Altai A3 Smart WiFi Configuration Manual

For Firmware Version 1.0.0.

Version 1.0

Date: 10-Jul-2009

Commercially Confidential

Copyright © 2009 Altai Technologies Limited

ALL RIGHTS RESERVED.

Altai Technologies Limited
2/F, East Wing,
Lakeside 2,
Hong Kong Science Park,
Shatin, Hong Kong,
China

Telephone: +852 2116 8087
Fax: +852 2607 4021
Web: www.altaitechnologies.com

Customer Support Centre:
Email: support@altaitechnologies.com

Radio Frequency Interference Requirements

This device complies with Part 15 of FCC Rules.
Operation is subject to the following conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.
3. This device should not be co-located or operating in conjunction with any other antenna or transmitter.

Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Warning

The user is advised to keep apart from the base-station and antenna with at least 45cm when the base-station is in operation.

Disclaimer

All specifications are subject to change without prior notice. Altai Technologies assumes no responsibilities for any inaccuracies in this document or for any obligation to update information in this document. This document is provided for information purposes only. Altai Technologies reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Table of Contents

1 INTRODUCTION 8
1.1 Total Performance 8
1.2 Compatible With 802.11n 8
1.3 Large Capacity 8
1.4 Different Operation Modes 8

2 A3 MODEL AND FIRMWARE VERSION 8

3 GETTING START 9
3.1 Setup Wireless Connection with Your PC 9
3.2 Check Access 12

4 CONFIGURATION WITH WEB-ADMIN 13
4.1 Web Browser Connection 13
4.2 Checking the A3 Versions 15
4.3 Setup – User Name, Password and System Name 15
4.4 NTP Configuration 16
4.5 SNMP Configuration 16
4.6 Telnet 17
4.7 Network Operation Mode 17
4.8 Switch Mode 18
4.8.1 Static IP address 18
4.8.2 VLAN Configuration 19
4.8.3 STP Configuration 19
4.8.4 DHCP Client 19
4.8.5 DNS Auto Update 19
4.9 Gateway Mode 20
4.9.1 WAN Configuration 20
4.9.1.1 WAN Interface 21
4.9.1.2 PPPoE Configuration 21
4.9.2 LAN Configuration 22
4.10 Access Link Safe Mode/ Backhaul Link Self-healing 23
4.11 Setup – Wireless Radio Parameter 24
4.12 AP Mode 24
4.12.1 Wireless Mode and Radio Frequency 25
4.12.2 Auto Channel Selection 25
4.12.3 Maximum Clients 25
4.12.4 Transmit Power 26
4.12.5 Advanced Radio Setting 26
4.12.6 Service Set IDentifier (SSID) and Virtual Access Point (VAP) 27
4.12.7 Access Control List (ACL) 28
4.12.8 Encryption and Authentication 29
4.13 Repeater Mode 32
4.14 Bridge Mode 33
4.14.1 Bridge Radio Wireless Mode 33
4.14.2 Data Rate & Radio Frequency 33
4.14.3 Bridge Radio Transmit Power 33
4.14.4 Advanced Radio Setting 33
4.14.5 Remote Bridge Configuration 35
4.14.6 Bridge Security 35
4.15 Disable Mode 37
4.16 Reboot 37
4.17 Restore Configuration to Default Setting 39

5 PERFORMANCE MANAGEMENT MONITORING IN WEB-ADMIN 40
5.1 System 40
5.2 Clients Statistics 41
5.3 Radio Association-AP Mode 42
5.4 Radio Association-Repeater Mode 44

5.5 Radio Association-Bridge Mode 45

6 SOFTWARE UPGRADE THROUGH WEB-ADMIN 46

6.1 Firmware Update Through HTTP or HTTPS 46

7 GLOSSARY 48

Table of Figures

FIGURE 1 CONTROL PANEL IN WINDOWS XP 9
FIGURE 2 NETWORK CONNECTIONS IN WINDOWS XP 10
FIGURE 3 LOCAL AREA CONNECTION PROPERTIES IN WINDOWS XP 10
FIGURE 4 INTERNET PROTOCOL (TCP/IP) PROPERTIES IN WINDOWS XP 11
FIGURE 5 ENTER USER NAME AND PASSWORD 13
FIGURE 6 WEB-ADMIN LOGIN PAGE 14
FIGURE 7 VERSION OF A3 SMART WIFI 15
FIGURE 8 SYSTEM CONFIGURATION 15
FIGURE 9 NTP CONFIGURATION 16
FIGURE 10 THE IP ADDRESS HERE IS THE ETHERNET INTERFACE OF THE A3 18
FIGURE 11 NETWORK CONFIGURATIONS UNDER SWITCH MODE 18
FIGURE 12 NETWORK CONFIGURATIONS UNDER GATEWAY MODE 20
FIGURE 13 PPPOE CONFIGURATION 21
FIGURE 14 CONFIGURE DHCP SERVER 22
FIGURE 15 CONFIGURE DHCP RELAY SERVER 23
FIGURE 16 WIRELESS RADIO PARAMETER CONFIGURATION 24
FIGURE 17 ADVANCED WIRELESS RADIO SETTING 27
FIGURE 18 VAP SETTING 27
FIGURE 19 ACL 29
FIGURE 20 WIRELESS RADIO SECURITY CONFIGURATION 29
FIGURE 21 WEP KEY SETTINGS 30
FIGURE 22 WPA SETTINGS 30
FIGURE 23 WPA-PSK SETTINGS 31
FIGURE 24 REPEATER MODE CONFIGURATION 32
FIGURE 25 ADVANCED BRIDGE RADIO SETTING 34
FIGURE 26 BRIDGE ENCRYPTION SETTING_WEP 36
FIGURE 27 BRIDGE ENCRYPTION SETTING_AES 36
FIGURE 28 WIRELESS RADIO DISABLE MODE 37
FIGURE 29 REBOOT WINDOW 38
FIGURE 30 A3 SMART WIFI ACCESS POINT IS REBOOTING 39
FIGURE 31 RESET TO FACTORY DEFAULT SETTING IN WEB-ADMIN 39
FIGURE 32 DETAILS OF THE SYSTEM 40
FIGURE 33 STATUSES OF THE VAPS 41
FIGURE 34 2.4GHZ RADIO STATISTICS MENU 42
FIGURE 35 RADIO ASSOCIATION TABLE 43
FIGURE 36 RADIO STATISTICS PER MAC ADDRESS (DATA IS CUMULATIVE) 43
FIGURE 37 RADIO ASSOCIATION AP LIST 44
FIGURE 38 ASSOCIATION AP STATISTICS PER MAC ADDRESS (DATA IS CUMULATIVE) 44
FIGURE 39 RADIO ASSOCIATION BRIDGE LIST 45
FIGURE 40 BRIDGE ASSOCIATION STATISTICS PER MAC ADDRESS 45
FIGURE 41 UPLOAD THE FIRMWARE THROUGH HTTP OR HTTPS 47
FIGURE 42 SUCCESSFUL FIRMWARE UPDATE – WEB-ADMIN 47

Manual Conventions

Bold	Bold type within paragraph text indicates commands, files names, directory names, paths, output, or returned values.
Italic	Within commands, italics indicate a variable that the user must specify. Titles of manuals or other published documents are also set in italics.
_____	Underline means that the words you have to pay attention.
`Courier`	The courier font indicates output or display.
[ ]	Within commands, items enclosed in square brackets are optional parameters or values that the user can choose to specify or omit.
{ }	Within commands, item enclosed in braces are options from which the user must choose.
|	Within commands, the vertical bar separates options.
…	An ellipsis indicates a repetition of preceding parameter.
>	The right angle bracket separates successive menu selection.

NOTE: This message denotes neutral or positive information that calls out important points to the text. A note provides information that applies only in special cases.

Caution: Cautions call special attention to hazards that can cause system damage or data corruption, to a lesser degree than warnings.

Warnings: Warnings call special attention to hazards that can cause system damage, data corruption, personal injury, or death.

1 INTRODUCTION

1.1 TOTAL PERFORMANCE

Altai A3 smart WiFi provides coverage for outdoor WiFi coverage and enhance the Altai indoor coverage solution. It combines IEEE 802.11a/b/g and Draft 802.11n to offer best WiFi access in different scenarios.

1.2 COMPATIBLE WITH 802.11N

By adopting MIMO technology, Altai A3 smart WiFi provides up to 300Mbps data rate to 802.11n clients. Maximum throughput is 150Mbps per radio.

1.3 LARGE CAPACITY

Altai A3 smart WiFi has three working radios. Two different radios can work as access radio to enhance the total capacity of A3 unit, while the other radio working as backhaul link.

1.4 DIFFERENT OPERATION MODES

There are multiple operation modes for each radio. AP mode means the radio is working for clients association; Sta mode is used to repeat remote 2.4GHz radio end as backhaul link; 5GHz radio can be selected as backhaul link when enabled Bridge mode; users can also disable the radio.

This manual is to summarize how to perform configuration for the ALTAI A3 smart WiFi through web-admin interface.

2 A3 MODEL AND FIRMWARE VERSION

This manual is applicable for the following models and firmware version:

Product name : **A3 smart WiFi**
Model number: **A3**
Firmware version: **v1.0.0.4**

Commercially Confidential

3 GETTING START

3.1 SETUP WIRELESS CONNECTION WITH YOUR PC

A3 Smart WiFi can be connected with your PC in wireless mode. In the followings, wireless mode will be introduced.

Please kindly refer to the Altai A3 Smart WiFi Installation Guide.

Start Network Configuration on your PC.

For Windows XP user,

1. Click the "**start**" menu and choose "**Control Panel**".
2. Click "**Network Connections**".

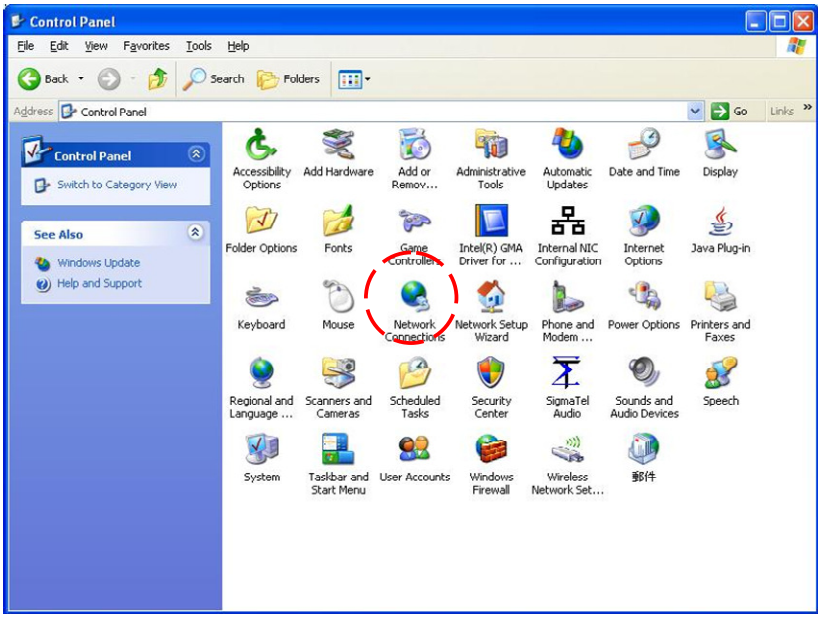


Figure 1 Control Panel in Windows XP

Commercially Confidential

3. Right-click on the "**Wireless Network Connection**" and select "**Properties**".

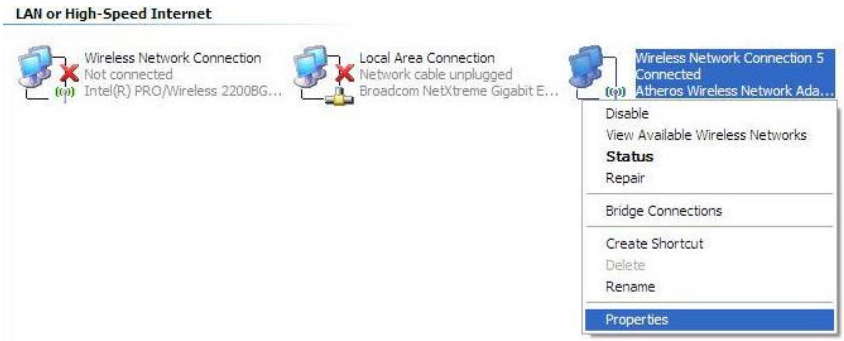


Figure 2 Network Connections in Windows XP

4. After clicking on "**Properties**", you will see the diagram as below.

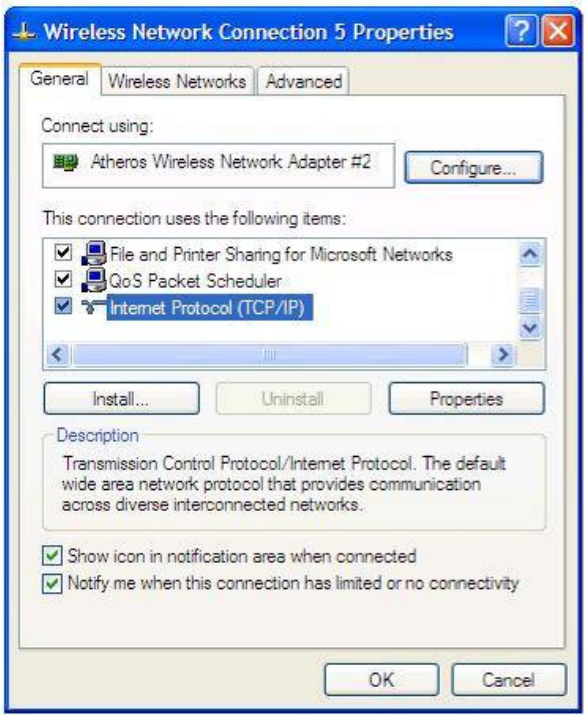


Figure 3 Wireless Network Connection Properties in Windows XP

5. Marking the "Internet Protocol (TCP/IP)" and click the "**Properties**".
6. Type in an "**IP address**", for example, 192.168.1.2, which is under the same subnet as the Default IP address of A3 smart WiFi (192.168.1.20).
7. Using the default "**Subnet mask**" (default: 255.255.255.0) setting at the first time.
8. Keep the "**Default gateway**" as "Blank".
9. Keep the "**Preferred DNS server**" and "**Alternate DNS server**" as "Blank" also.
10. Click "**OK**" when you finish setting and close the Window.

