



802.11a/n High Power Wireless Outdoor Bridge / AP

User Manual *WLO-15814N / WLO-15802N*

V2.0.3



Table of Contents

| | |
|---|-----------|
| Chapter 1. System Overview | 1 |
| 1.1 Introduction of WLO-15814N / WLO-15802N..... | 1 |
| 1.2 System Concept..... | 2 |
| 1.3 Applications in Wireless Network | 3 |
| 1.4 Product Benefit | 7 |
| 1.5 Specification..... | 8 |
| Chapter 2. Basic Installation | 12 |
| 2.1 Hardware Installation | 12 |
| 2.1.1 Package Contents..... | 12 |
| 2.1.2 Panel Function Descriptions | 12 |
| 2.1.3 Hardware Installation Steps | 13 |
| 2.2 Web Management Interface Instructions..... | 14 |
| Chapter 3. AP Mode Configuration | 16 |
| 3.1 External Network Connection..... | 16 |
| 3.1.1 Network Requirement | 16 |
| 3.1.2 Configure LAN IP | 17 |
| 3.2 Wireless LAN Network Creation..... | 19 |
| 3.2.1 Wireless General Setup | 19 |
| 3.2.2 Wireless Advanced Setup | 21 |
| 3.2.3 Create Virtual AP (VAP) | 27 |
| 3.2.3.1 Virtual AP Overview | |
| 3.2.3.2 Virtual AP Setup..... | |
| 3.2.4 Wireless MAC Filter Setup..... | 32 |
| 3.3 Wireless Network Expansion | 33 |
| 3.4 System Management | 34 |
| 3.4.1 Configure Management | 34 |
| 3.4.2 Configure System Time..... | 37 |
| 3.4.3 Configure SNMP Setup..... | 38 |
| 3.4.4 Backup / Restore and Reset to Factory | 40 |
| 3.4.5 Firmware Upgrade | 41 |
| 3.4.6 Network Utility..... | 42 |
| 3.4.7 Reboot | 43 |
| 3.5 System Status | 44 |
| 3.5.1 System Overview | 44 |
| 3.5.2 Associated Clients Status..... | 46 |
| 3.5.3 Show WDS Link Status | 47 |
| 3.5.4 Extra Information..... | 48 |
| 3.5.5 Event Log..... | 50 |
| Chapter 4. WDS Mode Configuration | 51 |
| 4.1 External Network Connection..... | 51 |
| 4.1.1 Network Requirement | 51 |
| 4.1.2 Configure LAN IP | 52 |
| 4.2 Wireless Network Expansion | 53 |
| 4.2.1 General Setup..... | 53 |
| 4.2.2 Wireless Advanced Setup | 55 |
| 4.2.3 WDS Setup | 61 |
| 4.3 System Management | 62 |
| 4.3.1 Configure Management | 62 |
| 4.3.2 Configure System Time..... | 65 |
| 4.3.3 Configure SNMP Setup..... | 66 |
| 4.3.4 Backup / Restore and Reset to Factory | 68 |
| 4.3.5 Firmware Upgrade | 69 |
| 4.3.6 Network Utility..... | 70 |
| 4.3.7 Reboot | 71 |

| | |
|---|------------|
| 4.4 System Status | 72 |
| 4.4.1 System Overview | 72 |
| 4.4.2 WDS List | 74 |
| 4.4.3 Extra Information | 75 |
| 4.4.4 Event Log | 77 |
| Chapter 5. CPE Mode Configuration | 78 |
| 5.1 External Network Connection | 78 |
| 5.1.1 Network Requirement | 78 |
| 5.1.2 Configure WAN Setup | 79 |
| 5.1.3 Configure DDNS Setup | 82 |
| 5.1.4 Configure LAN Setup | 83 |
| 5.2 Access Point Association | 84 |
| 5.2.1 Configure Wireless General Setting | 84 |
| 5.2.2 Configure Wireless Advanced Setting | 86 |
| 5.2.3 Site Survey | 87 |
| 5.2.4 Create Wireless Profile | 88 |
| 5.3 System Management | 90 |
| 5.3.1 Configure Management | 90 |
| 5.3.2 Configure System Time | 93 |
| 5.3.3 Configure UPnP | 94 |
| 5.3.4 Configure SNMP Setup | 95 |
| 5.3.5 Backup / Restore and Reset to Factory | 97 |
| 5.3.6 Firmware Upgrade | 98 |
| 5.3.7 Network Utility | 99 |
| 5.3.8 Reboot | 100 |
| 5.4 Access Control List | 101 |
| 5.4.1 IP Filter Setup | 101 |
| 5.4.2 MAC Filter Setup | 103 |
| 5.4.3 Parental Control Setup | 104 |
| 5.4.4 QoS Setup | 106 |
| 5.5 Resource Sharing | 109 |
| 5.5.1 DMZ | 109 |
| 5.5.2 Virtual Server (Port Forwarding) | 110 |
| 5.6 System Status | 112 |
| 5.6.1 Overview | 112 |
| 5.6.2 Station Statistics | 115 |
| 5.6.3 Extra Info | 117 |
| 5.6.4 QoS Plot | 119 |
| 5.6.5 Event Log | 120 |
| Chapter 6. CPE + AP Mode Configuration | 121 |
| 6.1 External Network Connection | 121 |
| 6.1.1 Network Requirement | 121 |
| 6.1.2 Configure WAN Setup | 122 |
| 6.1.3 Configure DDNS Setup | 125 |
| 6.1.4 Configure LAN Setup | 126 |
| 6.2 Access Point Association | 127 |
| 6.2.1 Configure Wireless General Setting | 127 |
| 6.2.2 Wireless Advanced Setup | 129 |
| 6.2.3 Site Survey | 135 |
| 6.2.4 Create Wireless Profile | 136 |
| 6.3 Wireless LAN Network Creation | 138 |
| 6.3.1 Repeater AP Setup | 138 |
| 6.3.2 Wireless MAC Filter Setup | 142 |
| 6.4 System Management | 143 |
| 6.4.1 Configure Management | 143 |
| 6.4.2 Configure System Time | 146 |

