Trimar - Tri-Mode Advanced Radio - AP

802.11a/g/b Advanced Wireless LAN Access Point

Technical Manual

www.otcwireless.com

Trimar-AP

Trimar Wireless LAN Access Point

Technical Manual

Copyright

Rev 1.00

Table of Contents

Trimar AP Technical Manual

Chapter 1: Introduction

Trimar-AP is an IEEE-802.11a|g|b compliant, maximum data rate of 54Mbps, full functional wireless Access Point, which provides seamless incorporation of a wireless network into an existing wired LAN infrastructure. Existing wired-network resources such as DHCP, VPN, firewall, etc., reach across the Trimar-AP to the wireless client workstations with total transparency. Trimar-AP wirelessly incorporates a group of workstations or other kinds of devices with wireless connectivity into a wired network—just like a hub and switch.

Trimar-AP can be used wherever an 802.11 wireless LAN AP is appropriate. The portable, compact form-factor of Trimar-AP, in conjunction with its non-intrusive nature, makes it ideal for quick deployment of wireless network at events that involve rapid setup: temporary offices, trade-shows, meetings, temporary POS, etc. There is no need to request an IP address for the AP ahead of the time for it to perform its networking functions. There is no worry about functionality conflicts with the incumbent network setup when traveling to a temporary event. Traveling businessmen can also carry this portable AP on the road to gain mobility in hotels.

In addition to higher speed, the Trimar-AP AP fully supports the current wireless security standard in force. The Trimar-AP AP supports the 64 and 128-bit WEP encryption and WPA – Wi-Fi Protected Access. WPA offers unprecedented wireless security including both access control with 802.1X and communications confidentiality with dynamic TKIP encryption. Please contact OTC for tutorial material on WPA. Trimar-AP may interoperate with any WPA-compliant station radios, including OTC's ACR-201-G, and their attached workstation.

Trimar-AP also offers MAC-address-based access control. This access control used in conjunction with the WPA for data encryption provides the highest degree of security for the wireless network.

Trimar-AP includes a built-in Web server providing a web-based administration utility to configure, monitor, and manage the radio. The network operator can access the Trimar-AP from any immediate or remote host with a Web browser on the connected network. Once the Trimar-AP is properly configured to match up with your wireless network, the radio runs self-sufficiently without the aid of any driver program or connected Web browser.

1.1 Key Features

Key Features
❑ Portable form factor and transparency to network settings allow quick deployment, especially suitable for temporary wireless network

❑ Industry standard IEEE 802.11ag-compliant wireless interface; Interoperable with compatible 802.11ag as well as 802.11b Station radios from all vendors
❑ Highest degree of security provided by the ***WPA capability,*** including WEP of 64 and 128 bits.
❑ Tight access control provided by checking the MAC-address of the Stations
❑ 54Mbps data rate at maximum and automatic selection of a suitable lower data rate in degraded RF environment
❑ Integrated omni-directional-antenna to provide best tradeoff between link-quality and portability
❑ Remote network management achievable through embedded web-based Administration Utility, accessible from any Web browser
❑ Capable of Remote firmware/software upgrade through web-based administration utility

1.2 Hardware Specification

Specifications	
Model	Trimar-AP
Standard	802.11 and 802.11agb; WPA
Host Interface	Ethernet, 100/10 Base T, 802.3, RJ-45 receptacle
Frequency	2.4GHz – 2.497GHz
RF Channels	11 channels (US, Canada, Brazil, Australia, New Zealand) 13 channels (Europe) 14 channels (Japan)
Transmission power	14dBm at antenna input typical
Receiver sensitivity	-65dBm@54Mpbs, -80dBm @11Mbps, at 1e-5 BER typical
Antenna	Dipole antenna with ~2dBi gain
Data Rate	1/ 2/ 5.5/ 6/ 9/ 11/ 12/ 18/ 24/ 36/ 48/ 54 Mbps, fixed or automatic rate selection
Modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM (11ag) CCK, DQPSK, DBPSK (11b)
Max. Link Distance	~1200 ft in open space
Network Types	Support both the ad hoc mode and the infrastructure mode
Data Encryption	Support the WPA: Wi-Fi Protected Access standard for highest level of access control and communications security. Support standard 64-bit WEP and the optional 128-bit WEP.
Input Power	5 VDC
Current consumption	<500mA (max. reached in transmit-mode)
LED Indicators	4: Power, Transmission, Receiving, Link/Ethernet-connection
Operating Temper.	-10°C – +70°C
Regulatory Compliance	Safety UL 1950, 3rd edition CSA-C22.2 No. 950-95, 3rd edition IEC60950, 2nd edition, 1991+A1, 1992+A2, 1993+A3, 1995+A4, 1996 EN60950, 2000 EMC/Wireless FCC Part 15, Class B, FCC 15.247 RSS-210 ETSI EN 300 328-1, ETSI EN 300 328-2, ETSI EN 301 489-1, ETSI EN 301 489-17
Physical Dimension	2.125” W x 4.625” L x 0.7” D

Chapter 2: Product Installation and Basic Operation

2.1 Safety Statements

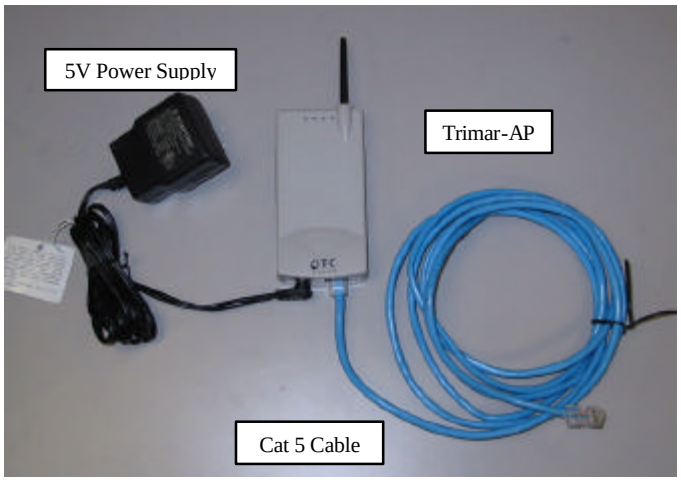
Use only the power adapter provided with this product or other OTC authorized replacement power adapter. Connect the power adapter to a properly grounded electrical outlet that is near the product and easily accessible.

Refer service or repairs, other than those described in the user documentation, to a professional service person.

2.2 Installing the Hardware

2.2.1 Power

Power is supplied to the radio via the supplied DC power adapter.



***WARNING*: Do not exceed more than 12A@120VAC or 6A@240VAC total current connected to the DC adapter.**

2.2.2 Ethernet Connection

The Trimar-AP connects to an Ethernet port of a switch or hub with the supplied *blue* cross-over UTP cable. To connect to a router, a DSL or cable modem, or a computer, use the *white* straight-through UTP cable supplied. Use the status-LED below as a guide to assure that the correct type of Ethernet cable is used.

