setup status.



Information

Information about the bridge. NOTE: You may have to re-load this page to see the current settings.

Connected to SSID:	1ded85
Using channel:	1
MAC address of Access Point:	00022D1DED85
Current transmission rate (Mbits/s):	11
Current communications quality (%):	89
Non-IP MAC address:	FFFFFFFFFFFF
MAC address of the wireless card:	00904B80BFCD
Current IP address:	192.168.5.99
Firmware revision:	1.6.0
Net-pages free:	22
Memory free (Kb):	1321

Results of the most recent scan

SSID	MAC address	Channel	Signal strength (%)	Mode
1ded85	00022D1DED85	1	31	AP
rkp380	00904B0FC111	6	31	AP
jessica3christine1	00032F0625BB	1	14	AP

Figure 3.3 – Information page

Current Communications Quality
Indicates the measured Communications Quality of the Basic Service Set to which the station is currently connected. The value in this field is based on signal and noise level measurements.

Firmware Revision
This indicates the device's firmware version. This is important when updating the firmware or reporting of any problems.

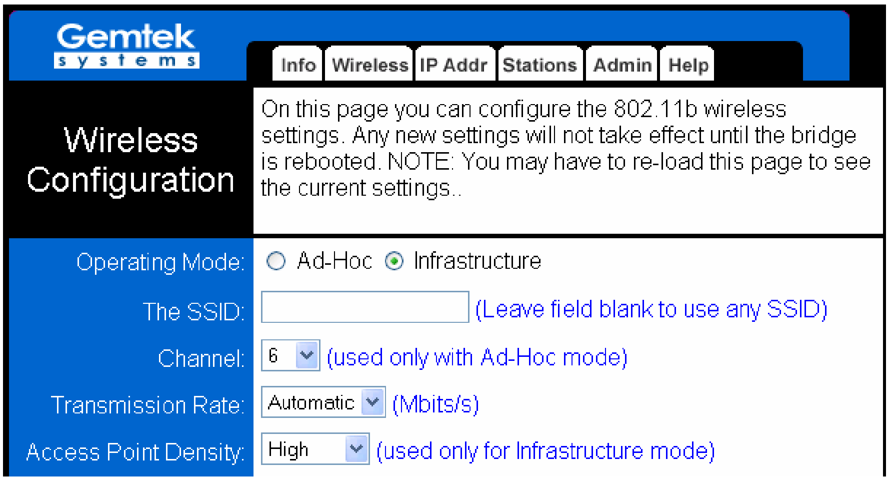
Current IP Address
Displays the device's IP address.

Non-IP MAC Address
This is the MAC Address of the Ethernet port that bridges to the Ethernet Client.

3.3.2 Wireless Configuration

Selecting the **Wireless** tab brings this page.

Only the top section of the page is shown here. The rest is covered in the section on Security.



Wireless Configuration

On this page you can configure the 802.11b wireless settings. Any new settings will not take effect until the bridge is rebooted. NOTE: You may have to re-load this page to see the current settings..

Operating Mode: ○ Ad-Hoc ● Infrastructure

The SSID: (Leave field blank to use any SSID)

Channel: 6 (used only with Ad-Hoc mode)

Transmission Rate: Automatic (Mbits/s)

Access Point Density: High (used only for Infrastructure mode)

Figure 3.4 – Wireless configuration page

Operating Mode *(default=Infrastructure)*
This is the default setting. Switch to Ad-Hoc mode when communicating to another client device without the presence of Access Point.

SSID *(default is blank)*
The SSID (Service Set ID) is the name given to the wireless network that the T-316 is associated with. Only Wireless Ethernet Clients and clients that share the same SSID are able to communicate with each other.