| | |
|---|------------|
| 6.4.3 Configure UPnP | 147 |
| 6.4.4 Configure SNMP Setup..... | 148 |
| 6.4.5 Backup / Restore and Reset to Factory | 150 |
| 6.4.6 Firmware Upgrade | 151 |
| 6.4.7 Network Utility..... | 152 |
| 6.4.8 Reboot | 153 |
| 6.5 Access Control List..... | 154 |
| 6.5.1 IP Filter Setup | 154 |
| 6.5.2 MAC Filter Setup..... | 156 |
| 6.5.3 Parental Control Setup..... | 157 |
| 6.5.4 QoS Setup | 159 |
| 6.6 Resource Sharing | 162 |
| 6.6.1 DMZ..... | 162 |
| 6.6.2 Virtual Server (Port Forwarding) | 163 |
| 6.7 System Status | 165 |
| 6.7.1 Overview..... | 165 |
| 6.7.2 Associated Clients Status..... | 168 |
| 6.7.3 Remote AP | 169 |
| 6.7.4 Extra Info | 170 |
| 6.7.5 QoS Plot | 172 |
| 6.7.6 Event Log..... | 173 |
| Chapter 7. Client Bridge + Universal Repeater Configuration..... | 174 |
| 7.1 External Network Connection..... | 174 |
| 7.1.1 Network Requirement | 174 |
| 7.1.2 Configure LAN IP | 175 |
| 7.2 Access Point Association | 177 |
| 7.2.1 Configure Wireless General Setting..... | 177 |
| 7.2.2 Wireless Advanced Setup | 179 |
| 7.2.3 Site Survey | 185 |
| 7.2.4 Create Wireless Profile | 186 |
| 7.3 Wireless LAN Network Creation..... | 188 |
| 7.3.1 Repeater AP Setup | 188 |
| 7.3.2 Wireless MAC Filter Setup..... | 192 |
| 7.4 System Management | 193 |
| 7.4.1 Configure Management | 193 |
| 7.4.2 Configure System Time..... | 196 |
| 7.4.3 Configure SNMP Setup..... | 197 |
| 7.4.4 Backup / Restore and Reset to Factory | 199 |
| 7.4.5 Firmware Upgrade | 200 |
| 7.4.6 Network Utility..... | 201 |
| 7.4.7 Reboot | 202 |
| 7.5 System Status | 203 |
| 7.5.1 System Overview | 203 |
| 7.5.2 Associated Clients Status..... | 206 |
| 7.5.3 Remote AP | 207 |
| 7.5.4 Extra Information..... | 208 |
| 7.5.5 Event Log..... | 210 |
| Chapter 8. Router AP Mode Configuration..... | 211 |
| 8.1 External Network Connection..... | 211 |
| 8.1.1 Network Requirement | 211 |
| 8.1.2 Configure WAN Setup..... | 212 |
| 8.1.3 Configure DDNS Setup..... | 215 |
| 8.1.4 Configure LAN Setup | 216 |
| 8.2 Wireless LAN Network Creation..... | 217 |
| 8.2.1 Wireless General Setup..... | 217 |
| 8.2.2 Wireless Advanced Setup | 219 |

| | |
|--|------------|
| 8.2.3 Create Virtual AP (VAP) | 225 |
| 8.2.3.1 Virtual AP Overview | 2 |
| 8.2.3.2 Virtual AP Setup..... | 2 |
| 8.2.4 Wireless MAC Filter Setup | 230 |
| 8.3 Wireless Network Expansion | 231 |
| 8.4 System Management | 232 |
| 8.4.1 Configure Management | 232 |
| 8.4.2 Configure System Time..... | 235 |
| 8.4.3 Configure UPnP | 236 |
| 8.4.4 Configure SNMP Setup..... | 237 |
| 8.4.5 Backup / Restore and Reset to Factory | 239 |
| 8.4.6 Firmware Upgrade | 240 |
| 8.4.7 Network Utility | 241 |
| 8.4.8 Reboot | 242 |
| 8.5 Access Control List..... | 243 |
| 8.5.1 IP Filter Setup | 243 |
| 8.5.2 MAC Filter Setup..... | 245 |
| 8.5.3 Parental Control Setup..... | 246 |
| 8.5.4 QoS Setup | 248 |
| 8.6 Resource Sharing | 251 |
| 8.6.1 DMZ | 251 |
| 8.6.2 Virtual Server (Port Forwarding) | 252 |
| 8.7 System Status | 254 |
| 8.7.1 Overview | 254 |
| 8.7.2 Associated Clients Status..... | 257 |
| 8.7.3 Show WDS Link Status | 258 |
| 8.7.4 Extra Info | 259 |
| 8.7.5 QoS Plot | 261 |
| 8.7.6 Event Log..... | 262 |
| Appendix A. Windows TCP/IP Settings..... | 263 |
| Appendix B. WEB GUI Valid Characters | 265 |
| Appendix C. MCS Data Rate..... | 268 |
| Appendix D. System Manager Privileges..... | 269 |
| Appendix E. Enabling UPnP in Windows XP | 270 |

PheeNet outdoor high power WiFi-N Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. PheeNet outdoor CPE/AP utilizes a 500mW output Tx Power connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

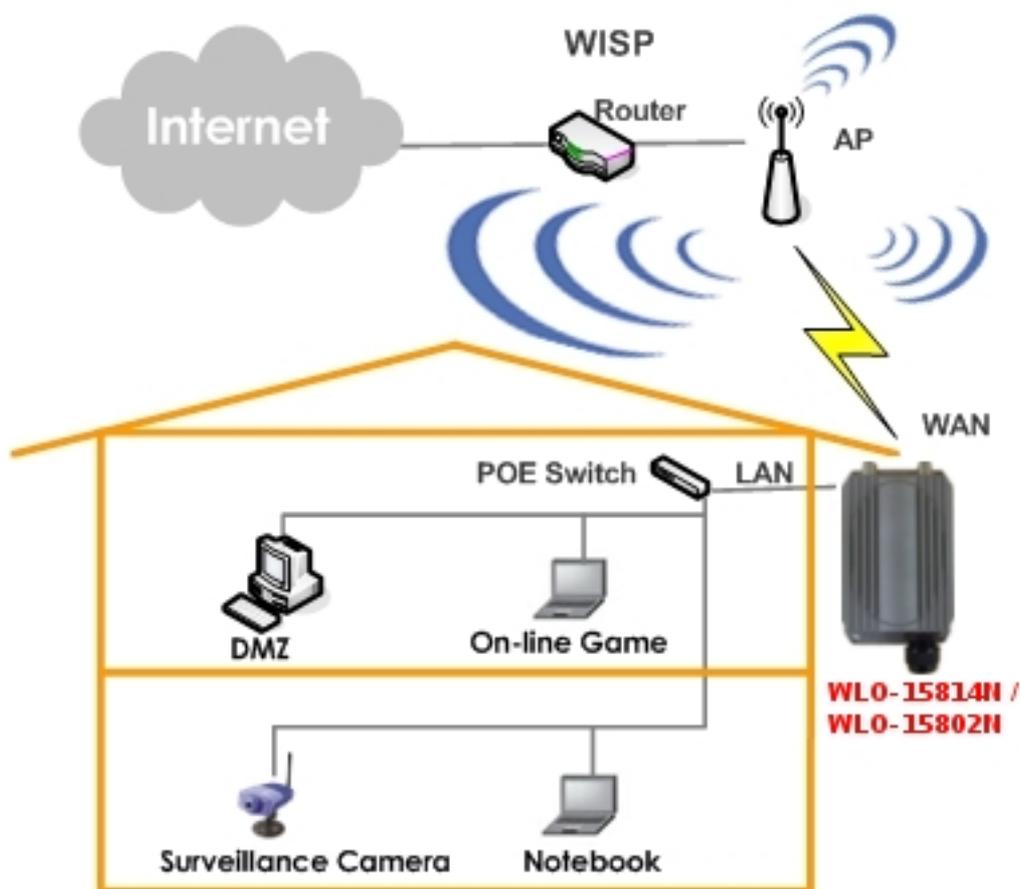
PheeNet outdoor high power Bridge can be used for nine different purposes in six different modes. In the Router AP mode, it can be deployed as a gateway with wireless Access Point(AP) and provides WDS link for network extension. In the AP mode, it can be deployed either as traditional fixed wireless Access Point, or combination of AP and WDS(AP+WDS). In the WDS mode, it's only used to expand or bridge Ethernet networks and deployed as a main base, relay based or remote base station. In the CPE mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless WAN gateway to access Internet. In the Client Bridge + Universal Repeater mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless or wired bridge to access to Internet. In the CPE + AP mode, it connects to Wireless Internet Service Provider's(WISP) outdoor network via wireless WAN gateway to access Internet, and it also can provide wireless clients associated via Access Point.