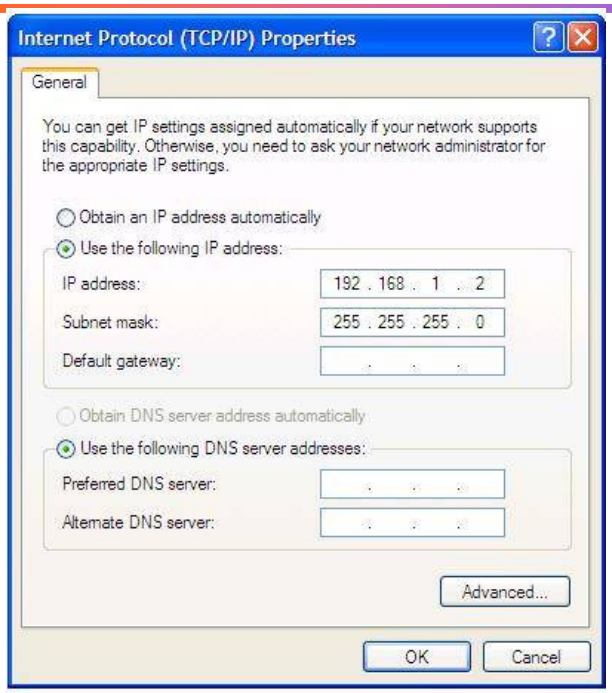


Figure 4 Internet Protocol (TCP/IP) Properties in Windows XP

11. Right-click on the "**Wireless Network Connection**" and select "**View Available Wireless Networks**".

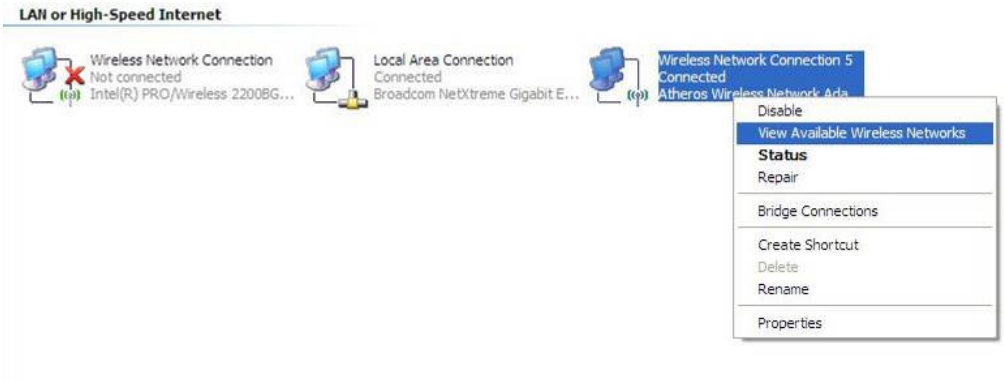


Figure 5 Network Connections in Windows XP

Commercially Confidential

12. Click on the "**Altai Wireless Network**"

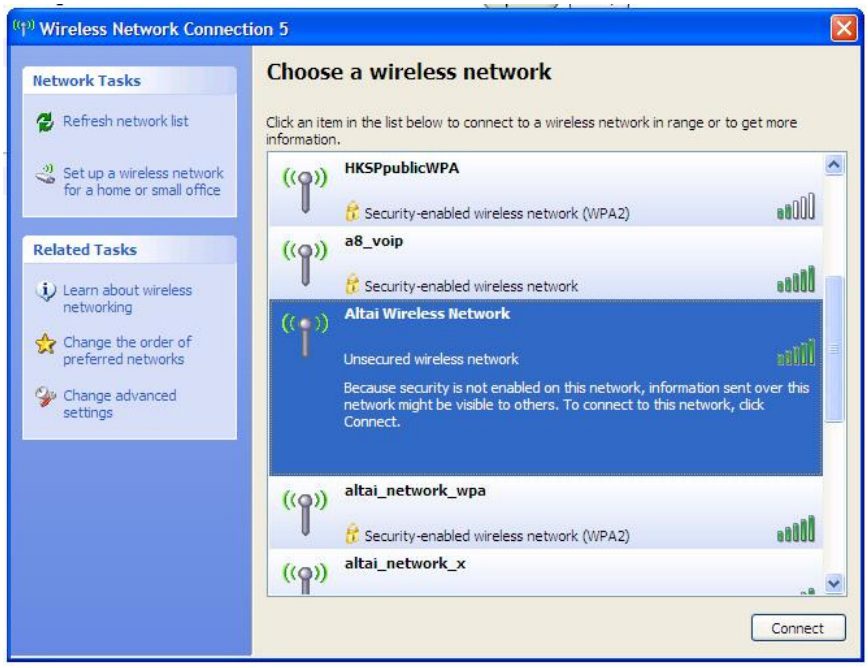


Figure 6 Showing Available Wireless Network Connections in Windows XP

3.2 CHECK ACCESS

"`ping`" utility of DOS mode is a handy tool to check the access to the A3 smart WiFi.

1. Go to DOS mode by typing "cmd" in "**Run**".
2. Type command:

   ```
   ping 192.168.1.20
   ```

   The A3 smart WiFi shall respond to your ping request if it has a correct connection with your PC.

NOTE: Using the same PC to ping different A3 smart WiFi may cause ping failure. This is because the A3 smart WiFi APs have the same default IP address but different MAC addresses. You need to type a command "`arp -d`" in DOS mode to clear ARP table on PC before each ping.

4 CONFIGURATION WITH WEB-ADMIN

4.1 WEB BROWSER CONNECTION

The A3 can be accessed through a Web Browser, for example, Internet Explorer (IE).

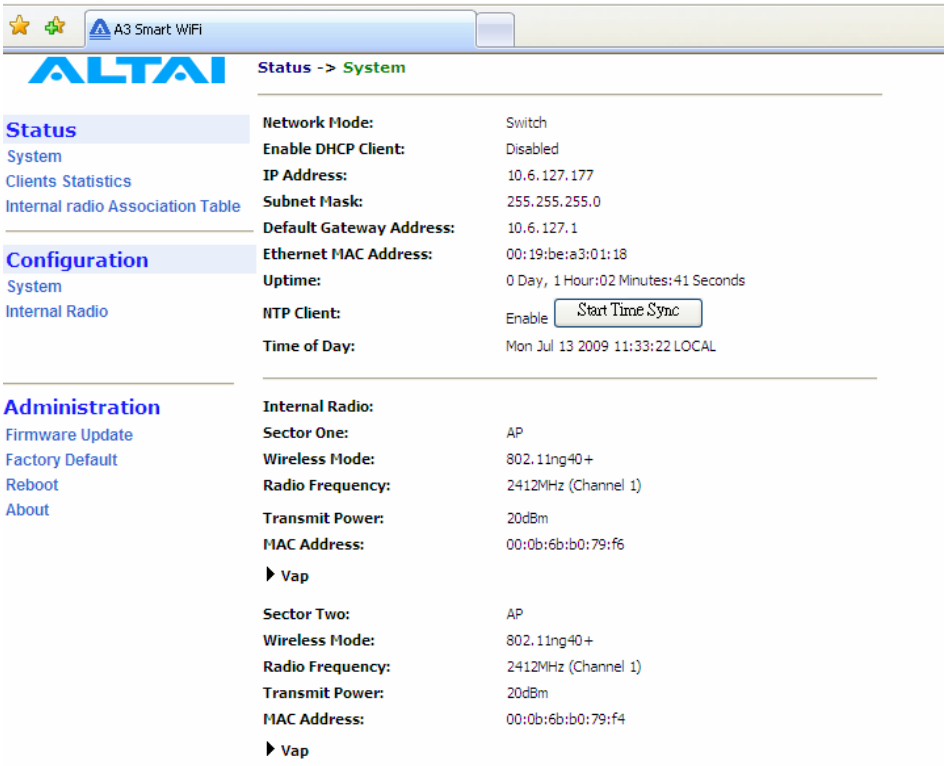
1. Open an IE session and type the IP address of the A3 Pico AP. Example: https://192.168.1.20, where 192.168.1.20 is the A3's IP address. The **A3 default IP Address** is **192.168.1.20**. Note: the release version 5.4.0. only supports **https format URL link.**
2. A window will pop up, as shown in Figure 5. Enter the user name and password in the corresponding fields. The **default User Name** and **Password** are shown in Table 1. They are **case sensitive**.

	Default User Name	Default Password
From version 5.0. onwards	***altai***	***wag***

Table 1 Default User Name and Password for logging in A3 smart WiFi

Figure 5 Enter User Name and Password

Commercially Confidential



3. Figure 6. A **Menu Bar** is located on the left hand side of the IE window. Different configurations can be chosen through the menu bar.

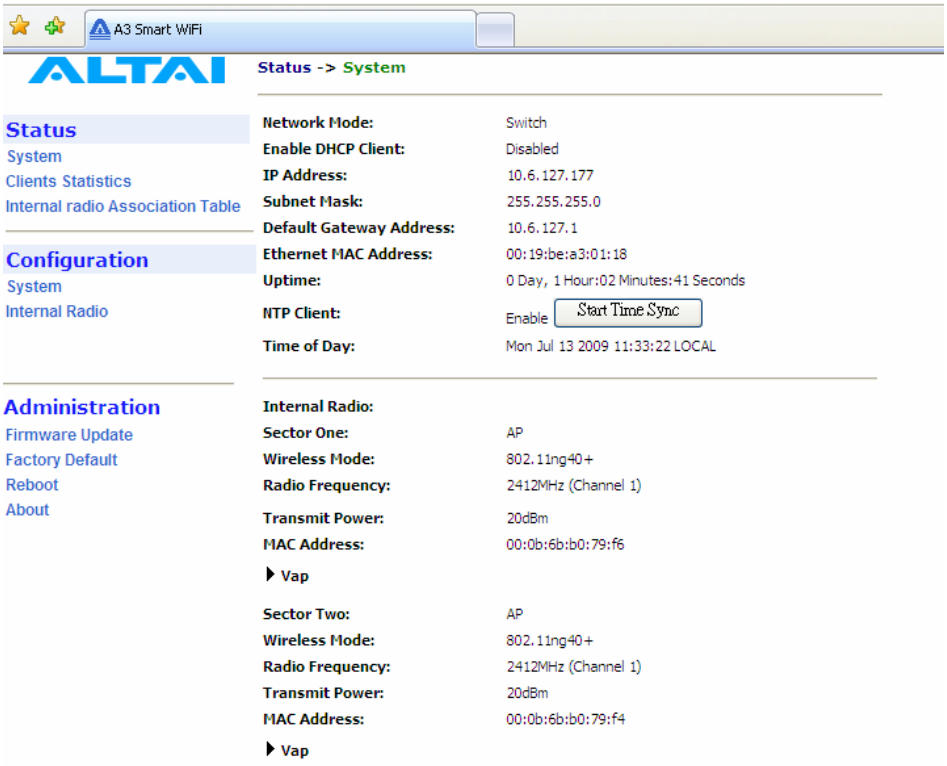


Figure 6 Web-admin Login Page

Commercially Confidential

4.2 CHECKING THE A3 VERSIONS

The running version can be checked by selecting **About** under **Administration** in the menu bar. In Figure 7, it shows:

Firmware Version: v1.0.0 or above versions

Figure 7 Version of A3 smart WiFi

4.3 SETUP – USER NAME, PASSWORD AND SYSTEM NAME

The ***Password*** and ***System Name*** can be configured by selecting **System** under **Configuration** in the menu bar, as shown in Figure 8

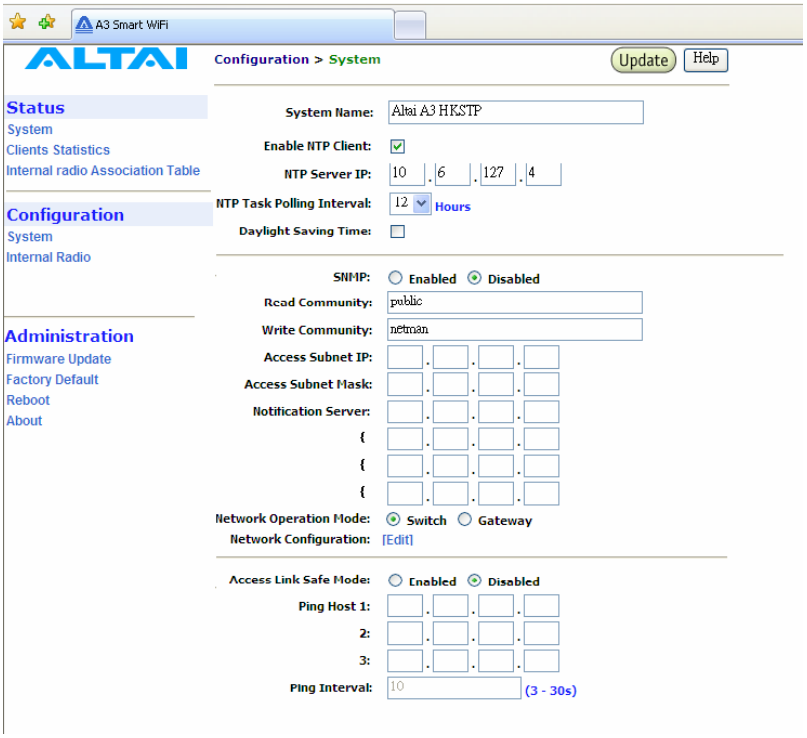


Figure 8 System Configuration

Commercially Confidential

The ***User Name*** and ***Password*** for login are mentioned in Section 4.1, but only password can be changed by entering a new string in the field of ***Password***. Note: it is need to **re-enter to confirm** the password. Please press ***Change Password*** button to store the new password.

The ***System Name*** is the name of the A3 smart WiFi.

NOTE: Click the ***Update*** icon to store the changed settings.

4.4 NTP CONFIGURATION

NTP is a network time protocol for the AP to synchronize the system time. There is no NTP server IP address by default. If NTP is needed, IP address of the NTP server must be added and A3 will synchronize with the NTP server. This measure is useful to maintain the network and make sure all APs using the same system time by setting the same NTP server.

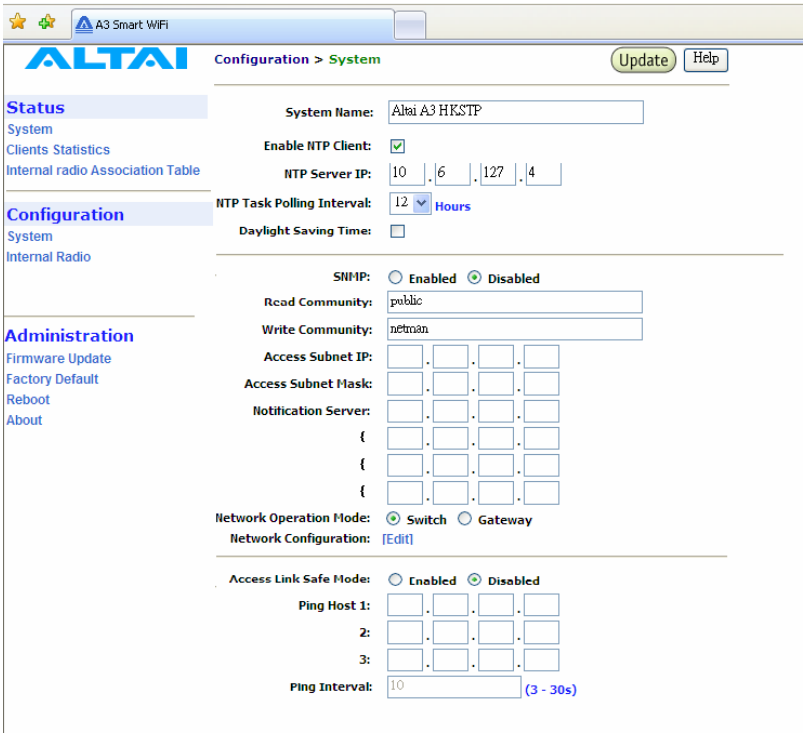


Figure 9 NTP Configuration

NOTE: Click the ***Update*** icon to store the changed settings.

4.5 SNMP CONFIGURATION

In the SNMP Manager, the administrator can change the **Read Community** and **Write Community**. **Access Subnet IP** and **Access Subnet Mask** can be configured to specify the A3's SNMP Manger. **Notification Server** IP addresses can be added for SNMP control. They are parameters used for SNMP control between Altai A3 and AWMS system.

By enabling SNMP Manager ACL mode, the A3 will only be managed by the AWMS which IP is located in the ACL list with correct Read Community, Write Community and SNMP IP

address.

It also supports SNMP Manager Access Control List which allows user to configure a list of allowed SNMP manager IPs for managing the A3. When the SNMP manger ACL mode is enabled, only SNMP request generated from the any of configured SNMP manger on the ACL will be handled.

NOTE: Click the ***Update*** icon to store the changed settings.

4.6 TELNET

Administrator can login to the A3 smart WiFi by telnet command in Command Prompt via Ethernet or WiFi. For example, to telnet A3 with IP address of 192.168.1.20; telnet command is "***telnet 192.168.1.20 2223***".

NOTE: The telnet port number is limited at ***2223***.

4.7 NETWORK OPERATION MODE

The default setting for the Network Operation Mode is ***Switch Mode***. If the A3 smart WiFi is set to ***Switch Mode***, it acts as a switch and routes traffic between the DS and wireless clients accordingly. When it is in ***Gateway*** mode, it acts as a gateway and the ***Local IP Address*** and ***Local IP Address Mask*** information must be entered to specify the A3 local interface for serving the wireless client.

In ***Switch*** mode, VLAN mode is by default disabled and clients in different SSID under the same A3 can communicate with each other. However, if VLAN is enabled, each SSID can be edited with a specific VLAN tag value. Only clients with same VLAN tag in same or different SSID can communicate. Moreover, in this mode, DHCPS, NAT and PPPoE configuration have no effort.

However, in ***Gateway*** mode, the DHCPS, NAT and PPPoE configurations can be configured but the VLAN has no effort.

In ***Switch*** mode,

- VLAN can be configured
- DHCPS, NAT and PPPoE are disabled

In ***Gateway*** mode

- VLAN is disabled
- DHCPS, NAT and PPPoE can be configured

4.8 SWITCH MODE

4.8.1 Static IP address

In *IP Assignation***, there are two kinds of working mode for A3 base station:** *Static IP address* **and** *DHCP Client***.** In ***Switch*** mode, by clicking ***Network Configuration*** in the System page, users can configure the ***IP Address***, ***Subnet Mask*** and ***Gateway Address***, as shown in Figure 10 and Figure 11.

