WTI®

www.gotowti.com

Wireless Technology, Inc.

MACH V SERIES

Installation and
Operation Manual

R0115

TABLE OF CONTENTS

FCC NOTICE
This device complies with Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

1.) This device may not cause harmful interference, and
2.) This device must accept any interference that may be received, including interference that may cause undesired operation.

IC NOTICE
This device complies with the RSS-210 Industry Canada.

Operation is subject to the following two conditions:

1.) This device may not cause interference, and
2.) This device must accept any interference, including interference that may cause undesired operation.

READ THIS MANUAL
Every effort has been made to insure that this WTI system is of the highest quality. This product has been carefully inspected to comply with rigid quality standards before shipment to you. In consideration of your investment and the desire to obtain full performance capability engineered into your new WTI product, we recommend that you read this manual before attempting to operate your system.

FOR MORE ASSISTANCE OR MORE INFORMATION:

Wireless Technology, Inc. (WTI)
2064 Eastman Avenue, Suite 113
Ventura, CA 93003-7787

TEL 805/339.9696
FAX 805/339.0932

EMAIL: sales@wirelesstech.com

INTERNET: http://www.wirelesstech.com or http://www.gotowti.com

The software/firmware furnished with the equipment is confidential to and is copyrighted by *Wireless Technology, Inc.* (WTI) and it is not to be copied or disclosed in any manner without the consent of *Wireless Technology, Inc.* (WTI) The software/firmware is furnished to the purchaser under a license for use on a single system.

Information furnished by *Wireless Technology, Inc.* (WTI) is believed to be accurate and reliable. However, no responsibility is assumed by *Wireless Technology, Inc.* (WTI) for its use or for any infringements of other rights of third parties, which may result from its use. No license is granted by implications or otherwise under any patent or patent rights of *Wireless Technology, Inc.* (WTI)

©2010 Wireless Technology, Inc. (WTI)
All rights reserved.

PRODUCT WARRANTY

We appreciate your purchase of W*ireless* T*echnology*, I*nc*. (WTI) security products. We take pride in the quality of our products and have manufactured each new WTI product to exacting quality standards. In normal use, it will provide you with years of satisfactory performance. However, should you experience difficulty; you are protected under the provisions of this warranty.

WTI warrants to the original user a product that is free of defects in materials and workmanship in normal use. WTI warrants to the original user that WTI's wireless RF transmission system products will be free of defects in materials and workmanship in normal use for a period of 12 months from the date of sale. WTI's obligation under this warranty shall be limited to the repair, including all necessary parts and the cost of labor connected therewith, or at our option, the replacement of any product that shows evidence of a manufacturing defect within the warranty period.

This warranty is extended to all WTI products purchased and used within the United States of America and is valid only when service is rendered by the authorized W*ireless* T*echnology*, I*nc*. (WTI) Warranty Station.

This warranty shall not apply to appearance or accessory items including, but not limited to, knobs, connectors, cabinets and connecting cables. This warranty shall not, in addition, apply to repairs or replacements necessitated by any cause beyond the control of WTI including, but not limited to, acts of nature, improper installation, misuse, lack of proper maintenance, accident, voltage fluctuations, unauthorized repairs or modifications.

This warranty becomes void in the event serial numbers are altered, defaced or removed, or an attempt is made to field service or alter performance of any RF transmission component.

WTI reserves the right to make changes in design, or to make additions to, or improvements upon, products without incurring any obligation to install the same on products previously manufactured.

The foregoing is in lieu of all other warranties expressed or implied and WTI neither assumes nor authorizes any person to assume for it any other obligation or liability in connection with the sale of our products. In no event shall WTI or its Authorized Dealers be liable for special or consequential damage arising from the use of this product, or any delay in the performance of this warranty due to causes beyond its control.

REPAIR AUTHORIZATION AND RETURNS

REPAIR AUTHORIZATION

Please contact *Wireless Technology, Inc.* (WTI), to obtain a repair authorization number (RA) and provide the following information:

1.) Product Model & Serial Numbers

2.) Date of shipment, purchase order number, sales order number or WTI invoice number.

3.) Details of the defect or malfunction. If there is a dispute regarding the warranty or product, which does not fall under the warranty conditions stated within the description of the written warranty, please include a written explanation with the product when returned.

SHIP FREIGHT PRE-PAID TO:

Wireless Technology, Inc. (WTI)
2064 Eastman Avenue, Suite 113
Ventura, CA 93003-7787
TEL 805/339-9696
FAX 805/339-0932

RETURNS

No unauthorized returns will be accepted. All returns must have an authorized (RA) number issued by the factory (CA number if returned for credit and RA number if returned for repair). Products returned for repair or credit will be rejected if no authorization number has been issued or freight has not been pre-paid. All merchandise returned for credit will be subject to a 20% restocking and refurbishing charge.

IMPORTANT SAFEGUARDS

1.) Read Instructions. It is important to read all safety and operating instructions before installing or using this equipment.

2.) Retain Instructions. Retain this manual and any supplements for future reference.

3.) Follow Instructions. Follow all instructions herein for use of this equipment.

Do not attempt to open the sealed Transmitter and Receiver Assembly. There are no user-serviceable parts inside. Refer servicing to the W*ireless* T*echnology*, I*nc*. (WTI) factory service center only.

4.) Heed warnings. Adhere to all warnings on the equipment, and in this manual.

5.) To reduce the risk of electric shock or equipment damage, work on the unit only when the power is shut off and is unplugged from its power source to prevent accidental activation. Also take precautions to avoid contact between the equipment and other electrical wires or power sources that may be present at the installation site.

RECOMMENDED TOOLS AND ACCESSORIES FOR PROPER INSTALLATION:

1.) Tie-wraps to secure cable runs.
2.) #1 and #2 Phillips screwdriver.
3.) #3 Slot screwdriver.
4.) Cordless power drill.
5.) Set of open end or SAE wrenches.
6.) Silicone caulking compound for antenna connector.
7.) Self-sealing connector tape - Used to weatherproof all outdoor cable connections.
8.) Appropriate conduit if boxes are mounted outdoors.
9.) Hand held radios.

WTI's MACH V is the answer to the ever growing demand for higher bandwidth and security in a wireless network environment. It is based on a brand new redesigned platform that not only offers faster performance and capacity but also supports all current pre IEEE 802.11i wireless security standards. WTI's MACH V is the IEEE 802.11a version of the platform that directly targets the need for the more secure, less crowded 4.9GHz frequency spectrum.

Product Features

- Compact size for small enterprise or system integrate service market.
- Compliant with IEEE 802.11a specifications.
- Supports 64/128-bit WEP, WPA and IEEE802.1x.
- Supports Atheros Super A (up to 108Mbps).
- Intelligent firmware upgrade via Web browser.
- Built-in Web-based utility for easy configuration from any Web browser.
- Support POE (IEEE 802.3af) function.
- Supports wireless bridging and MAC address filtering.
- Super bright LED indicating status and signal level (RSSI).
- Provide 10/100M, auto sensing MDI/MDI-X Ethernet port.

**Atheros Super G (Proprietary technology of Atheros Communication Inc.) would only work in situations where both ends of the communication link are using the Atheros radio chipset.*

Part List

1. MACH V 802.11a radio
2. Weatherproof NEMA 4x housing
3. Mounting Hardware (1)
4. User Manual

Note: *If any item listed above is damaged or missing, please contact* WTI *immediately.*

System Requirements

- Any desktop or laptop with an Ethernet interface
- TCP/IP protocol suite installed
- Standard CAT5 Ethernet cables with RJ45 connectors
- Internet Explorer 5.0 or later / Firefox 1.0 or higher

Preparation for Installation

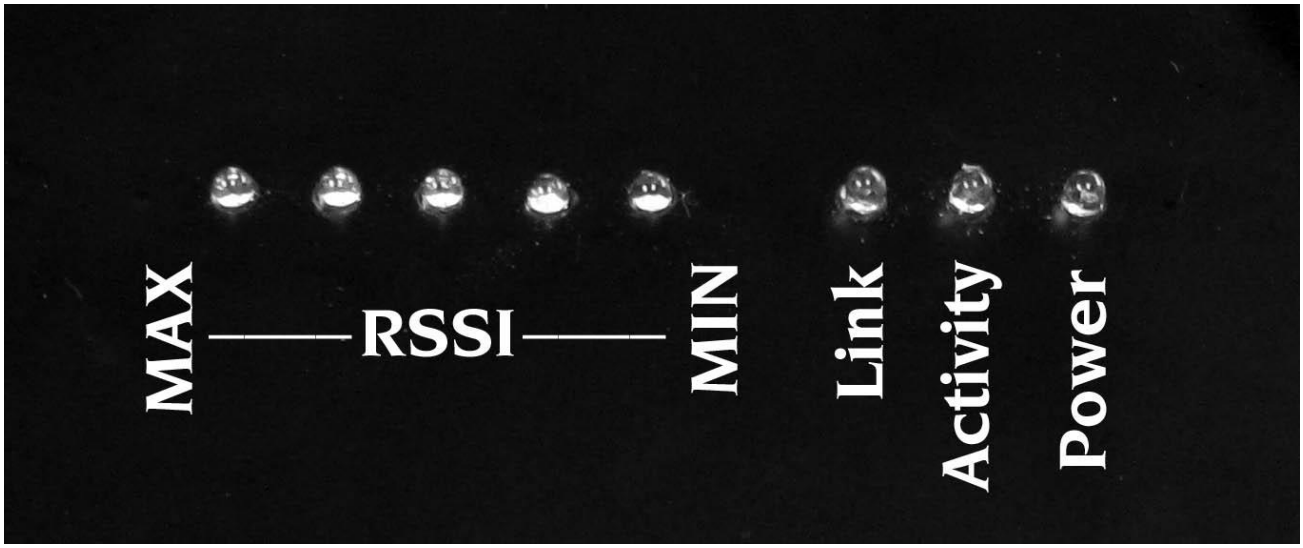
Always double check for any missing parts from the kit you received before deployment. The next step is to set up the computer Ethernet interface for configuring the MACH V. Since the default IP Address of the unit is on the 192.168.10.x IP range in both Client Bridge and AP mode you will need to set the Ethernet interface within the same IP range, where x will have to be a free IP address number from 1-254.

Hardware Installation

Follow the procedure below to install your MACH V:

1. Select a suitable place on the network to install the MACH V. For best wireless reception and performance the external antenna should be positioned within Line of Sight from the AP with proper alignment.
2. Check the LEDs on the MACH V to confirm if the status is okay. At this point the Power (PWR) LED indicator should be red and Ethernet (LAN) LED should be green. The RF light should light up once the unit is associated wirelessly with another wireless device. However at this point the unit is still in factory default setting so do not be alarmed that the WLAN light doesn't light up.

LED Indicator Layout

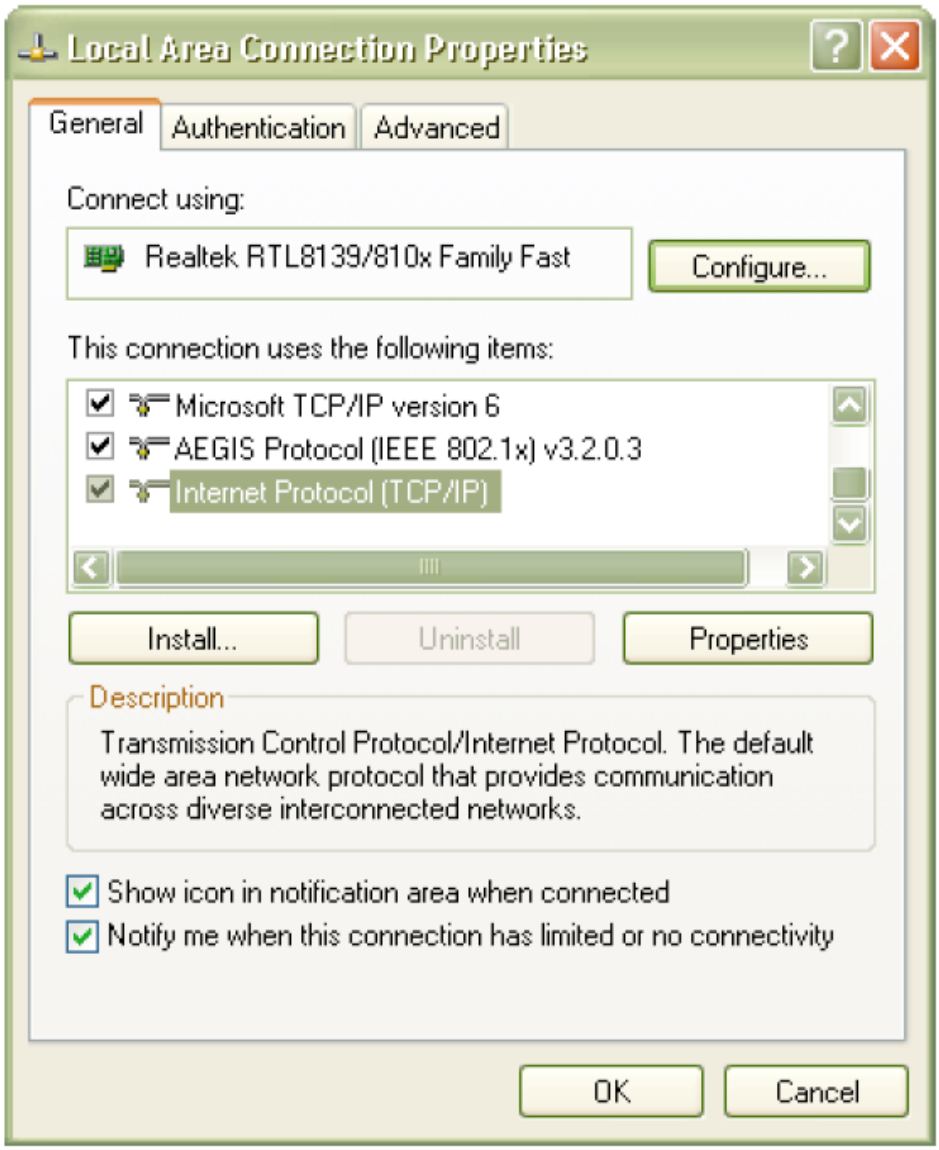


CONFIGURING WINDOWS FOR IP NETWORKING

To establish a communication link between your PC and MACH V, you will need to set up a static IP address for your computer first. This section helps you configure the network settings for your operating system. Please follow the procedures below to complete the settings:

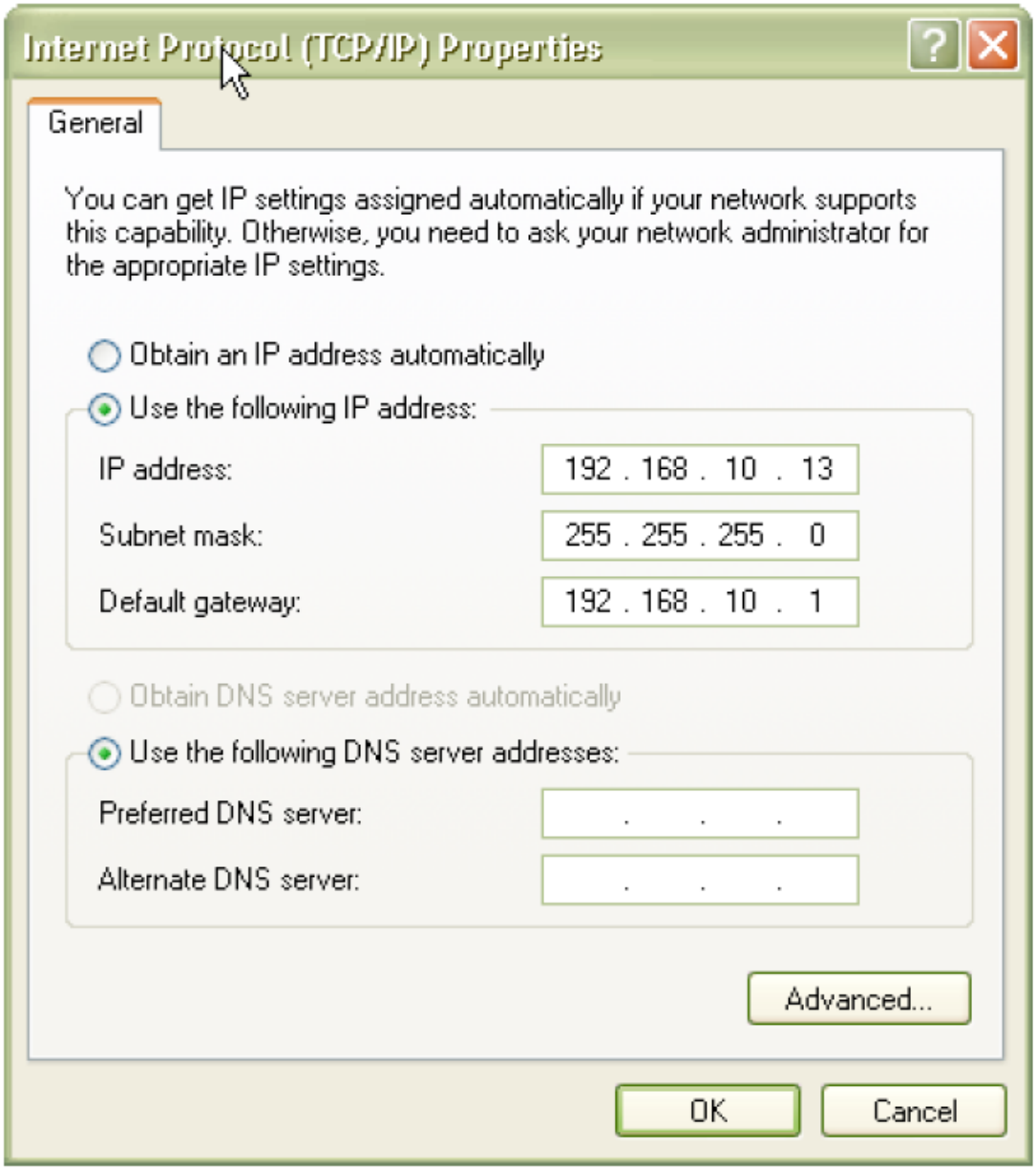
Windows XP

1. Click **Start** on the taskbar and from the **Control Panel** choose **Network Connections**. Right-click the **Local Area Connection** icon and then choose **Properties** from the menu. You should see the **Local Area Connection Properties** dialog box shown below.