1. Router AP+WDS : It can be deployed as a gateway with wireless Access Point and provides WDS link for network extension.
2. Access Point : It can be deployed as a traditional fixed wireless Access Point
3. Repeater : To expand wireless service by repeating prior AP
4. WDS : It can be used to expand Ethernet network via wireless WDS Link
5. AP+WDS : Not only to extend Ethernet network, but also provide wireless access to the expanded network
6. CPE (Customer Premises Equipment) : It is a wireless gateway with NAT and DHCP Server functions to connects to Wireless Internet Service Provider's (WISP)
7. Client Bridge + Universal Repeater : It is a wireless repeater or bridge to connects to Wireless Internet Service Provider's (WISP)
8. CPE+AP: It is a wireless repeater or gateway with NAT and DHCP Server functions to connects to Wireless Internet Service Provider's (ISP)

1.2 System Concept

The WLO-15814N / WLO-15802N is not only designed and used as traditional outdoor AP, but also with rich features tailored for WISP applications. The two-level management capability and access control ease WISP and owners to maintain and manage wireless network in a more controllable fashion. Main applications are listed as follows with illustration:

- Wireless CPE for Multi Dwelling Unit/Multi Tenant Unit(MDU/MTU) complexes including apartments, dormitories, and office complexes.
- Outdoor Access Point for school campuses, enterprise campuses, or manufacture plants.
- Indoor Access Point for hotels, factories, or warehouses where industrial grade devices are preferred.
- Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
- Wireless coverage for indoor and outdoor grounds in private resorts, home yards, or gulf course communities.



1.3 Applications in Wireless Network

WLO-15814N / WLO-15802N is a multiple mode system which can be configured either as a wireless gateway or an access point as desired. It also can be used as a WDS link for Ethernet network expansion. This section depicts different applications on **Router AP Mode**, **AP Mode**, **WDS Mode**, **CPE Mode**, **Client Bridge + Universal Repeater Mode** and **CPE + AP Mode**.



■ Configuration on Router AP Mode (Gateway + Access Point + WDS)

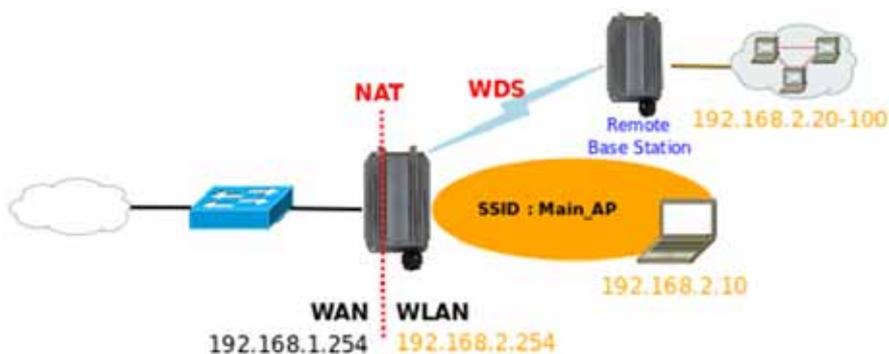
→ Example 1 : Router AP without WDS

- ✓ It can be deployed as a gateway with wireless Access Point



→ Example 2 : Router AP with WDS

- ✓ It can be deployed as a gateway with wireless Access Point and provides WDS link for network extension.



■ Configuration in AP Mode (including Access Point + WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly.