You can leave this blank and then reboot it to scan the environment

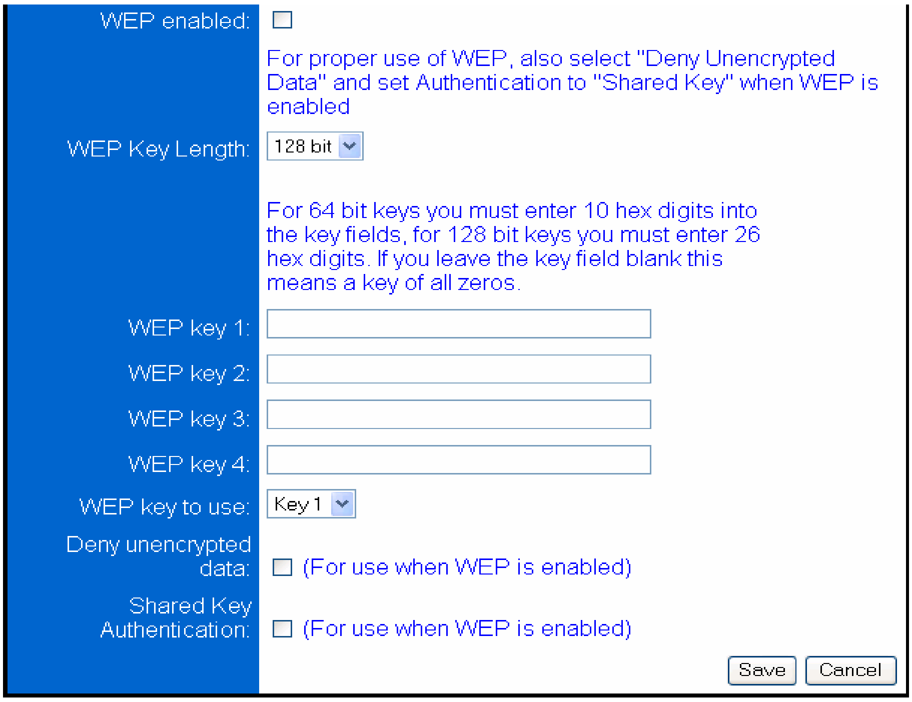
You will see what AP available around you at Info page.

Channel *(default=6)*
This is the channel that the Wireless Ethernet Client uses to transmit and receive data. The channel that you select here is restricted to the channels that can be used within your regulatory domain. It is best to leave this set to Auto so the device can find the best channel to connect with. When operating in Ad Hoc mode, this must be set to the same channel as all other devices in that network.

TX rate *(default=Automatic)*
The transmit rate identifies the preferred data transmission speed of the Ethernet Client. Transmissions at higher rates allow for higher data throughput and quicker network response times. However, transmissions at lower rates are usually more reliable and cover longer distances than the higher rates.

Access Point Density *(default=High)*
When connecting to the Access Point, it is generally necessary to specify an Access Point Density. This provides some control over handoff of clients during roaming between Access Points. Low, Medium, or High can be selected.

3.3.3 Security (part of the Wireless page)



WEP enabled: □

For proper use of WEP, also select "Deny Unencrypted Data" and set Authentication to "Shared Key" when WEP is enabled

WEP Key Length: 128 bit

For 64 bit keys you must enter 10 hex digits into the key fields, for 128 bit keys you must enter 26 hex digits. If you leave the key field blank this means a key of all zeros.

WEP key 1:

WEP key 2:

WEP key 3:

WEP key 4:

WEP key to use: Key 1

Deny unencrypted data: □ (For use when WEP is enabled)

Shared Key Authentication: □ (For use when WEP is enabled)

Figure 3.5 – Security page

WEP Enabled *(default is unchecked)*
Encryption (WEP)—additional measure of security on your wireless network which can be achieved by using WEP (Wired Equivalent Privacy) encryption. When an encrypted frame is received it will only be accepted if it decrypts correctly. This happens only if the receiver has the WEP Key used by the transmitter. All devices on the network, and the Wireless Ethernet Client, must share the same WEP selection – either Enable or Disable.
To enable WEP Encryption, click on WEP Enable.