2.2.3 Status LED's

Use the proper UTP cable to connect the 100/10BaseT port (which resembles an over-sized telephone jack) on the Trimar-AP to the 100/10BaseT port of the network equipment (router or switch). Power on the Trimar-AP, the LED's on the front panel should exhibit the following patterns:

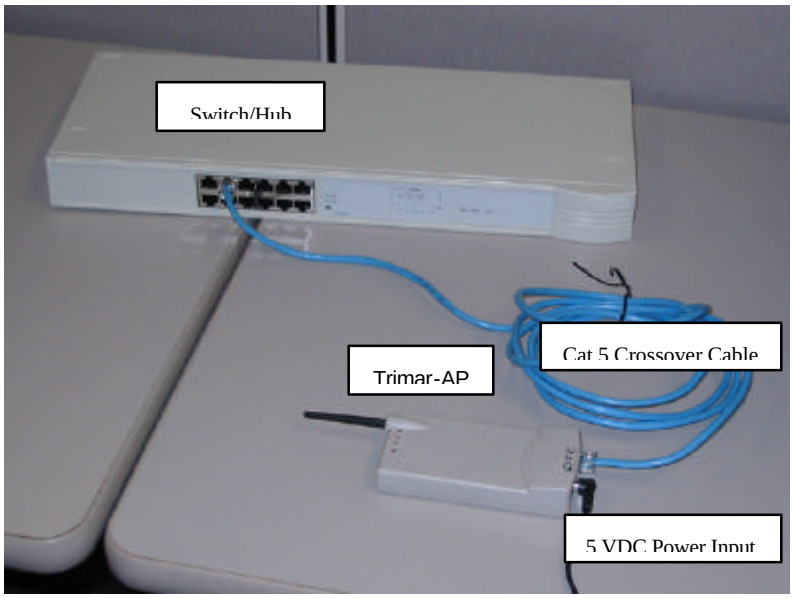
LED	*Color*	*Light Pattern*
ON	Red	Steady ON or Blinking ON
RX	Green	Blinking ON, when communicating over the wireless port; Steady OFF, when wireless connection is not present.
TX	Red	Blinking, when transmitting wireless data. Steady OFF, when not transmitting data

LINK	Yellow	Blinking ON, when communicating over the Ethernet port; Steady OFF, when Ethernet connection is not present.

If the yellow LED stays off, then the Ethernet connection to the Ethernet port is not made. Check your UTP cable and make sure that the correct type (straight-through or cross-over) of UTP cable is used. If one cannot communicate and the green LED is off, you may want to re-position the Trimar-AP to a different location for better RF transmission/reception. You may also want to check if the unit is configured with the proper RF channel and security settings by using the Web-based Administration Utility.

Once the hardware is checked out to work properly with the network equipment, the radio can be secured in the desired location by the pair of Velcro tabs.

Typical Installation:



Chapter 3: Operating Modes & Functional Features

In addition to performing standards-compliant AP functions, OTC Trimar-AP has many features of convenience and it provides several modes of operation.

3.1 DHCP Client for Self

Dynamic Host Configuration Protocol client automatically gets IP address and DNS addresses from the DHCP server. Wireless DHCP client can be configured to provide host name to DHCP server for better management.

3.2 Wireless DHCP Server

Dynamic Host Configuration Protocol server that automatically assigns IP addresses to wireless client stations logging onto a TCP/IP network. It eliminates having to manually assign permanent IP addresses. DHCP server runs in Access Point and is capable of assigning IP address only to wireless clients who is authorized to use the AP. DHCP servers also dynamically update the DNS servers information when connected.

Source filtering

DHCP server will filter the request based upon source port, namely wireless, wired and WDS.

3.3 WDS – Wireless Distribution System

Wireless Distribution System (WDS) allows packets to pass through without modification from one wireless access point to another. This feature is especially interesting to those who require transparent bridge because application only runs on a wired Ethernet switch due to special network protocol it use. One throw back of using this feature is one cannot use any of the stronger WPA authentication and encryption[1].

Enable WDS - Enable or disable WDS.
WDS MAC - Up to 6 MAC addresses of adjacent WDS Access Point.

3.4 STP- Spanning Tree Protocol

Trimar-AP is equipped with STP. Spanning Tree Protocol is used in transparent bridges to dynamically determine the best path from source to destination. It avoids bridge loops (two or more paths linking one segment to another), which can cause the bridges to send packets to wrong destination in infinite loop. This protocol creates a hierarchical "tree" that "spans" the entire network including all

[1] IEEE802.11 Standards neglect to define how APs in WDS relationship would authenticate each other.

switches. It determines all redundant paths and makes only one of them active at any given time. The spanning tree protocol (STP) is part of the IEEE 802.1 standard. New STP will be capable of informing network topology change to the transparent bridge causing forwarding table to be refreshed.

Enable STP - Enable or disable STP feature.

3.5 Transparent Bridge

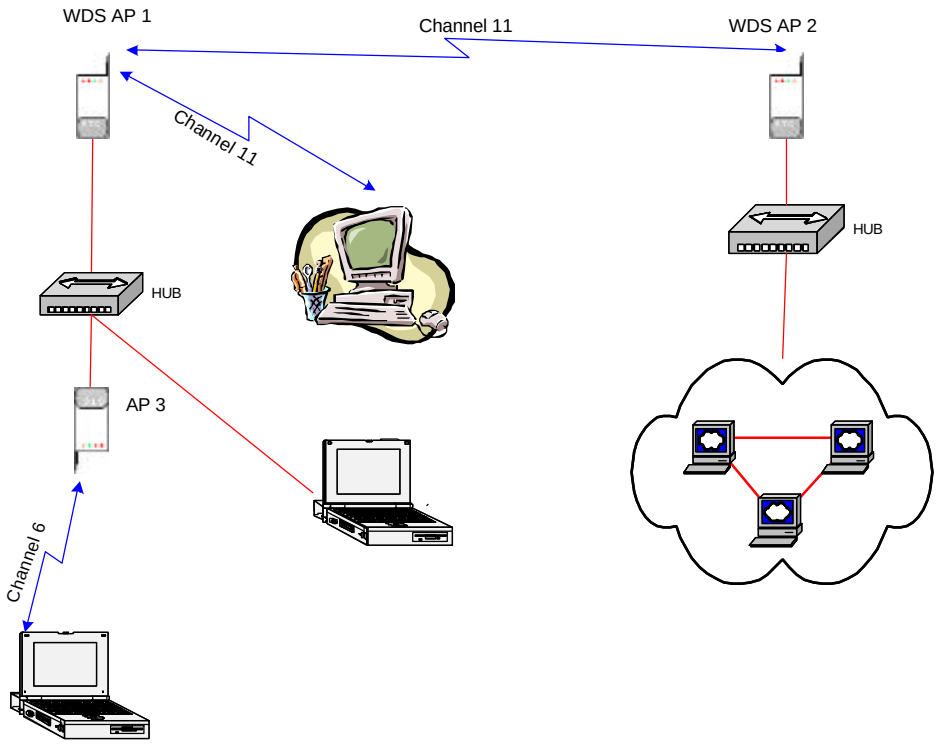
New transparent bridge will use unique MAC address for Ethernet port to fully utilize Spanning Tree Protocol's capabilities. In the past most of wireless Access Point use wireless radio's MAC address as Ethernet MAC address causing STP to misinterpret the forwarding path.

Use Ethernet MAC address - Flag transparent bridge to use separate Ethernet MAC address

MAC address - Ethernet MAC address to use if value is none-zero. If the value is all zeros then use burned in unique MAC address.