2. Select the **Internet Protocol (TCP/IP)** for your network card, and then click **Properties.**
3. In the opened dialog box, choose **Use the following IP address.**

4. Under the **General** tab, choose **Use the following IP address**, and then specify an IP address. For example, type in **192.168.10.X** in the **IP Address** (where X is any free IP number from 1-254, excluding 241) area and **255.255.255.0** in the **Subnet Mask** area.



5. Click **OK** to finish configuration.

Client Bridge Mode

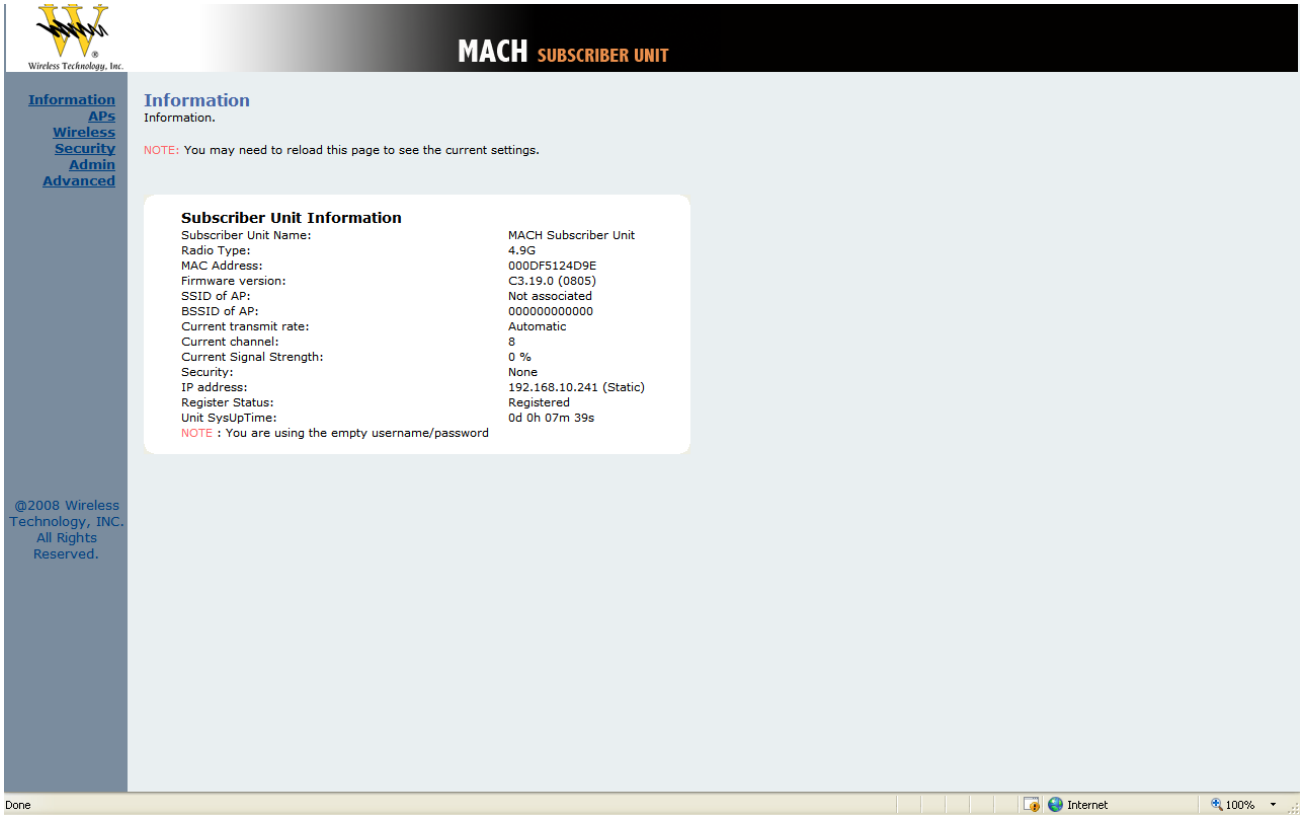
Default IP Address in Client Bridge Mode: **192.168.10.241.** To access the web control interface please open up a browser window and type in the factory default IP address in the URL.

Press Enter on your keyboard and a login prompt window similar to the one shown below will appear.

There is no default User name or Password. Leave User name and Password field blank and click OK.

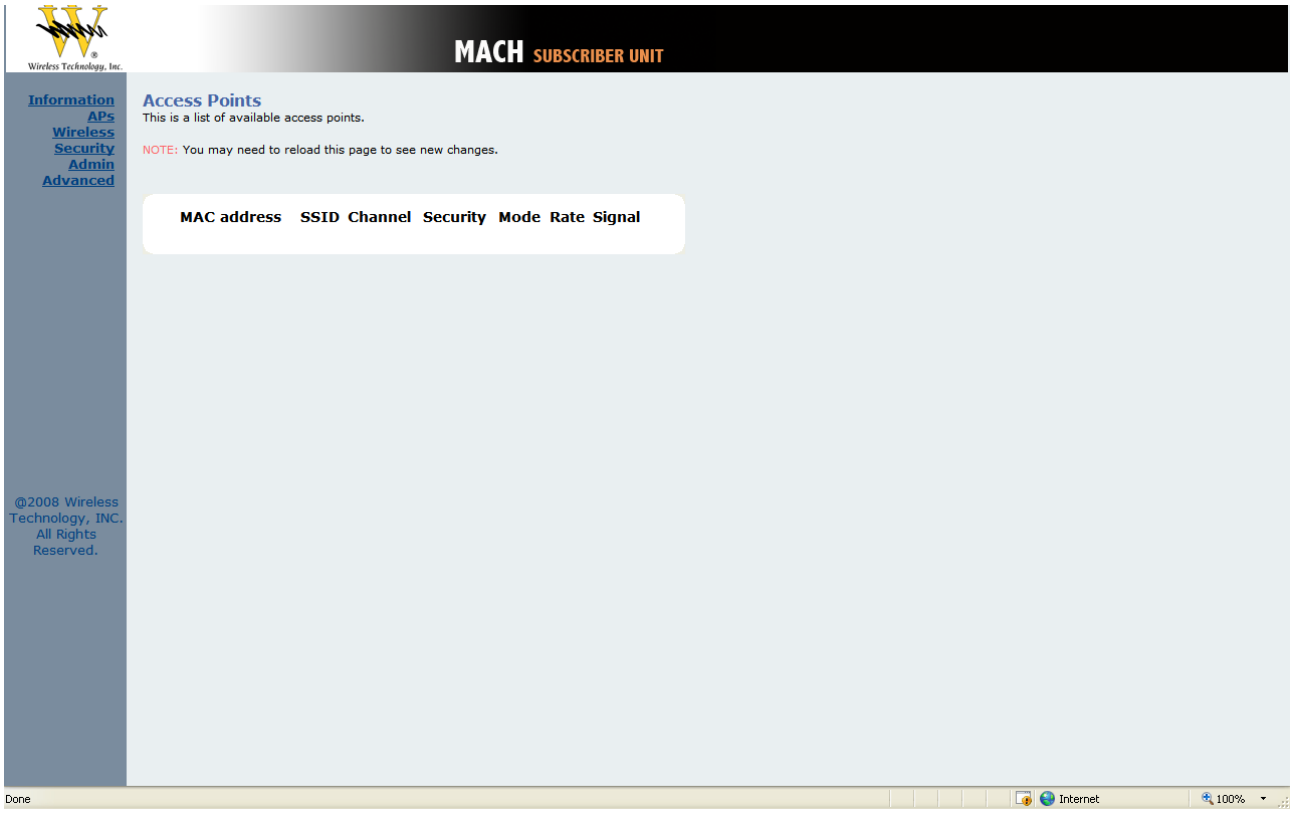
Note: You may set a new password by clicking the Admin tab after you enter the Web Configuration page.

Information



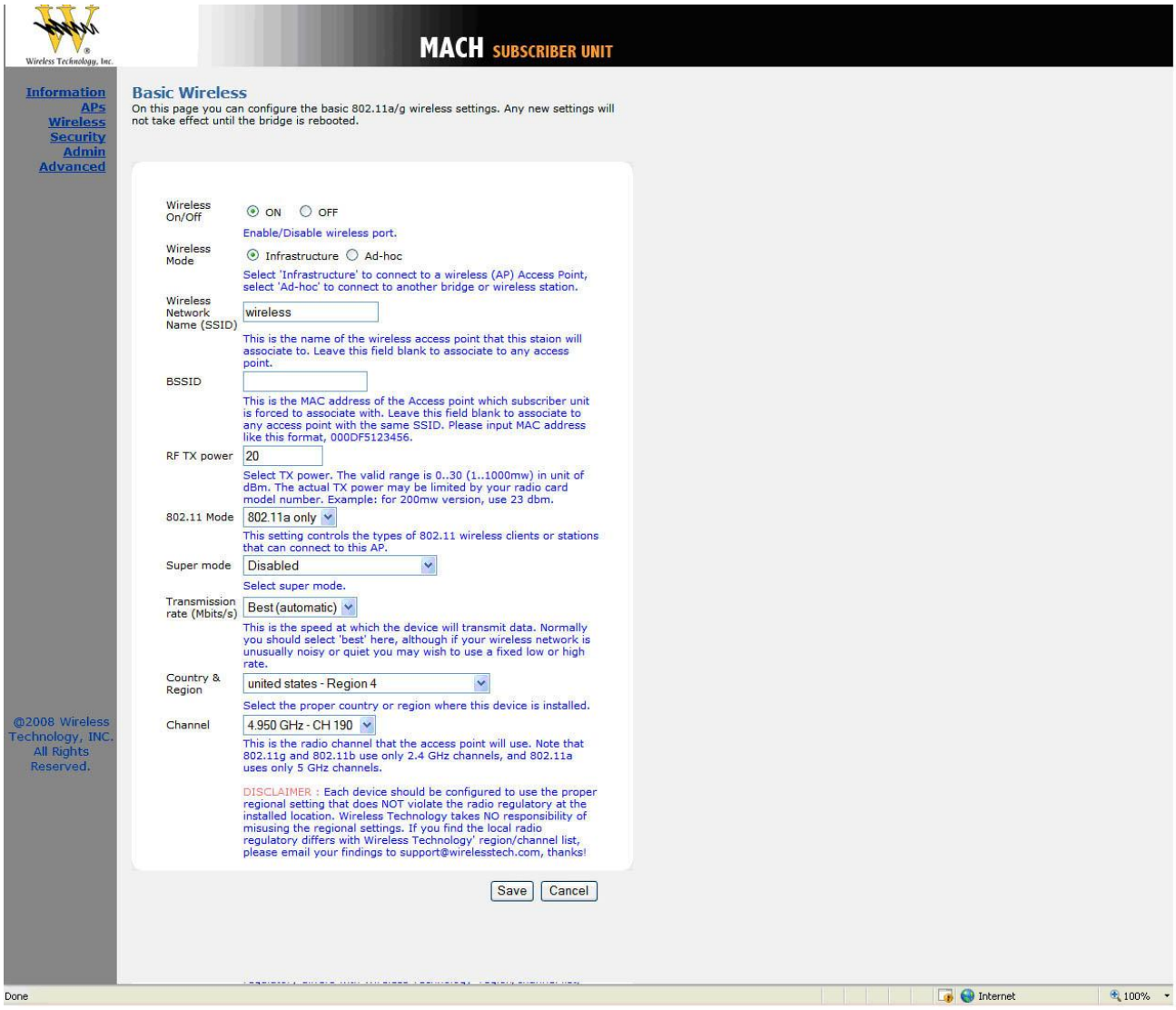
Under the main web interface home page you will see the following configuration menu pages: **Information**, **APs**, **Wireless**, **Security**, **Admin** and **Advanced.** Detailed information for each section is provided below:

Access Points (APs)



The APs section displays available hotspots in the area along with the MAC address, SSID, Channel, Wireless mode, signal strength and transmission rate for each access point.

Wireless



Wireless On/Off

This is the on/off switch of the radio card.

Wireless Mode

Infrastructure: An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP).

Ad-hoc: An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Use this mode if there is no wireless infrastructure or where services are not required.

Wireless Network Name (SSID)
Network Name is also known as SSID, which stands for Service Set Identifier. Any client in Infrastructure mode has to indicate the SSID of an Access Point to access a service such as internet access through the Access point.

Access Point Identifier (BSSID)
The Basic Service Set Identifier is the unique identifier (MAC address) of an access point in a Basic Service Set (BSS) network. The subscriber unit is forced to associate with this particular unit if there are multiple access points in the network.

Transmission Rate (Mbits/s)
This option indicates the transmission rate of the bridge. Specify the rate according to the speed of your wireless network from the list. Most of the time the default setting, Best (automatic), should be selected for best performance.
The setting can be adjusted manually if the link quality and signal strength are unusually low or high to get the best performance.

802.11 Mode
Wireless mode allows the user to select whether this subscriber unit will connect to an 802.11b only network, an 802.11g only network, an 802.11a only network or both b/g networks. For b or g only wireless devices on the network, selecting 802.11b or 802.11g only mode will provide better performance than mixed mode. In the case of WTI'S MACH V only 802.11a mode is allowed.

RF Transmit Power
This section controls the power output of the radio. The valid input range for this section is in the range of 0-30 in dBm units or (1mw – 1000mw). The default value is 23 dBm or 200mW.

Super Mode
Super Mode is only supported if both the client and the AP are using compatible Atheros radio chipsets.

- Disabled
- Super A/G without Turbo
- Super A/G with Static Turbo
- Super A/G with Dynamic Turbo (AR enabled)

Country and Region
This option selects the country and region of operation. Every device should be configured to use the proper regional settings which comply with and do NOT violate the radio regulatory laws at the installed location.

Channels

Channels are important to understand because they affect the overall capacity of your Wireless LAN. A channel represents a narrow band of radio frequency. A radio frequency modulates within a band of frequencies; as a result there is a limited amount of bandwidth within any given range to carry data. It is important that the frequencies do not overlap or else the throughput would be significantly reduced as the network sorts and reassembles the data packets sent over the air.

For the MACH Series: 2.4 GHz – 2.497 GHz frequency range, there are only 3 channels out of the 11 available that do not overlap with one another. To avoid interference within a network with multiple APs, set each AP to use one of the 3 channels (e.g. Channel 1) and then the other AP to be one of the other 2 channels (i.e. Channel 6 or Channel 11) within the range of the wireless radio. This simple method will reduce interference and improve network reliability.

802.11 b/g Wireless Channel Frequency Range: 2.4 GHz – 2.497 GHz

802.11 b/g Non-Overlapping Channel Frequency Ranges.