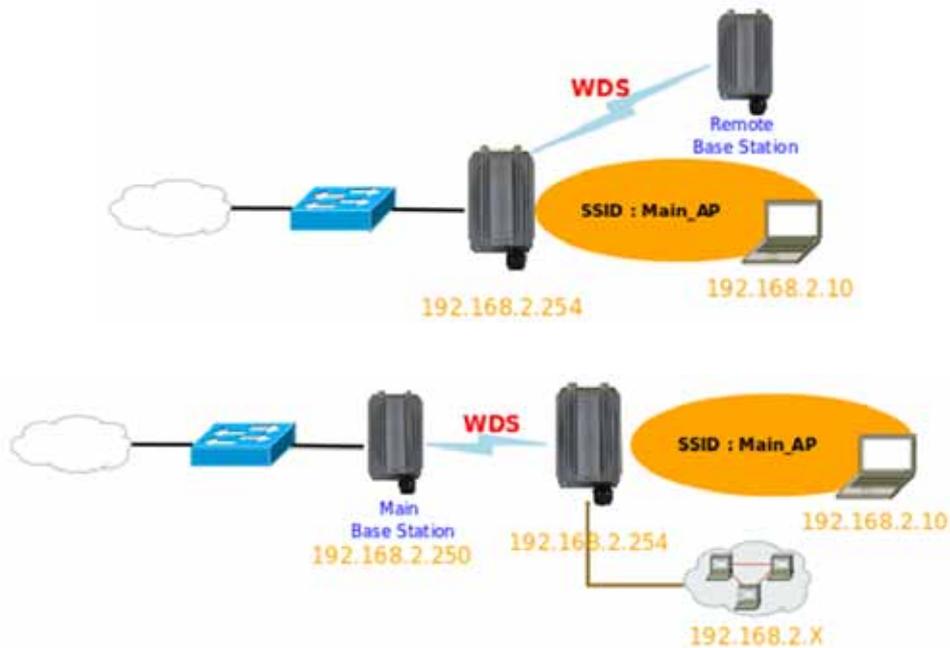
→ Example 1 : Access Point without WDS

- ✓ It can be deployed as a tradition fixed wireless Access Point



→ Example 2 : Access Point with WDS

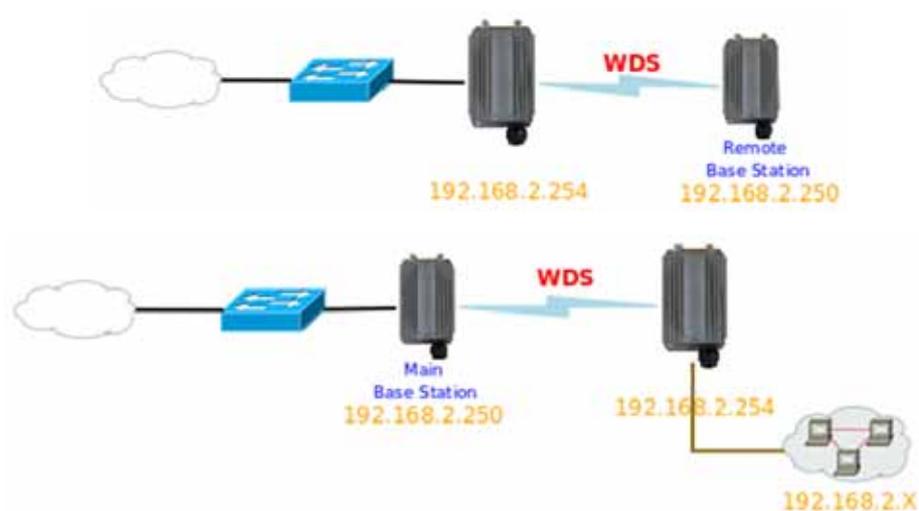
- ✓ It can be deployed as a tradition fixed wireless Access Point and provides WDS link to expand network



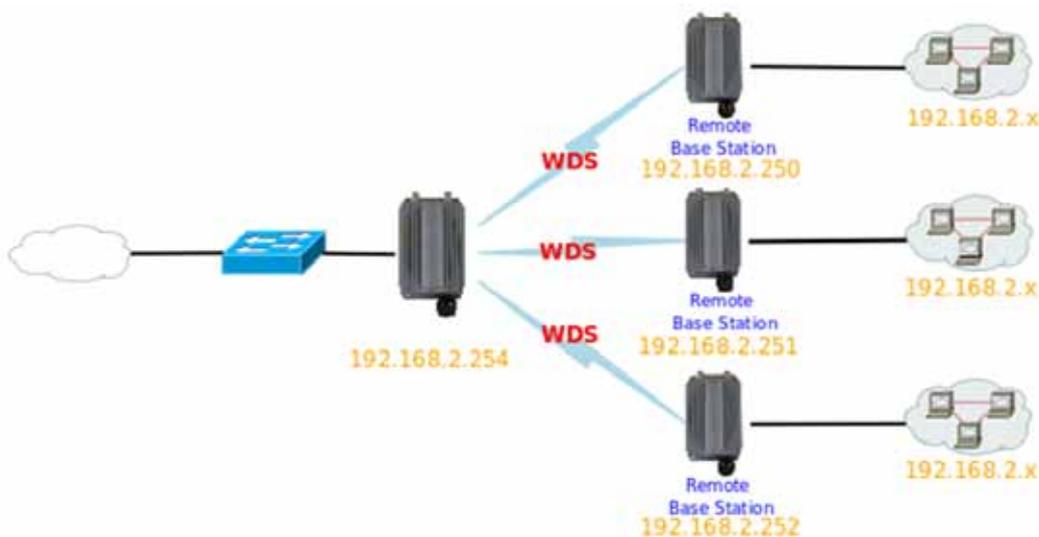
■ Configuration in WDS Mode (Pure WDS)

An access point can be either a main, relay or remote base station. A main base station is typically connected to a wired network via the Ethernet port. A relay base station relays data between main base stations and relay stations or remote base stations with clients. A remote base station is the end point to accept connections from wireless clients and pass data upwards to a network wirelessly. In this mode, it can support single or multiple WDS links and no wireless clients **can** associate with it.

→ Example 1 : Point-to-Point



→ Example 2 : Point-to-Multi-Point

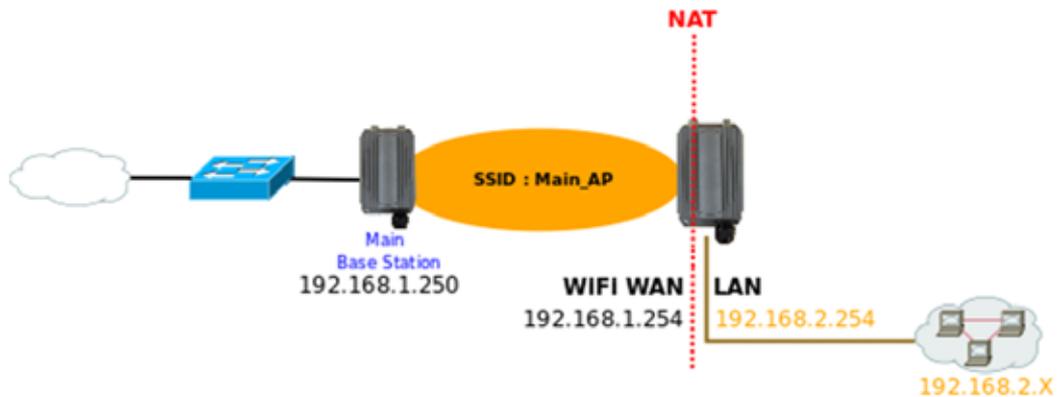


→ Example 3 : Multi-Point Repeating bridge



■ Configuration in CPE Mode

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, WLO-15814N / WLO-15802N is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to WLO-15814N / WLO-15802N are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.