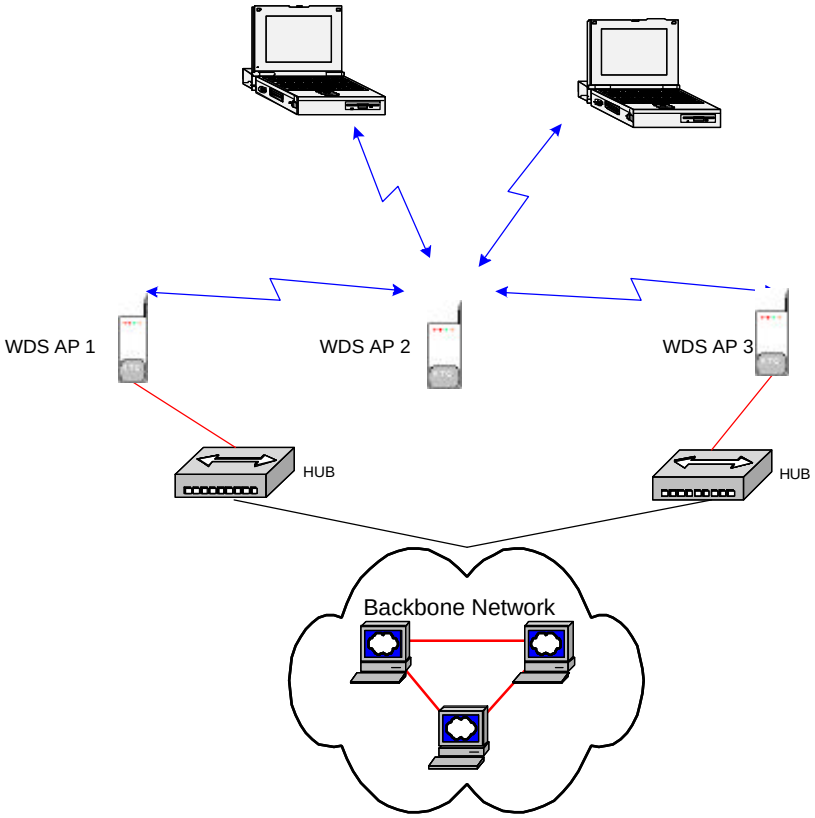
3.6 WDS Configurations

To Enable WDS feature, click on the Enable WDS check box and enter MAC address of adjoining WDS unit (AP2). Then repeat the same procedure from the adjoining WDS unit but enter MAC address of initial WDS unit (AP1). Two linked WDS units should have MAC address pointing to each other's unit. Also, linked WDS units must share same wireless channel. This can be accomplished from the "Wireless" Web page Channel selection option. When WDS radio sees adjoining WDS unit, INFO Web page should display neighboring WDS information.

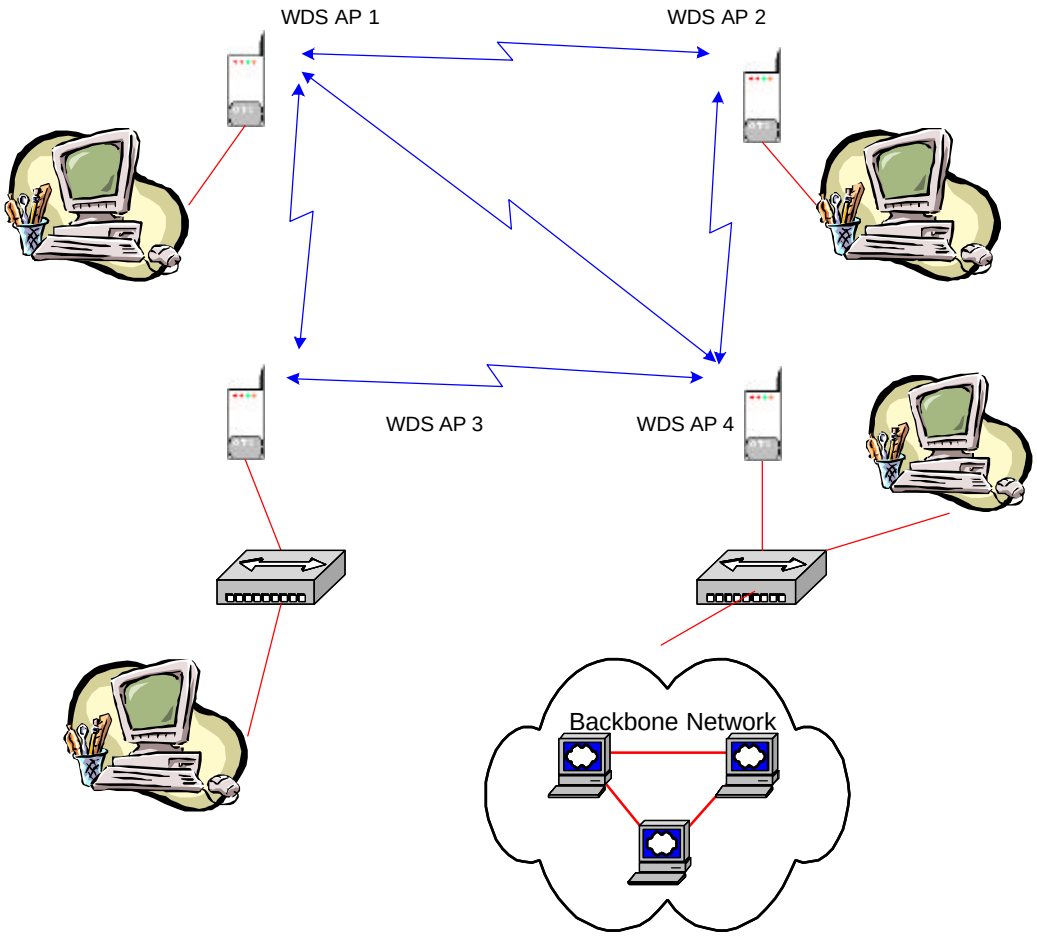


WDS bridging between two remote locations.

WDS with redundant path to backbone network - Clients on WDS AP2 can access backbone network through AP1 or AP3 automatically using WDS , Spanning Tree Protocol and transparent bridge software. To configure following topology, enable STP and use separate Ethernet MAC address must be checked for all three WDS units.



Meshed WDS set provides ultimate fault tolerance to wireless clients



3.7 VLAN

Virtual LAN is a convenient way of creating a network that is independent of physical location by logically sub grouping within a local area network via software rather than manually moving cables in the wiring closet. It is excellent way of creating independent networks based upon business organization need. VLAN easily adapts to organization change regardless of the physical LAN segment they are attached to and allows traffic to flow more efficiently within populations of mutual interest.

VLANs function at layer 2. Since their purpose is to isolate traffic within the VLAN, in order to bridge from one VLAN to another, a router is required. The router works at the higher layer 3 network protocol, which requires that network layer segments are identified and coordinated with the VLANs.

IEEE 802.1q

An IEEE standard for providing VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame, increasing the maximum frame size from 1518 to 1522 bytes. Three bits are used to allow eight priority levels (QoS) and 12 bits are used to identify up to 4096 VLANs.

3.8 WPA

WPA, Wi-Fi Protected Access is a new standard based security enhancement to WEP to increase the level of data protection and access control. WPA combines extra strong encryption (TKIP, AES) and access control (802.1x) to prevent unauthorized users from gain access to the physical network. To gain an access to the physical network, user must be first authenticated with RADIUS server, than security information is exchanged to create a unique secret key per connection. In addition, encryption key is changed synchronously every frame it send and user must be re-authenticated and new secret key is negotiated after specified time interval to prevent unauthorized use of authenticated system and malicious hackers. WPA-PSK is a simpler version of WPA for home or small business environment where, info-structure is not available for the RADIUS server authentication. Like WEP, it use pre-shared key but uses extra strong TKIP or AES encryption to protect the data. In WPA-PSK, encryption keys are automatically changed periodically to make sure that integrity of data is not compromised. OTC Trimar-AP is fully compliant with WPA specification and capable of handling EAP-TLS, EAP-TTLS, and EAP-MD5.

3.9 WLAN packet counter

All packets passing through the wireless card are counted and displayed in groups and also for each client. Grouped packet counters are displayed in Information web page in four groups,

Packets received - Number of packets destine for this unit.

Packets transmitted - Number of packets originates from this unit.

Ethernet port rx packets - Number of packets received from Ethernet port.

Ethernet port tx packets - Number of packets transmitted to Ethernet port.

Ethernet port broadcast packets - Number broadcast packets received from Ethernet port.

WLAN port rx packets - Number of packets received from wireless LAN port

WLAN port tx packets - Number of packets transmitted to wireless LAN port.

WLAN port broadcast packets - Number of packets received from wireless LAN port.