- Channel 1 = 2.401 GHz – 2.423 GHz
- Channel 6 = 2.426 GHz – 2.448 GHz
- Channel 11 = 2.451 GHz – 2.473 GHz

Americas: Wireless Channels 1 – 11

Asia: Wireless Channels 1 – 14

Europe: Wireless Channels 1 – 13

802.11a Wireless Channel Frequency Range: 5.15 GHz – 5.35 GHz, 5.725 – 5.825

802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5 GHz band.

802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. Unlike that of 802.11b/g, 802.11a standard separates its channels into 3-100MHz segments in the US. The lower and middle band accommodates 8 channels in a total bandwidth of 200 MHz and the upper band accommodates 4 channels in a 100 MHz bandwidth. The frequency channel center frequencies are spaced 20 MHz apart. The outermost channels of the lower and middle bands are centered 30 MHz from the outer edges. In the upper band the outermost channel centers are 20 MHz from the outer edges.

In addition to the frequency and channel allocations, transmit power is a key parameter regulated in the 5 GHz U-NII band. Three transmit power levels are specified: 40 mW, 200 mW and 800 mW. The upper band defines RF transmit power levels suitable for bridging applications while the lower band specifies a transmit power level suitable for short range indoor home and small office environments.

802.11a Non-overlapping Channel Frequency Ranges
Lower Band (5.15 - 5.25 GHz) – Maximum Output Power 40mW

- Channel 36 = 5.15 – 5.18
- Channel 40 = 5.18 – 5.20
- Channel 44 = 5.20 – 5.22
- Channel 48 = 5.22 – 5.25

Middle Band (5.25 - 5.35 GHz) – Maximum Output Power 200mW

- Channel 52 = 5.25 – 5.28
- Channel 56 = 5.28 – 5.30
- Channel 60 = 5.30 – 5.32
- Channel 64 = 5.32 – 5.35

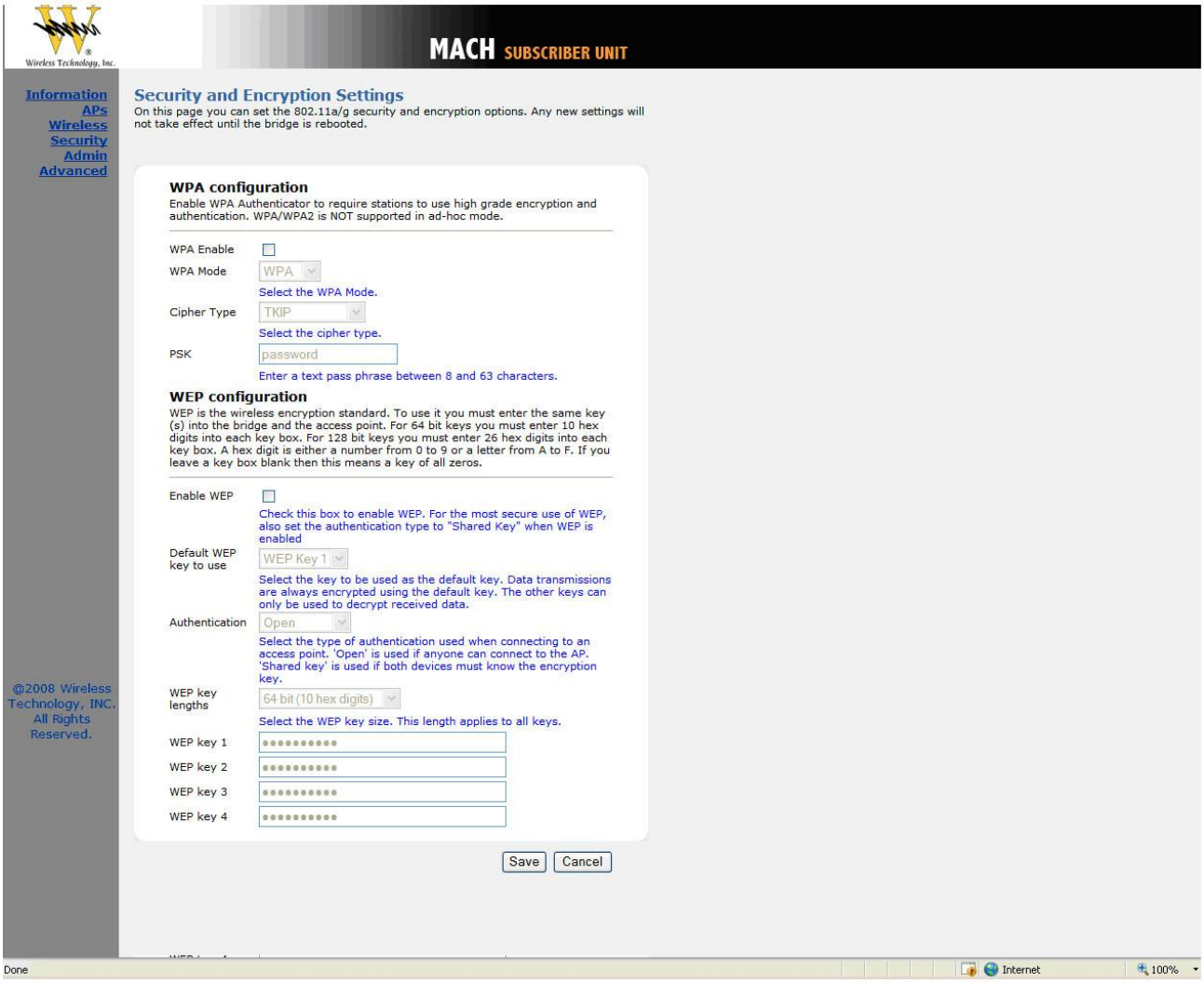
Upper Band (5.725 - 5.825 GHz) – Maximum Output Power 800mW

- Channel 149 = 5.725 – 5.745
- Channel 153 = 5.745 – 5.765
- Channel 157 = 5.765 – 5.785
- Channel 161 = 5.785 – 5.805
- Channel 165 = 5.805 – 5.825

Special Atheros Turbo Mode Channels
*U*se this setting only when both side of the wireless connection is using the Atheros chipset. The radio will combine 2 free channels for the wireless transmission to double the bandwidth.*

- Channel 42 = 5.210
- Channel 50 = 5.250
- Channel 58 = 5.290
- Channel 152 = 5.760
- Channel 160 = 5.800

Security



WPA Configuration

Short for Wi-Fi Protected Access, WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP. WPA has the following improvements over WEP:

- Improved data encryption through temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm. By adding an integrity-checking feature, TKIP ensures that keys have not been tampered with.
- User authentication through the Extensible Authentication Protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA Enable
This option enables the WPA Authenticator. Note that any client that does not support the WPA standard will not be able to handshake / authenticate with a WPA enabled device.

WPA Mode

- WPA: Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification. WPA addresses all known vulnerabilities in WEP. WPA also provides user authentication, since WEP lacks any means of authentication. WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. WPA was designed and has been scrutinized by well-known cryptographers. It can be implemented immediately and inexpensively as a software or firmware upgrade to most existing Wi-Fi CERTIFIED™ access points and client devices with minimal degradation in network performance. WPA offers standards-based, Wi-Fi CERTIFIED security. It assures users that the Wi-Fi CERTIFIED devices they buy will be cross-vendor compatible. When properly installed, WPA provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1X authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.
- WPA2: WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi® users with a high level of assurance that only authorized users can access their wireless networks. Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES satisfies U.S. government security requirements. It has been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). Organizations that require the AES encryption available in WPA2 should be aware that upgrading to it may require new hardware. Section II of this document offers a roadmap for organizations planning to upgrade to WPA2. Considerations for its deployment are outlined in Section III.

Cipher Type

- TKIP: Temporal Key Integrity Protocol is an upgrade to the WEP known as WEP 1.1 that fixes known security problems in WEP's implementation of the RC4 stream cipher. TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- AES: Advanced Encryption Standard (Rijndael Cypher) is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES. AES works at multiple network layers simultaneously. AES Supports 128, 192 and 256 bit keys. Unlike the older standard, AES and 802.11i (WEP version 2) are based on 32bit processing.
- TKIP and AES: If clients support both the TKIP and AES standards then this would be the strongest cipher type to use that combines both TKIP and AES security.

PSK

PSK stands for Pre-Shared-Key and serves as a password. User may key in 8 to 63 characters string to set the password and activate 802.1x Authentication. Note that the same password must be used at both ends of the communication link (access point and client end).

WEP Configuration

Short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN.

Enable WEP

To enable the WEP Authenticator:

Default WEP Key to Use

WEP Key 1-4

Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

Authentication

O*pen* - Open system authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If it is "successful", the station shall be mutually authenticated. Open system authentication does not provide authentication. It provides identification using the wireless adapter's MAC address. Open system authentication is used when no authentication is required. It is the default authentication algorithm.

Open system authentication uses the following process:

1. The authentication-initiating wireless client sends an IEEE 802.11 authentication management frame that contains its identity.
2. The receiving wireless AP checks the initiating station's identity and sends back an authentication verification frame.
3. With some wireless APs, you can configure the MAC addresses of allowed wireless clients. However, configuring the MAC address does not provide sufficient security because the MAC address of a wireless client can be spoofed.

Shared Key - Shared key authentication supports authentication of stations as either a member of those who know a shared secret key or a member of those who do not. Shared key authentication is not secure and is not recommended for use. It verifies that an authentication-initiating station has knowledge of a shared secret.

This is similar to pre-shared key authentication for Internet Protocol security (IPSec). The 802.11 standard currently assumes that the shared secret is delivered to the participating wireless clients by means of a more secure channel that is independent of IEEE 802.11. In practice, a user manually types this secret for the wireless AP and the wireless client.

Shared key authentication uses the following process:

1. The authentication-initiating wireless client sends a frame consisting of an identity assertion and a request for authentication.
2. The authenticating wireless node responds to the authentication-initiating wireless node with challenge text.
3. The authentication-initiating wireless node replies to the authenticating wireless node with the challenge text that is encrypted using WEP and an encryption key that is derived from the shared key authentication secret.
4. The authentication result is positive if the authenticating wireless node determines that the decrypted challenge text matches the challenge text originally sent in the second frame. The authenticating wireless node sends the authentication result.
5. Because the shared key authentication secret must be manually distributed and typed, this method of authentication does not scale appropriately in large infrastructure network mode, such as corporate campuses.

WEP Key Lengths

64 bit (10 Hex Digit)

WEP *Key type*	***Example***
64-bit WEP with 5 characters	Key1= 2e3f4 Key2= 5y7js Key3= 24fg7 Key4= 98jui
64-bit WEP with 10 hexadecimal digits ('0-9', 'A-F')	Key1= 123456789A Key2= 23456789AB Key3= 3456789ABC Key4= 456789ABCD

128 bit (26 Hex Digit)

WEP *Key type*	***Example***
128-bit WEP with 13 characters	Key1= 2e3f4w345ytre Key2= 5y7jse8r4i038 Key3= 24fg70okx3fr7 Key4= 98jui2wss35u4
128-bit WEP with 26 hexadecimal digits ('0-9', 'A-F')	Key1= 11223344556677889 9AABBCDEF Key2= 2233445566778899AABBCCDDEE Key3= 3344556677889900AABBCCDDFF Key4= 44556677889900AABBCCDDEEFF

Administration

Device Name

This is the name that the bridge will use to identify itself to external configuration and IP address programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

SNMP Setting

SNMP Enable

Option to enable or disable SNMP support.

Community

The SNMP Read-only Community string is like a user id or password that allows access to a router's or other device's statistics or management information. InterMapper sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Factory default setting for the read-only community string is set to "public". It is standard practice to change all the community strings so that outsiders cannot see information about the internal network. (In addition, the administrator may also employ firewalls to block any SNMP traffic to ports 161 and 162 on the internal network.) Change this value to have InterMapper use the new string when querying SNMP devices.

IP Settings

IP Address Mode

- **Static**
  - Manually setup an IP address for this device.
- **DHCP**
  - Set up the bridge as a DHCP client which will pick up an IP address from a DHCP server.

Default IP Address

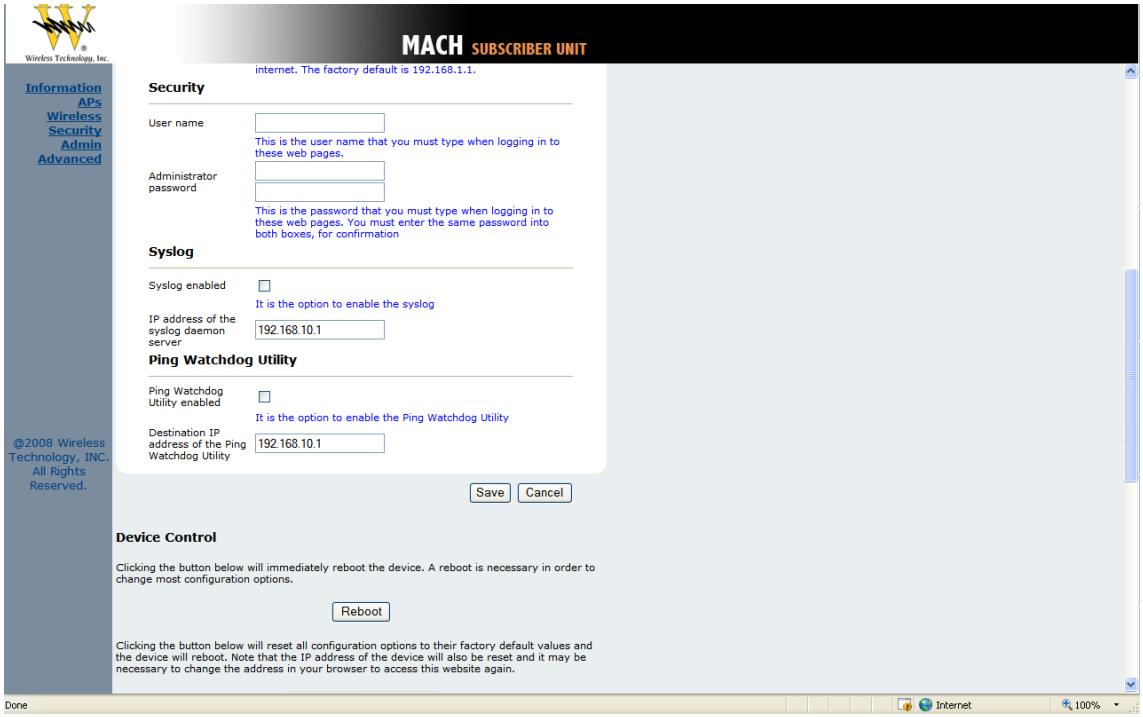
The default Client Bridge Mode IP address: 192.168.10.241

Default Subnet Mask

The factory subnet default value is 255.255.255.0

Default Gateway

The factory gateway default address is 192.168.10.1



Security

This section is used to set up the administrative login name and password.

User Name
This is the user name that you must type when logging into the web interface.

Administrator Password
This is the password that you must type when logging into the web interface. You must enter the same password into both boxes for confirmation.

Syslog

Syslog Enabled
Option to enable or disable Syslog support.

Syslog Daemon Server
The Syslog server IP address input box.