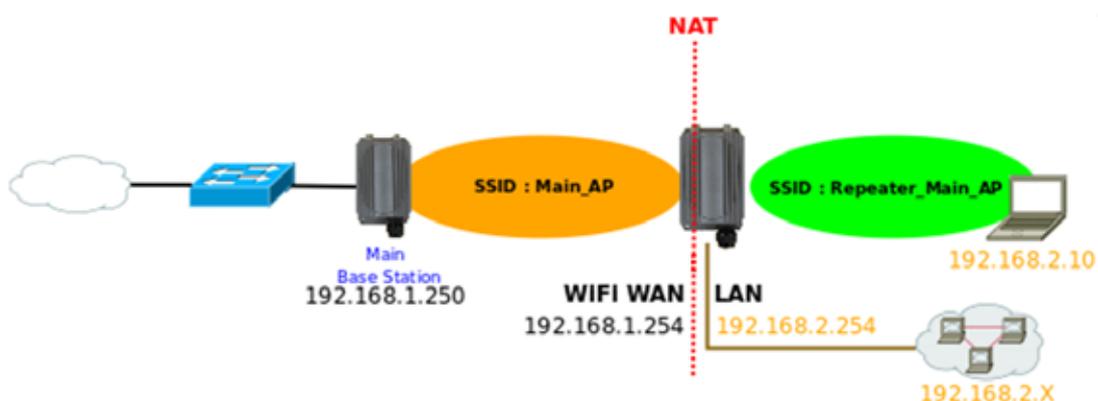
■ Configuration in Client Bridge + Universal Repeater Mode

It can be used as an Client Bridge + Universal Repeater to receive wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, WLO-15814N / WLO-15802N is enabled with DHCP Server functions. The wired clients of WLO-15814N / WLO-15802N are in **the same subnet** from Main Base Station and it **accepts** wireless connections from client devices.



■ Configuration on CPE + AP Mode (Router Client + Access Point)

It can be used as an Outdoor Customer Premised Equipment(CPE) to receive wireless signal over the last mile, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, the WLO-15814N / WLO-15802N is a gateway with NAT and DHCP Server functions. The wireless and wired clients of WLO-15814N / WLO-15802N are on the **different subnet** from Main Base Station and it **accepts** wireless connections from client devices.



- IEEE 802.11n Draft 2.0 Compliance in 2Tx / 2Rx Design
- Support IEEE 802.11n and 802.11a
- Operates in the 5GHz ISM Band
- Enables Bandwidth of up to 300Mbps(Tx), 300Mbps(Rx) link rate
- Topology : Point to Point ; Point to Multi Point
 - Router AP Mode
 - Access Point Mode : Pure Access Point Function and Access Point /Bridge(WDS) Function
 - WDS Mode
 - CPE Mode (Router Client)
 - Client Bridge + Universal Repeater
 - CPE + AP Mode
- Security with 802.1X, WPA, and WPA2
- Support QoS(Quality of Service) & WMM
- Integrated Power over Ethernet (PoE)
- Multiple Virtual AP & Capability of Client Isolation
- Business-class WLAN Security and Client Authentications
- Provide Advanced Wireless Setting
- Support Web Management and SNMP MIB II
- Over Load Current Protection
- Client Isolation Through Layer 2 VLAN Technology
- Two administrator accounts for manager authorities
- QoS for bandwidth management and traffic prioritization

WLO-15814N / WLO-15802N outdoor high power WiFi-A/N Bridge is the point of connection to Wireless Outdoor Network for service provider deploying last mile services to business or residential broadband subscribers.. Network administrators can create multiple subscriber service tier using per-subscriber rate limiting features, and manage centrally. WLO-15814N / WLO-15802N outdoor bridge utilizes a 500mW output Tx Power to connect to the WiFi mesh or WDS infrastructure and provides the subscriber with an Ethernet connection for a local access.

WLO-15814N / WLO-15802N outdoor high power Bridge can be used for nine different purposes in six different modes, the Router AP mode , AP mode, the WDS mode, the CPE mode, Client Bridge + Universal Repeater mode and CPE + AP mode, respectively with built-in remote management features.

1.5 Specification

■ Wireless Architecture Mode

→ Router AP Mode

- ✓ Wire connection as WAN , in this mode , the device run as DHCP server to assign IP address to wireless clients out of a private IP address pool behind a NAT
- ✓ This enables the wireless interconnection of Access Point in an IEEE802.11 network .and accept wireless clients at the same time

→ AP Mode

✓ Pure AP Mode

- It can be deployed as a tradition fixed wireless Access Point
- It allow wireless clients or Stations(STA) to access

✓ AP/WDS Mode

- This enables the wireless interconnection of Access Point in an IEEE802.11 network .and accept wireless clients at the same time

→ WDS Mode

- ✓ This enables the wireless interconnection of Access Point in an IEEE802.11 network.
- ✓ It allows a wireless network to be expanded using multiple access point without the need for a wired backbone to link them.
- ✓ This also be referred to as repeater mode.
- ✓ It can't allow wireless clients or Stations (STA) to associate.

→ CPE Mode

- ✓ WiFi connection as WAN , in CPE mode , the device run as DHCP server to assign IP address to wire clients out of a private IP address pool behind a NAT

→ Client Bridge(CB) + Universal Repeater(UR) Mode

- ✓ A wireless repeater and bridge with DHCP server enabled, clients on the same subnet as host AP(Primary Router).

→ CPE + AP Mode

- ✓ WiFi connection as WAN , in this mode , the device run as DHCP server to assign IP address to wire and wireless clients out of a private IP address pool behind a NAT

■ Networking

- Support Static IP, Dynamic IP(DHCP Client), PPPoE and PPTP on WAN Connection
- Support MPPE-64 and MPPE-128 Encryption on PPTP Connection
- Support PPTP/L2TP/IP Sec Pass Through
- PPPoE and PPTP Reconnect – Always On , On demand, Manual
- MAC Cloning

- DHCP Server in Router AP , CPE/CPE + AP and Client Bridge + Universal Repeater Mode
- 802.3 Bridging
- Masquerading (NAT)
- Proxy DNS
- Dynamic DNS
- NTP Client
- Virtual DMZ
- Virtual Server (IP/ Port Forwarding)
- Support MAC Filter
- Support IP Filter
- Bandwidth traffic Shaping

■ Wireless Feature

- Transmission power control : 1~100 %
- Channel selection : Manual or Auto
- No of associated clients per AP : 32
- Setting for max no associated clients : Yes
- No. of ESSID (Virtual AP) : 7
- No. of Max. WDS setting : 4
- Preamble setting : Short/ Long
- Setting for 802.11a/n mix or 802.11a only
- Setting for transmission speed
- Dynamic Wireless re-transmission
- IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- IEEE 802.11i Preauth (PMKSA Cache)
- IEEE 802.11h - TPC(Transmission Power Control) and DFS(Dynamic Frequency Select)
- IEEE 802.11d -Multi country roaming
- Wireless Site Survey
- Channel Bandwidth setting : 20MHz or 20/40MHz
- HT Tx/Rx Stream selection : 1 or 2
- A-MSDU and A-MPDU support
- Maximal MPDU density for TX aggregation setting
- Short Slot support
- Slot time and ACK Timeout support
- RTS Threshold and Fragment Threshold support