WEP Key Length *(default is 128-bit)*
The WEP key is generated from Hexadecimal entries that are either 64 or 128-bit in length. (This is also sometimes referred to as 40-bit or 104-bit encryption) When enabling encryption, select the Key Length, either 64 or 128-bit, and then input the Hexadecimal digits. For 64 bit keys you must enter 10 hex digits into the key fields, for 128 bit keys you must enter 26 hex digits. If you leave the key field blank this means a key of all zeros.

!	Only the following alphanumeric characters are allowed in the entry, which is 0 to 9, a to f.

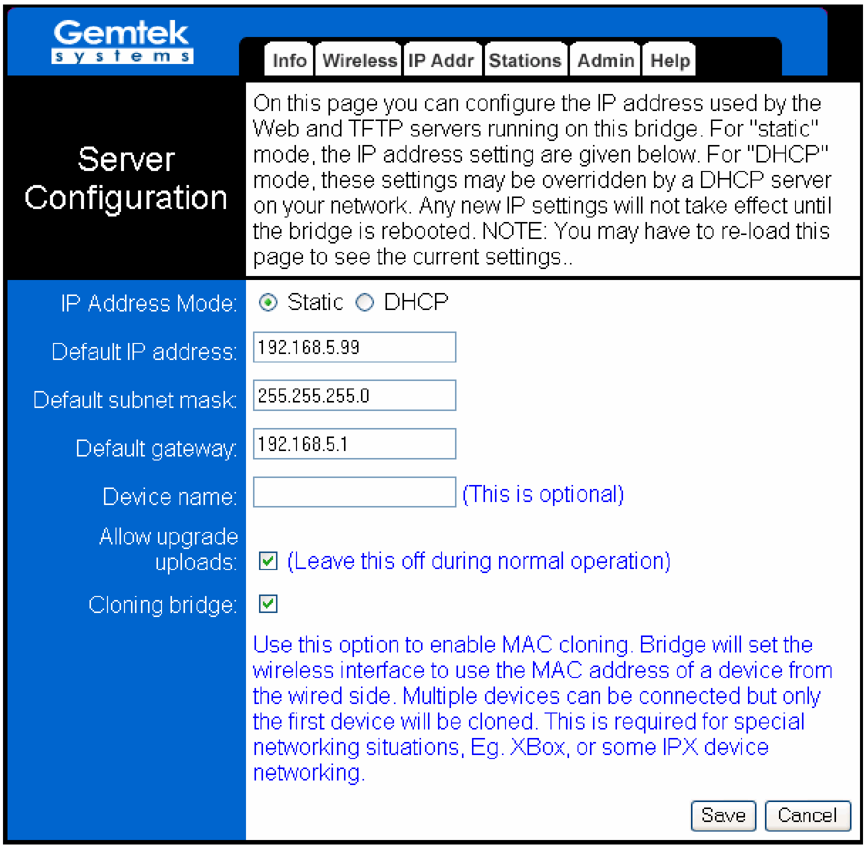
WEP Key to Use *(default is Key 1)*
Use the pull-down menu to select the WEP key. All devices on the network must use the same key to communicate with one another.

Deny Unencrypted Data *(default is unchecked)*
For additional security when WEP is enabled, select Deny Unencrypted Data.
Data received without a WEP key is rejected when Deny Unencrypted Data is selected.

Shared Key Authentication *(default is unchecked)*
Shared Key Authentication is when both the sender and the recipient share a secret key. All points on your network must use the same authentication type. It is recommended that you use the default setting.

3.3.4 Server Configuration

Selecting the **IP Addr** tab brings this page.



Server Configuration

On this page you can configure the IP address used by the Web and TFTP servers running on this bridge. For "static" mode, the IP address setting are given below. For "DHCP" mode, these settings may be overridden by a DHCP server on your network. Any new IP settings will not take effect until the bridge is rebooted. NOTE: You may have to re-load this page to see the current settings..