WDS port rx packets - Total number of packets received from 6 WDS links.

WDS port tx packets - Total number of packets sent to 6 WDS links.

WDS port broadcast packets - Total number of broadcast packets received from 6 WDS links and individual client

Chapter 4: Web-Based Administration

Trimar-AP provides Web-served administration tool.

4.1 System Requirements for Using Web-Based Administration Tool

Your computer must meet the following requirements in order to access the Trimar-AP web-based Administration Utility:

(1) A Web browser must be installed on the computer. The supported Web browsers include Internet Explorer 5.0 and above, Netscape 6.0 and above, Mozilla 1.0 and above. ***JavaScript for the browser must be enabled***.

(2) Ethernet capable computer with RJ-45 port (either built-in or add-on NIC).

(3) A network (or direct) connection to the Trimar-AP with proper IP addressing.

No installation of any other software program is necessary.

4.1.1 Access the Web-Based Administration Tool

Once the Trimar-AP radio is properly turned on and connected either directly or through network to a compute, the Web-based Utility is ready for use. To access the web-based administration utility, open a Web browser and type in the IP address of the Trimar-AP AP in the address bar. For factory default IP settings, see below:

4.1.2 The factory default IP settings:

IP address: 169.254.1.240

Subnet mask: 255.255.0.0

Gateway: 169.254.1.1

User name: admin

Password: public

NOTE: ***The IP address of the network interface of the computer must be in the same IP subnet as the IP address of Trimar-AP radio. For example, the computer network interface should have an IP address like 169.254.1.100***

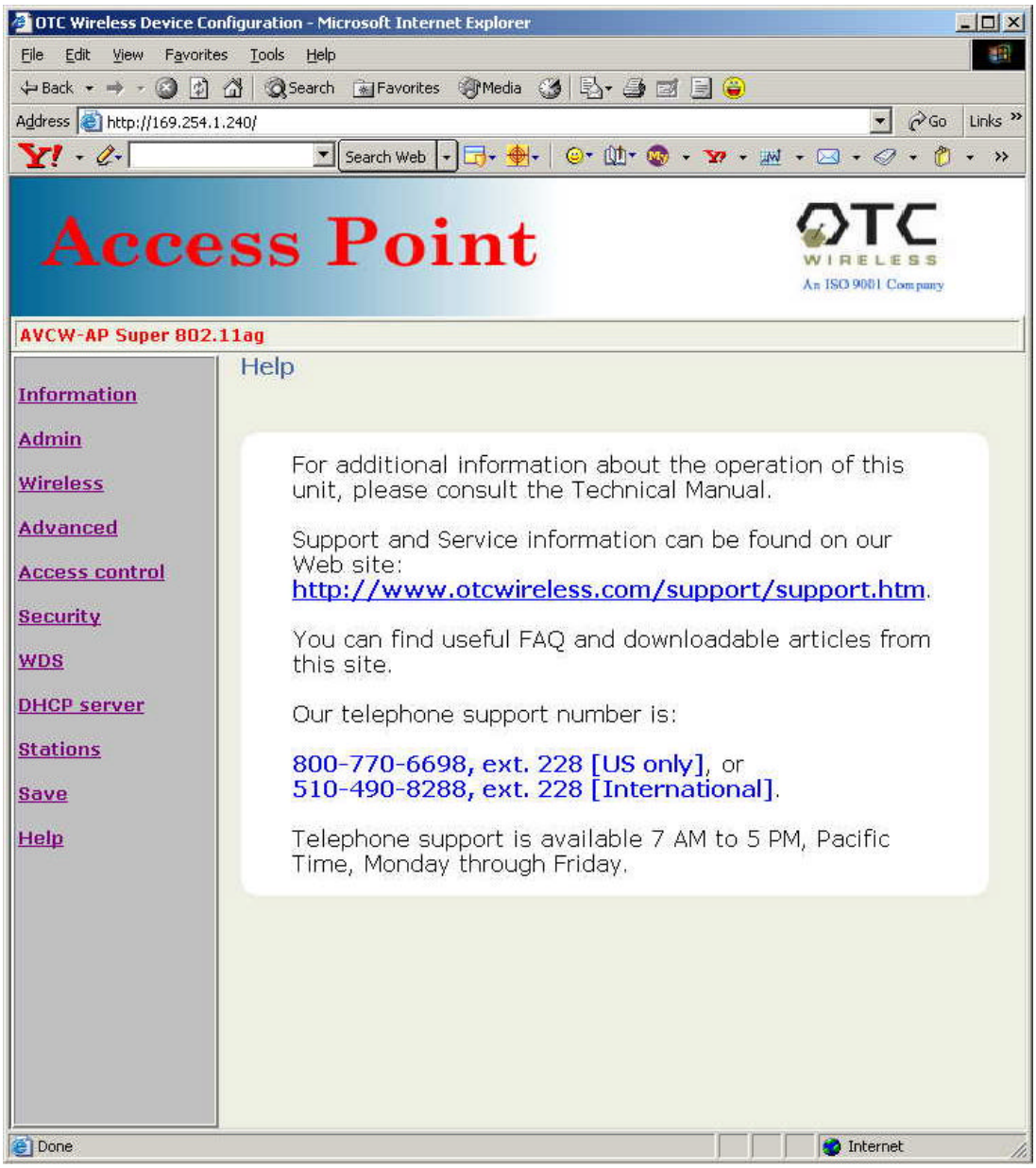
Warning: ***You must keep good record of the IP settings, if changed. Else, you won't be able to access the Administration Utility.***

Upon initial connection with the Administration Utility Web site, a user login page will be shown at the Web Browser. Enter the correct user name and password which you may have modified last time. Otherwise, use the factory default settings shown above.