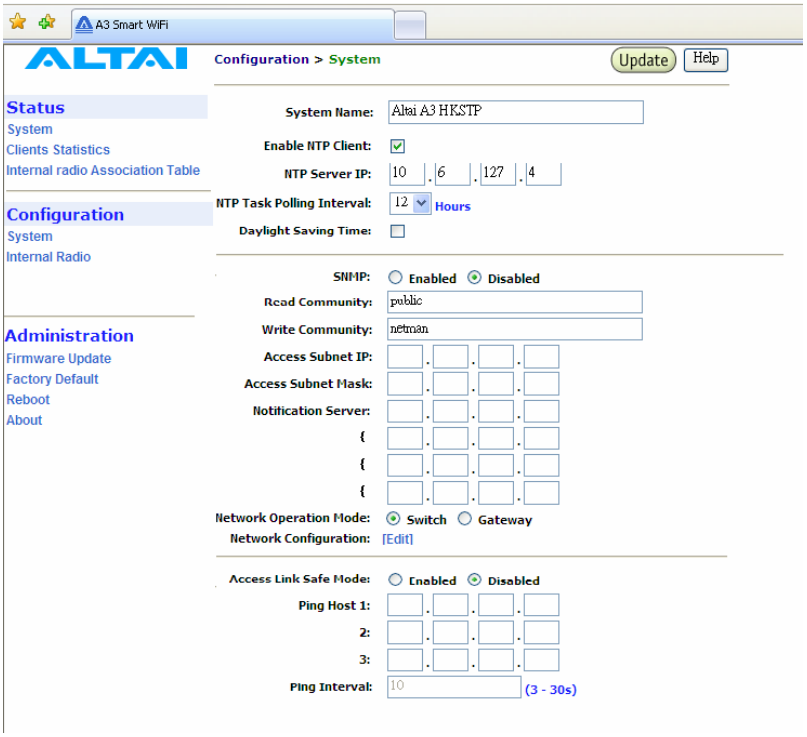


Figure 10 The IP address here is the Ethernet interface of the A3

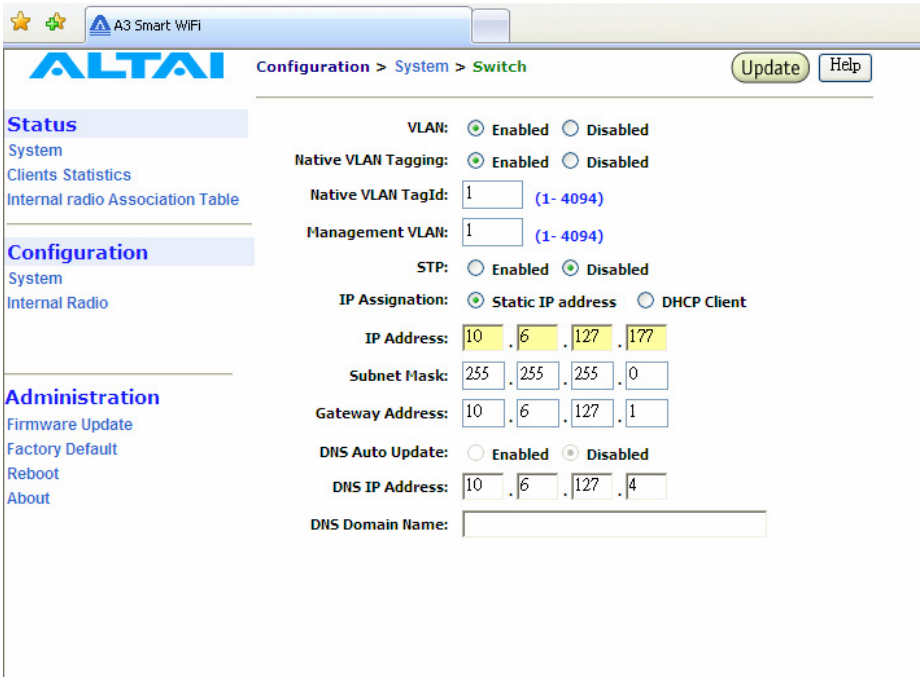


Figure 11 Network Configurations under Switch mode

Commercially Confidential

4.8.2 VLAN Configuration

Default setting of ***VLAN*** is "***Disabled***". By clicking "***Enabled***", VLAN can be enabled. A3 supports VLAN to VAP mappings to provide network security.

Management VLAN is used to configure the management VLAN of A3. A3 can only be accessed through the specified management VLAN when VLAN is enabled. It will be ignored when VLAN is disabled.

Native VLAN Tagging control is used to control the untagged packet when VLAN is enabled. All the packets without VLAN tags should be sent to the VLAN with Native VLAN Tag ID. The default setting of Native VLAN Tagging is "***Disabled***". Native VLAN Tagging can be enabled when VLAN is enabled.

4.8.3 STP Configuration

STP ensures a loop free topology for any bridged LAN. Under switch mode, STP can be configured with choice of "***Enabled***" and "***Disabled***", where the default setting is "***Disabled***".

The system supports the following fixed default STP parameters:

- Bridge priority: 32768
- Bridge maximum age: 20 seconds
- Bridge hello time: 2 seconds
- Bridge forwarding delay: 15 seconds
- Ethernet port path cost: 80
- Ethernet port priority: 128
- 802.11a bridge port path cost for each bridge link: 100
- 802.11a bridge port path priority for each bridge link: 128

4.8.4 DHCP Client

By enabling DHCP Client and clicking the icon ***Update***, the A3 smart WiFi will acquire a dynamic IP address from a DHCP server after rebooting.

Without enabling DHCP Client, the ***IP Address***, ***Subnet Mask*** and the ***Default Gateway Address*** should be configured by the user, **unless** the user prefers using the default setting.

NOTE: It is not recommend enabling DHCP client to allocate the IP address of A3 smart WiFi which is hard to predict after rebooting the A3. If the IP address of A3 smart WiFi is unknown, there is no way to maintain the A3 smart WiFi via web-admin page.

4.8.5 DNS Auto Update

By setting DNS Auto Update to ***Enabled*** and clicking the icon ***Update***, the A3 smart WiFi will acquire a DNS Server IP address via the DHCP Server after **rebooting**. User need not to set a DNS Server IP Address manually.

Without enabling the A3 as a DHCP Client, the ***DNS IP Address*** and ***DNS Domain Name*** should be configured by the user.

NOTE: DNS Auto Update can only be enabled when DHCP client is enabled. If the DNS Auto Update is enabled, it must be used in conjugation with either the DHCP Client or the PPPoE Mode being enabled. If both the DHCP Client and the PPPoE Mode are disabled then the DNS Auto Update must also be set to ***Disabled***.

4.9 GATEWAY MODE

In ***Gateway*** mode, by clicking ***Network Configuration*** in the System page, users can configure the WAN and LAN settings.

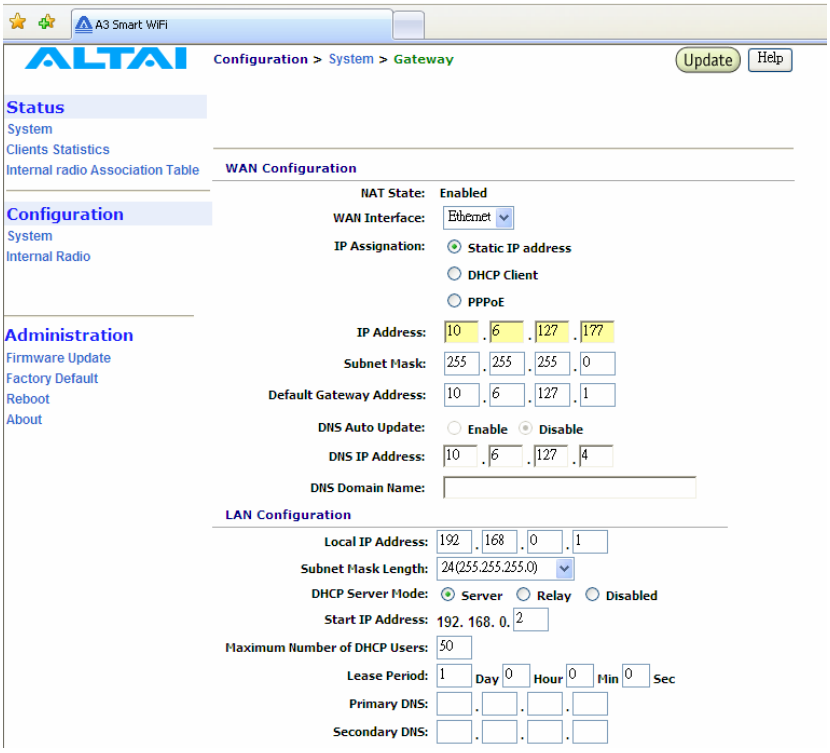


Figure 12 Network Configurations under Gateway mode

4.9.1 WAN Configuration

NAT is set to “Enabled” as default.

The settings for Static IP address and DHCP Client are similar to those in switch mode. Please refer to the previous section for details.

4.9.1.1 WAN Interface

Default setting is "Ethernet". This control is used to specify the WAN interface. The **Ethernet interface** or **5G bridge interfaces** can be used as the WAN interface when **VAP0** works on the **AP mode**. Use the pull down menu to select either one. The **2.4G Radio Client interface** is used as the WAN interface when **VAP0** works on the **Station mode**.

4.9.1.2 PPPoE Configuration

If PPPoE is chosen, a PPPoE login will be attempted for the ***PPPoE Username***, ***PPPoE Password*** and ***PPPoE Service Name***, see Figure 13.

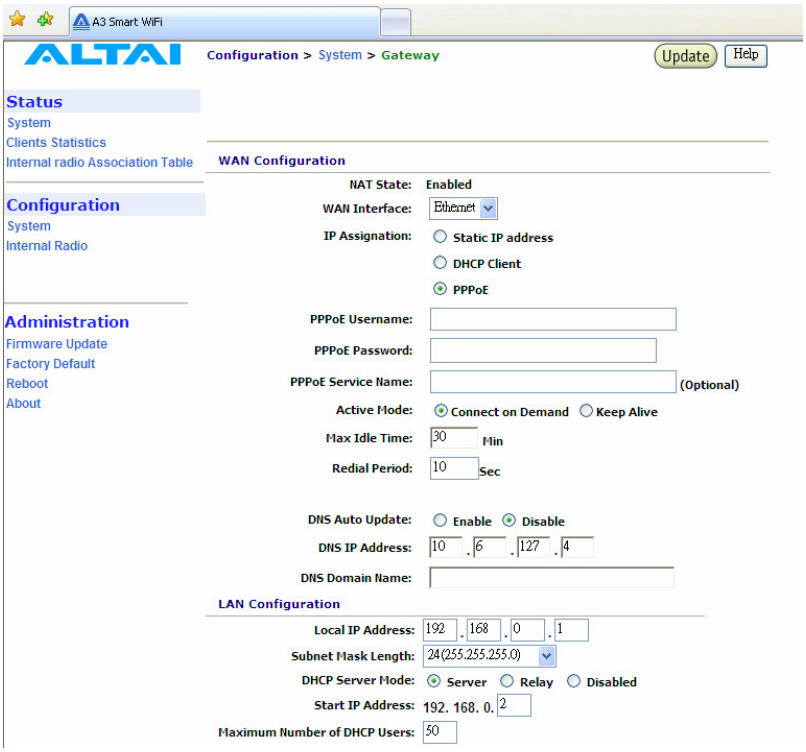


Figure 13 PPPoE Configuration

NOTE: The DNS Auto Update should be set to ***Disable*** when using PPPoE. User need to configure the DNS server IP address manually.

PPPoE ***Active Mode***, ***Max Idle Time*** and ***Redial Period*** can be configured.

When "***Connect on Demand***" is selected, PPPoE will establish the connection with the remote access concentrator only when hosts in the local subnet need to access the internet. If the parameter is set "***Keep Alive***", PPPoE will establish the connection with the remote access concentrator upon boot-up.

Default setting of ***Max Idle Time*** is ***30*** minutes. Only when PPPoE works under **Connect on Demand** mode, it will be disconnected if PPPoE connection has been idle for the Max Idle Time.

When last attempt failed, A3 smart WiFi will attempt to establish the PPPoE connection at ***Redial Period***.

4.9.2 LAN Configuration

In ***Gateway*** Mode, the A3 can be a DHCP server, a DHCP relay or none of them.

When the DHCP Server Mode sets to ***Server***, the A3 will act as a DHCP server and use the settings specified in the field ***Start IP Address***, ***Maximum Number of DHCP Users*** and ***DNS*** to serve the wireless clients.

1. Configure the ***Local IP Address*** and ***Subnet Mask Length***. Local IP Address is the gateway IP address for the client who associates A3 smart WiFi. Only the clients under the same subnet of local IP address can get IP address from A3 smart WiFi.
2. Configure the ***Start IP Address, Maximum Number of DHCP Users***, and ***DNS,*** see Figure 14.
3. Reboot the A3

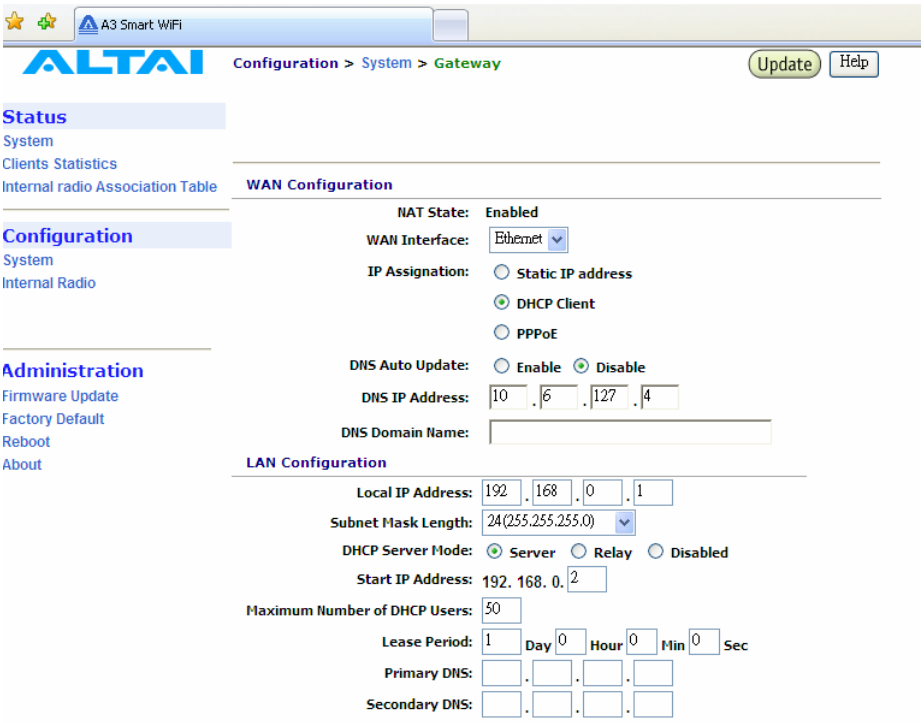


Figure 14 Configure DHCP Server

When the DHCP Server Mode sets to ***Relay***, the A3 will redirect all DHCP requests from the wireless clients to a backend DHCP server with IP address specified by the Relay Server IP Address.