IP Address Mode: ● Static ○ DHCP

Default IP address: 192.168.5.99

Default subnet mask: 255.255.255.0

Default gateway: 192.168.5.1

Device name: (This is optional)

Allow upgrade uploads: ☑ (Leave this off during normal operation)

Cloning bridge: ☑

Use this option to enable MAC cloning. Bridge will set the wireless interface to use the MAC address of a device from the wired side. Multiple devices can be connected but only the first device will be cloned. This is required for special networking situations, Eg. XBox, or some IPX device networking.

Figure 3.6 – Server configuration page

Static *(default=selected)*
Select Static (recommended) to assign the IP, Subnet Mask and Gateway Address.

DHCP *(default=not selected)*
If the Wireless Ethernet Client is part of a network with a DHCP server, the DHCP server will assign the IP settings to the Wireless Ethernet Client automatically. (This is not recommended because a DHCP-assigned IP Address will change frequently, making the Wireless Ethernet Client impossible to configure.)

Default IP address *(default=192.168.5.99)*

Default subnet mask *(default=255.255.255.0)*

Default gateway *(default=192.168.5.1)*

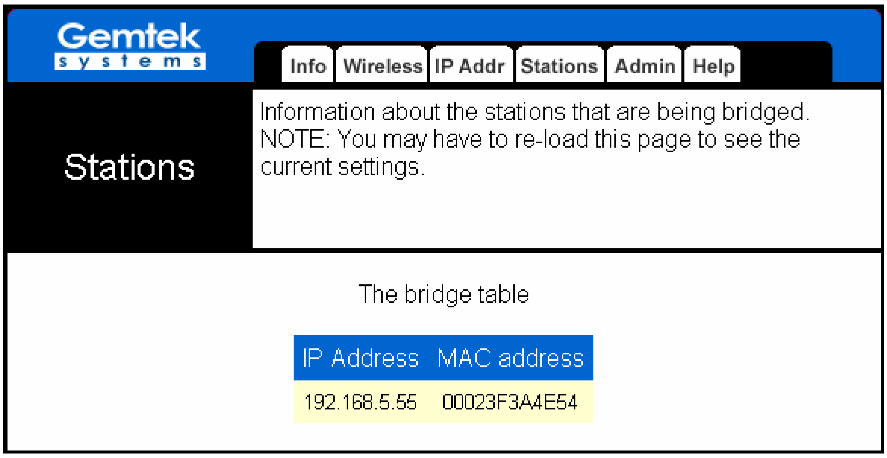
(Optional) Device Name *(default is blank)*
The device can be assigned a name for identification purposes within the network.

Allow Upgrade Uploads *(default is unchecked)*
Select this checkbox when performing firmware upgrade.

Cloning bridge *(default is unchecked)*
This function currently has limited applications.

3.3.5 Stations

Selecting the **Stations** tab brings this page. It shows the device that is bridging with the Ethernet Client.



Stations

Information about the stations that are being bridged.
NOTE: You may have to re-load this page to see the current settings.