4.1.3 Overview of the Web Pages

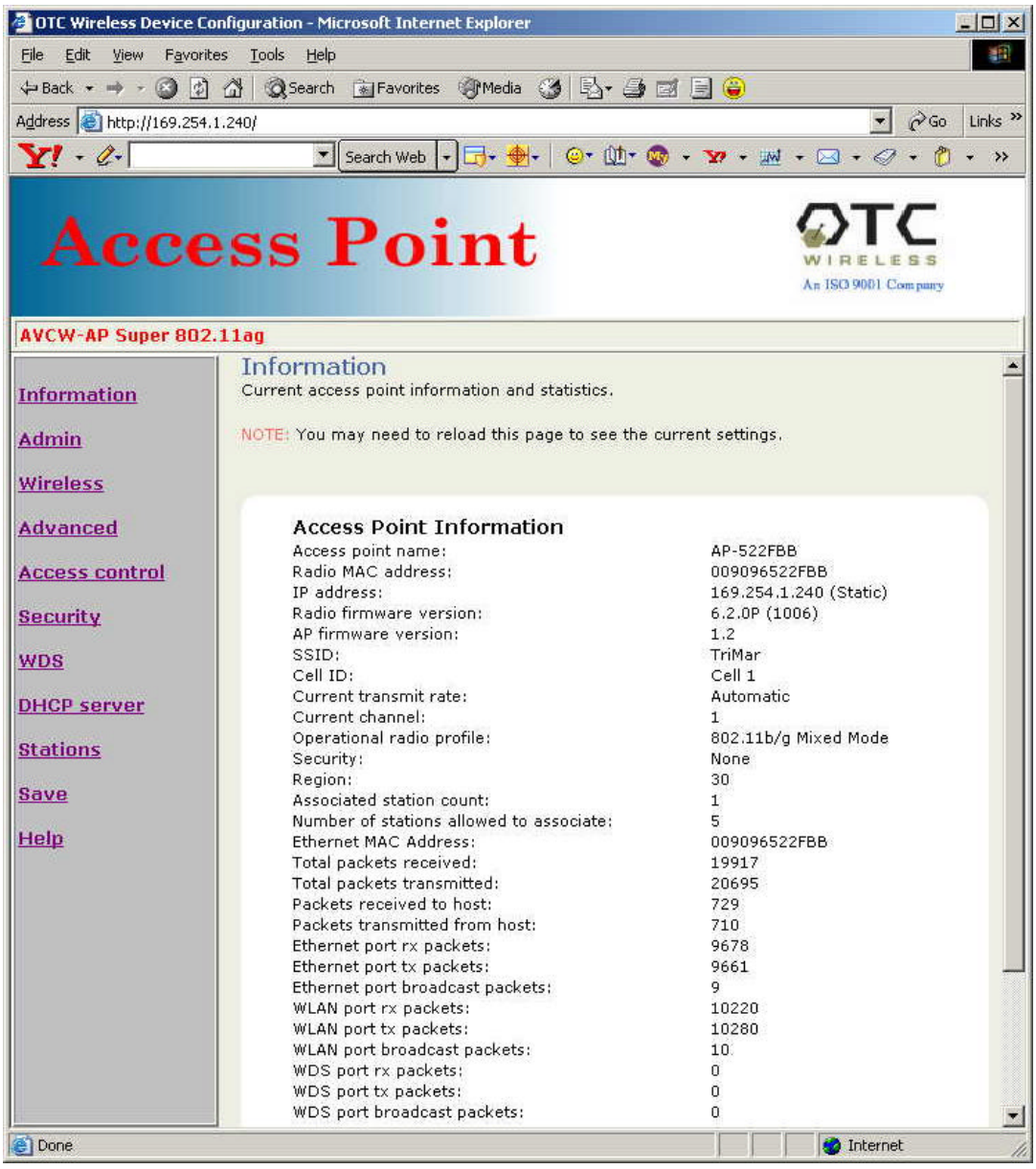
Trimar-AP web-based administration utility allows you to set and modify many operating parameters of the AP. The parameters are organized into nine categories and each category has its own web page. The categories are: *Info, Admin, Wireless, Advanced, Access control, Security, WDS, DHCP server, Stations, Save,* and *Help*. Clicking the tab of interest on the left border of all web pages let you access each category.

The “Help” page is shown below as an example:



4.2 Home Page: the "Information" Page

The home page, which is the Info page, is shown below. The home page can be re-accessed and refreshed by clicking on the "Info" tab. The title box just below the OTC logo tells you the current page being accessed. In this case, it is the "Information" page. The purpose of each web page is briefly explained in the area to the right of the title box. The remainder of the page shows the parameters in their groups.



Home Page: Information Page

The information on this page is explained below:

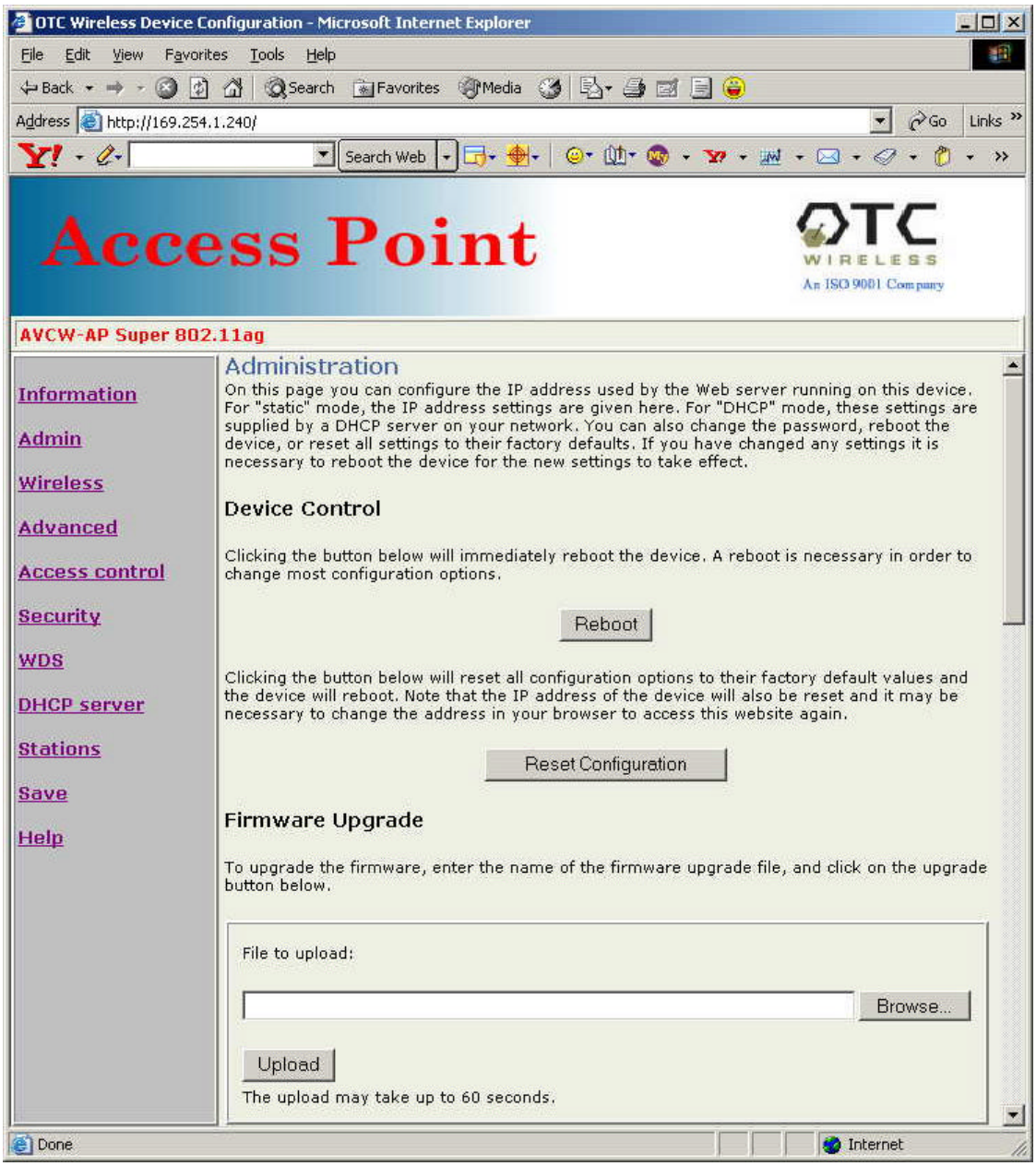
Number of stations allowed to associate:

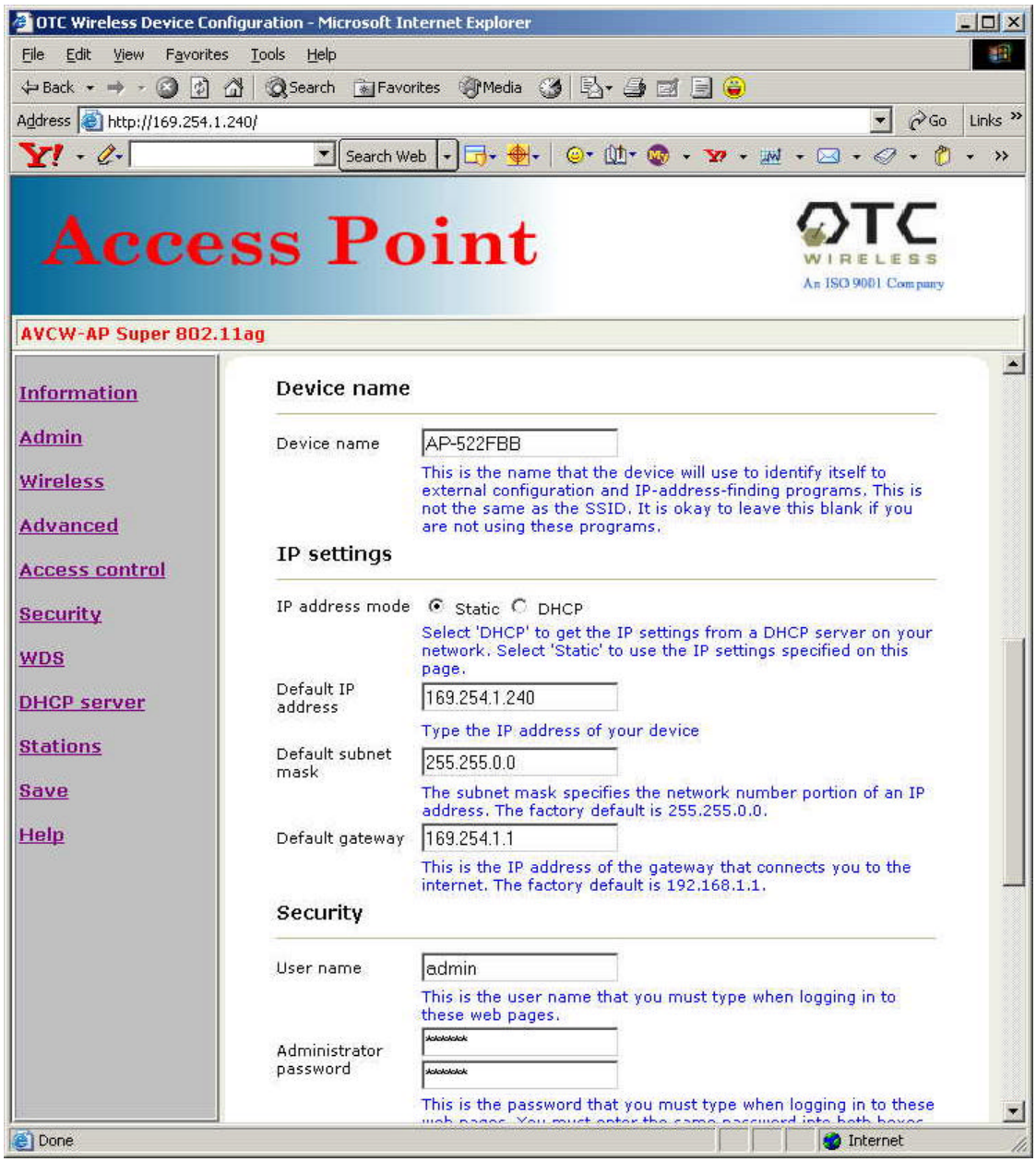
This value may change if the AP is under active load balance control.

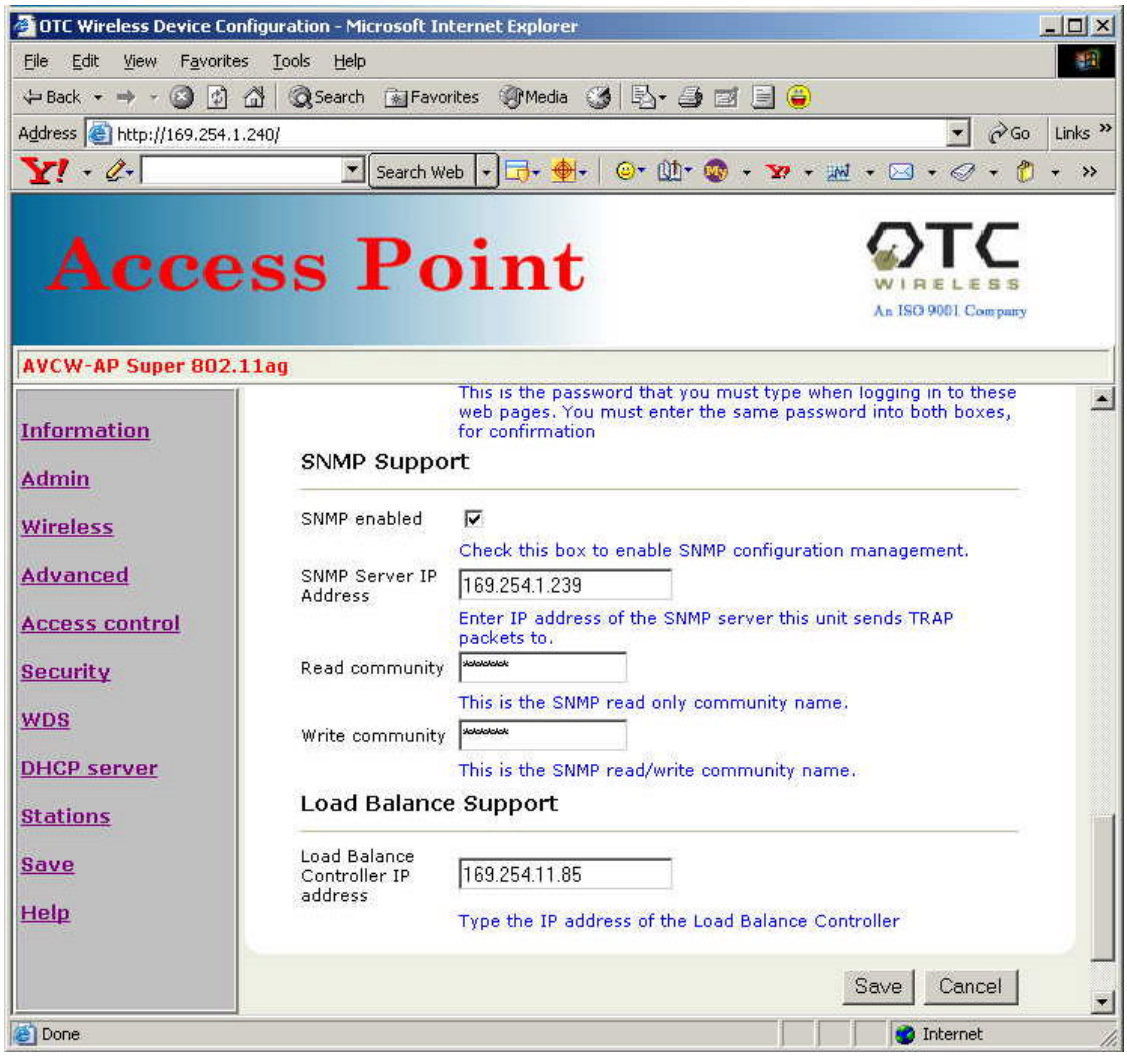
4.3 Administration

This page covers several groups of administrative settings:

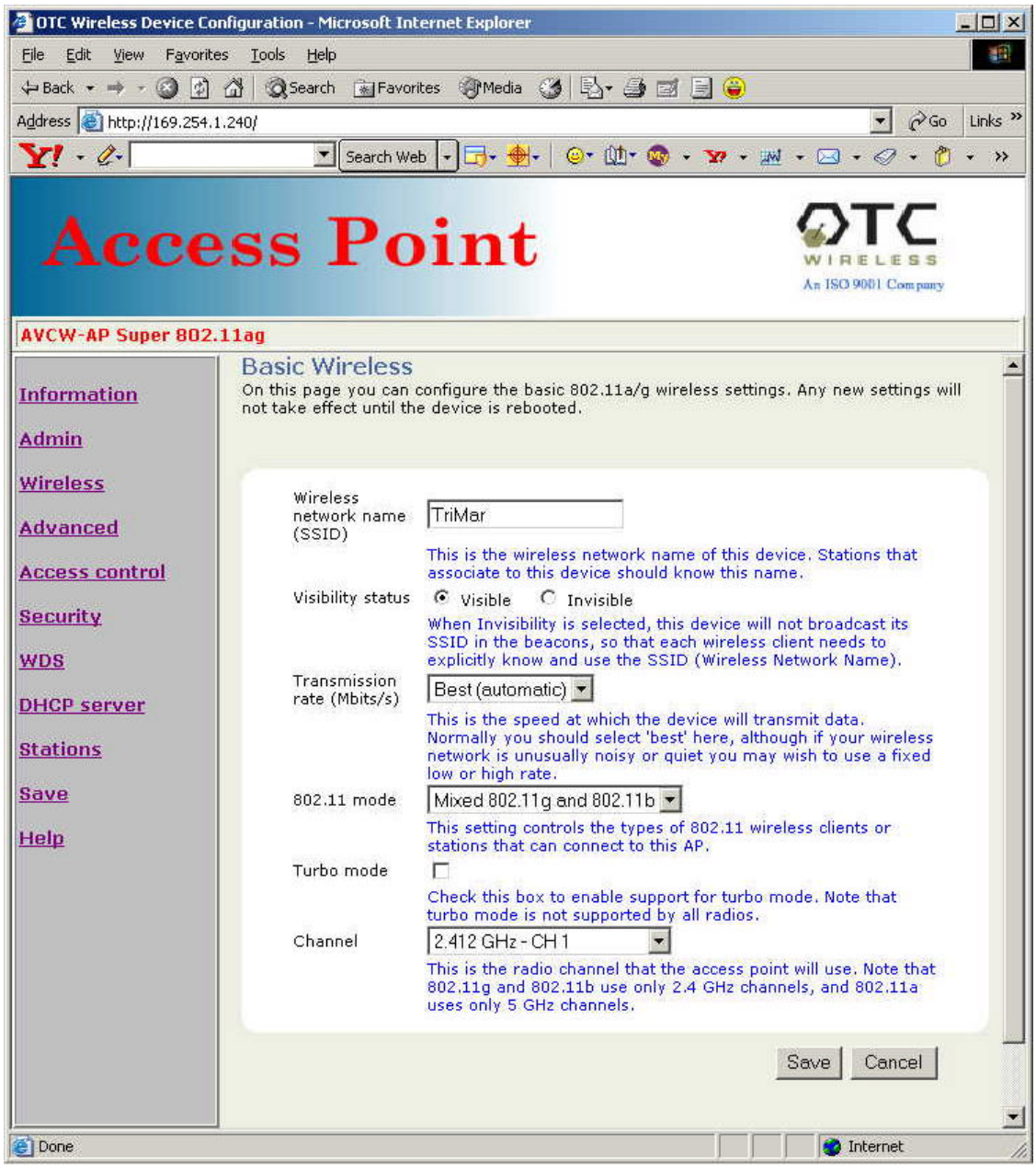
- Device Naming;
- Device Control;
- Firmware Upgrade;
- IP Settings;
- Security;
- SNMP Support; and
- Load Balance Support:
  - Load Balance Controller IP Address:
    - *If this IP is to be controlled in load, enter the Controller's IP address.*
    - *A valid Controller puts the AP under active load balance mode.*
    - *All load balance operations are controlled by the Controller. There is no additional parameter setting at the AP.*


OTC Wireless Device Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://169.254.1.240/
Go Links
Search Web
Access Point
OTC WIRELESS
An ISO 9001 Company
AVCW-AP Super 802.11ag
Information
Admin
Wireless
Advanced
Access control
Security
WDS
DHCP server
Stations
Save
Help
Administration
On this page you can configure the IP address used by the Web server running on this device. For "static" mode, the IP address settings are given here. For "DHCP" mode, these settings are supplied by a DHCP server on your network. You can also change the password, reboot the device, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the device for the new settings to take effect.
Device Control
Clicking the button below will immediately reboot the device. A reboot is necessary in order to change most configuration options.
Reboot
Clicking the button below will reset all configuration options to their factory default values and the device will reboot. Note that the IP address of the device will also be reset and it may be necessary to change the address in your browser to access this website again.
Reset Configuration
Firmware Upgrade
To upgrade the firmware, enter the name of the firmware upgrade file, and click on the upgrade button below.
File to upload:
Browse...
Upload
The upload may take up to 60 seconds.
Done
Internet

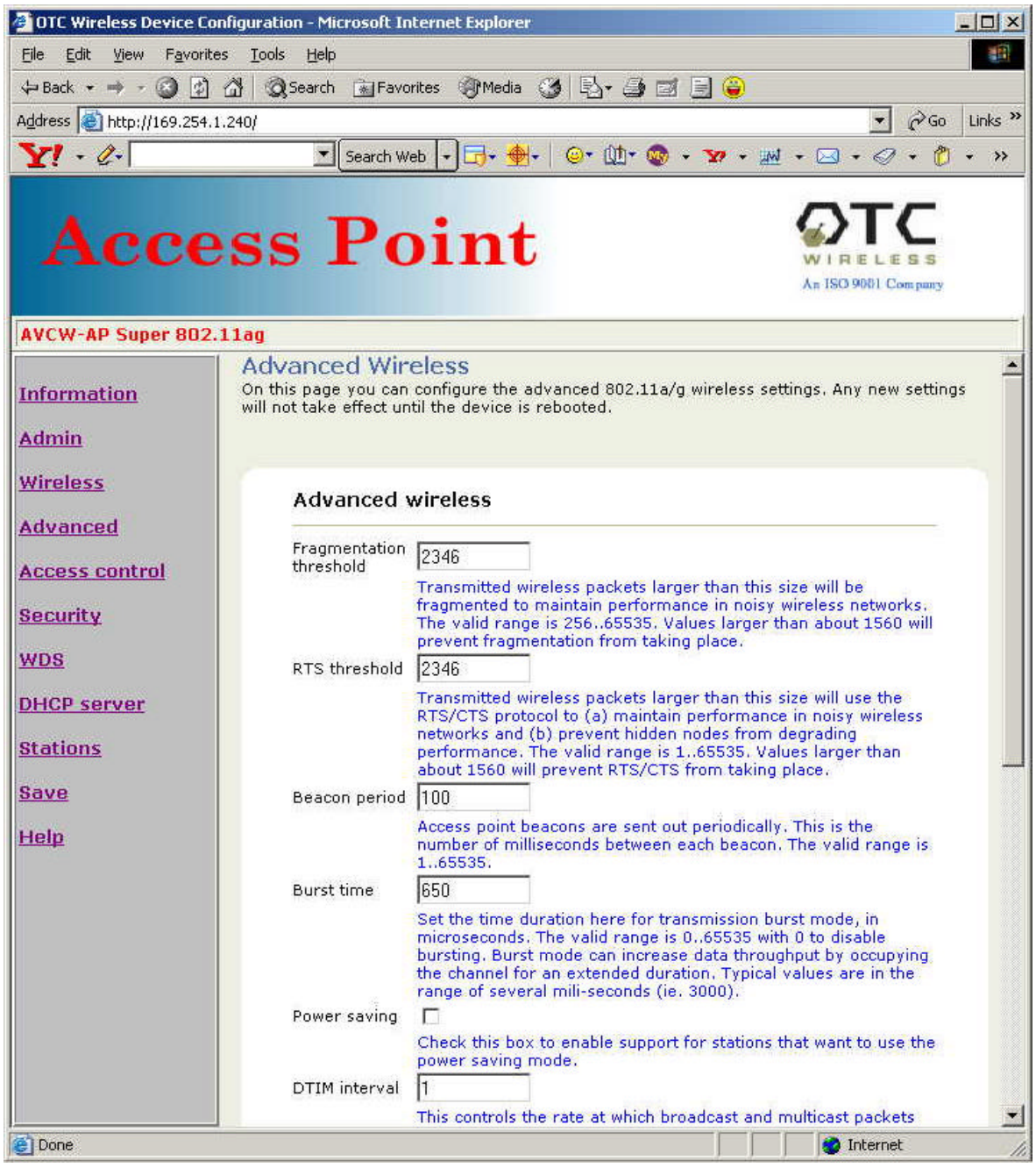

OTC Wireless Device Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://169.254.1.240/
Go Links
Search Web
Access Point
OTC WIRELESS
An ISO 9001 Company
AVCW-AP Super 802.11ag
Information
Admin
Wireless
Advanced
Access control
Security
WDS
DHCP server
Stations
Save
Help
Device name
Device name
AP-522FBB
This is the name that the device will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.
IP settings
IP address mode
Static
DHCP
Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.
Default IP address
169.254.1.240
Type the IP address of your device
Default subnet mask
255.255.0.0
The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.0.0.
Default gateway
169.254.1.1
This is the IP address of the gateway that connects you to the internet. The factory default is 192.168.1.1.
Security
User name
admin
This is the user name that you must type when logging in to these web pages.
Administrator password
This is the password that you must type when logging in to these
Done
Internet