■ Authentication/ Encryption (Wireless Security)

- Layer 2 User Isolation and AP Isolation
- Blocks client to client discovery within a specified VLAN
- WEP 64/ 128 Bits
- EAP-TLS + Dynamic WEP
- EAP-TTLS + Dynamic WEP
- PEAP/ MS-PEAP+Dynamic WEP
- WPA (PSK +TKIP)
- WPA (802.1x certification + TKIP)
- 802.11i WPA2 (PSK + CCMP/ AES)
- 802.11i WPA2 (802.1x certification + CCMP/ AES)
- Setting for TKIP/ CCMP/ AES key's refreshing period
- Hidden ESSID support
- Setting for "Deny ANY " connection request
- MAC Address filtering (MAC ACL)
- No. of registered RADIUS servers : 1
- VLAN assignment on ESSID
- Support WEP, AES and TKIP data encryption over WDS link

■ Quality of Service

- Download and Upload traffic control
- Packet classifications via DSCP (Differentiated Services Code Point)
- Control Policy by IP/IP Range/ MAC Group/ Port/ Layer-7 Protocol
- Traffic Analysis and Statistics
- No. of Max. Policy setting : 10
- DiffServ/ ToS
- IEEE802.1p/ CoS
- IEEE 802.1Q Tag VLAN priority control
- IEEE802.11e WMM

■ Parental Control

- Blocking Control Policy by IP Range/ MAC Group/ Port/ Layer-7 Protocol
- URL Blocking

■ System Administration

- Intuitive Web Management Interface
- Password Protected Access
- Firmware upgrade via Web
- Reset to Factory Defaults
- Profiles Configuration Backup and Restore
- One-button-click to reset factory default
- Two administrator accounts
- Remote Link Test – Display connect statistics
- Full Statistics and Status Reporting
- Real time QoS Flow Plot
- NTP Time Synchronization
- Even Log
- Support SNMP v1, v2c, v3
- SNMP Traps to a list of IP Address
- Support MIB II
- CLI access via Telnet and SSH
- Administrative Access : HTTP and HTTPS
- UPnP (Universal Plug and Play)
- Ping Watchdog

Chapter 2. Basic Installation

2.1 Hardware Installation

2.1.1 Package Contents

The standard package contents of WLO-15814N / WLO-15802N :

| | |
|-------------------------------------|-----|
| ■ WLO-15814N / WLO-15802N | x 1 |
| ■ Quick Installation Guide | x 1 |
| ■ CD-ROM (with User Manual and QIG) | x 1 |
| ■ Power Adapter DC24V 0.5A | x 1 |
| ■ PoE Injector | x 1 |
| ■ Mounting Kit | x 2 |



It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.

2.1.2 Panel Function Descriptions

WLO-15814N / WLO-15802N

Front Panel



Rear Panel



1. Reboot Button : Unscrew the screw and click Reset button to restart system or reset to default configurations.
 - ➔ Press and hold the Reset button for 2 seconds and release to restart system. The LED except Power indicator will be off before restarting.
 - ➔ Press and hold the Reset button for more than 10 seconds to reset the system to default configurations.
2. Power : Green LED ON indicates power on, and OFF indicates power off.
3. WLAN : Green LED FLASH indicates Wireless Transmit.
4. LAN : Green LED ON indicates connection, OFF indicates no connection, FLASH indicates Packets transmit
5. PoE Connector : For connecting to PSE

2.1.3 Hardware Installation Steps

Please follow the steps mentioned below to install the hardware of WLO-15814N / WLO-15802N :

WLO-15814N / WLO-15802N



Front Panel



Rear Panel

- Connect N-type antenna to the N-type connector on the rear panel.
- Connect PSE to the PoE connector on the front panel.
- Connect an Ethernet cable to the PSE and the other end to a computer.
- Power on the PSE in order to supply power to WLO-15814N / WLO-15802N

2.2 Web Management Interface Instructions

WLO-15814N / WLO-15802N supports web-based configuration. Upon the completion of hardware installation, WLO-15814N / WLO-15802N can be configured through a PC/NB by using its web browser such as Internet Explorer version 6.0.

- **Default IP Address** : 192.168.2.254
- **Default IP Netmask** : 255.255.255.0
- **Default User Name and Password** :

The default user name and password for both root manager account and admin manager account are as follows :

| Mode | Router AP | CPE | | AP | WDS | UR + CB | CPE + AP | |
|---------------------------|--------------|--------------|---------------|--------------|--------------|--------------|--------------|---------------|
| Management Account | Root Account | Root Account | Admin Account | Root Account | Root Account | Root Account | Root Account | Admin Account |
| User Name | root | root | admin | root | root | root | root | admin |
| Password | default | default | admin | default | default | default | default | admin |

Step

- **IP Segment Set-up for Administrator's PC/NB**

Set the IP segment of the administrator's computer to be in the same range as WLO-15814N / WLO-15802N for accessing the system. Do not duplicate the IP Address used here with IP Address of WLO-15814N / WLO-15802N or any other device within the network

Example of Segment :

The valid range is 1 ~ 254 and 192.168.2.254 shall be avoided because it is already assigned to WLO-15814N / WLO-15802N . 192.168.2.10 is used in the example below.

- IP Address : 192.168.2.10
- IP Netmask : 255.255.255.0

- **Launch Web Browser**

Launch web browser to access the web management interface of system by entering the default IP Address, <http://192.168.2.254>, in the URL field, and then press **Enter**.



■ System Login

The system manager Login Page then appears.

Enter **“root”** as **User name** and **“default”** as **Password**, and then click OK to login to the system; the root manager account is used as an example here.



■ Login Success

System Overview page will appear after successful login.