1. Configure the ***Relay Server IP Address***, see Figure 15.
2. Reboot the A3

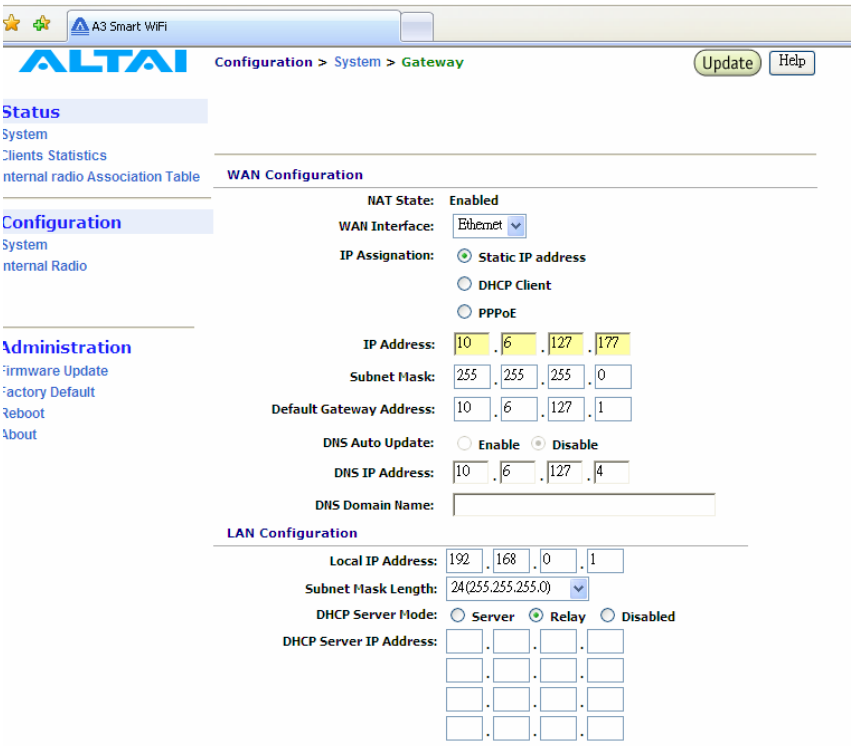


Figure 15 Configure DHCP Relay Server

When the DHCP Server Mode sets to ***Disabled***, the A3 will neither be a DHCP server nor a DHCP Relay and hence the wireless clients CANNOT get IP addresses from the A3 smart WiFi to access the Internet. Instead, each wireless client should set a fixed static IP address which is in the same network domain as the A3.

4.10 ACCESS LINK SAFE MODE/ BACKHAUL LINK SELF-HEALING

Access Link Safe Mode is for detecting the backhaul link integrity. If the AP loses its backhaul connectivity, it forces the clients to re-associate with another AP by changing its SSID to a default "A3 Safe Mode XXX", where "XXX" is the MAC address of the 2.4GHz radio in hexadecimal. This action can protect the client from connecting to a AP which has no backhaul to the Internet end. Default Access Link Safe Mode is ***Disabled***. Press the icon ***Enabled***, A3 smart WiFi will work under Access Link Safe Mode.

In the case where **multiple physical backhauls** are available, the ***Backhaul Link Self-Healing*** feature will switch to other backhaul if the current one goes down. For example, when default backhaul is set to 5GHz Radio, once the 5GHz Bridge link is broken down, A3 smart WiFi will try Ethernet end as its new backhaul. Default setting is ***Disabled***. After enabled the Backhaul Link Self-Healing, Default Backhaul Link can be configured.

Three **different *Ping Host*** can be added to the list **for monitoring the connectivity**. If either Access Link Safe Mode or Backhaul Link Self-Healing is enabled, the AP will ping those specified hosts periodically at the ***Ping Interval*** configured.

4.11 SETUP – WIRELESS RADIO PARAMETER

Wireless radio parameters can be modified under **Configuration** in the menu bar. ***Internal Radio*** uses the antennas at the side of A3. By selecting the icons, ***Internal Radio*** can operate on different modes separately: ***AP mode***, ***Repeater mode***, ***Bridge mode*** and ***Disable***. The default setting of Internal Radio is ***AP mode***.

4.12 AP MODE

Wireless Radio working on AP mode is used for clients association. Altai A3 smart WiFi combine 802.11b/g and draft 802.11n together to offer both 2.4GHz radio and 5GHz radio access for clients.

The ***Radio Enable Mode***, ***Wireless Mode***, ***Auto Channel Selection, Radio Frequency*** (Channel), ***Maximum Clients, Transmit Power***, ***Advanced Settings*** and ***VAP*** can be configured by selecting ***AP*** icon under **Internal Radio**, as shown in Figure 16.

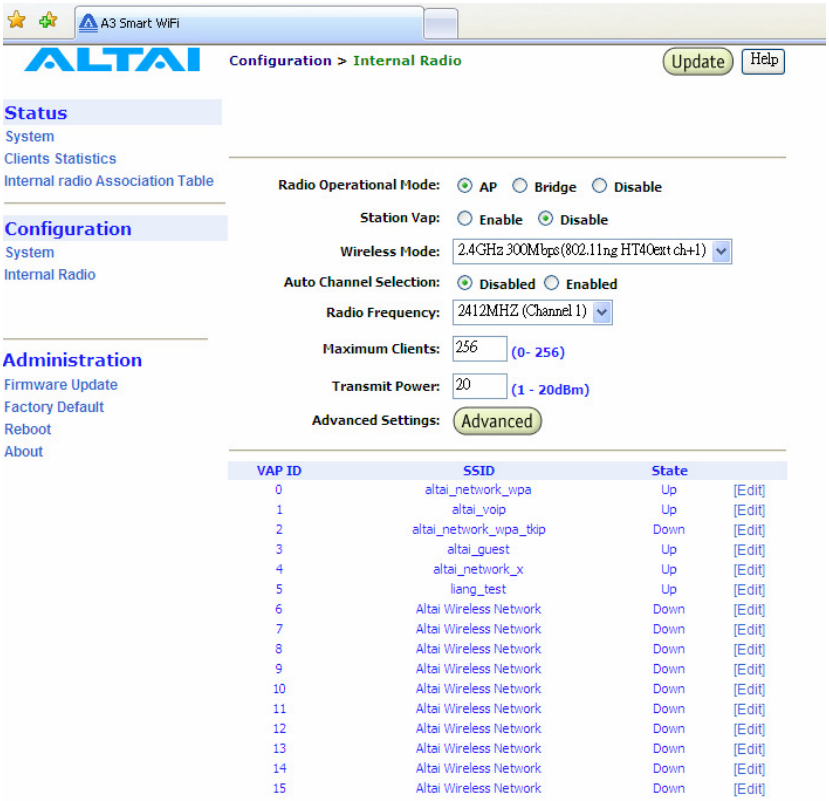


Figure 16 Wireless Radio Parameter Configuration

Commercially Confidential

4.12.1 Wireless Mode and Radio Frequency

Altai A3 smart WiFi can offer both 2.4GHz radio and 5GHz radio access, the following tables list the operation mode and available frequency under the particularly wireless mode. Default setting of AP mode radio is working on 2.4GHz 300Mbps (802.11n HT 40ext ch+1) and default channel is channel 6 (2437MHz).

2.4GHz Radio Mode	Data Rate	Channels	Radio Frequency
802.11b	11 Mbps	1,2,3,4,5,6,7,8,9,10,11	2.412GHz-2.462GHz
802.11b/g	54 Mbps	1,2,3,4,5,6,7,8,9,10,11	2.412GHz-2.462GHz
802.11g	54 Mbps	1,2,3,4,5,6,7,8,9,10,11	2.412GHz-2.462GHz
802.11na HT20	130 Mbps	1,2,3,4,5,6,7,8,9,10,11	2.412GHz-2.462GHz
802.11n HT40ext ch+1	300 Mbps	1,2,3,4,5,6,7	2.412GHz-2.442GHz
802.11n HT40ext ch-1	300 Mbps	5,6,7,8,9,10,11	2.432GHz-2.462GHz

5GHz Radio Mode	Data Rate	Channels	Radio Frequency
802.11a	54 Mbps	149, 153, 157, 161, 165	5.745GHz-5.825GHz
802.11na HT20	130 Mbps	149, 153, 157, 161, 165	5.745GHz-5.825GHz
802.11na HT40ext ch+1	300 Mbps	149, 157	5.745GHz-5.785GHz
802.11na HT40ext ch-1	300 Mbps	153, 161	5.765GHz-5.805GHz

Table 2 AP mode Radio operation wireless mode, channel and Radio Frequency

4.12.2 Auto Channel Selection

By default, the Auto Channel Selection is disabled; the A3 is fixed on Channel 6. When ***Enabled*** of Auto Channel Selection is chosen, A3 smart WiFi can scan all available radio channels which are assigned to the regulatory domain. The "cleanest" channel is then selected as the operating channel.

NOTE: After changing frequency channel, it takes around 3 minutes for A3 to optimize its radio performance.

4.12.3 Maximum Clients

A value between the ranges from ***0*** to ***256*** can be filled in ***Maximum Clients*** blank. This feature can limit the total associated clients under the particular radio.

4.12.4 Transmit Power

The value of the ***Transmit Power*** depends on both the gain of the antenna and the maximum value of the Effective Isotropic Radiated Power (***Max EIRP***) allowed by the country in which A3 is used. The ***Transmit Power*** should be configured within the given range as shown in Figure 16.

NOTE: Click the ***Update*** icon to store the changed settings.

4.12.5 Advanced Radio Setting

More radio parameters can be verified and altered by selecting the ***Advanced*** icon in the field of ***Advanced Setting***. The parameters are shown in Figure 17. The following table showed is the best suggested interval worked with the current operated APs. Note that it is not suggested to change the parameters in Advanced Radio Settings unless you are experienced administrators.

Number of active VAPs	Auto Beacon Interval (ms)
1	100
2	150
3	150
4	200
5	200
6	240
7	280
8	320
9	360
10	400
11	440
12	480
13	520
14	560
15	600
16	640

Table 3 Beacon Interval

Fragment Threshold: It means the size of each frame. If it is set to 256 bytes and the size of data block is 1024 bytes, the data block will be divided to four frames to send.

RTS/CTS Threshold: RTS is a flow control mechanism to prevent collision between 802.11b and 802.11g mobile stations to send data to the access point in the same time. CTS is another flow control mechanism to prevent collision when two mobile stations, who do not know the existence of each other, send data to the access point in the same time. RTS and CTS are used for point-to-multipoint bridge application and they are enabled when the threshold set to 2346.

Figure 17 Advanced Wireless Radio Setting

4.12.6 Service Set IDentifier (SSID) and Virtual Access Point (VAP)

In order for the A3 smart WiFi and mobile clients to communicate, they must all be configured to use the same SSID for communication both at the VAP and clients ends. SSID broadcast can be enabled or disabled by selecting ***Suppress SSID***. ***Suppress SSID*** is used to prevent unauthorized users scanning for SSID while still allowing users who know the correct SSID to connect.

VLAN can be enabled by adding different ***VLAN Tag*** ID. The traffic will pass through the specific VLAN switch port when VLAN is enabled.

Each VAP setting (including SSID) can be altered by selecting ***Edit***. The setting of each VAP is shown in Figure 18. The ***default SSID*** for each ***VAP ID*** is ***Altai Wireless Network***. ***VLAN Tag*** can also be set here.

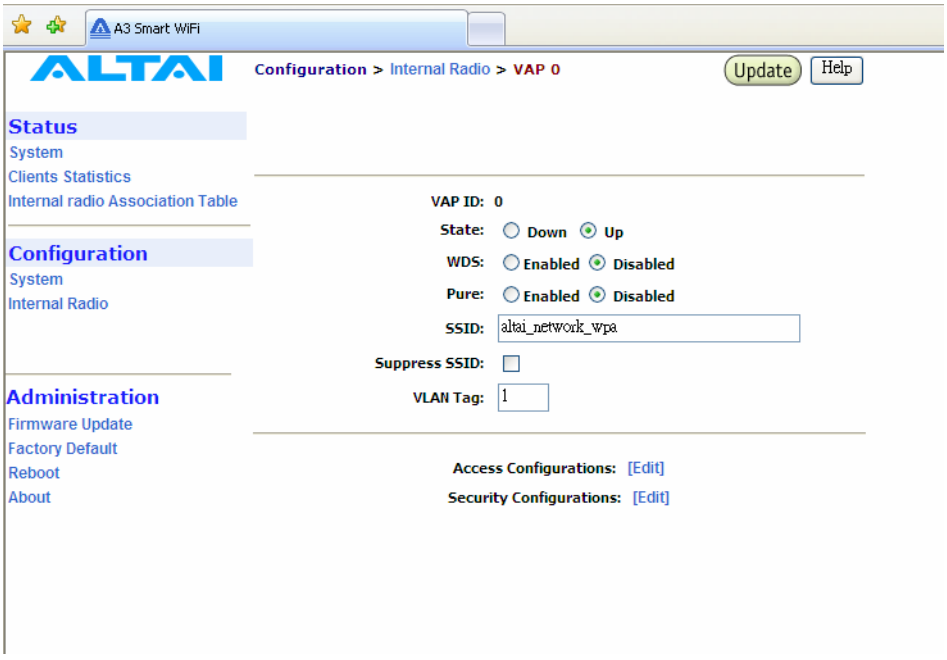


Figure 18 VAP Setting

Commercially Confidential

4.12.7 Access Control List (ACL)

By selecting ***Access Configurations,*** a window, as shown in Figure 19, is brought up for choosing the ACL mode, adding ***MAC Address*** with ***ACL Type*** (***Allow*** or ***Deny***).

There are three modes in the Access Control List (ACL). They are ***Disabled***, ***Enabled-Allow*** and ***Strict-Deny***:

1. ***Disabled***
   - The function of ACL is **disabled**.
2. ***Enabled–Allow***
   - The function of ACL is **enabled**.
   - The MAC addresses which are specified in the ACL will consider as Allow.
   - i.e. **No** computer can access to the base station, **unless** the computer which has an MAC address **matches** one of the entries of the ACL with its ACL Type is ***Allow***.
3. ***Enabled–Deny***
   - The function of ACL is **enabled**.
   - The MAC addresses which are specified in the ACL will consider as Deny.
   - i.e. **Every** computer can access to the base station, **unless** the computer which has an MAC address **matches** one of the entries of the ACL with its ACL Type is ***Deny***.

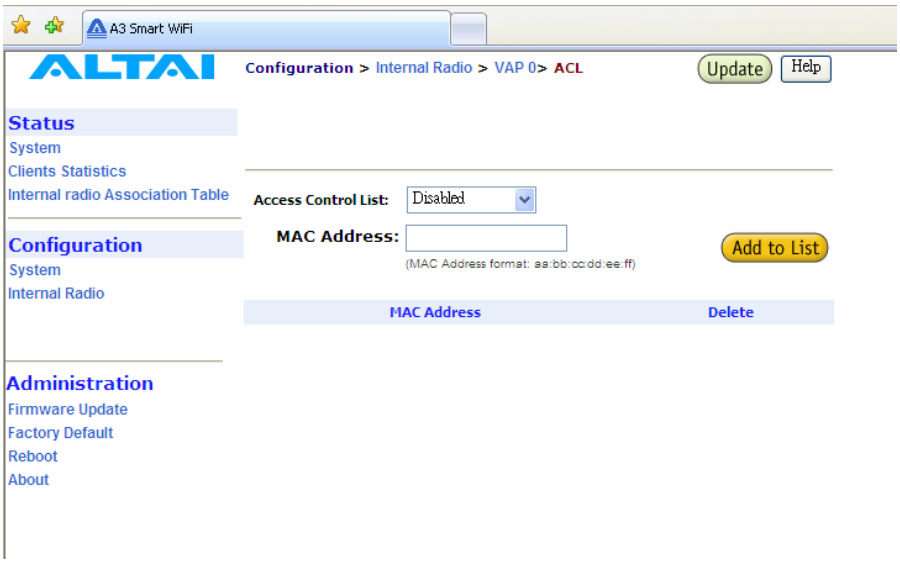


Figure 19 ACL

4.12.8 Encryption and Authentication

By selecting ***Security Configurations,*** a window, as shown in Figure 20, is brought up for choosing the ***Authentication Mode*** and ***Cipher Mode***.

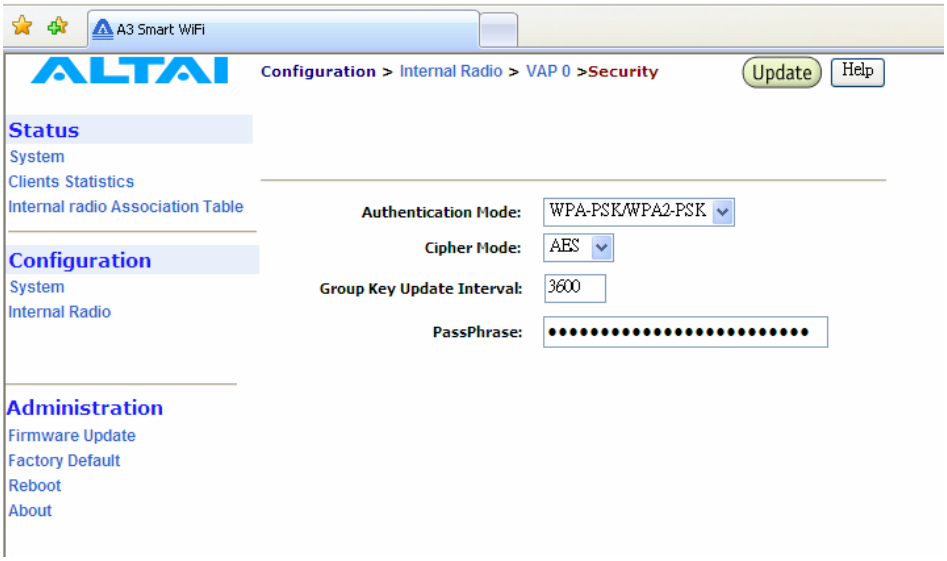


Figure 20 Wireless Radio Security Configuration

After selecting ***Open*** or ***Shared-Key*** for Authentication Mode, ***WEP*** for Cipher Mode, the WEP key settings can be defined as shown in Figure 21.