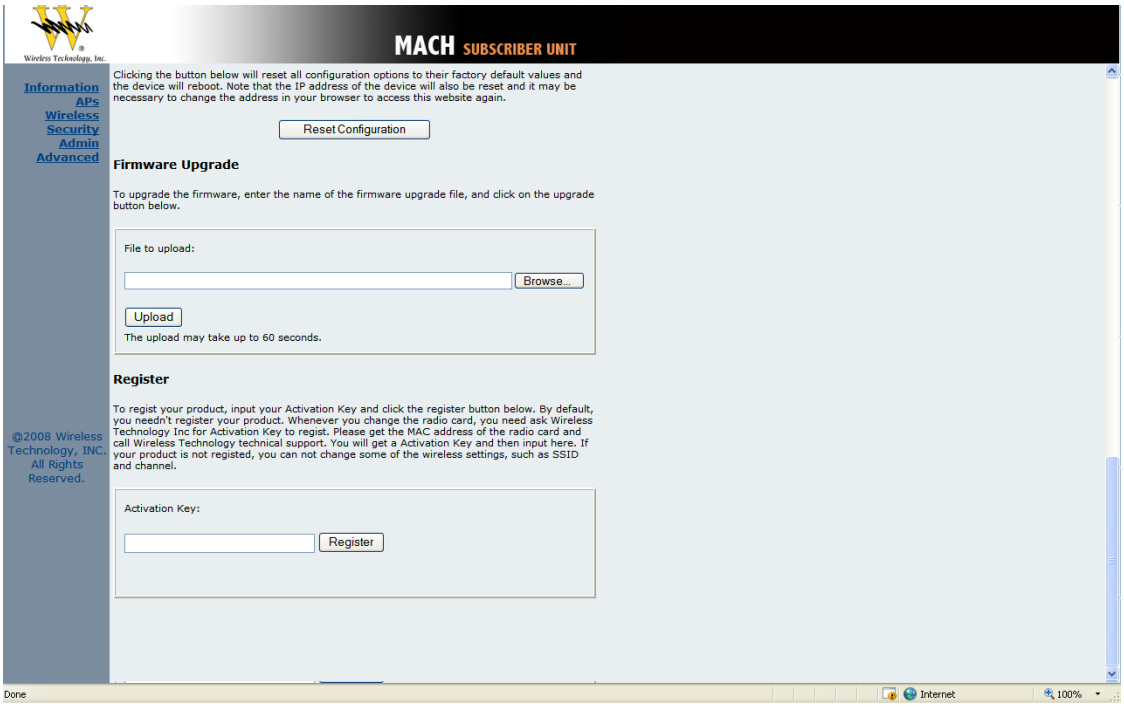
Ping Watchdog Utility

Ping Watchdog Utility Enabled
If enabled, the Ping Watchdog utility tracks the TCP/IP link between this device and another remote destination at the other end of the wireless link. When the remote destination is unreachable (loss of connection) the Ping Watchdog Utility will reboot the unit in an attempt to re-establish the connection. When the TT is up for 2 minutes, the ping watchdog utility will start to ping the remote network device every 20 seconds, if there is no icmp response 3 times in a row then the ping watchdog will kick off the reboot action.

Destination IP Address of the Ping Watchdog Utility
This is the IP address of the remote destination.

Device Control

This section has functions that will allow the MACH V to Reboot and Reset the system configuration to factory defaults.



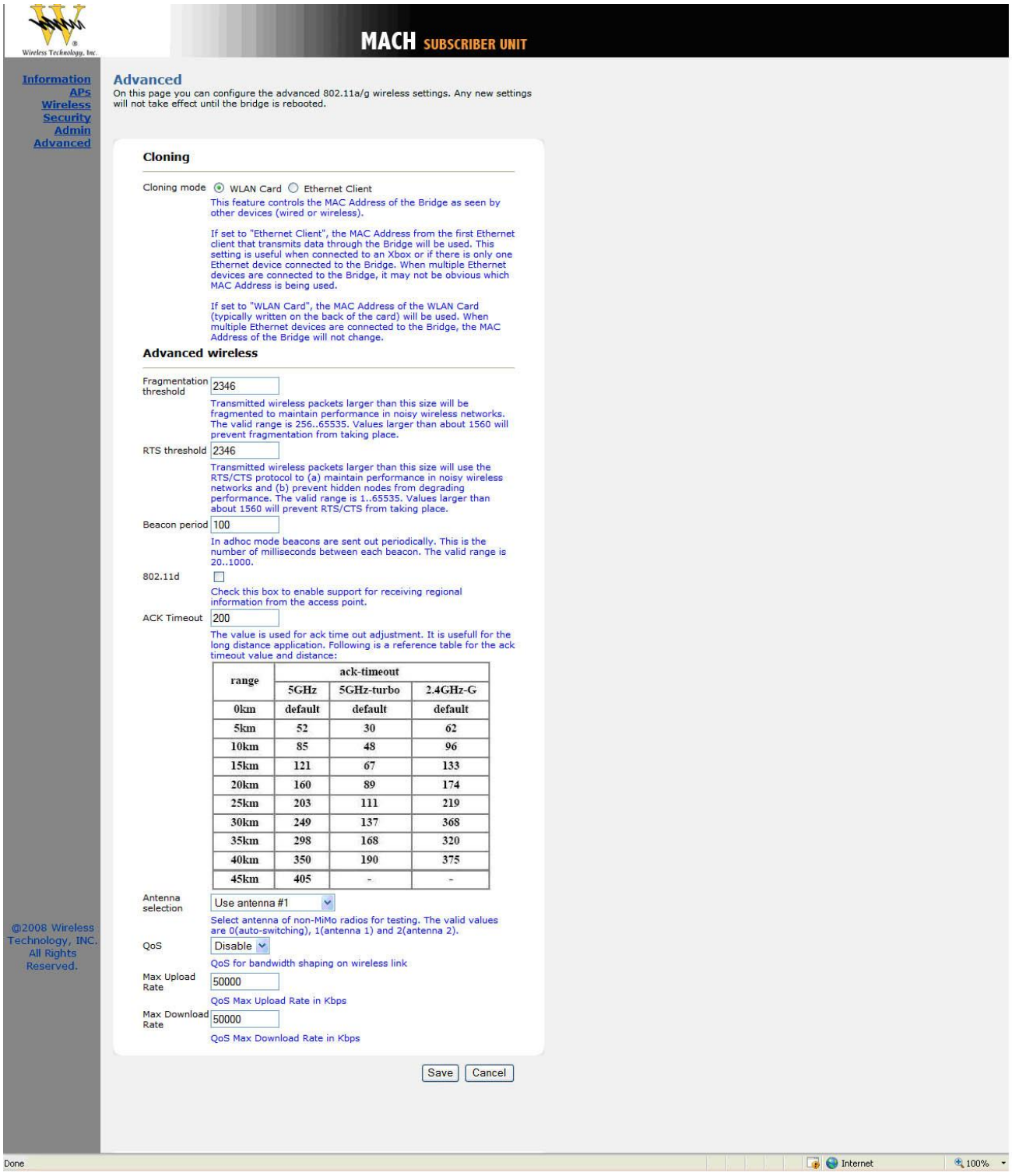
Firmware Upgrade

This section allows the MACH V firmware to be upgraded or changed directly from the web interface. Click on the Browse button to select a file from the host machine.

Register

The MACH V has implemented a hardware modification authorization process to prevent use by fraudulent hardware from other manufacturers. This will require any hardware change on the radio card used on the MACH V to input a serial code generated based on each unique MAC address. Please contact WTI's Support to pickup a valid serial number to deactivate the pre-registration protection after a radio card swap. If the unit is not registered some features such as SSID and Wireless Channel selection will be disabled.

Advanced


MACH SUBSCRIBER UNIT
Information
APs
Wireless
Security
Admin
Advanced
Advanced
On this page you can configure the advanced 802.11a/g wireless settings. Any new settings will not take effect until the bridge is rebooted.
Cloning
Cloning mode WLAN Card Ethernet Client
This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless).
If set to "Ethernet Client", the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC Address is being used.
If set to "WLAN Card", the MAC Address of the WLAN Card (typically written on the back of the card) will be used. When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change.
Advanced wireless
Fragmentation threshold 2346
Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks. The valid range is 256..65535. Values larger than about 1560 will prevent fragmentation from taking place.
RTS threshold 2346
Transmitted wireless packets larger than this size will use the RTS/CTS protocol to (a) maintain performance in noisy wireless networks and (b) prevent hidden nodes from degrading performance. The valid range is 1..65535. Values larger than about 1560 will prevent RTS/CTS from taking place.
Beacon period 100
In adhoc mode beacons are sent out periodically. This is the number of milliseconds between each beacon. The valid range is 20..1000.
802.11d
Check this box to enable support for receiving regional information from the access point.
ACK Timeout 200
The value is used for ack time out adjustment. It is usefull for the long distance application. Following is a reference table for the ack timeout value and distance:
range | ack-timeout | | |
5GHz | 5GHz-turbo | 2.4GHz-G
0km default default default
5km 52 30 62
10km 85 48 96
15km 121 67 133
20km 160 89 174
25km 203 111 219
30km 249 137 368
35km 298 168 320
40km 350 190 375
45km 405 - -
Antenna selection Use antenna #1
Select antenna of non-MiMo radios for testing. The valid values are 0(auto-switching), 1(antenna 1) and 2(antenna 2).
QoS Disable
QoS for bandwidth shaping on wireless link
Max Upload Rate 50000
QoS Max Upload Rate in Kbps
Max Download Rate 50000
QoS Max Download Rate in Kbps
Save
Cancel
@2008 Wireless Technology, INC. All Rights Reserved.
Done
Internet
100%

Cloning

Cloning Mode

- WLAN Card: If set to "WLAN Card", the MAC Address of the WLAN Card will be used. When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change.
- Ethernet Client: If set to "Ethernet Client", the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This means the client MAC address will become the alias address to the Bridge.

Advanced Wireless

Fragmentation Threshold

Fragmentation Threshold is the maximum length of the frame beyond which payload must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because sending them occupies the channel for a longer period of time, increasing the chance that another station will transmit and cause collision. Reducing Fragmentation Threshold results in shorter frames that "busy" the channel for shorter periods, reducing packet error rate and resulting retransmissions. However, shorter frames also increase overhead, degrading maximum possible throughput, so adjusting this parameter means striking a good balance between error rate and throughput.

RTS Threshold

RTS Threshold is the frame size above which an RTS/CTS handshake will be performed before attempting to transmit. RTS/CTS asks for permission to transmit to reduce collisions but adds considerable overhead. Disabling RTS/CTS can reduce overhead and latency in WLANs where all stations are close together but can increase collisions and degrade performance in WLANs where stations are far apart and unable to sense each other to avoid collisions (aka Hidden Nodes). If you are experiencing excessive collisions you can try turning RTS/CTS on or (if already on) reduce RTS/CTS Threshold on the affected stations.

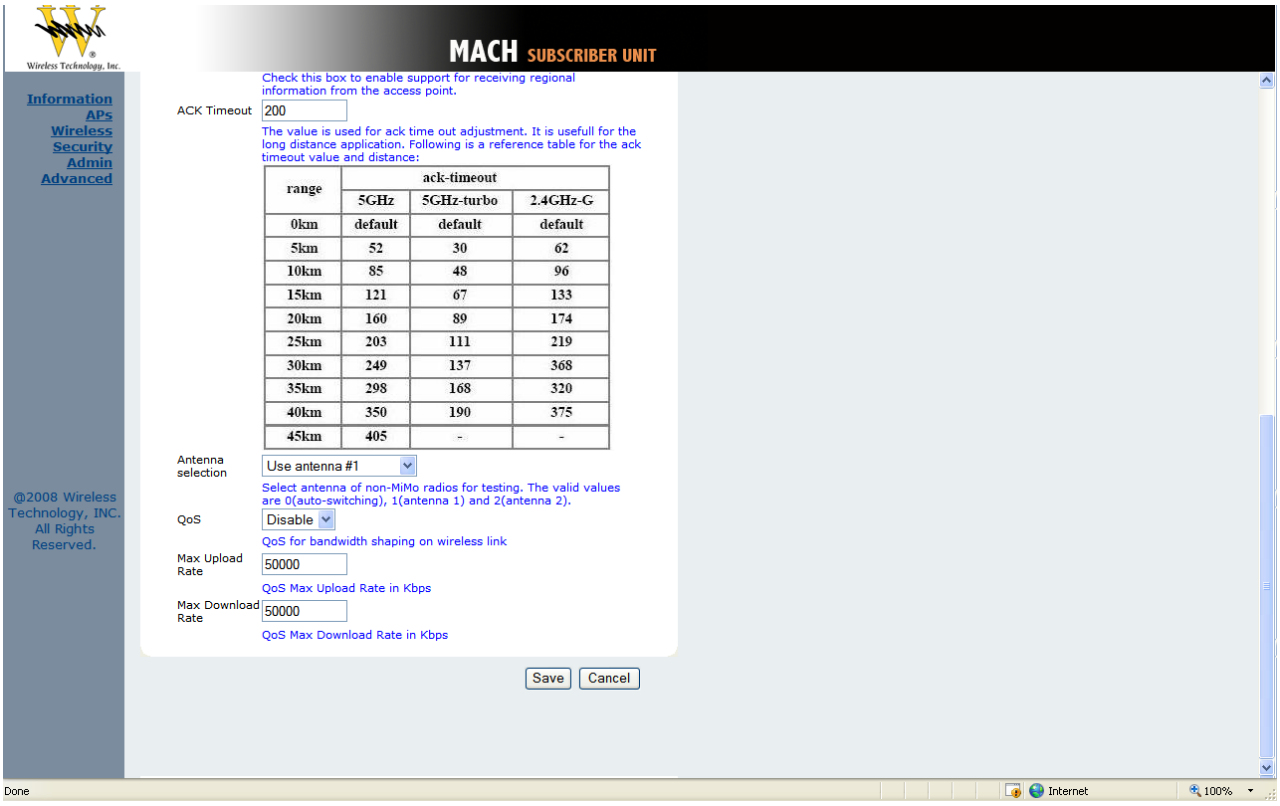
Beacon Period

In wireless networking, a beacon is a packet sent by a connected device to inform other devices of its presence and readiness. When a wirelessly networked device sends a beacon, it includes with it a beacon interval which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. Network managers can adjust the beacon interval, usually measured in milliseconds (ms) or its equivalent, kilo microseconds (K_sec).

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. The 802.11d specification is well suited for systems that want to provide global Roaming.

ACK Timeout



When a packet is sent out from 802.11 Station A it will wait for an 'ACKnowledgement frame' from 802.11 Station B. Station A will only wait for a certain amount of time (ACK timeout) or ACK window. If the ACK is NOT received within that timeout period then the packet will be re-transmitted from Station A resulting in reduced throughput. When sending LOTS of packets as in 802.11g and 802.11a the constant re-transmission could cost severe performance degradation due to the ACK frame not making it back to 802.11 Station A in time. This will have a dramatic impact on the throughput of the link regardless of the quantity of signal strength and good receiver sensitivity.

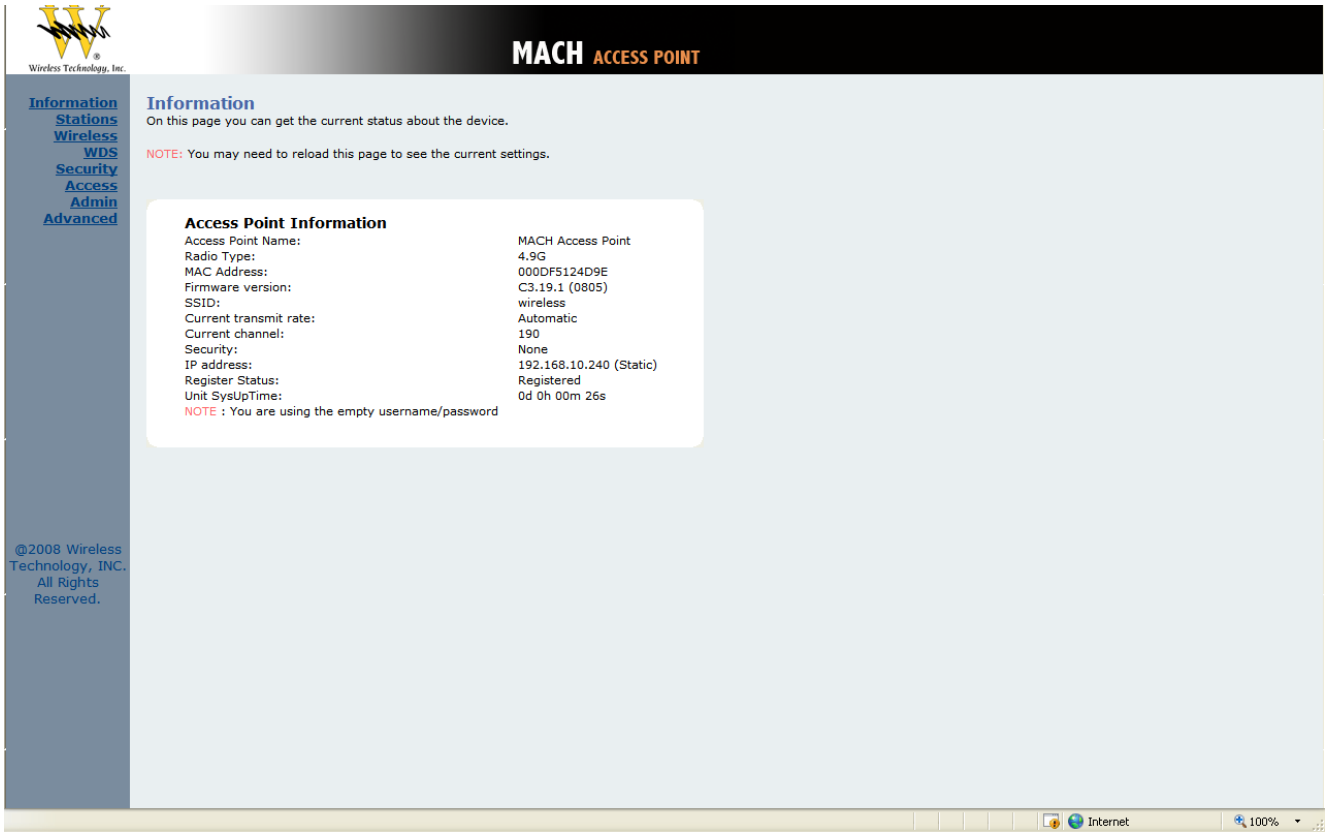
Default IP Address in Access Point Mode: **192.168.10.240.** To access the web control interface please open up a browser window and type in the factory default IP address in the URL.