The screenshot shows the "System Overview" page of the web interface. The page has a header with the product name "802.11a/n MIMO Wireless Outdoor Bridge" and a navigation menu with tabs for "Wizard", "System", "Wireless", "Utilities", and "Status". Below the navigation, there are sub-tabs for "Overview", "Clients", "WDS Status", "Extra Info", and "Event Log". The main content area is titled "System Overview" and contains several information boxes:

- System:** Host Name: WLO-15802N, Operating Mode: AP Mode, Location, Description: 802.11a/n Wireless Outdoor Bridge, 200mW, Firmware Version: Cam-CP6-R5H2 V1.0.10 Version, Firmware Date: 2010-03-19 04:24:31, Device Time: 2009-01-01 00:00:42, System Up Time: 00:42.
- LAN Information:** MAC Address: 00:26:CE:01:08:91, Receive Bytes: 23963, Receive Packets: 232, Transmit Bytes: 319736, Transmit Packets: 291.
- Wireless Information:** MAC Address: 00:26:CE:01:08:92, Channel: 44, Rate: 300 Mbit/s, Receive Bytes: 2348, Receive Packets: 18, Transmit Bytes: 4660, Transmit Packets: 51.
- Network:** Mode: Static Mode, IP Address: 192.168.2.254, IP Netmask: 255.255.255.0, IP Gateway: 192.168.2.1, Primary DNS, Secondary DNS.

A "Refresh" button is located in the top right corner of the System Overview section. The footer of the page contains the text "©Copyright Phoenix. All rights reserved."

Chapter 3. AP Mode Configuration

When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

| Option | System | Wireless | Utilities | Status |
|-----------|----------------|----------------|-------------------|-----------------|
| Functions | Operating Mode | General Setup | Profiles Settings | System Overview |
| | LAN | Advanced Setup | Firmware Upgrade | Clients |
| | Management | Virtual AP | Network Utility | WDS Status |
| | Time Server | WDS Setup | Reboot | Extra Info |
| | SNMP | | | Event Log |

Table 3-1: AP Mode Functions

3.1 External Network Connection

3.1.1 Network Requirement

Normally, WLO-15814N / WLO-15802N connects to a wired LAN and provides a wireless connection point to associate with wireless client as shown in Figure 3-1. Then, Wireless clients could access to LAN or Internet by associating themselves with WLO-15814N / WLO-15802N set in AP mode.



Figure 3-1 Access Point on a Wired LAN Configuration

3.1.2 Configure LAN IP

Here are the instructions to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

LAN Setup

Ethernet Connection Type
Mode : Static IP Dynamic IP

Static IP
IP Address : 192.168.2.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.2.1

DNS
DNS : No Default DNS Server Specify DNS Server IP
Primary :
Secondary :

Save

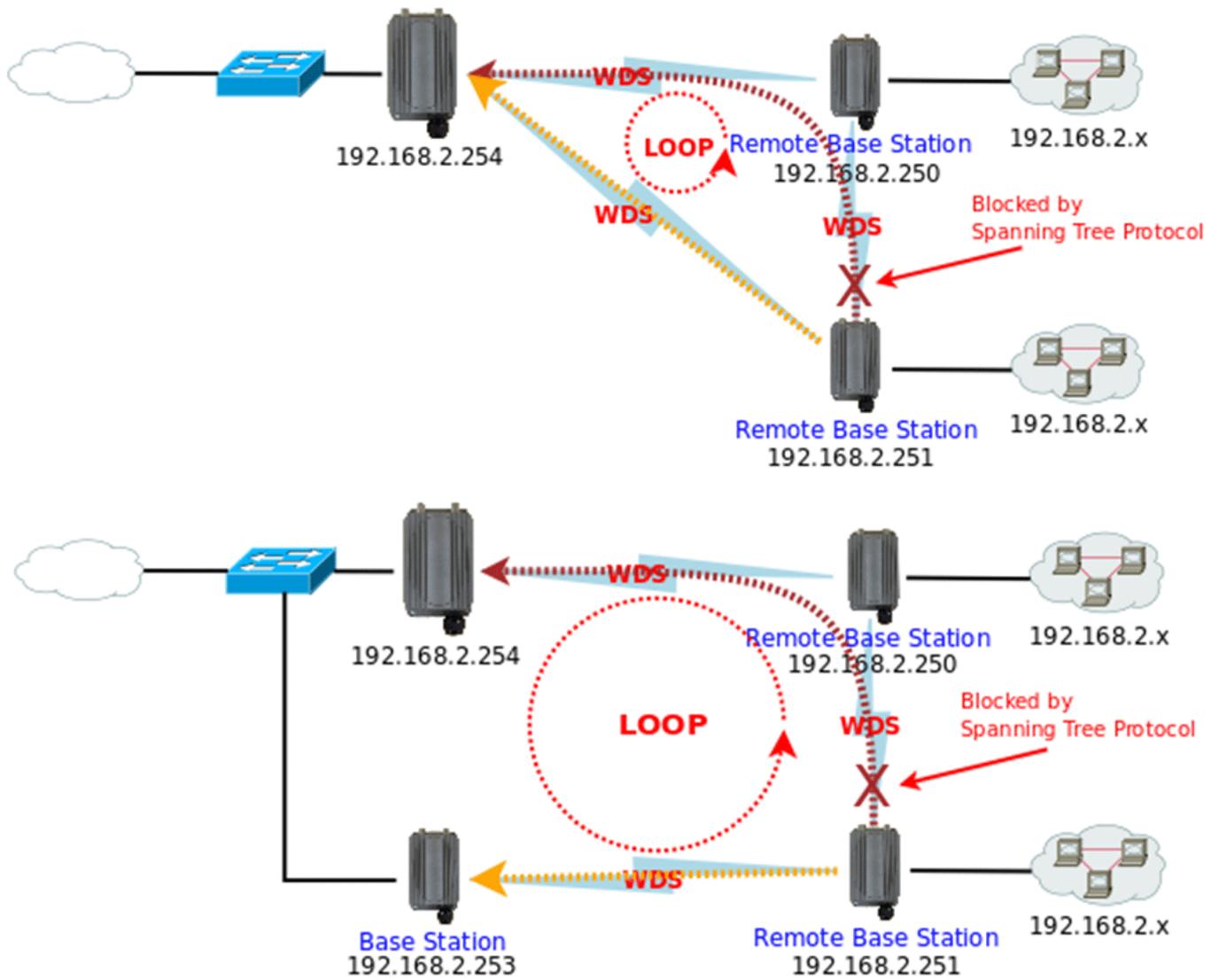
- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
 - ➔ **Static IP** : The administrator can manually setup the LAN IP address when static IP is available/ preferred.
 - ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
 - ➔ **Dynamic IP** : This configuration type is applicable when the WLO-15814N / WLO-15802N is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

Dynamic IP
Hostname :

- ✓ **Hostname** : The Hostname of the LAN port
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.