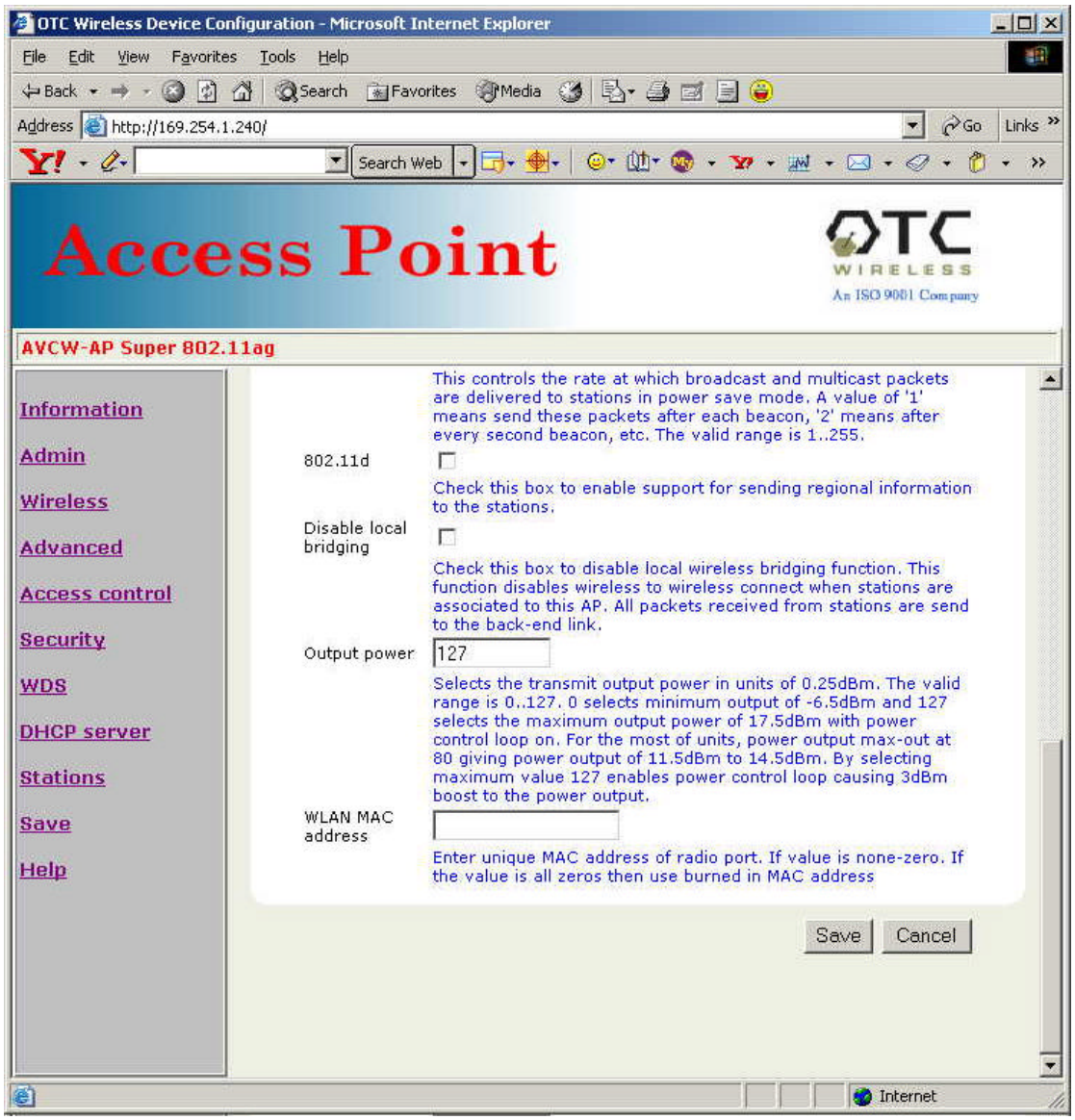

OTC Wireless Device Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://169.254.1.240/
Go Links
Search Web
Access Point
OTC WIRELESS
An ISO 9001 Company
AVCW-AP Super 802.11ag
Information
Admin
Wireless
Advanced
Access control
Security
WDS
DHCP server
Stations
Save
Help
This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation
SNMP Support
SNMP enabled
Check this box to enable SNMP configuration management.
SNMP Server IP Address
169.254.1.239
Enter IP address of the SNMP server this unit sends TRAP packets to.
Read community
This is the SNMP read only community name.
Write community
This is the SNMP read/write community name.
Load Balance Support
Load Balance Controller IP address
169.254.11.85
Type the IP address of the Load Balance Controller
Save
Cancel
Done
Internet

4.4 Wireless



4.5 Advanced Wireless


OTC Wireless Device Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://169.254.1.240/
Go Links
Search Web
Access Point
OTC WIRELESS
An ISO 9001 Company
AVCW-AP Super 802.11ag
Information
Admin
Wireless
Advanced
Access control
Security
WDS
DHCP server
Stations
Save
Help
Advanced Wireless
On this page you can configure the advanced 802.11a/g wireless settings. Any new settings will not take effect until the device is rebooted.
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
Access point beacons are sent out periodically. This is the number of milliseconds between each beacon. The valid range is 1..65535.
Burst time
650
Set the time duration here for transmission burst mode, in microseconds. The valid range is 0..65535 with 0 to disable bursting. Burst mode can increase data throughput by occupying the channel for an extended duration. Typical values are in the range of several mili-seconds (ie. 3000).
Power saving
Check this box to enable support for stations that want to use the power saving mode.
DTIM interval
1
This controls the rate at which broadcast and multicast packets
Done
Internet


OTC Wireless Device Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://169.254.1.240/
Go Links
Search Web
Access Point
OTC WIRELESS
An ISO 9001 Company
AVCW-AP Super 802.11ag
Information
Admin
Wireless
Advanced
Access control
Security
WDS
DHCP server
Stations
Save
Help
This controls the rate at which broadcast and multicast packets are delivered to stations in power save mode. A value of '1' means send these packets after each beacon, '2' means after every second beacon, etc. The valid range is 1..255.
802.11d
Check this box to enable support for sending regional information to the stations.
Disable local bridging
Check this box to disable local wireless bridging function. This function disables wireless to wireless connect when stations are associated to this AP. All packets received from stations are send to the back-end link.
Output power
127
Selects the transmit output power in units of 0.25dBm. The valid range is 0..127. 0 selects minimum output of -6.5dBm and 127 selects the maximum output power of 17.5dBm with power control loop on. For the most of units, power output max-out at 80 giving power output of 11.5dBm to 14.5dBm. By selecting maximum value 127 enables power control loop causing 3dBm boost to the power output.
WLAN MAC address
Enter unique MAC address of radio port. If value is none-zero. If the value is all zeros then use burned in MAC address
Save
Cancel
Internet