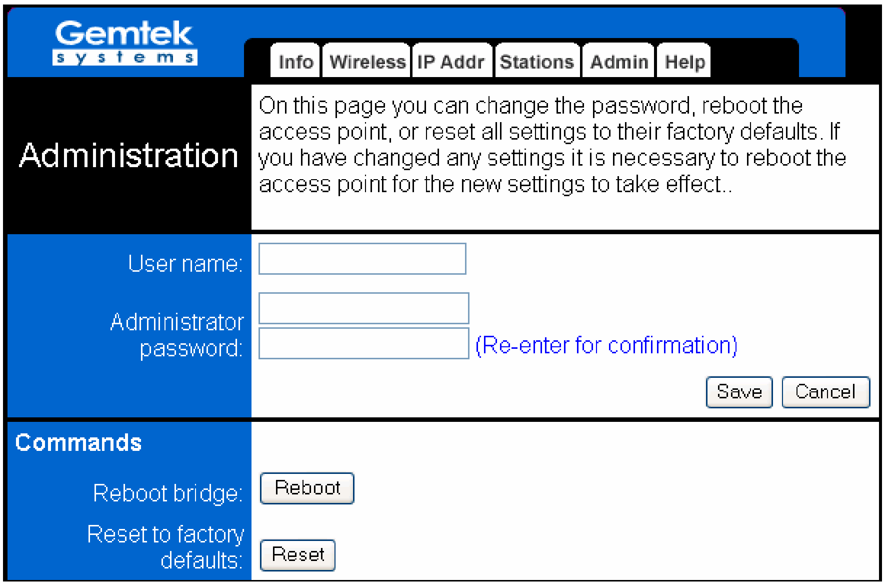
The bridge table

IP Address	MAC address
192.168.5.55	00023F3A4E54

Figure 3.7 – Stations page

3.3.6 Administration

Selecting the **Admin** tab brings this page.



On this page you can change the password, reboot the access point, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the access point for the new settings to take effect..

User name:

Administrator password: (Re-enter for confirmation)

Commands

Reboot bridge: Reboot

Reset to factory defaults: Reset

Figure 3.9 – Administration page

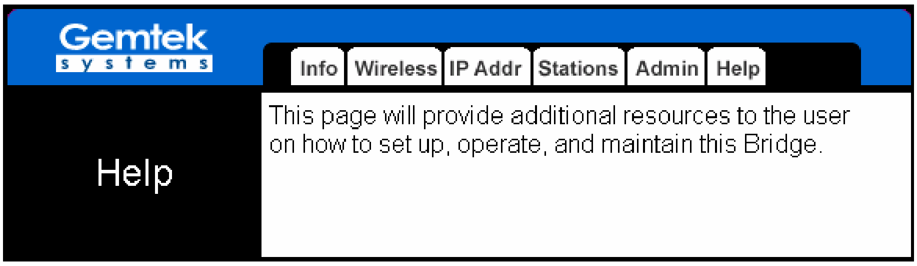
Change Username and Password *(default is blank)*
A password can be used to prevent unauthorized access to the configuration of the T-316. However, should you choose to use a password, it must be 15 characters in length or less. Re-enter the password in the next field to verify that it is correct, and click Change Password for the change to take effect.

Reboot Bridge
Click **Reboot** to restart the Wireless Ethernet Client.

Reset to Factory Defaults
Click on **Factory Reset** to return all settings to the Factory Default values. (This can also be done by pressing the Reset button on the back of the unit.)

3.3.7 Help

ℹ	This is reserved for future use.



This page will provide additional resources to the user on how to set up, operate, and maintain this Bridge.

Figure 3.10 – Help page

Chapter 4 – Troubleshooting

Because the T-316 requires no driver installation, it is less problematic than devices that do. Using the three LED indicators, most problems can be isolated very easily.

POWER LED (Power)

- Must be on. If it is not on:
  - Check to see that the USB cable is securely plugged into a USB port; and
  - Make certain that it is a powered USB port
- If it is not on, and the cable is plugged into a powered USB port:
  - The cable may be defective, or
  - The T-316 is faulty.

LINK LED (Wired network activity)

- Should be on or blinking. If it is off:
  - Check to see that the Ethernet cable is securely plugged into an Ethernet port on the computer
  - Check to see that the indicator LEDs associated with the Ethernet port are on or blinking
- If the connection appears to be correct:
  - The cable may be defective; or
  - The settings of the Ethernet port should be checked

ACT LED (RF link activity)

- Should be on or blinking. If it is off:
  - Check to see that the Access Point the T-316 is associating with is working and within range (300' maximum with no obstructions)
  - Check the settings of the T-316 to see that it is capable of associating with the AP
    - DHCP client must be enabled unless the network administrator states otherwise
    - WEP settings must be the same as those for the AP (disabled or identical keys)