Press Enter on your keyboard and a login prompt window similar to the one shown below will appear.

There is no default User name or Password. Leave User Name and Password field blank and then click OK.

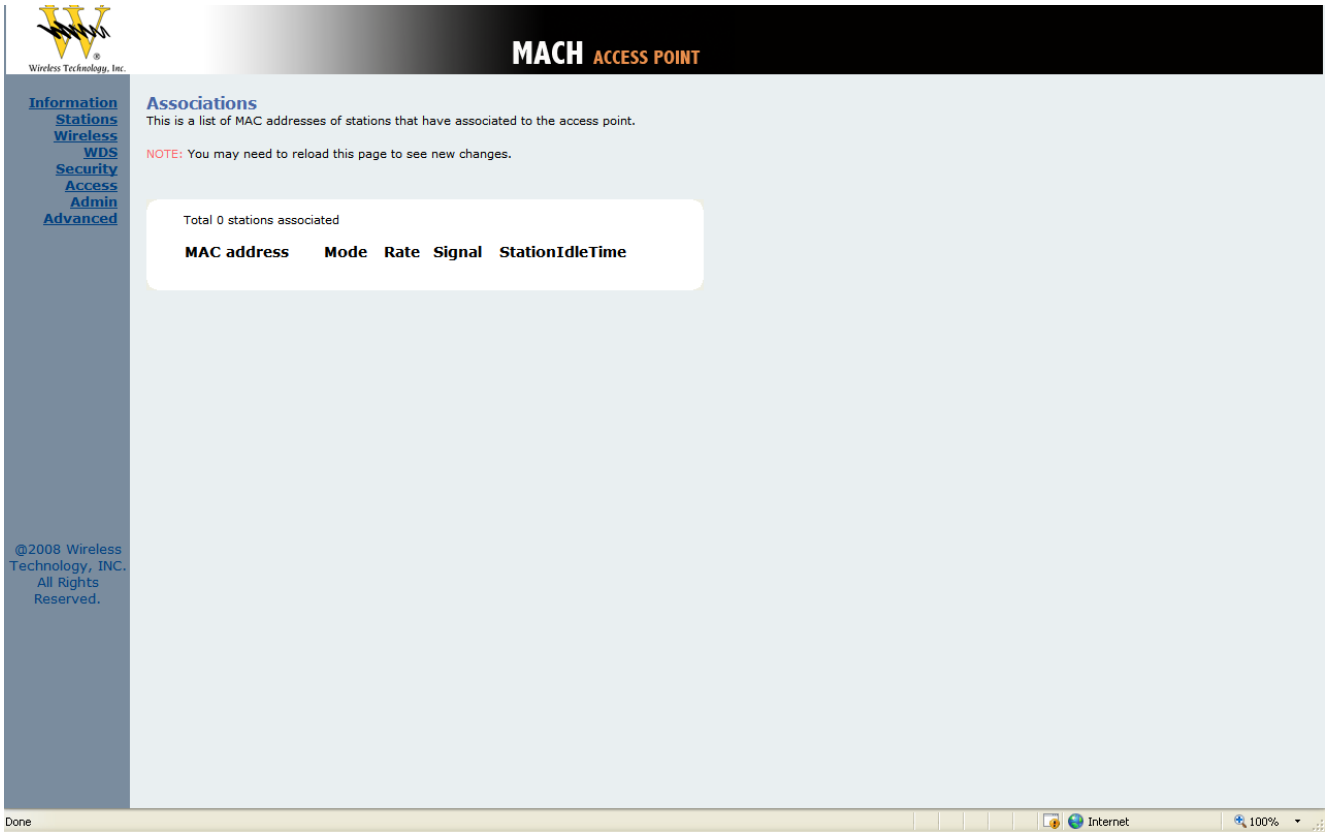
Note: You may set a new password by clicking the Admin tab after you enter the Web Configuration page

Information



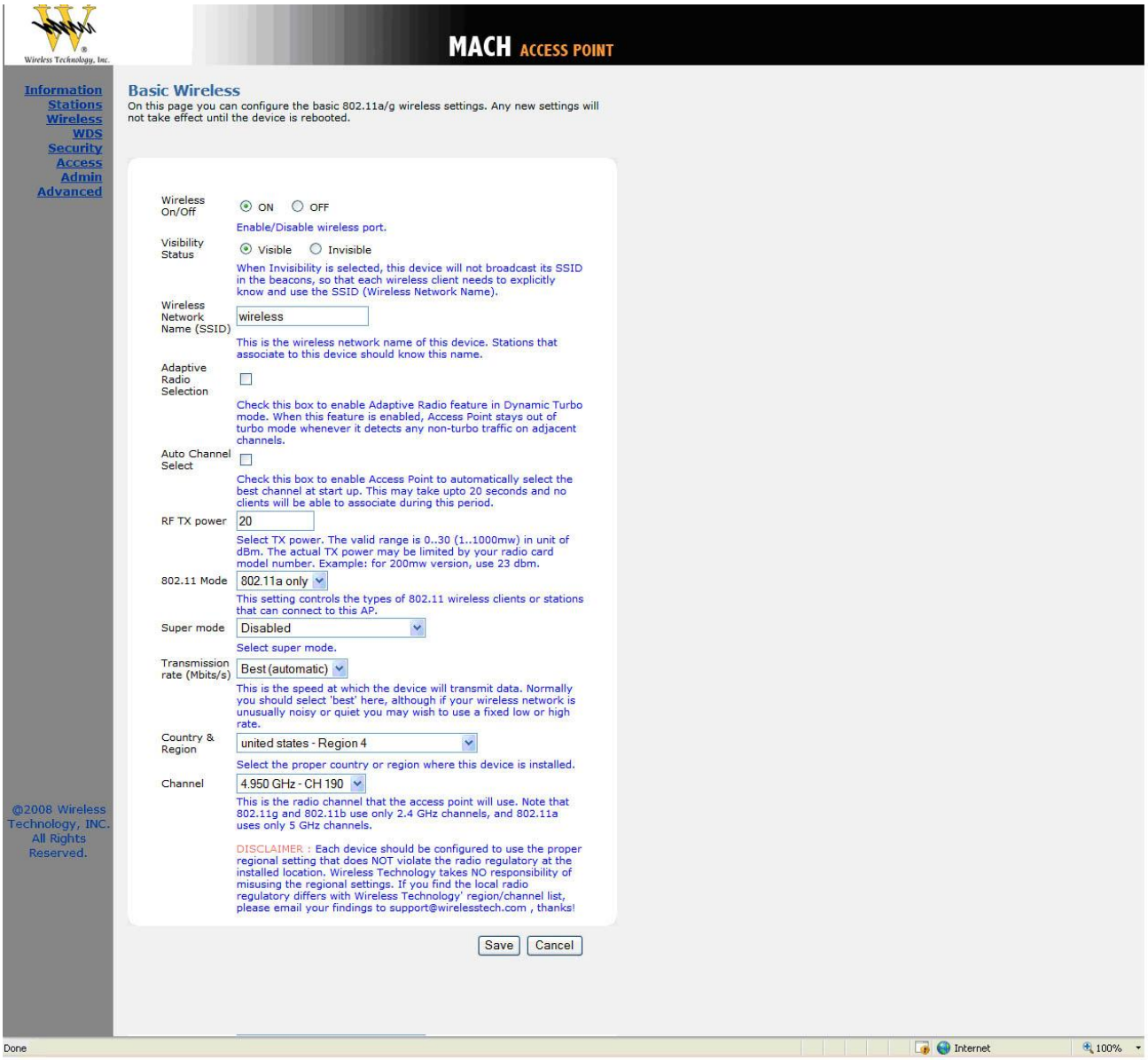
Under the main web interface home page you will see the following configuration menu pages: **Information, Stations, Wireless, WDS, Security, Access, Admin, Advanced.** Detailed information on each section is provided below.

Stations



The Stations section will display all the associated clients along with the MAC address and basic RF related information on the Mode, Rate, Signal and Station Idle Time for each associated client.

Wireless



Wireless On/Off

Enable or disable the wireless port.

Wireless Network Name (SSID)

Network Name is also known as SSID, which stands for Service Set Identifier. This is where you're going to setup the Service Set Identifier name for this AP. Remember that the SSID is cap sensitive just like the password.

Visibility Status
This controls the SSID broadcasting function. If enabled, the SSID will be broadcasted to all wireless clients in the area. If disabled, wireless clients will not be able to pickup the SSID but must explicitly know the SSID of the unit in order to associate. The recommended practice is to set the visibility status to invisible after setting up the wireless network.

Transmission Rate (Mbits/s)
This option indicates the transmission rate of the bridge. Specify the rate according to the speed of your wireless network from the list. Most of the time the default setting, Best (automatic), should be selected for best performance. The setting can be adjusted manually if the link quality and signal strength are unusually low or high to get the best performance.

802.11 Mode
Wireless mode allows the user to select whether this Access Point will connect to an 802.11b only network, an 802.11g only network, an 802.11a only network or both b/g networks. For b or g only wireless devices on the network, selecting 802.11b or 802.11g only mode will provide better performance than mixed mode. In the case of MACH V only 802.11a mode is allowed.

Adaptive Radio Selection
When using dynamic turbo mode with a compatible Atheros radio chipset, this option allows the Access point to switch to non-turbo mode when non-turbo traffic is detected and vice versa.

Super Mode
Super Mode is only supported if both the client and the AP are using compatible Atheros radio chipsets.

- Disabled
- Super A/G without Turbo
- Super A/G with Static Turbo
- Super A/G with Dynamic Turbo (AR enabled)

Auto Channel Select
Check this box to enable the Access Point to automatically select the best channel at start up. This may take up to 20 seconds and during this period no clients will be able to associate.

RF Transmit Power
This section controls the power output for the mini-PCI radio card. The valid input range for this section is in the range of 0-30 in dBm units. The default value is 23 dBm or 200mW.

Channel
Channels are important to understand because they affect the overall capacity of your Wireless LAN. A channel represents a narrow band of radio frequency. A radio frequency modulates within a band of frequencies; as a result there is a limited amount of bandwidth within any given range to carry data. It is important that the frequencies do not overlap or else the throughput would be significantly reduced as the network sorts and reassembles the data packets sent over the air.

For the MACH Series: 2.4 GHz – 2.497 GHz frequency range, there are only 3 channels out of the 11 available that do not overlap with one another. To avoid interference within a network with multiple APs, set each AP to use one of the 3 channels (e.g. Channel 1) and then the other AP to be one of the other 2 channels (i.e. Channel 6 or Channel 11) within the range of the wireless radio. This simple method will reduce interference and improve network reliability.

802.11b/g Wireless Channel Frequency Range: 2.4 GHz – 2.497 GHz

802.11b/g Non-overlapping Channel Frequency Ranges

- Channel 1 = 2.401 GHz – 2.423 GHz
- Channel 6 = 2.426 GHz – 2.448 GHz
- Channel 11 = 2.451 GHz – 2.473 GHz

Americas: Wireless Channels 1 – 11

Asia: Wireless Channels 1 – 14

Europe: Wireless Channels 1 – 13

802.11a Wireless Channel Frequency Range: 5.15 GHz – 5.35 GHz, 5.725 – 5.825

802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band.

802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. Unlike that of 802.11b/g, 802.11a standard separates its channels into 3-100MHz segments in the US. The lower and middle band accommodates 8 channels in a total bandwidth of 200 MHz and the upper band accommodates 4 channels in a 100 MHz bandwidth. The frequency channel center frequencies are spaced 20 MHz apart. The outermost channels of the lower and middle bands are centered 30 MHz from the outer edges. In the upper band the outermost channel centers are 20 MHz from the outer edges.

In addition to the frequency and channel allocations, transmit power is a key parameter regulated in the 5 GHz U-NII band. Three transmit power levels are specified: 40 mW, 200 mW and 800 mW. The upper band defines RF transmit power levels suitable for bridging applications while the lower band specifies a transmit power level suitable for shortrange indoor home and small office environments.

802.11a Non-overlapping Channel Frequency Ranges

Lower Band (5.15 - 5.25 GHz) – Maximum Output Power 40mW

- Channel 36 = 5.15 – 5.18
- Channel 40 = 5.18 – 5.20
- Channel 44 = 5.20 – 5.22
- Channel 48 = 5.22 – 5.25

Middle Band (5.25 - 5.35 GHz) – Maximum Output Power 200mW

- Channel 52 = 5.25 – 5.28
- Channel 56 = 5.28 – 5.30
- Channel 60 = 5.30 – 5.32
- Channel 64 = 5.32 – 5.35

Upper Band (5.725 - 5.825 GHz) – Maximum Output Power 800mW

- Channel 149 = 5.725 – 5.745
- Channel 153 = 5.745 – 5.765
- Channel 157 = 5.765 – 5.785
- Channel 161 = 5.785 – 5.805
- Channel 165 = 5.805 – 5.825

Special Atheros Turbo Mode Channels

Use this setting only when both side of the wireless connection is using the Atheros chipset. The radio will combine 2 free channels for the wireless transmission to double the bandwidth.

- Channel 42 = 5.210
- Channel 50 = 5.250
- Channel 58 = 5.290
- Channel 152 = 5.760
- Channel 160 = 5.800

WDS (Wireless Distribution System)

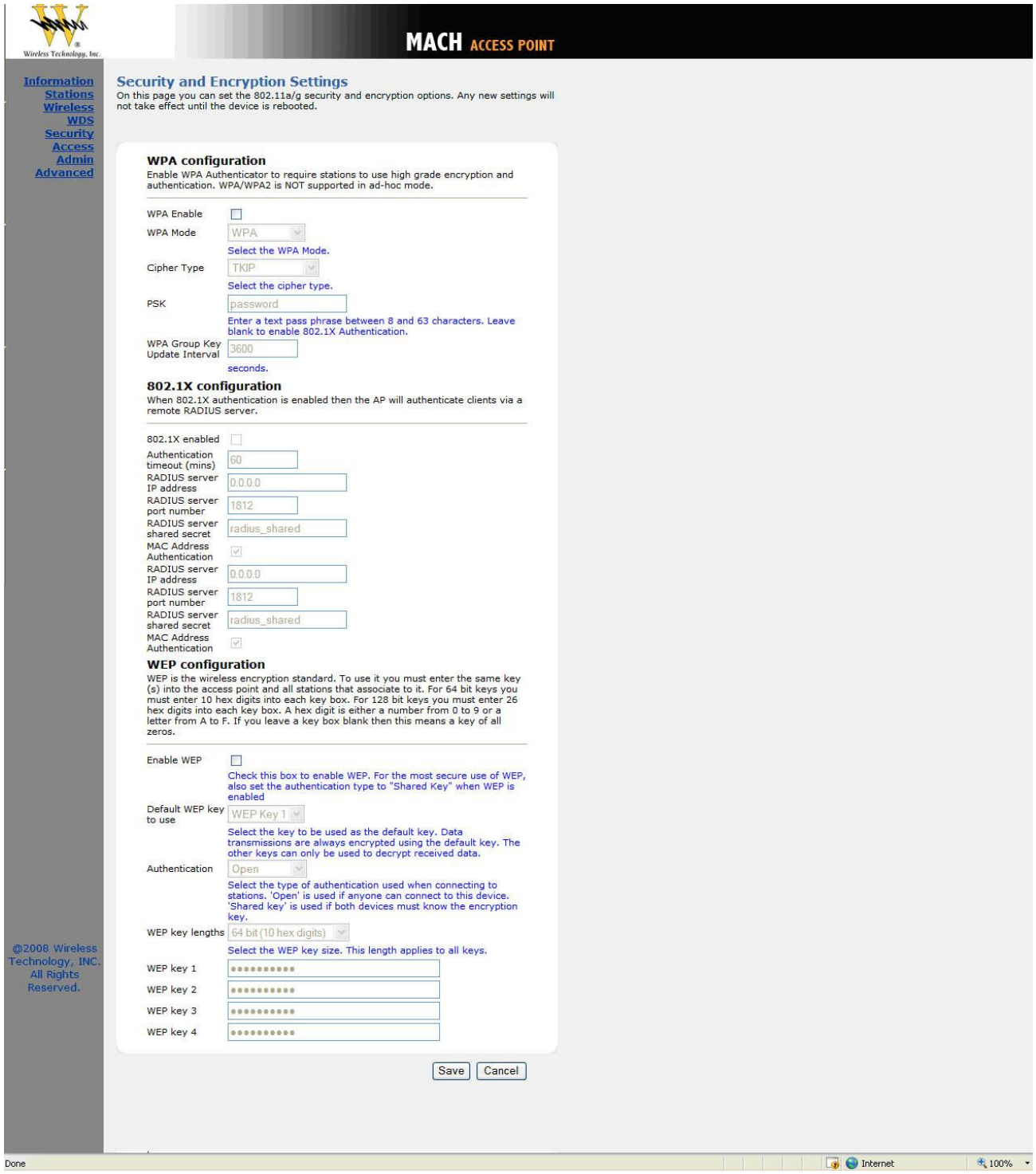
Enable WDS

The Wireless Distribution System (Repeater) functionality enables this AP to support wireless traffic to other WDS relay Access Points. In other words it is like bridging between the 2 access points in order to extend the reach of the wireless network beyond that of a single AP. By enabling the WDS feature the coverage area of the wireless network is thus extended for authenticated client devices that can roam from this Access Point to another. WDS can extend the reach of your network into areas where cabling might be difficult. The MACH V in Access Point mode can support up to 6 other Access Points for WDS communication.