WPA/WPA2 or WPA-PSK/WPA2-PSK can be enabled by selecting ***WPA/WPA2 or WPA-PSK/WPA2-PSK*** for Authentication Mode. The ***AES*** and ***TKIP*** are the two available options for Cipher Mode. The related settings are shown in Figure 20 and Figure 23.

NOTE: Click the ***Update*** icon to store the WEP or WPA settings.

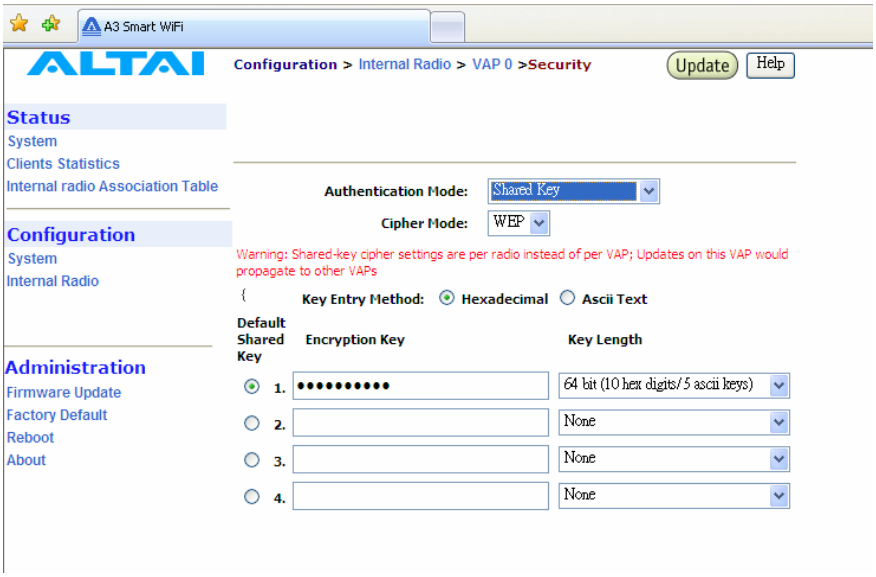


Figure 21 WEP Key Settings

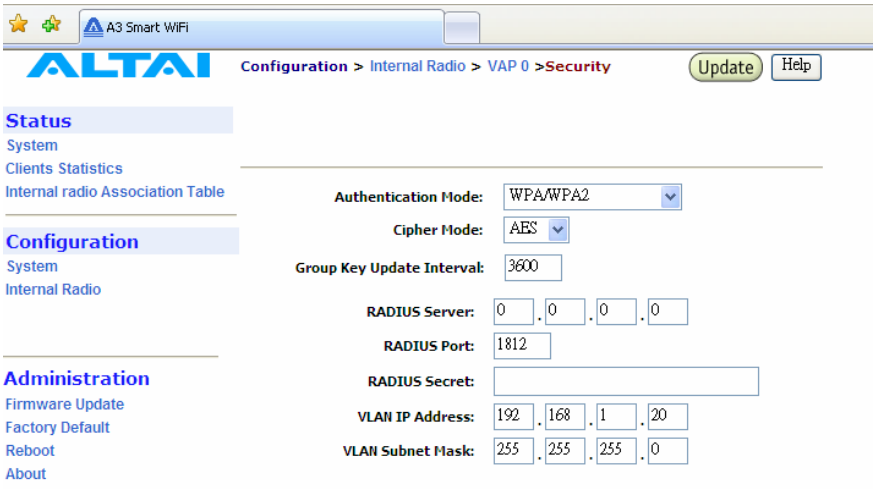


Figure 22 WPA Settings

RADIUS server is used for authentication. A3 smart WiFi can store separate RADIUS server address for each VAP. It is only visible when the **Authentication** Mode is set to "***WPA***". The default setting of ***RADIUS server port*** is 1812. ***RADIUS secret*** shared password between the RADIUS server and A3 smart WiFi. A password up to 128 characters long can be added. The ***VLAN IP address*** and ***VLAN Subnet Mask*** configured on the VAP security web page will be used only when A3 runs in the following conditions.

1. A3 smart WiFi runs in **switch** mode and VLAN is **enabled**.
2. The VAP does **not** belong to **native VLAN**.
3. The authentication mode is **WPA**.

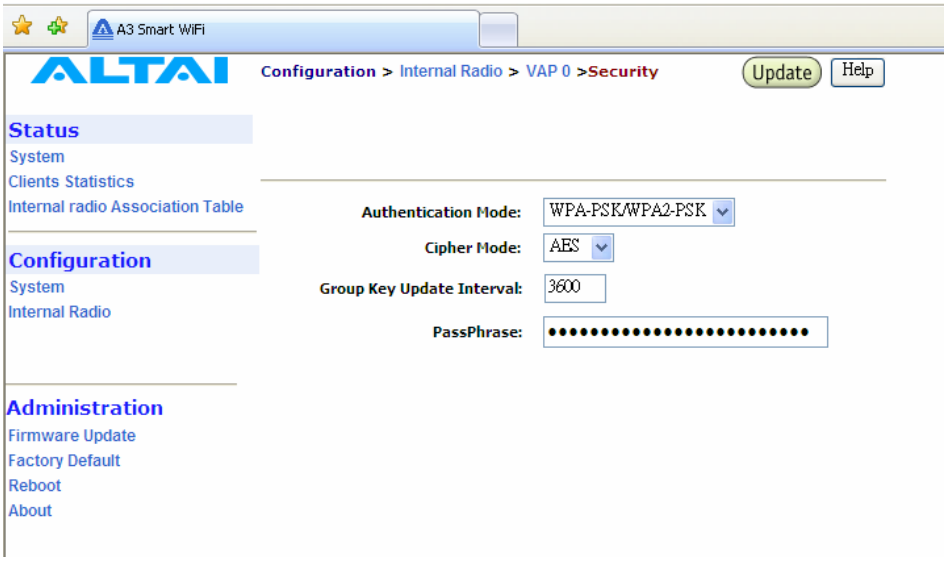


Figure 23 WPA-PSK Settings

Commercially Confidential

4.13 REPEATER MODE

Under Wireless Radio web-site interface, **Station** VAP can be enabled. By clicking ***Enable*** icon, backhaul link can be established through associating the Station VAP with the remote APs. That means the Wireless Radio works as backhaul link, clients can associate with other VAPs who works under AP mode. The local wireless clients associating with the other AP mode Radios can communicate with remote AP through the backhaul link which is established by repeater mode radio.

Edit the ***remote SSID*** index by clicking the Edit icon, and make sure the **security** setting is same with the repeater mode input SSID security method.

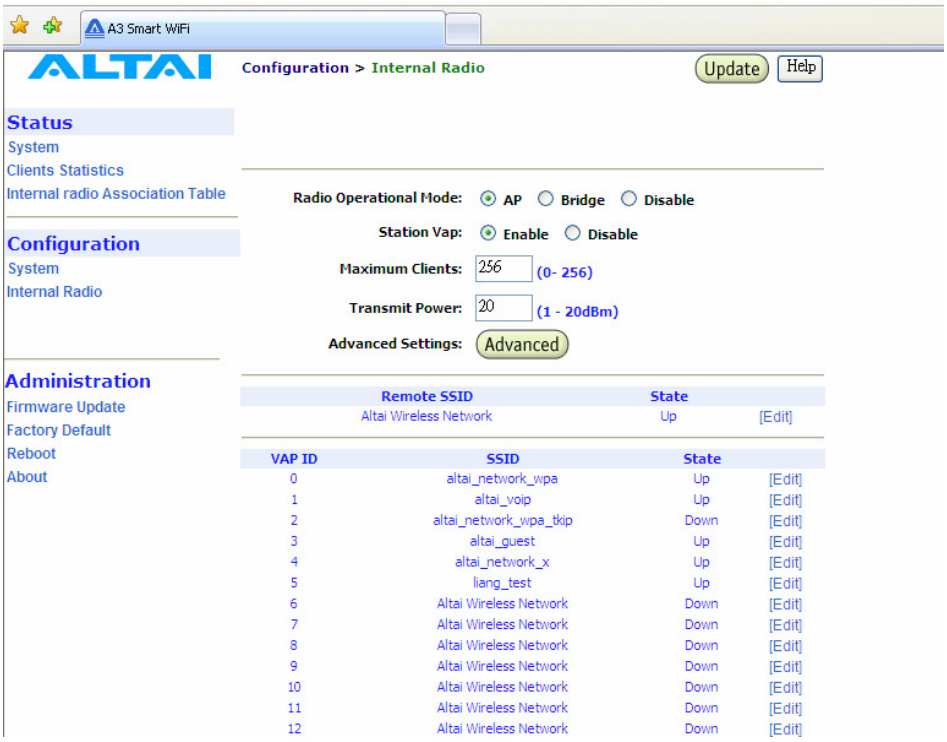


Figure 24 Repeater Mode Configuration

There are three different repeater modes: **NAT mode**, **WDS mode** and **MAC address translation mode (MAT mode).**

When repeater works in **NAT mode**, A3 works in ***Gateway*** mode **and** the ***Station*** mode VAP is enabled. Repeater works in **WDS mode** when ***WDS*** is enabled **and** A3 works in ***Station*** mode. WDS mode requires the remote AP enabled WDS function. The **MAT mode** can be enabled when A3 runs in ***Switch*** mode and ***WDS*** is enabled.

Repeater Mode	System Mode	VAP0 working mode	WDS status
NAT mode	***Gateway*** mode	***Station*** mode	***Disabled***
WDS mode	***Switch*** mode	***Station*** mode	***Enabled***
MAC mode	***Switch*** mode	***Station*** mode	***Enabled***

Table 4 Repeater Mode Setting Method

Commercially Confidential

4.14 BRIDGE MODE

The ***5GHz Radio***, ***Regulatory Domain, Wireless Mode***, ***Radio Frequency*** (Channel), ***Transmit Power***, ***Encryption Configuration***, ***Advanced Settings*** and ***Remote Bridge Configuration*** can be configured by selecting **5GHz Radio** under **Configuration** in the menu bar.

4.14.1 Bridge Radio Wireless Mode

A3 smart WiFi can work under either ***802.11a*** mode or ***802.11na*** mode by selecting on pulling down list. If A3 is set to 802.11a mode, A3 allows only **802.11a** bridges to connect as peers, if A3 work in 802.11a turbo static mode, A3 will allows only **same 802.11na** bridges to connect as peers.

4.14.2 Data Rate & Radio Frequency

The choice of this item depends on the environment where A3 is used and which wireless mode A3 is working in.

5GHz Radio Mode	Data Rate	Channels
802.11a	54 Mbps	149, 153, 157, 161, 165
802.11na HT20	130 Mbps	149, 153, 157, 161, 165
802.11na HT40ext ch+1	300 Mbps	149, 157
802.11na HT40ext ch-1	300 Mbps	153, 161

Table 5 5GHz Radio channel and Data Rate

In 802.11a mode:
User can select a 5GHz channel in the pool from channel 149 to 165 (5.745GHz to 5.825GHz).

In 802.11na HT20:
Users can select a 5GHz channel in the pool from channel 149 to 165 (5.745GHz to 5.825GHz).

In 802.11na HT40ext ch+1:
Users can select a 5GHz channel in the pool from channel 149 to 157 (5.745GHz to 5.785GHz).

In 802.11na HT40ext ch-1:
Users can select a 5GHz channel in the pool from channel 153 to 161 (5.765GHz to 5.805GHz).

4.14.3 Bridge Radio Transmit Power

The power for 5GHz Radio (802.11a) is set in this area. The value of the ***Transmit Power*** depends on both the gain of the 5GHz antenna and the Max EIRP allowed by the country in which A3 is used. The ***Transmit Power*** can be configured within the given range.

NOTE: Click the ***Update*** icon to store the Transmit Power settings.

4.14.4 Advanced Radio Setting

More radio parameters can be verified and altered by selecting the ***Advanced*** icon in the field of ***Advanced Setting***. The parameters are shown in Figure 255.

Figure 25 Advanced Bridge Radio Setting

Fragment Threshold: It means the size of each frame. If it is set to 256 bytes and the size of data block is 1024 bytes, the data block will be divided to four frames to send.

RTS/CTS Threshold: RTS is a flow control mechanism to prevent collision between 802.11b and 802.11g mobile stations to send data to the access point in the same time. CTS is another flow control mechanism to prevent collision when two mobile stations, who do not know the existence of each other, send data to the access point in the same time. RTS and CTS are used for point-to-multipoint bridge application and they are enabled when the threshold set to 2347.

Super bridge mode provides 3 mechanisms to improve the bridge throughput:

- **Compression**: Frame is compressed by hardware before transmitting. Note that the compression may save bandwidth but would consume frame process time. In case the data is already compressed (e.g. mpeg frame), please do NOT turn on this function.

- **Bursting**: Turning on Bursting function enables multiple frames are transmitted at SIFS intervals which may reduce transmission overhead. But this may increase packet error rate on the other side.

- **Fast Frame**: Turning on Fast Frame function enables two Ethernet frames bundled into a single wireless frame.

Warnings 1: It is required to setup the same options of Super Bridge Mode between local AP and remote AP to communicate properly.

Warnings 2: It depends on which mode the associated clients run in to decide whether turning on Bursting and Fast Frame function or not.

4.14.5 Remote Bridge Configuration

The MAC address of the **remote AP** should be added into the field ***MAC Address***, and the **remote AP** should add the **MAC address** of **local AP** to form a bridge. Moreover, all bridging equipments including both local AP and remote APs should be set at the **Same Radio Frequency**.

4.14.6 Bridge Security

By enabling ***Bridge Security*** in the *5GHz Configuration*, as shown in Figure 26, users can input an encryption key for the bridge. Note: if the Local AP and Remote AP mismatch the encryption type or encryption key, there will be no link established by 5GHz radio. Please make sure the security parameter setting at the both ends of the bridge.