Chapter 5 – Technical Specifications

T-316 Technical Specification	
Standards supported	IEEE 802.11 standard for Wireless LAN All major networking standards (including IP, IPX)
Environmental	Operating temperature (ambient): -10 ~ 50°C Humidity: Max. 95% Non-condensing
Power specifications	DC power supply - Input : DC 100-240 50-60 Hz 2A - Output: 5V DC 2A converter incl.
Radio specifications	Range: - per cell indoors approx. 35-75 meters - per cell outdoors up to 100-250 meters Transmit power: - Nominal Temp Range: 15 dBm, 12min. Frequency range: - 2.4-2.4835 GHz, direct sequence spread spectrum Number of Channels: - Most European countries: 13 (1-13) - US and Canada: 11 (1-11) (3 non-overlapping) - France: 4 (10-13) (1 non-overlapping) - Japan : 14 (1-14)
Specific features	Supported bit rates: - 11 Mbps : CCK - 5.5 Mbps : CCK - 1 Mbps : DBSK - 2 Mbps : DQPSK
Data encryption	64-bits WEP Encryption 128-bits WEP Encryption
Utility Management	Web management and TFTP firmware upgrade

Chapter 6 – Glossary

802.11: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become “industry standards”. 802.11b adds CCK modulation enabling data rates of up to 11Mbps, and 802.11a specifies OFDM modulation in frequency bands in the 5 to 6GHz range, and enables data rates up to 54Mbps.

Authentication: The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

DHCP: Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DNS: Domain Name Service. An Internet service that translates a domain name such as gemtek-systems.com to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hex number.

Gateway: A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

Hot-spot: A hot-spot is wireless public access system that allows subscribers to be connected to a wireless network in order to access the Internet or other devices, such as printers. Hot-spots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

HTTPS: HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering.

ICMP: ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

IEEE: Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world’s largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

IP: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

ISP: An ISP (Internet Service Provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

LAN: A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many as thousands of users (for example, in an FDDI network).

MAC: Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

NAT: NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

NAT is included as part of a router and is often part of a corporate firewall.

POP3: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

SNMP: Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

SSL: The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

TCP: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Telnet: Telnet is the way to access someone else's computer, assuming they have given permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Web, HTTP and FTP protocols allow to request specific files from remote computers, but not to actually be logged on as a user of that computer.

WAN: A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN).

WECA: The Wireless Ethernet Compatibility Alliance. A nonprofit organization formed in 1999 to certify interoperability of Wi-Fi (IEEE 802.11b) products. WECA has defined a test suite that defines how member products are tested and certifies that they are interoperable with other Wi-Fi certified products. An independent test lab conducts the testing. When a product successfully passes the test, the company is granted the Wi-Fi seal.

Wi-Fi: Wi-Fi is short for ***wi**reless **fi**delity* and is another name for IEEE 802.11b. It is a trade term promulgated by the Wireless Ethernet Compatibility Alliance (WECA). "Wi-Fi" is used in place of 802.11b in the same way that "Ethernet" is used in place of IEEE 802.3. Products certified as Wi-Fi by WECA are interoperable with each other even if they are from different manufacturers. A user with a Wi-Fi product can use any brand of access point with any other brand of client hardware that is built to the Wi-Fi standard.

WISP: A wireless Internet service provider (WISP) is an Internet service provider (ISP) that allows subscribers to connect to a server using medium-range wireless links. This type of ISP offers broadband service and allows subscriber computers, called stations, to access the Internet and the Web from anywhere within the zone of coverage provided by the server antenna. This is usually a region with a radius of several kilometers.

The simplest WISP is a basic service set (BSS) consisting of one server and numerous stations all linked to that server by wireless. More sophisticated WISP networks employ the extended service set (ESS) topology, consisting of two or more BSSs linked together at access points (APs). Both BSS and ESS are supported by the IEEE 802.11b specification.