Enter the MAC Address of other Access Points in the area that you want to add to the WDS. The MAC Address of this Access Point should be also be added to other access points in the same WDS network to enable intra-AP communication.

* ***Please consult page 50 for a more detailed explanation of* WDS.**

Security


MACH ACCESS POINT
Information
Stations
Wireless
WDS
Security
Access
Admin
Advanced
Security and Encryption Settings
On this page you can set the 802.11a/g security and encryption options. Any new settings will not take effect until the device is rebooted.
WPA configuration
Enable WPA Authenticator to require stations to use high grade encryption and authentication. WPA/WPA2 is NOT supported in ad-hoc mode.
WPA Enable
WPA Mode
WPA
Select the WPA Mode.
Cipher Type
TKIP
Select the cipher type.
PSK
password
Enter a text pass phrase between 8 and 63 characters. Leave blank to enable 802.1X Authentication.
WPA Group Key Update Interval
3600
seconds.
802.1X configuration
When 802.1X authentication is enabled then the AP will authenticate clients via a remote RADIUS server.
802.1X enabled
Authentication timeout (mins)
60
RADIUS server IP address
0.0.0.0
RADIUS server port number
1812
RADIUS server shared secret
radius_shared
MAC Address Authentication
RADIUS server IP address
0.0.0.0
RADIUS server port number
1812
RADIUS server shared secret
radius_shared
MAC Address Authentication
WEP configuration
WEP is the wireless encryption standard. To use it you must enter the same key (s) into the access point and all stations that associate to it. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. If you leave a key box blank then this means a key of all zeros.
Enable WEP
Check this box to enable WEP. For the most secure use of WEP, also set the authentication type to "Shared Key" when WEP is enabled
Default WEP key to use
WEP Key 1
Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
Authentication
Open
Select the type of authentication used when connecting to stations. 'Open' is used if anyone can connect to this device. 'Shared key' is used if both devices must know the encryption key.
WEP key lengths
64 bit (10 hex digits)
Select the WEP key size. This length applies to all keys.
WEP key 1
WEP key 2
WEP key 3
WEP key 4
Save
Cancel
@2008 Wireless Technology, INC. All Rights Reserved.
Done
Internet
100%

WPA Configuration
Short for Wi-Fi Protected Access, WPA is a Wi-Fi standard that was designed to improve upon the security features of WEP. WPA has the following improvements over WEP:

- Improved data encryption through temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm. By adding an integrity-checking feature, TKIP ensures that keys have not been tampered with.
- User authentication through the Extensible Authentication Protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA Enable
This option enables the WPA Authenticator. Note that any client that does not support the WPA standard will not be able to handshake / authenticate with a WPA enabled device.

WPA Mode
WPA: Designed to secure present and future versions of IEEE 802.11 devices, WPA is a subset of the IEEE 802.11i specification. WPA addresses all known vulnerabilities in WEP. WPA also provides user authentication, since WEP lacks any means of authentication. WPA replaces WEP with a strong new encryption technology called Temporal Key Integrity Protocol (TKIP) with Message Integrity Check (MIC). It also provides a scheme of mutual authentication using IEEE 802.1X/Extensible Authentication Protocol (EAP) authentication or pre-shared key (PSK) technology. WPA was designed and has been scrutinized by well-known cryptographers. It can be implemented immediately and inexpensively as a software or firmware upgrade to most existing Wi-Fi CERTIFIED™ access points and client devices with minimal degradation in network performance. WPA offers standards-based, Wi-Fi CERTIFIED security. It assures users that the Wi-Fi CERTIFIED devices they buy will be cross-vendor compatible. When properly installed, WPA provides a high level of assurance to enterprises, small businesses and home users that data will remain protected and that only authorized users may access their networks. For enterprises that have already deployed IEEE 802.1X authentication, WPA offers the advantage of leveraging existing authentication databases and infrastructure.

WPA2: WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi® users with a high level of assurance that only authorized users can access their wireless networks. Launched in September 2004 by the Wi-Fi Alliance, WPA2 is the certified interoperable version of the full IEEE 802.11i specification which was ratified in June 2004. Like WPA, WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. It also includes a new advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). AES satisfies U.S. government security requirements. It has been adopted as an official government standard by the U.S. Department of Commerce and the National Institute of Standards and Technology (NIST). Organizations that require the AES encryption available in WPA2 should be aware that upgrading to it may require new hardware. Section II of this document offers a roadmap for organizations planning to upgrade to WPA2. Considerations for its deployment are outlined in Section III.

Cipher Type

- TKIP: Temporal Key Integrity Protocol is an upgrade to the WEP known as WEP 1.1 that fixes known security problems in WEP's implementation of the RC4 stream cipher. TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- AES: Advanced Encryption Standard (Rijndael Cypher) is the U.S. government's next-generation cryptography algorithm, which will replace DES and 3DES. AES works at multiple network layers simultaneously. AES Supports 128, 192 and 256 bit keys. Unlike the older standard, AES and 802.11i (WEP version 2) are based on 32bit processing.
- TKIP and AES: If clients support both the TKIP and AES standards then this would be the strongest cipher type to use that combines both TKIP and AES security.

PSK

PSK stands for Pre-Shared-Key and serves as a password. User may key in 8 to 63 characters string to set the password and activate 802.1x Authentication. Note that the same password must be used at both ends of the communication link (access point and client end).

WPA Group Key Update Interval

The Group Key (Group Transient Key) is a shared key among all Supplicants connected to the same AP, and is used to secure multicast/broadcast traffic. It is not used for normal unicast traffic. A pair wise Transient Key secures the unicast traffic. Group Key renewal controls how often the Group Transient Key is changed. The Group Key renewal does not control the update period for the pair wise Transient Key. The pair wise Transient Key is changed each time the Supplicant authenticates or re-authenticates.

802.1X Configuration

Remote RADIUS server configuration settings. There are two sections to setup 2 RADIUS servers for the MACH V to connect to. At any given time the MACH V will connect to one RADIUS server for authentication and will use the other one as a backup if that option is configured.

802.1X Enabled

Option that enables or disables remote RADIUS authentication.

Authentication Timeout (minutes)

The default value is 60 (minutes). When the time expires, the device will re-authenticate with RADIUS server.

RADIUS Server IP Address

Enter the RADIUS server IP address.

RADIUS Server Port Number

Port used for RADIUS, the port number must be the same as the RADIUS server's, normally the port is 1812.

RADIUS Server Shared Secret
When registered with a RADIUS server, a password will be assigned. This would be the RADIUS server shared secret.

MAC Address Authentication
Use client MAC address for authentication with RAIDUS server.

WEP Configuration
Short for Wired Equivalent Privacy, a security protocol for wireless local area networks (WLANs) defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN.

Enable WEP
To enable the WEP Authenticator

Default WEP Key to Use
WEP Key 1-4
Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.

Authentication
Open - Open system authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If it is "successful", the station shall be mutually authenticated. Open system authentication does not provide authentication. It provides identification using the wireless adapter's MAC address. Open system authentication is used when no authentication is required. It is the default authentication algorithm.

Open system authentication uses the following process:

1. The authentication-initiating wireless client sends an IEEE 802.11 authentication management frame that contains its identity.
2. The receiving wireless AP checks the initiating station's identity and sends back an authentication verification frame.
3. With some wireless APs, you can configure the MAC addresses of allowed wireless clients. However, configuring the MAC address does not provide sufficient security because the MAC address of a wireless client can be spoofed.

Shared Key - Shared key authentication supports authentication of stations as either a member of those who know a shared secret key or a member of those who do not. Shared key authentication is not secure and is not recommended for use. It verifies that an authentication-initiating station has knowledge of a shared secret. This is similar to pre-shared key authentication for Internet Protocol security (IPSec). The 802.11 standard currently assumes that the shared secret is delivered to the participating wireless clients by means of a more secure channel that is independent of IEEE 802.11. In practice, a user manually types this secret for the wireless AP and the wireless client.

Shared key authentication uses the following process:

1. The authentication-initiating wireless client sends a frame consisting of an identity assertion and a request for authentication.
2. The authenticating wireless node responds to the authentication-initiating wireless node with challenge text.
3. The authentication-initiating wireless node replies to the authenticating wireless node with the challenge text that is encrypted using WEP and an encryption key that is derived from the shared key authentication secret.
4. The authentication result is positive if the authenticating wireless node determines that the decrypted challenge text matches the challenge text originally sent in the second frame. The authenticating wireless node sends the authentication result.
5. Because the shared key authentication secret must be manually distributed and typed, this method of authentication does not scale appropriately in large infrastructure network mode, such as corporate campuses.

WEP Key Lengths

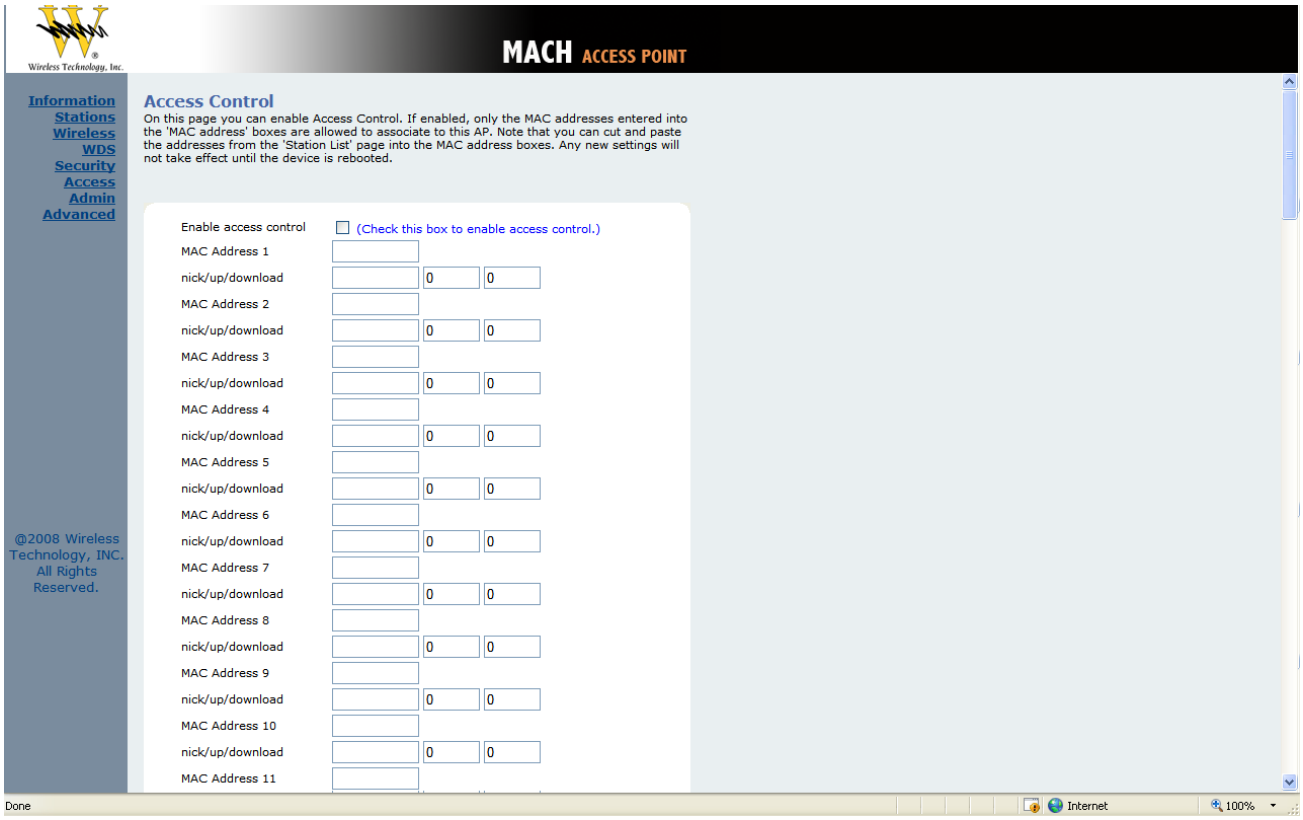
64 *bit* (10 H*ex* D*igit*)

WEP Key type	Example
64-bit WEP with 5 characters	Key1= 2e3f4 Key2= 5y7js Key3= 24fg7 Key4= 98jui
64-bit WEP with 10 hexadecimal digits ('0-9', 'A-F')	Key1= 123456789A Key2= 23456789AB Key3= 3456789ABC Key4= 456789ABCD

128 *bit* (26 H*ex* D*igit*)

WEP Key type	Example
128-bit WEP with 13 characters	Key1= 2e3f4w345ytre Key2= 5y7jse8r4i038 Key3= 24fg70okx3fr7 Key4= 98jui2wss35u4
128-bit WEP with 26 hexadecimal digits ('0-9', 'A-F')	Key1= 112233445566778899AABBCDEF Key2= 2233445566778899AABBCCDDEE Key3= 3344556677889900AABBCCDDFF Key4= 44556677889900AABBCCDDEEFF

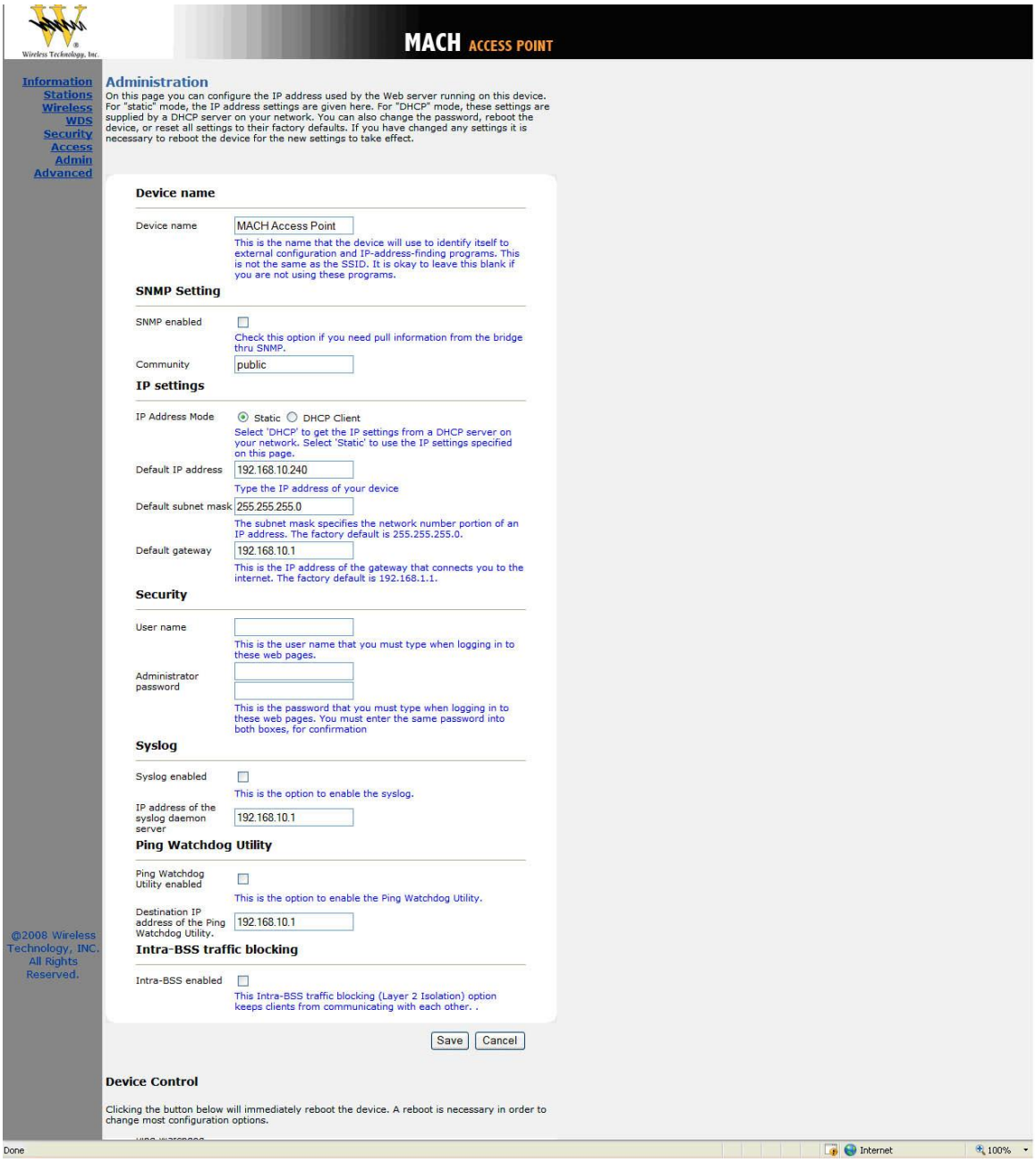
Access Control



Enable Access Control

If enabled, this feature allows you to associate up to 64 different units/devices by MAC addresses. Any MAC addresses not programmed into the list will be prohibited from associating with this unit.