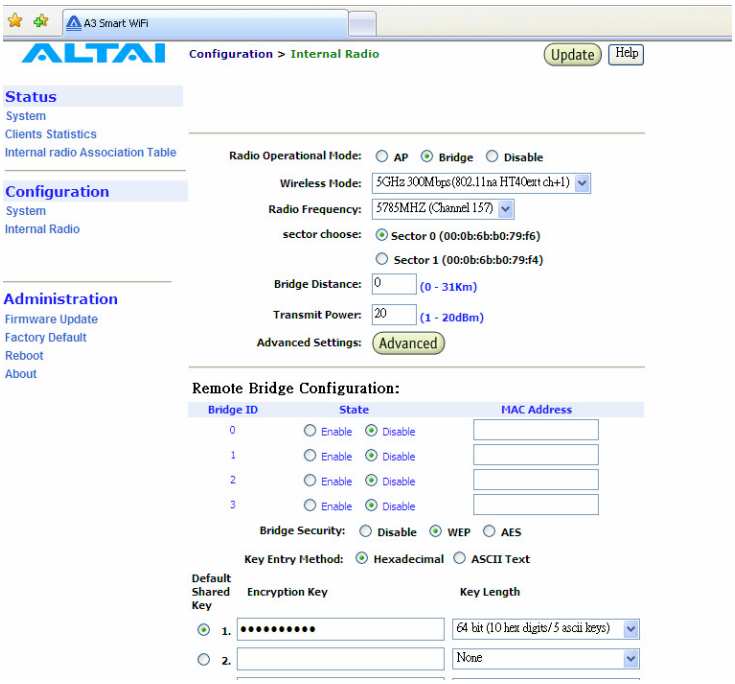


Figure 26 Bridge encryption setting_WEP

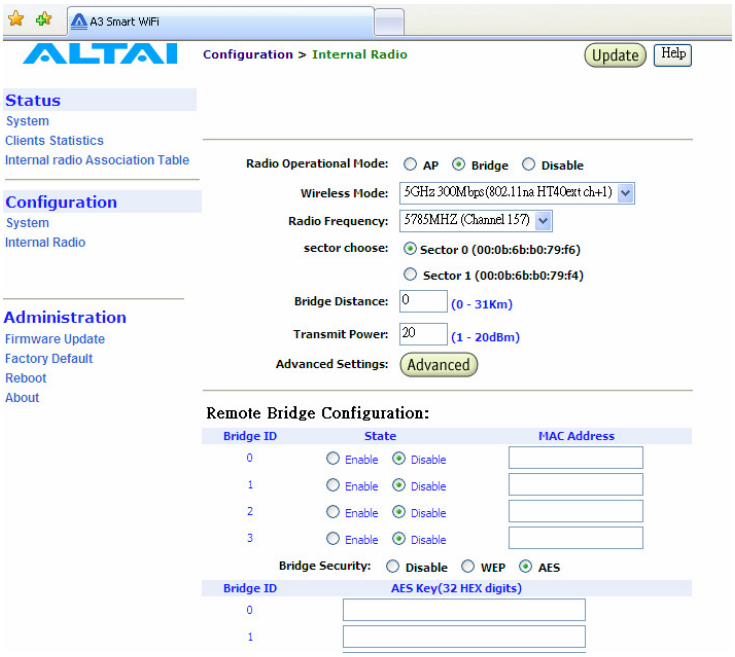


Figure 27 Bridge encryption setting_AES

Commercially Confidential

4.15 DISABLE MODE

The particular radio of A3 smart WiFi can be disabled by click the ***Disable*** icon. There is no need to configure the Transmit Power and Advanced Settings.

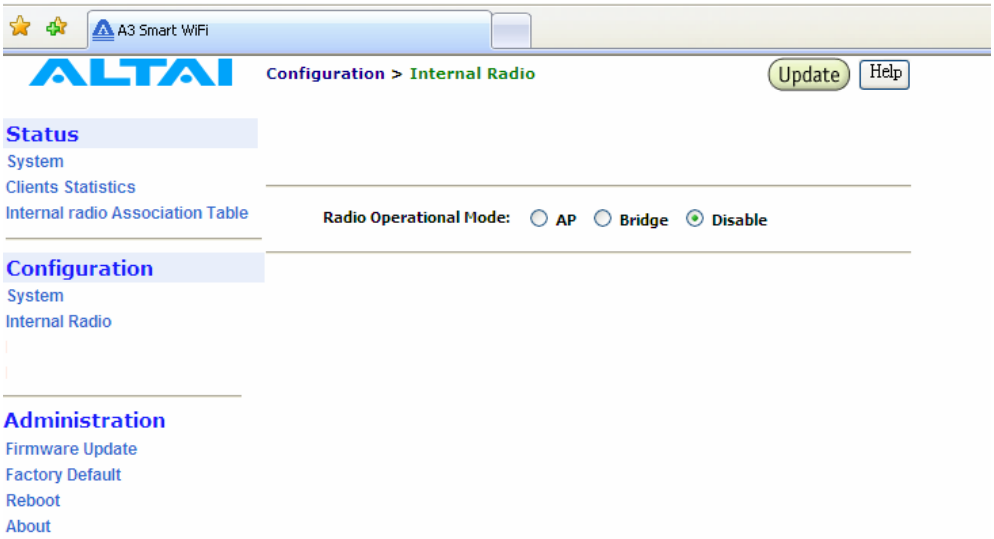


Figure 28 Wireless Radio Disable Mode

4.16 REBOOT

System reboot of A3 smart WiFi can be chosen by selecting **Reboot** under **Administration** in the menu bar. It is required to select ***Reboot Base Station*** to confirm this action, as shown in Figure 29.

When the A3 smart WiFi is rebooting, a message "**Please wait… Base Station is Rebooting**" is shown on the window, as shown in Figure 30. It will take about 20 seconds for the access point to boot up.

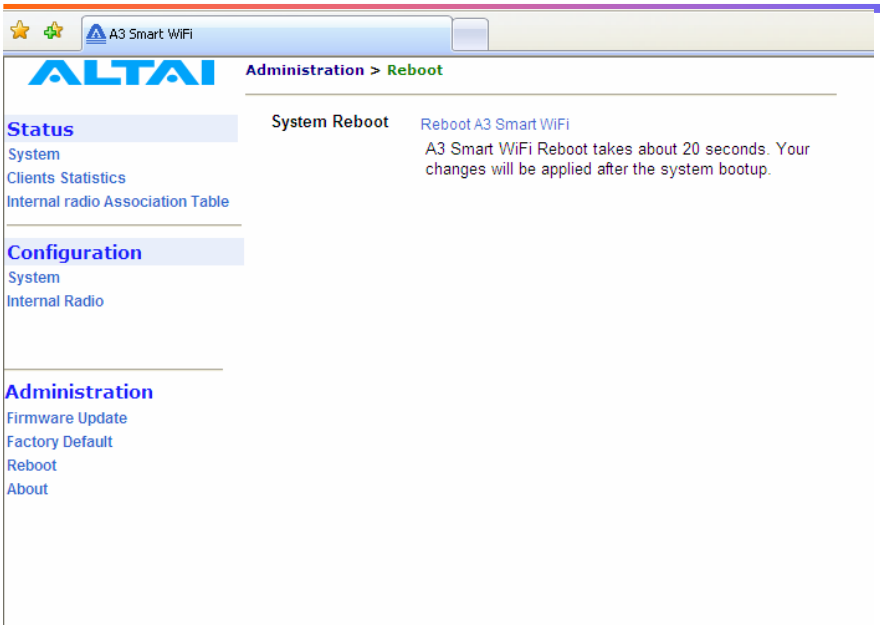


Figure 29 Reboot Window

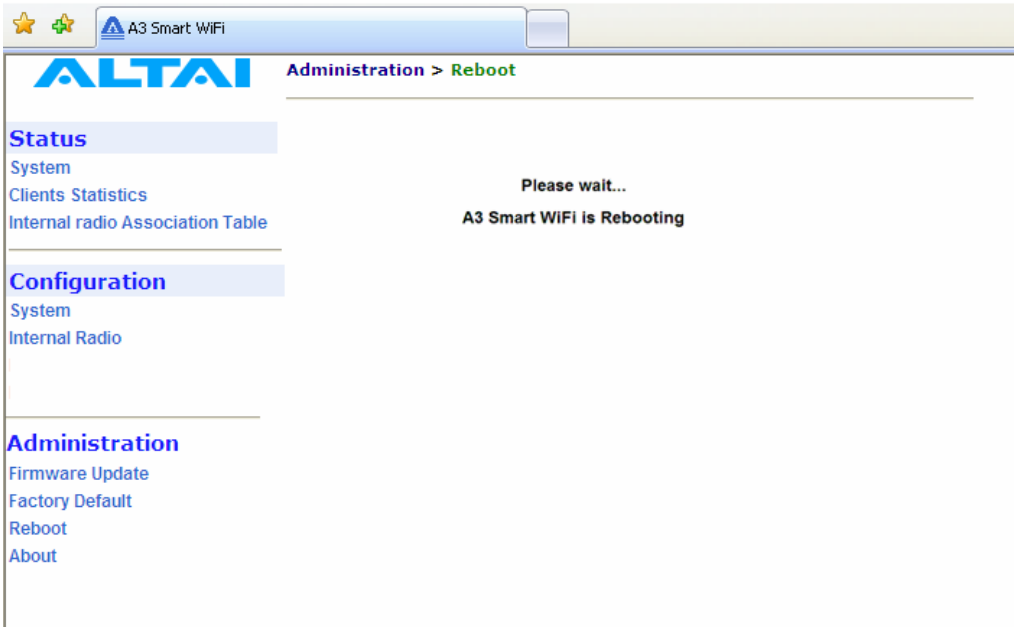


Figure 30 A3 smart WiFi Access Point is Rebooting

4.17 RESTORE CONFIGURATION TO DEFAULT SETTING

The choices of factory default can be chosen by selecting **Factory Default** under **Administrations** in the menu bar.

The default settings (**IP Address, Subnet Mask, Default Gateway Address and Remote Bridge Configurations are retained**) can be restored by selecting the icon ***Reset to Factory Default (address retained)*** or ***Reset to Factory Default***, as shown in Figure . Please reboot the A3 smart WiFi afterwards.

Note: after resetting to factory default **without address retained**, please type <*https://192.168.1.20*> to open A3 smart WiFi web-admin.

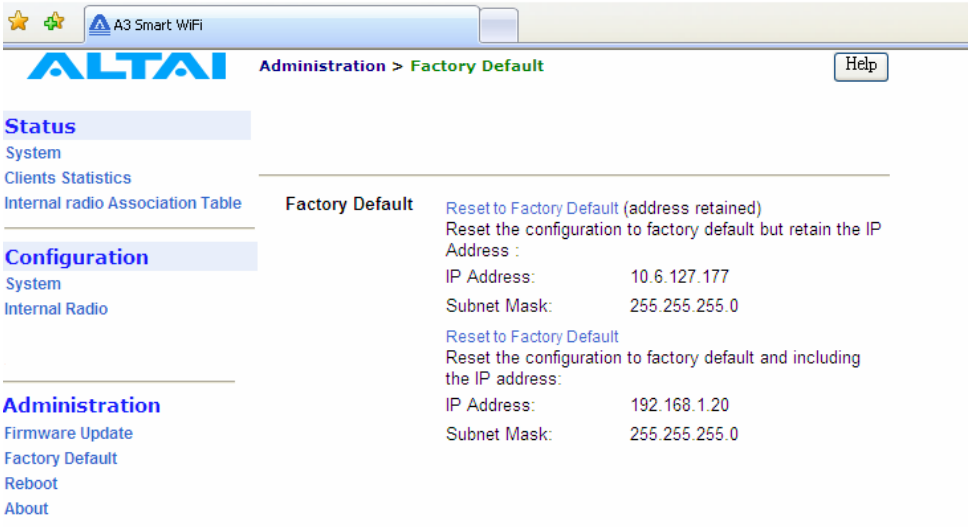


Figure 31 Reset to Factory Default Setting in Web-admin

Commercially Confidential

5 PERFORMANCE MANAGEMENT MONITORING IN WEB-ADMIN

5.1 SYSTEM

The statistics can be monitored by selecting **System** under **Status** in the menu bar. All details are shown on the window, as shown in Figure .

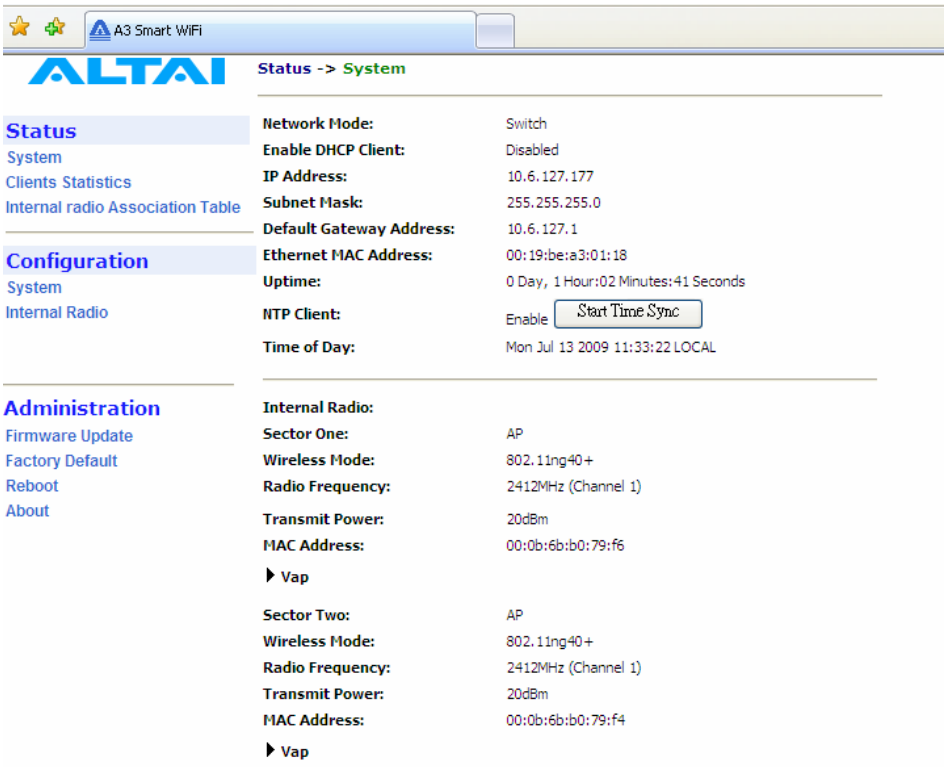


Figure 32 Details of the system

Commercially Confidential

The status of each VAP can be shown by clicking ***Vap*** under the field of ***Wireless Radio***, as shown in Figure .

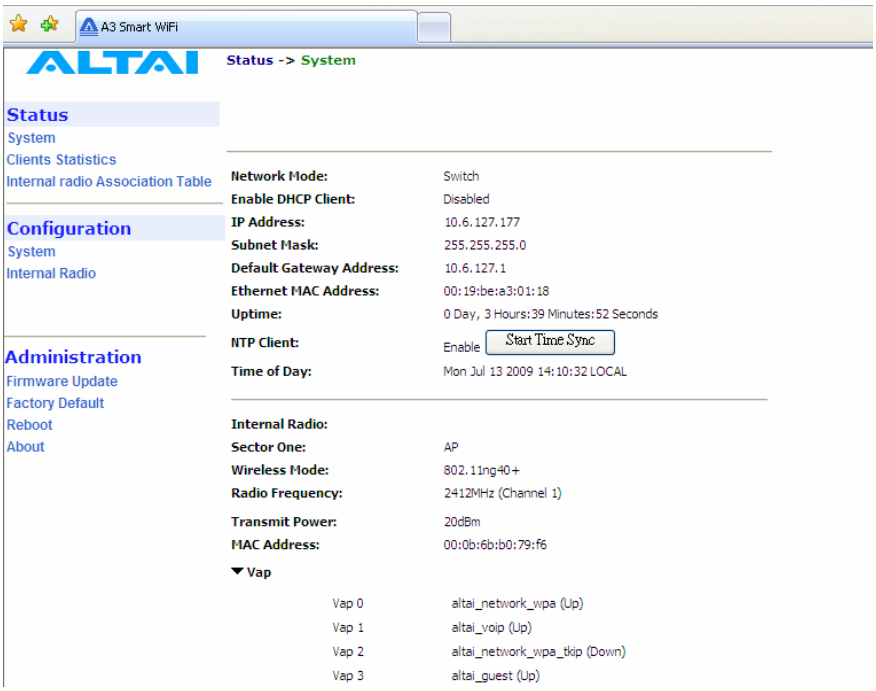


Figure 33 Statuses of the Vaps

The status and MAC address of each remote bridge can be shown by selecting ***Remote Bridge*** under the field of 5GHz Radio.

5.2 CLIENTS STATISTICS

The clients association statistics can be monitored by selecting **Clients Statistics** under the field of **Status** in the menu bar, as shown in Figure .

The Address Lease Table shows the ***Client MAC Address***, ***Client IP Address*** of each end user.

Figure 34 2.4GHz Radio Statistics Menu

5.3 RADIO ASSOCIATION-AP MODE

The each radio association statistics can be monitored by selecting **Radio Association** under the field of **Status** in the menu bar, as shown in Figure . The corresponding statistics can be shown by selecting the related ***MAC Address***, as shown in Figure 36**.**

The Association Table shows the ***ID***, ***Mac Address***, ***RSSI***, and ***VAP*** of each station as shown in Figure . A more detailed 2.4GHz Association Statistic of each station can be brought up by selecting the related ***Mac Address*** as shown in Figure 38.

Status	Description
ID	Station ID, a number randomly generated by A3 to represent a mobile client
Mac Address	Station Mac Address
RSSI	Receiver Signal Strength
VAP	Virtual Access Point ID Number that the mobile client associates to

Table 6 2.4GHz Client Association Status

NOTE: The association page would be refreshed for every 15 seconds

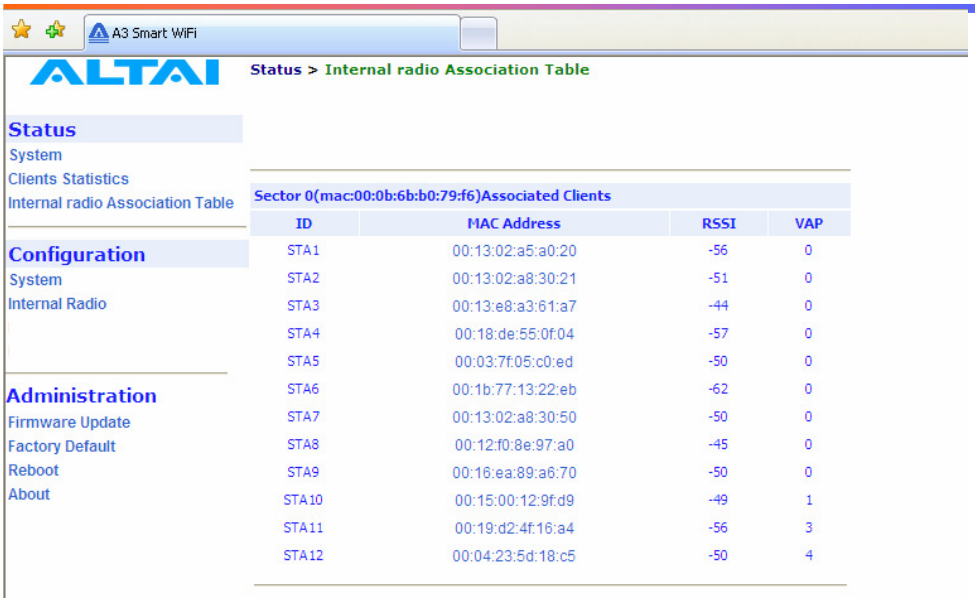


Figure 35 Radio Association Table

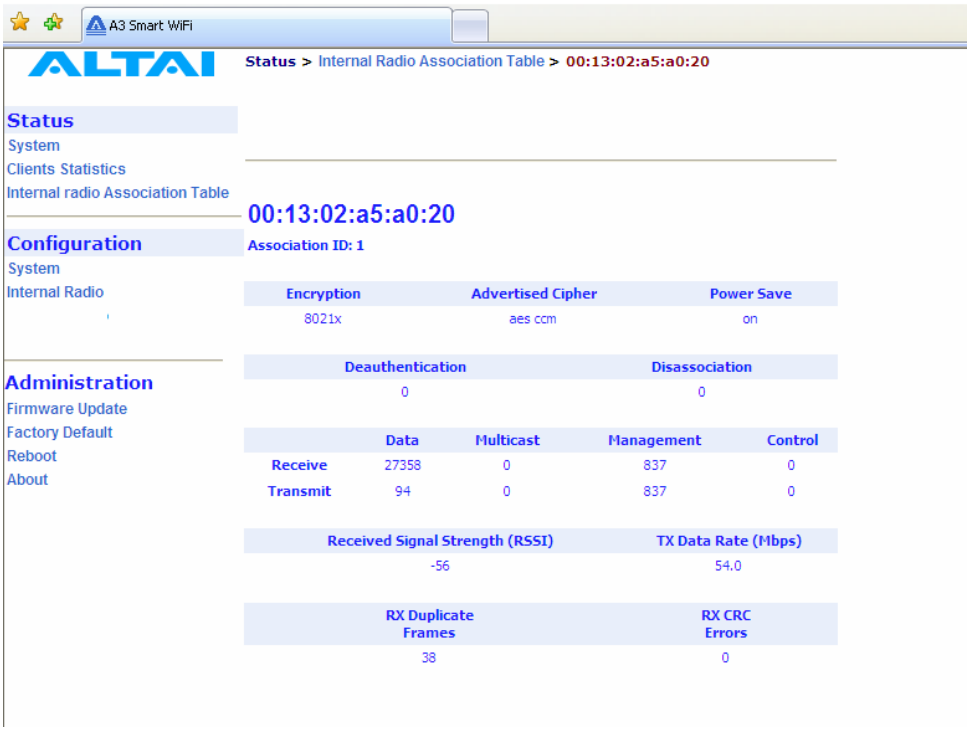


Figure 36 Radio Statistics per MAC Address (data is cumulative)

5.4 RADIO ASSOCIATION-REPEATER MODE

The association status of radio working on repeater mode can be monitored by selecting **Radio Association** under the field of **Status** in the menu bar, as shown in Figure 37 and Figure 38.

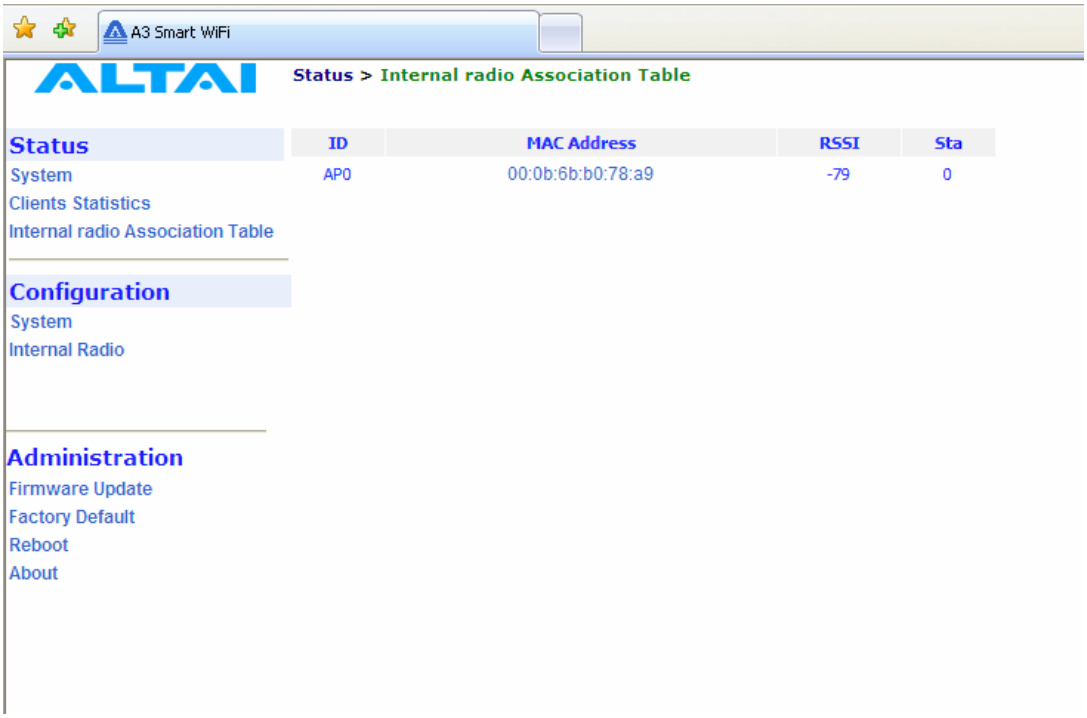


Figure 37 Radio Association AP List

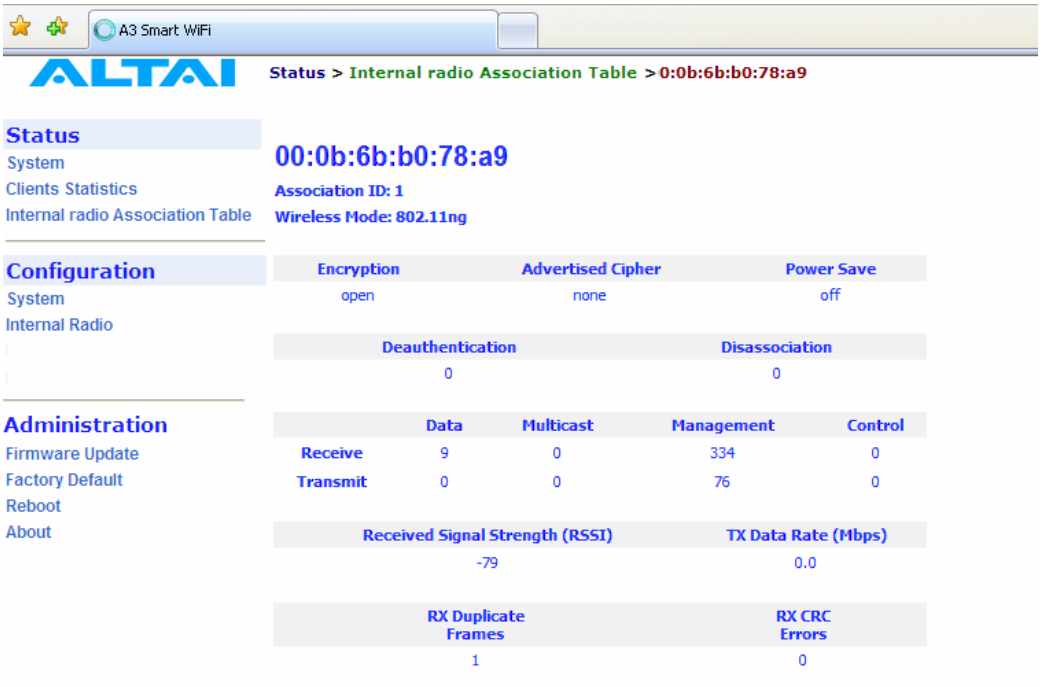


Figure 38 Association AP Statistics per MAC Address (data is cumulative)

Commercially Confidential

5.5 RADIO ASSOCIATION-BRIDGE MODE

The bridge radio association can be monitored by selecting **Radio Association** under the field of **Status** in the menu bar, as shown in Figure 39 and Figure 40.

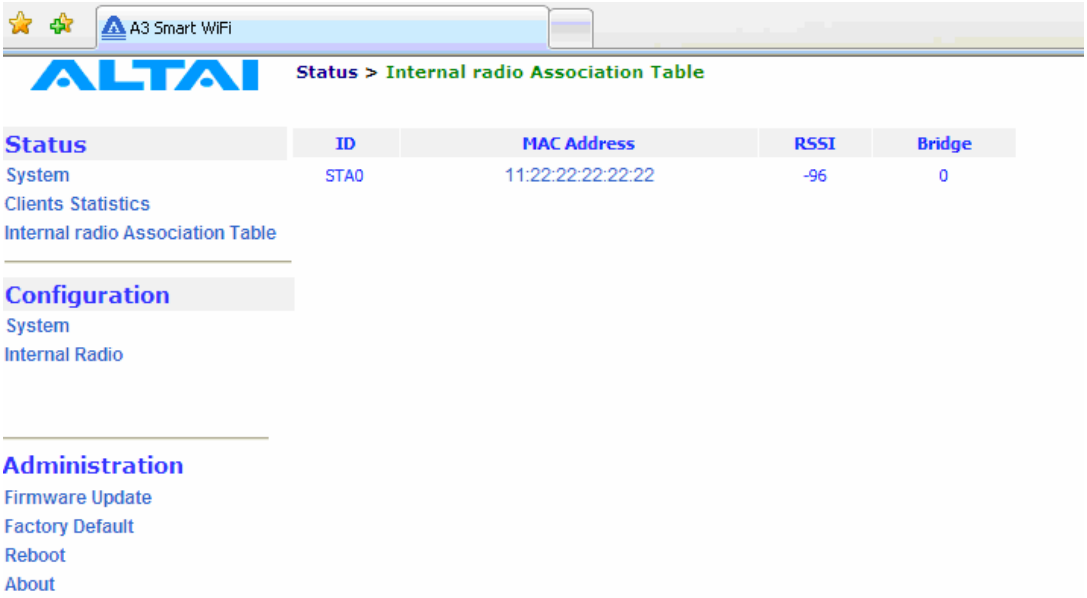


Figure 39 Radio Association Bridge List

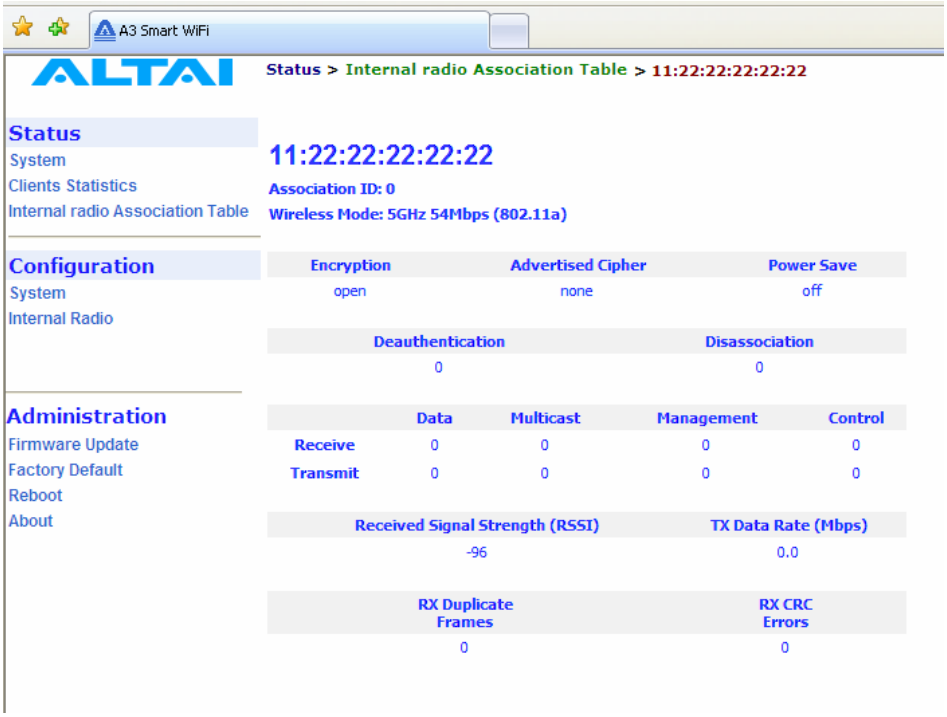


Figure 40 Bridge Association Statistics per MAC address

Commercially Confidential

6 SOFTWARE UPGRADE THROUGH WEB-ADMIN

The firmware can be upgraded by selecting **Firmware Update** under the field of **Administrations** in the menu bar respectively. Please note that the connection link should be maintained during file transfer to prevent interruption to the system.

6.1 FIRMWARE UPDATE THROUGH HTTP OR HTTPS

Follow the steps below to perform the Firmware Update with a firmware image file (.bin) in local directory through HTTP or HTTPS.

1. Click the ***Browse…*** bottom to bring up a file chooser dialog which you can specify the name and location of the firmware image you want to import.
2. Click the ***Update Firmware*** bottom to start uploading the new firmware from the local directory, see Figure .
3. If the firmware upgrade is successful, a window will appear as Figure . A3 smart WiFi will reboot automatically.
4. Type in URL with **https**://<*ip address of A3*>, note 'http' can not link to the web admin of A3 under the new firmware version.
5. After the A3 reboots, check the firmware version by selecting **About** under the field of **Administrations** in the menu bar, as discussed in Section 4.2, to ensure the expected firmware is uploaded.
6. Select **Factory Default** under the field **Administrations** in the menu bar and click **Reset to Factory Default** (**address retained**) or **Reset to Factory Default** to make the default settings effective. Note: If press **Reset to Factory Default** with **address retained**, the IP address of A3 web-admin will not be changed after rebooting the AP. While **Reset to Factory Default** is chosen, IP address of A3 smart WiFi will be changed into **192.168.1.20** .
7. Click the icon ***REBOOT AP*** to reboot the A3 smart WiFi.

Warning: The A3 smart WiFi will not be working properly if there is some mistaken in the upgrade process. You are NOT advised to perform firmware upgrade if you have not received any training from ALTAI or its partners.