Administration



Device Name

This is the name that the Access Point will use to identify itself to external configuration and IP address programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

SNMP Setting

SNMP Enabled
Option to enable or disable SNMP support

Community
The SNMP Read-only Community string is like a user id or password that allows access to a router's or other device's statistics. InterMapper sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.

Factory default setting for the read-only community string is set to "public." It is standard practice to change all the community strings so that outsiders cannot access/read information about the internal network. (In addition, the administrator may also employ firewalls to block any SNMP traffic to ports 161 and 162 on the internal network). Change this value to have InterMapper use the new string when querying SNMP devices.

IP Settings

IP Address Mode

- **Static**
  - Manually setup a static IP address for this device.
- **DHCP**
  - Set up the access point as a DHCP client which will pick up an IP from a DHCP server.

Default IP Address
The default Access Point Mode IP address: 192.168.10.240

Default Subnet Mask
The factory subnet default value is 255.255.255.0

Default Gateway
The factory gateway default address is 192.168.10.1

Security
This section is used to set up the administrative login name and password.

User Name
This is the user name that you must type when logging into the web interface.

Administrator Password
This is the password that you must type when logging into the web interface. You must enter the same password into both boxes for confirmation.

Syslog

Syslog Enabled
Option to enable or disable Syslog support.

Syslog Daemon Server
The Syslog server IP address input box.

Ping Watchdog Utility

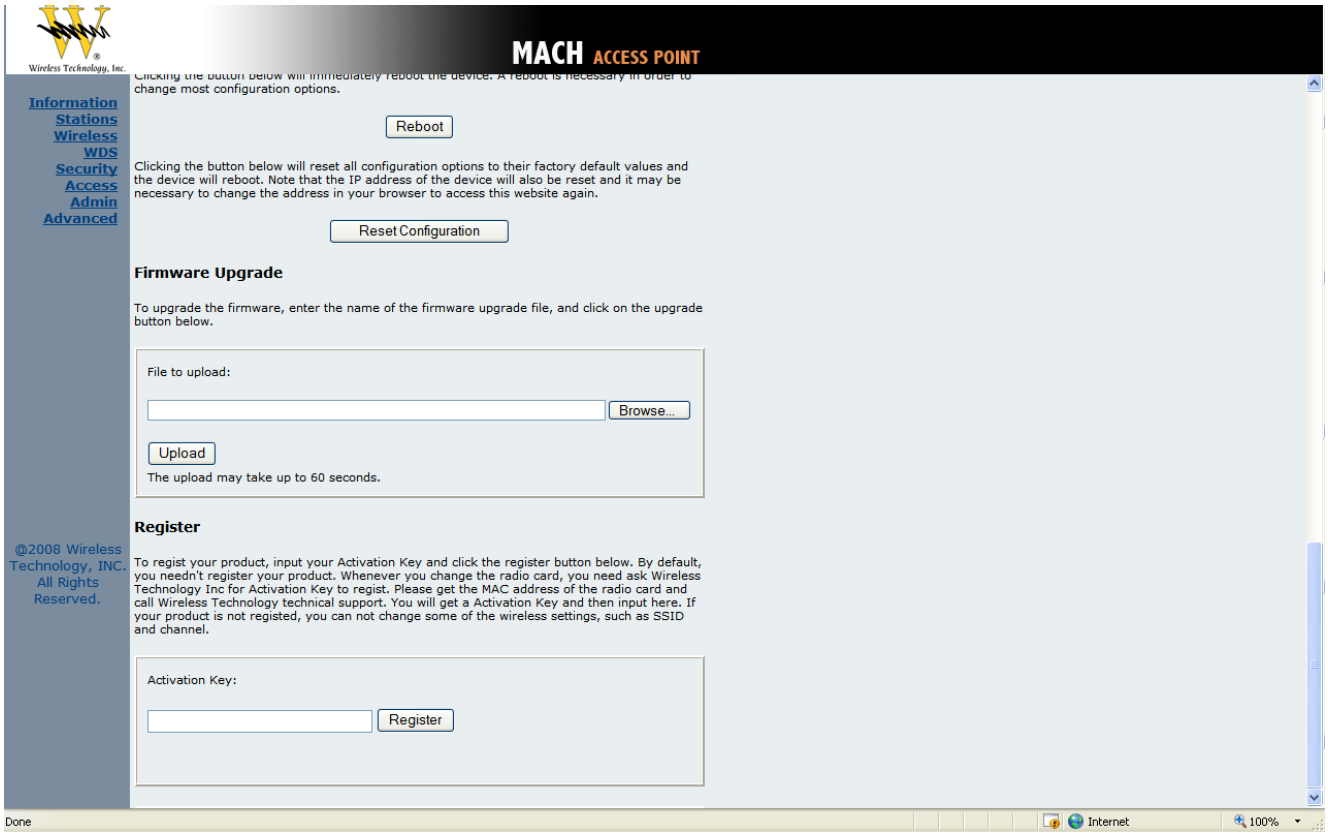
Ping Watchdog Utility Enabled
If enabled, the Ping Watchdog utility tracks the TCP/IP link between this device and another remote destination at the other end of the wireless link. When the remote destination is unreachable (loss of connection) the Ping Watchdog Utility will reboot the unit in an attempt to re-establish the connection.

Destination IP Address of the Ping Watchdog Utility
This is the IP address of the remote destination.

Intra-BSS Traffic Blocking
This option blocks clients in the same BSS from communicating with each other. (Layer 2 Isolation)

Device Control

This section has functions that will allow the MACH V to Reboot and Reset the system configuration to factory defaults.



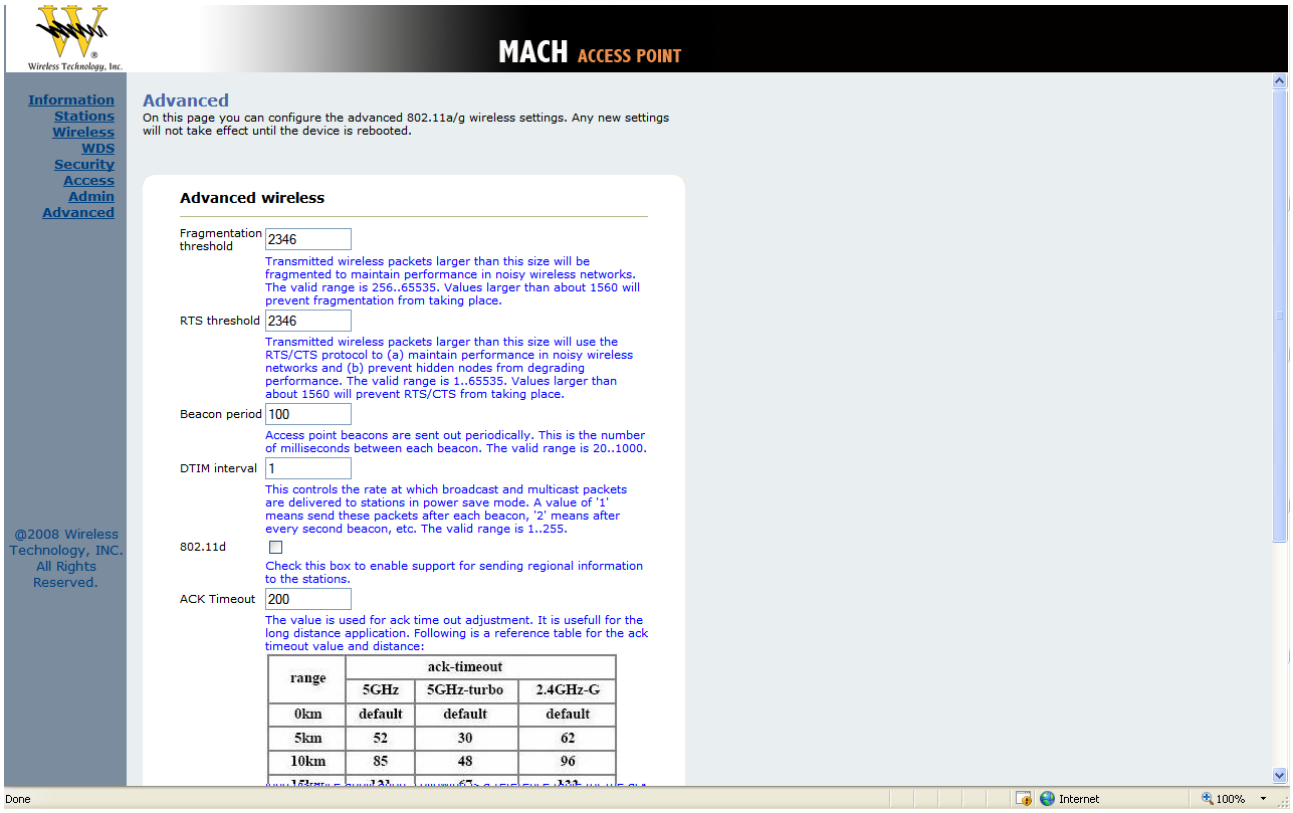
Firmware Upgrade

This section allows the MACH V firmware to be upgraded or changed directly from the web interface. Click on the Browse button to select a file from the host machine.

Register

The MACH V has implemented a hardware modification authorization process to prevent use by fraudulent hardware from other manufacturers. This will require any hardware change on the radio card used on the MACH V to input a serial code generated based on each unique MAC address. Please contact WTI's Solutions Specialists to a pickup a valid serial number to deactivate the pre-registration protection after a radio card swap. If the unit is not registered some features such as SSID and Wireless Channel selection will be disabled.

Advanced



Fragmentation Threshold

Fragmentation Threshold is the maximum length of the frame beyond which payload must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because sending them occupies the channel for a longer period of time, increasing the chance that another station will transmit and cause collision. Reducing
Fragmentation Threshold results in shorter frames that "busy" the channel for shorter periods, reducing packet error rate and resulting retransmissions. However, shorter frames also increase overhead, degrading maximum possible throughput, so adjusting this parameter means striking a good balance between error rate and throughput.

RTS Threshold

RTS Threshold is the frame size above which an RTS/CTS handshake will be performed before attempting to transmit. RTS/CTS asks for permission to transmit to reduce collisions but adds considerable overhead. Disabling RTS/CTS can reduce overhead and latency in WLANs where all stations are close together but can increase collisions and degrade performance in WLANs where stations are far apart and unable to sense each other to avoid collisions (aka Hidden Nodes). If you are experiencing excessive collisions you can try turning RTS/CTS on or (if already on) reduce RTS/CTS Threshold on the affected stations.

Beacon Period

In wireless networking, a beacon is a packet sent by a connected device to inform other devices of its presence and readiness. When a wirelessly networked device sends a beacon, it includes with it a beacon interval which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. Network managers can adjust the beacon interval, usually measured in milliseconds (ms) or its equivalent, kilo microseconds (K_sec).

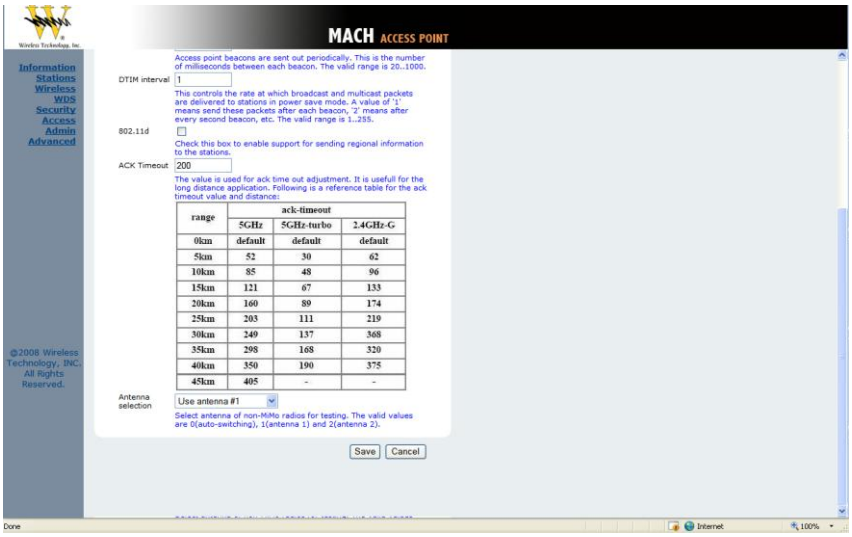
DTIM Interval

A Delivery Traffic Indication Message (DTIM) is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery. A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM. This frequency is usually measured in milliseconds (ms) or its equivalent, kilo microseconds (K_sec).

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. The 802.11d specification is well suited for systems that want to provide global roaming.