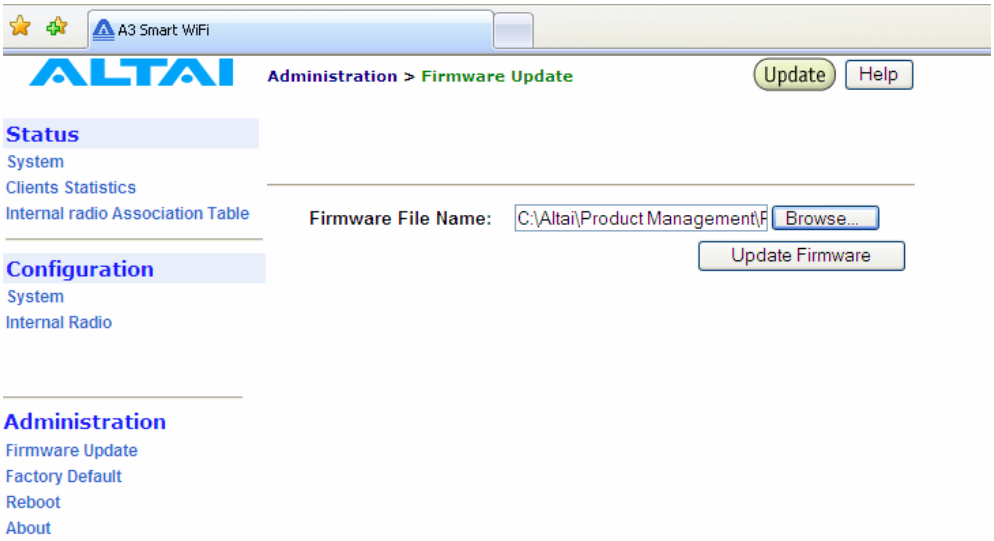


Figure 41 Upload the Firmware through HTTP or HTTPS

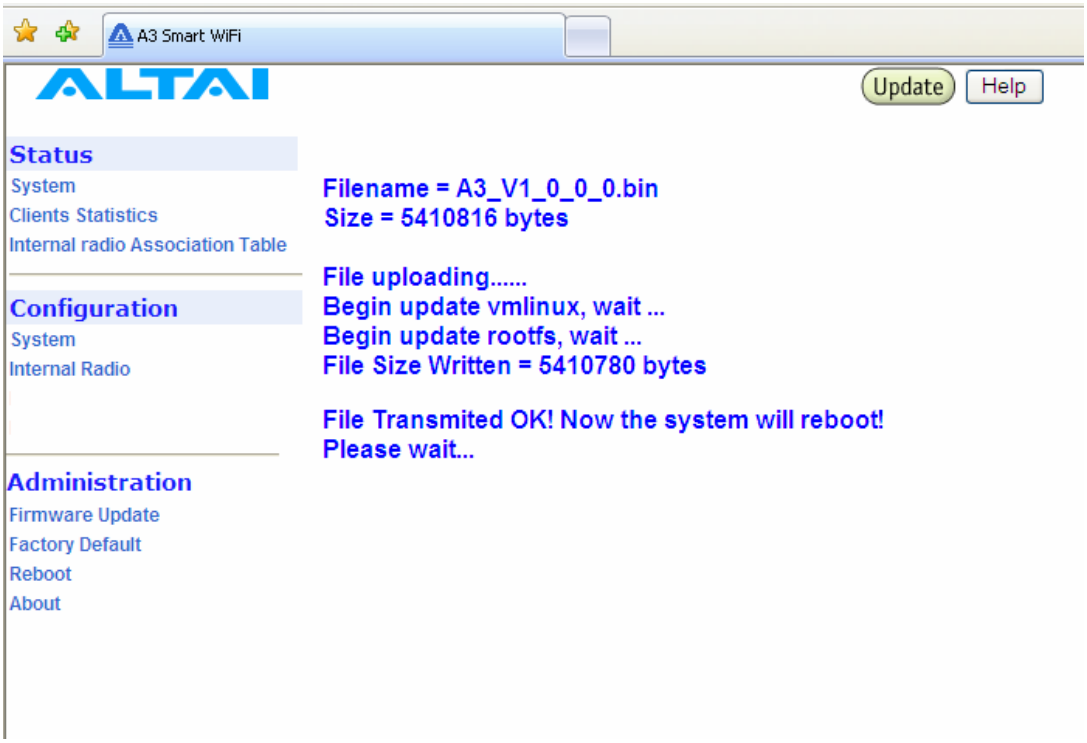


Figure 42 Successful Firmware Update – Web-admin

Commercially Confidential

7 GLOSSARY

802.1q IEEE 802.1Q was a project in the IEEE 802 standards process to develop a mechanism to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e. trunking). IEEE 802.1Q is also the name of the standard issued by this process, and in common usage the name of the encapsulation protocol used to implement this mechanism over Ethernet networks. This protocol allows for individual VLANs to communicate with one another with the use of a layer-3 (network) router.

802.11 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

802.11a 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 (OFDM) encoding scheme rather than Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum.

802.11b Also referred to as 802.11 High Rate or Wi-Fi. It is an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

802.11e A supplement to the IEEE 802.11 wireless LAN (WLAN) specification for enhancements to the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service (QoS), provide Classes of Service (CoS), and enhanced security and authentication mechanisms.

802.11g The 802.11g specification is a standard for Wireless Local Area Networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum with the earlier 802.11b standard. Networks employing 802.11g operate at radio frequencies between 2.400 GHz and 2.4835 GHz, the same band as 802.11b. But the 802.11g specification employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps. This feature makes 802.11b and 802.11g devices compatible within a single network. Modification of an 802.11b access point to 802.11g compliance usually involves only a firmware upgrade.

802.11i A supplement to the IEEE 802.11 wireless LAN (WLAN) specification for enhanced security through the use of stronger encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and AES Counter-Mode Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). These protocols provide replay protection, cryptographically keyed integrity checks, and key derivation based on the IEEE 802.1X port authentication standard.

802.11n A supplement to the previous 802.11 standards. 802.11n combines the MIMO (Multiple-input Multiple-output) and channel-bonding (40MHz) operation to physical layer and frame aggregation to the MAC layer. The current state of 802.11n supports a data rate of 300Mbit/s and the throughput can achieve at 150Mbit/s.

ACL Access Control List: It is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

ad-hoc mode An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an Access Point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required.

antenna gain The measure of an antenna assembly performance relative to a theoretical antenna, called an isotropic radiator (radiator is another term for antenna). Certain antenna designs feature higher performance relative to vectors or frequencies.

AP Access Point: A hardware unit that acts as a communication hub by linking wireless mobile 802.11 stations such as PCs to a wired backbone network. A Trapeze Networks Mobility System has Mobility Point APs.

ASCII American Standard Code for Information Interchange: An 8-bit code for representing characters, consisting of 7 data bits plus 1 parity bit.

association The relationship established between mobile (wireless) stations and a wireless AP (AP) in which the stations receive services from the AP.

bandwidth The gap between the highest and lowest frequencies employed by network signals. More commonly, it refers to the rated throughput capacity of a network protocol or medium. The frequency range necessary to convey a signal measured in units of hertz (Hz).

broadcast A data frame or packet that is transmitted to every node on the local network segment (as defined by the broadcast domain). Broadcasts are known by their broadcast address, which is a destination network and host address with all the bits turned on.

channel Communication path wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments.

dB decibels: Unit for measuring relative power ratios in terms of gain or loss. Units are expressed in terms of the logarithm to base 10 of a ratio and typically are expressed in watts. dB is not an absolute value, rather it is the measure of power lost or gained between two devices. Because antennas and other RF devices/systems commonly have power gains or losses on the orders of magnitude or even orders of four orders of magnitude, dB is a more easily used expression.

dBd decibels over Dipole: A relative gain measurement with respect to a half wave dipole (0 dBd = 2.14 dBi) using a standard dipole antenna as a reference.

dBi dBi referenced to an isotropic antenna, which theoretically is perfect in terms of symmetric patterns of radiation. Real world antennas do not perform with even nominal amounts of symmetry, but this effect generally is used to the advantage of the system designer.

dBm decibels per Milliwatt: 0 dBm is defined as 1 mw at 1 kHz of frequency at 600 ohms of impedance.

DHCP Dynamic Host Configuration Protocol: Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS Domain Name Server: System used on the Internet for translating names of network nodes into addresses.

DSSS Direct Sequence Spread Spectrum: One of two types of spread spectrum radio technology used in wireless LAN (WLAN) transmissions. To increase a data signal's resistance to interference, the signal at the sending station is combined with a higher-rate bit sequence that spreads the user data in frequency by a factor equal to the spreading ratio.

EIRP Effective Isotropic Radiated Power: Term for the expression of the performance of an antenna in a given direction relative to the performance of a theoretical (isotropic) antenna and is expressed in watts or dBW. EIRP is the sum of the power sent to the antenna plus antenna gain.

encryption The conversion of information into a scrambled form that effectively disguises it to prevent unauthorized access. Every encryption scheme uses some well-defined algorithm, which is reversed at the receiving end by an opposite algorithm in a process known as decryption.

Ethernet Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mbps. Ethernet is similar to the IEEE 802.3 series of standards.

FastRoaming™ The Trapeze Mobility System feature that quickly hands off a roaming user's credentials. Mobility Exchanges in a Trapeze Mobility Domain pass each other this vital user information to permit seamless roaming. This allows 802.1X and non-802.1X, MAC-authenticated devices, such as 802.11 phones, to roam quickly between Mobility Exchanges.

FCC Federal Communications Commission: U.S. government agency that supervises, licenses, and controls electronic and electromagnetic transmission standards. The FCC Rules in Title 47 of the Code of Federal Regulations govern telecommunications in the United States. Wireless LANs must comply with Part 15 of the FCC rules, which are written specifically for RF devices.

firmware Software instructions set permanently or semipermanently in ROM.

FHSS Frequency Hopping Spread Spectrum: One of two types of spread spectrum radio technology used in wireless LAN (WLAN) transmissions. The FHSS technique modulates the data signal with a narrowband carrier signal that “hops” in a predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. Interference is reduced, because a narrowband interferer affects the spread spectrum signal only if both are transmitting at the same frequency at the same time. The transmission frequencies are determined by a spreading (hopping) code. The receiver must be set to the same hopping code and must listen to the incoming signal at the proper time and frequency to receive the signal.

FPGA Field Programmable Gate Array: An FPGA is a specially made digital semiconductor often used for prototyping. With an FPGA, a design engineer is able to program electrical connections on site for a specific application, without paying thousands of dollars to have the chip manufactured in mass quantities.

FTP File Transfer Protocol: Defined in RFC 959, it is a Application protocol that is part of the TCP/IP protocol stack, used for transferring files between network nodes.

gateway In the IP community, an older term referring to a routing device. Today, the term router is used to describe nodes that perform this function, and gateway refers to a

special-purpose device that performs an application-layer conversion of information from one protocol stack to another.

handoff The process of transferring the handling of that cellular call to the new base station.

host address Logical address configured by an administrator or server on a device. Logically identifies this device on an internetwork.

https Hypertext Transfer Protocol over Secure Sockets Layer: An Internet protocol developed by Netscape to encrypt and decrypt network connections to web servers. Built into all secure browsers, HTTPS uses the Secure Sockets Layer (SSL) protocol as a sublayer under the regular HTTP application layer, and uses port 443 instead of HTTP Port 80 in its interactions with the lower layer, TCP/IP.

ICMP Internet Control Message Protocol: Defined in RFC 792, it is a Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

IEEE Institute of Electrical and Electronic Engineers: An American professional society whose standards for the computer and electronics industry often become national or international standards. In particular, the IEEE 802 standards for LANs are widely followed.

infrastructure network In an infrastructure network, all communications are relayed through an AP (AP). Wireless devices can communicate with each other or with a wired network. The network is defined by the distance of mobile stations from the AP, but no restriction is placed on the distance between stations. Stations must request association with the AP to obtain network services, which the AP can grant or deny based on the contents of the association request. Like most corporate wireless LANs (WLANs), which must access a wired LAN for file servers and printers, Trapeze Networks Mobility System is an infrastructure network.

IP Internet Protocol: Defined in RFC 791, it is a Network Layer protocol that is part of the TCP/IP stack and allows connectionless service. IP furnishes an array of features for addressing, type-of-service specification, fragmentation and reassembly, and security.

IP address Often called an “Internet address”, this is an address uniquely identifying any device (host) on the Internet (or any TCP/IP network). Each address consists of four octets (32 bits), represented as decimal numbers separated by periods (a format known as “dotted-decimal”). Every address is made up of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number addresses an individual host within the network or subnetwork. The network and subnetwork information is extracted from the IP address by using the subnet mask. There are five classes of IP addresses (A-E), which allocate different numbers of bits to the network, subnetwork, and host portions of the address.

LOS Line Of Sight: Refers to the fact that there must be a clear, unobstructed path between the transmitters and receivers. This is essential for our LMDS products and enhances general performance in every RF deployment as opposed to partial or completely obstructed data paths. The opposite to LOS is NLOS, or Non Line Of Sight.

MAC address Media Access Control address: A Data Link Layer hardware address that every port or device needs to connect to a LAN segment. These addresses are used by various devices in the network for accurate location of logical addresses. MAC addresses are defined by the IEEE standard, and their length is six characters, typically using the burned-in address

(BIA) of the local LAN interface. Variously called “hardware address”, “physical address”, “burned-in address” or “MAC-layer address”.

MTU Maximum Transmission Unit: The largest packet size, measured in bytes, that an interface can handle.

NAT Network Address Translation: An algorithm instrumental in minimizing the requirement for globally unique IP addresses, permitting an organization whose addresses are not all globally unique to connect to the Internet, regardless, by translating those addresses into globally routable address space.

NLOS Non Line Of Sight. Also known as obstructed path or pathway.

noise Undesirable communications channel signals.

NTP Network Time Protocol: Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

OFDM Orthogonal Frequency Division Multiplexing: A technique that splits a wide frequency band into a number of narrow frequency bands and sends data across the subchannels. The wireless networking standards 802.11a and 802.11g are based on OFDM.

open system authentication The sender and the recipient do not share a secret key. Each party generates its own key-pair and asks the receiver to accept the (usually randomly) generated key. Once accepted, this key is used for a short time only, then a new key is generated and agreed upon. So, it is a two-step authentication method, in which sender first sends its identity and in response of that it gets the authentication results.

ping Packet Internet Groper: ICMP echo message and its reply. Often used in IP networks to test the reach ability of a network device.

PoE Power over Ethernet: A technology, defined in the developing IEEE 802.3af standard, to deliver dc power over twisted-pair Ethernet data cables rather than power cords. The electrical current, which enters the data cable at the power-supply end and comes out at the device end, is kept separate from the data signal so neither interferes with the other.

Remote Bridge A bridge located on a network system separate from the host system.

RF Radio Frequency: Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

RFC Request For Comments: Document series used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.

shared key authentication Shared key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. Shared key authentication accomplishes this with the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. The

required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. During the shared key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

SNMP Simple Network Management Protocol: SNMP forms part of the Internet Protocol suite, as defined by the Internet Engineering Task Force (IETF). It is a Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP2 Simple Network Management Protocol Version 2: Version 2 of the popular network management protocol. SNMP2 supports centralized as well as distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.

SSID Service Set Identifier: A 32-character (maximum) unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the Basic Service Set.

STP Spanning-Tree Protocol: Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.

subnet mask A 32-bit address mask used in IP to identify the bits of an IP address that are used for the subnet address. Using a mask, the router does not need to examine all 32 bits, only those selected by the mask.

telnet The standard terminal emulation protocol within the TCP/IP protocol stack. Defined in RFC 854, it is a method of remote terminal connection, enabling users to log in to remote networks and use those resources as if they were locally connected.

throughput Rate of information arriving at, and possibly passing through, a particular point in a network system.

VAP Virtual Access Point: It is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present.

VLAN Virtual LAN: Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN tag It works by tagging each frame, i.e. an Ethernet header extension that enlarges the header from 14 to 18 bytes. The VLAN tag contains the VLAN ID and priority.

WEP 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. LANs are inherently more secure than WLANs because LANs are somewhat protected by the physicalities of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which are over radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

Wi-Fi Wireless Fidelity: Wi-Fi is a label for devices conforming to the IEEE 802.11b standard for WLAN. The IEEE 802.11b standard has been published by the IEEE, which does not perform conformance testing. In order to establish such a conformance testing process, the Wi-Fi Alliance (formerly known as WECA) has been formed, which tests devices for conformance with the IEEE 802.11b standard and issues the Wi-Fi label for conforming devices.

WME Wireless Multimedia Extensions: Also known as Wi-Fi Multimedia (WMM), it is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

WPA Wi-Fi Protected Access: WPA was created by the Wi-Fi Alliance in 2002, in part out of impatience with the slow-moving IEEE 802.11i standard. The industry consortium's consensus was that an alternative to WEP was needed quickly, and WPA was the result. To avoid multiple standards and conflicts later on, WPA was designed from the get-go to be compatible with IEEE 802.11i and was based on its early draft specifications.