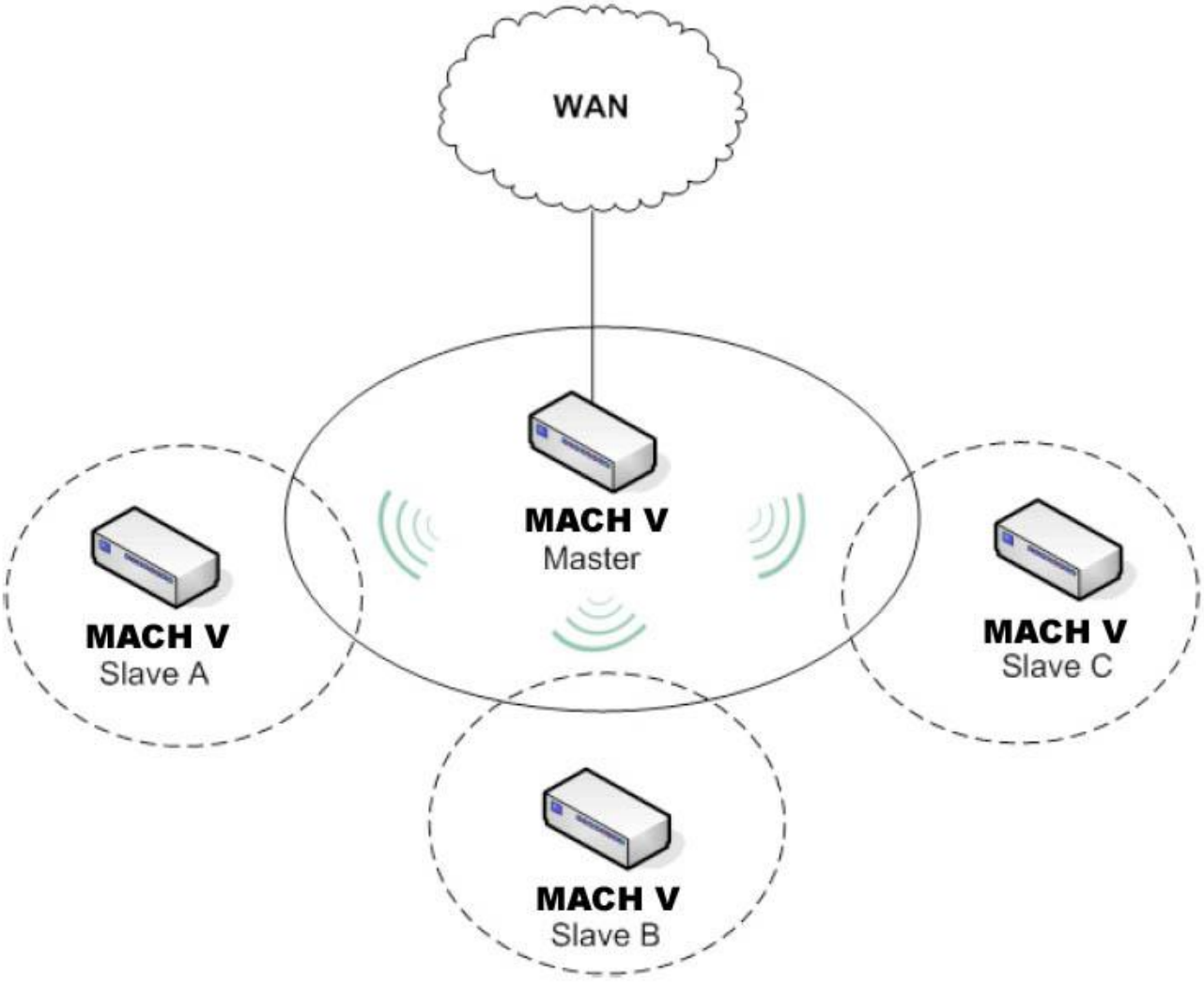
ACK Timeout



When a packet is sent out from 802.11 Station A it will then wait for an 'ACKnowledgement frame' from 802.11 Station 48 B. Station A will only wait for a certain amount of time (ACK timeout) or ACK window. If the ACK is NOT received within that timeout period then the packet will be re-transmitted from Station A resulting in reduced throughput. When sending lots of packets as in 802.11g and 802.11a the constant re-transmission could cost severe performance degradation due to the ACK frame not making it back to 802.11 Station A in time. This will have a dramatic impact on the throughput of the link regardless of signal strength or good receiver sensitivity.

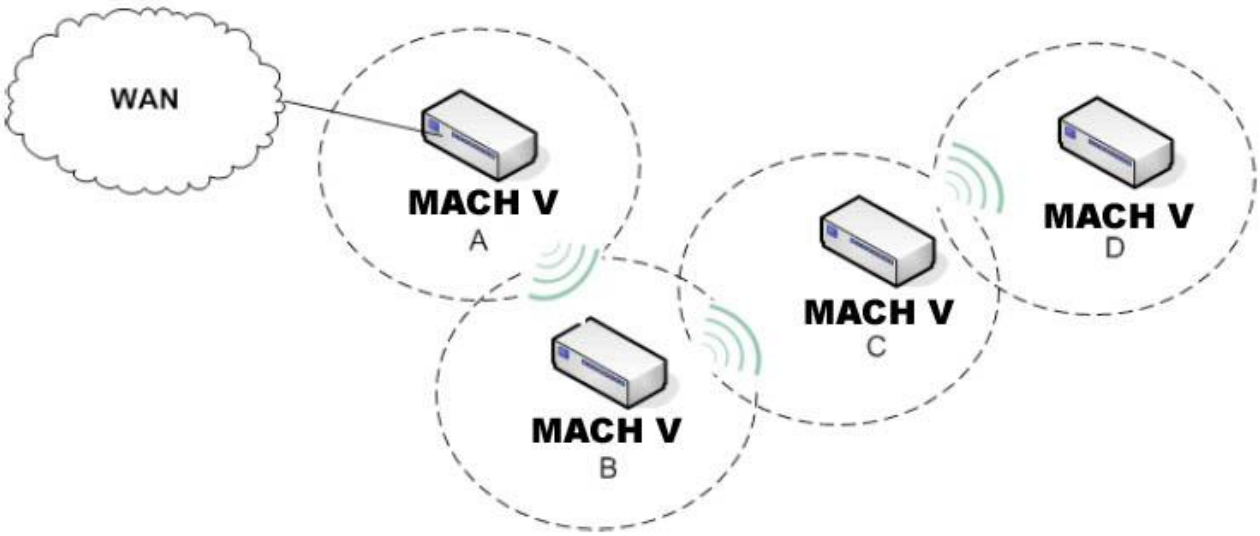
One of the requirements for a WDS network is that the operational frequency channel on all the APs must be the same. This is one of the reasons why there is a huge bandwidth penalty when setting up a wireless network in WDS mode. How to properly configure your APs in a WDS network will foremost depend on the locations of your wireless hotspots. Please take a look at the following two WDS topology examples:

WDS in a Star Configuration:



This is the mode to use if you're expanding the hotspots in the area around your master AP that is connected to the WAN. What you'll need to do is enable WDS and ACL on all the APs. Then input each of the MAC addresses of Slave A,B,C into the Master AP under both the WDS and ACL section. For the Slave APs A,B,C you'll input only the MAC address of the Master AP into the WDS and ACL list to limit them to direct their traffic through the Master AP only.

WDS in Chain Configuration:



In this configuration setup example you'll be expanding your wireless network coverage that will span an area in length.

- AP A will have only AP B's MAC address in its WDS and ACL configuration setting.
- AP B will have AP A and C's MAC address in its WDS and ACL configuration setting.
- AP C will have AP B and D's MAC address in its WDS and ACL configuration setting.
- AP D will have only AP C's MAC address in its WDS and ACL configuration setting.

How do I upgrade?
The MACH V could be upgraded either through the web interface. Please check Web Configuration Interface and Installation sections of this manual for detailed instructions.

Will upgrading keep my previous configuration?
Although the upgrade might keep your previous configuration, we suggest customer to reset the unit to factory default located in "admin" section and configure it again.

PROBLEM: I can not access the MACH V through the web browser.
POSSIBLE SOLUTIONS:

- Check that the IP address in the URL field is correct.
- Check your host computer IP address. If the IP address of the MACH V is 192.168.10.241 then the host computer IP must set to the 192.168.1.X subnet.
- Clear out all internet cache and cookies.
- Clear the ARP table by going into the dos prompt and type in the following: arp –d
- Reset unit back to factory default by holding down the reset bottom for 10 seconds while the unit is powered on.

PROBLEM: I forgot the IP address.
POSSIBLE SOLUTION: If you forgot the IP address of the MACH V you can press reset button to restore the default factory settings by holding down the reset button for 10 seconds. The factory default IP for Client Bridge mode is 192.168.10.241, and Access Point mode is 192.168.10.240.

PROBLEM: The web control interface graphics isn't showing up properly.
POSSIBLE SOLUTION: Due to anti-malware software on the market some features of these programs may disable certain IE functions which can then lead to pictures not being displayed correctly. If this happens try turning off some of the more restrictive features of these anti-malware software or try accessing the web control interface with a different browser such as the firefox.

PROBLEM: I can not connect to the MACH V with a wireless client.
POSSIBLE SOLUTIONS:

- Make sure that the client supports the wireless mode that the MACH V is set to.
- Make sure that the Mode, SSID (Cap Sensitive), Channel and encryption settings are set the same on both sides.
- Make sure that your computer is within range and free from any strong electrical devices that may cause interference.
- Double check that the wireless client is set to the appropriate transmission speed under the advanced tab of the wireless connection property.
- Temporary disable all securities and encryption settings.
- Try it on a different client.
- If DHCP is enabled make sure that the client is set to obtain an IP automatically.

802.1x - The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Ad-Hoc Network - The wireless network based on a peer-to-peer communications session. Also referred to as AdHoc.

Access Point - Access points are stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication - Authentication refers to the verification of a transmitted message's integrity.

Beacon - In wireless networking, a beacon is a packet sent by a connected device to inform other devices of its presence and readiness.

Beacon interval - When a wirelessly networked device sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. Network managers can adjust the beacon interval, usually measured in milliseconds (ms) or its equivalent, kilo microseconds (Kmsec).

BSS - Basic Service Set. When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID - The unique identifier for an access point in a BSS network. See SSID for more details.

DHCP - DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DSSS (Direct Sequence Spread Spectrum) - Method of spreading a wireless signal into wide frequency bandwidth.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. DNS (Domain Name System): System used to map readable machine names into IP addresses

DTIM - DTIM (Delivery Traffic Indication Message) provides client stations with information on the next opportunity to monitor for broadcast or multicast messages.

DTIM interval - A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM. This frequency is usually measured in milliseconds (ms) or its equivalent, kilo microseconds (Kmsec).

ESS - Extended Service Set. ESS is the collective term for two or more BSSs that use the same switch in a LAN.

ESSID - Extended Service Set Identifier. An ESSID is the unique identifier for an ESS. See SSID for more details.

Filter - Filters are schemes, which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses. Firmware: Programming inserted into programmable read-only memory, thus becoming a permanent part of a computing device.

Fragmentation - Refers to the breaking up of data packets during transmission.

Gateway – Is the place where two or more networks connect

IBSS - Independent Basic Service Set. See ad-hoc network

Infrastructure Mode - When a wireless network functions in infrastructure mode, every user communicates with the network and other users through an access point; this is the typical way corporate WLANs work. An alternative is adhoc mode, but users would have to switch to infrastructure mode to access a network's printers and servers.

ISP - An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines. LAN(Local Area Network): A group of computers and peripheral devices connected to share resources.

MAC (Medium Access Control) Address - A unique number that distinguishes network cards.

MTU - MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT - NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

Preamble - Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors' communications between roaming wireless enabled devices and access points.

Protocol - A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service) - A server that issues authentication key to clients. RAM (Random Access Memory): Non-permanent memory.

RIP - RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

Router - A router is a device that forwards data packets along networks. The device is connected to at least two networks, commonly two LANs or WANs or a LAN and an ISP. Routers are located at gateways, the places where two or more networks connect and use headers and forwarding tables to determine the best path for forwarding the packets. And they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts. Very little filtering of data is done through routers.

Roaming - The ability to use a wireless device while moving from one access point to another without losing the connection.

RTS - RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server - Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

Static IP Address - A permanent IP address is assigned to a node in a TCP/IP network. Also known as global IP.

Subnet Mask - Subnet Masks (SUBNET work masks) are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an incoming IP ad-dress to determine whether to accept or reject the packet.

SSID - SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

TCP/IP - TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in real-time video and audio transmission).

TFTP (Trivial File Transfer Protocol) - Simple form of FTP (File Transfer Protocol), which Uses UDP (User Datagram Protocol), rather than TCP/IP for data transport and provides no security features.

TKIP (Temporal Key Integrity Protocol) - An encryption method replacing WEP.TKIP uses random IV and frequent key exchanges.

UDP (User Datagram Protocol) - A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

Uplink - Link to the next level up in a communication hierarchy.

UTP (Unshielded Twisted Pair) cable - Two or more unshielded wires twisted together to form a cable.

Virtual Servers - Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

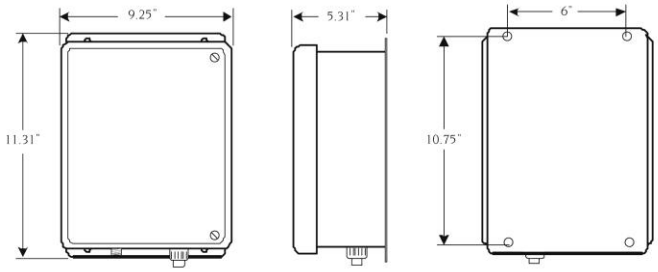
WEP (Wired Equivalent Privacy) - An encryption method based on 64 or 128bit algorithm.

WLAN - WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points, which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

PRODUCT SPECIFICATIONS

Board Specifications	
Network Standard	IEEE 802.11 a, IEEE 802.3, IEEE802.3x
Ethernet	10/100 BaseT Ethernet, Auto MDI/MDI-
Network Architecture	Infrastructure, Ad-Hoc, MAC, CSMA/CA
Status Indicators	POWER, Wireless LAN (RF), Ethernet LAN, Receives Signal Strength (RSS)
Push Button	Reset to Default Button
Radio Specifications	
Power Consumption	IEEE 802.11a, TX: ~1000 mA, RX: ~400 mA
Antenna Connector	N-type Female
Output Power	16 dBm (± 2 dB) @ 54 Mbps, 17 dBm (± 2 dB) @ 48 Mbps, 18 dBm (± 2 dB) @ 36 Mbps, 19 dBm (± 2 dB) @ 6 Mbps
Receiver Sensitivity	IEEE 802.11a Sensitivity @ 10% Packet Error Rate
	54 Mbps: -70 dBm, 48 Mbps: -71 dBm, 36 Mbps: -75 dBm, 24 Mbps: -79 dBm, 18 Mbps: -82 dBm, 12 Mbps: -84 dBm, 9 Mbps: -86 dBm, 6 Mbps: -87 dBm
Modulation	IEEE 802.11a (OFDM), 48/54 Mbps (QAM-64), 24/36 Mbps (QAM-16), 12/18 Mbps (QPSK), 6/9 Mbps (BPSK)
Environmental	
Operating Temperature	-20° C to 40° C (-5° F to 105° F), 10 to 90% (non-condensing)
Storage Temperature	-25° C to 70° C (-13° F to 158° F), 10 to 90% (non-condensing)

LED Definition	
Power	On (red) = Power on Off = No power
RF (WLAN)	On (yellow) = Connected Off = Not connected Blinking (green) = Connected and transmitting
LAN	On (green) = Connected Off = Not connected Blinking (green) = Connected and transmitting
Received Signal Strength Indicator (RSSI)	Blinking left to right = Not connected (Scanning for AP) On = Connected, indicating Received Signal Strength. 5 LEDs: > 80% (-68 dBm) 4 LEDs: > 60% (-75 dBm) 3 LEDs: > 40% (-82 dBm) 2 LEDs: > 20% (-88 dBm) 1 LED: > 3% (-94 dBm) 0 LEDs: No Signal (-95 dBm)
Software Specifications	
Bridge Features	Universal Bridging, MAC Address Cloning, RTS, Threshold/ Fragmentation Threshold, Infrastructure or Ad-Hoc Mode, Non-IP Traffic Bridging
Security Features	64-Bit/128-Bit WEP Encryption, WPA Personal Using TKIP or AES, WPA Enterprise Using TKIP or AES, 802.1x Authenticator, Cisco LEAP Support, MAC Address Filter.
Management Features	Web Access (Username/Password Protected), Static IP, Automatic Device Discovery & Configuration, SNMP v1, DHCP and PPPoE (Ethernet or Wireless), Firmware Upgrade via Web Browser, Transmit Power Adjustment.
Operating Frequency	
USA/FCC	5.15 GHz ~ 5.25 GHz, 5.25 GHz ~ 5.35 GHz, 5.47 GHz ~ 5.725 GHz, 5.725 GHz ~ 5.825 GHz
Europe/ETSI	5.15 GHz ~ 5.35 GHz, 5.47 GHz ~ 5.725 GHz
Japan/TELEC	5.15 GHz ~ 5.25 GHz



Dimensions
Weight 8 lbs.
Size 9.3" W X 11.3" H X 5.3" D
Weatherproof NEMA-4X *non-metallic enclosure provided with a mast mount bracket (2" diameter mast, minimum size)*

www.gotowti.com

An ISO 9001 Certified Company

Wireless Technology, Inc.

Wireless Technology, Inc. (WTI)
2064 Eastman Avenue, Suite 113
Ventura, CA 93003-7787 USA
tel 805/339-9696 • fax 805/339-0932 • email: sales@wirelesstech.com
www.wirelesstech.com • www.gotowti.com

Due to Wireless Technology, Inc. (WTI) continuing efforts to engineer the best product that is most responsive to our customer's needs, the above specifications are subject to change without notice. *All products are trademarks or registered trademarks of their respective holders. The use of these marks does not suggest any association between these companies.*