■ 802.1d Spanning Tree

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 4 WDS interfaces from wds0 to wds3. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d. The Spanning tree always enabled on WLO-15814N / WLO-15802N. Below Figures depict a loop for a bridged LAN between LAN and WDS link



Click **Save** button to save your changes. Click **Reboot** button to activate your changes

3.2 Wireless LAN Network Creation

The network manager can configure related wireless settings, **General Settings**, **Advanced Settings**, **Virtual AP(VAP) Setting**, **Security Settings** and **MAC Filter Settings**.

3.2.1 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

- **MAC Address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **AP Isolation** : Select **Enable**, all clients will be isolated from each VAP, that means different VAP's clients can not reach to each other.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Channel/Frequency** : The channel range will be changed by selecting different country code. Below depicts the channel range for different **Country**.

| Country | Channel |
|---------|---|
| US | 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 |
| ETSI | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 |
| JP | 36, 40, 44, 48 |
| NONE | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161 |

- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between **1** to **100** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput)** settings should be hidden immediately.

- **HT TxStream/RxStream** : By default, it's 2.
- **Operating Mode** : By default, it's Mixed Mode.
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "Auto" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG)** : Disable or enable reserve direction grant. Default is enabled.
- **A-MSDU** : Aggregated Mac Service Data Unit. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU. Default is disabled.
- **Auto Block ACK** : Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request** : Disable or enable decline BA request. Default is disabled.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **all VAPs** and **WDS Links**.

3.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Short Slot : Enable Disable

Extra Slot Time : us

ACK Timeout : us

Beacon Interval : ms

DTIM Interval : ms

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

Pkt_Aggregate : Enable Disable

IEEE 802.11H(DFS) : Enable Disable

WMM : Enable Disable

Save

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time** : Slot time is in the range of **1~255** and set in unit of **microsecond**. The default value is **9** microsecond.



When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout** : ACK timeout is in the range of **1~255** and set in unit of *microsecond*. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.

- **RTS Threshold** : TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.

- **Short Preamble** : By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.

- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.

- **Pkt_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.

- **IEEE802.11H (DFS)** : By default, it's "**Enable**". To **Disable** is to deactivate IEEE802.11H(DFS)

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

| | |
|---------------------|--|
| DFS Channels | 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140 |
|---------------------|--|

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.



*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When WLO-15814N / WLO-15802N detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
|-------|-------|-------|-------|------|--------------------------|--------------------------|
| AC_BE | 3 | 15 | 63 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VI | 1 | 7 | 15 | 94 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VO | 1 | 3 | 7 | 47 | <input type="checkbox"/> | <input type="checkbox"/> |

| | Aifsn | CWMin | CWMax | Txop | ACM |
|-------|-------|-------|-------|------|--------------------------|
| AC_BE | 3 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_VI | 2 | 7 | 15 | 94 | <input type="checkbox"/> |
| AC_VO | 2 | 3 | 7 | 47 | <input type="checkbox"/> |



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

→ **WMM Parameters of Access Point** : This affects traffic flowing from the access point to the client station

| Queue | Data Transmitted AP to Clients | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : *This affects traffic flowing from the client station to the access point.*

| Queue | Data Transmitted Clients to AP | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is

the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".

- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **all VAPs** and **WDS Links**.

3.2.3 Create Virtual AP (VAP)

The WLO-15814N / WLO-15802N support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **7** logical access points, each of which can have a different set of security, VLAN Tag(ID) and network settings. **Figure 3-2** shows multiple SSIDs with different security type and VLAN settings.

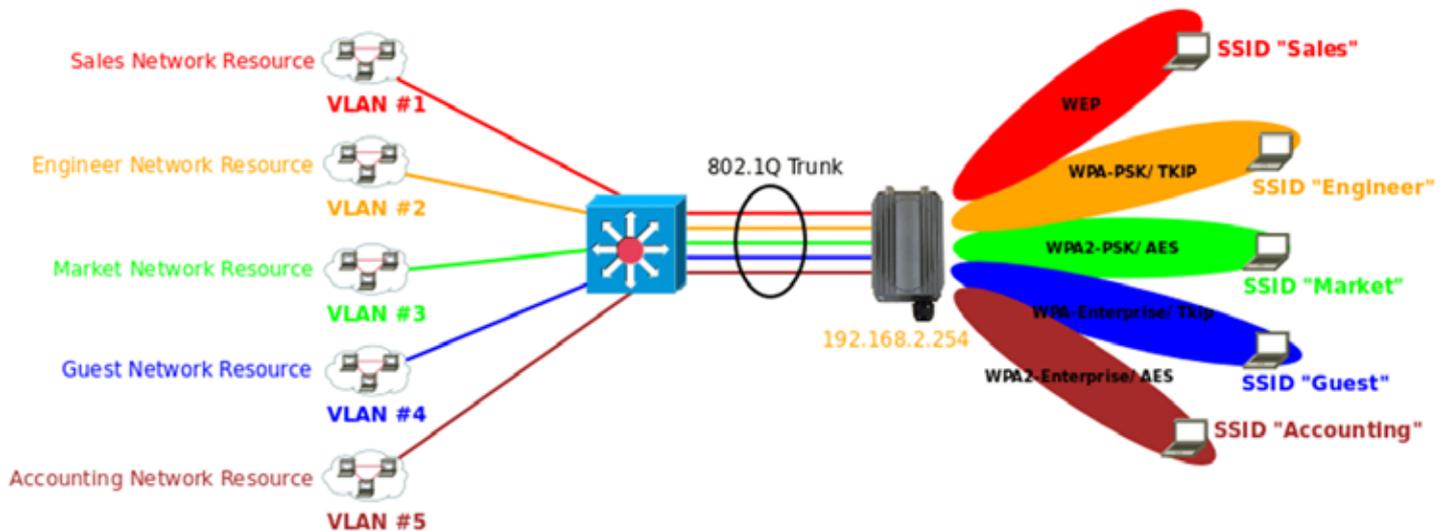


Figure 3-2 Multiple SSIDs with different Security Type and VLAN Tag

3.2.3.1 Virtual AP Overview

The administrator can view all of the Virtual AP's settings via this page.

Please click on **Wireless -> Virtual AP Setup** and the Virtual AP Overview Page appears.

Virtual AP Overview

| VAP List | | | | | | |
|------------|---------|-------------------|--------|---------------|------------|----------------------|
| VAP | ESSID | MAC Address | Status | Security Type | MAC Filter | Edit |
| Primary AP | Main_AP | 00:26:CE:01:C6:92 | On | Disable | Disable | Edit |
| VAP1 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP2 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP3 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP4 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP5 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP6 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |

- **VAP** : Indicate the system's Virtual AP.
- **ESSID** : Indicate the ESSID of the respective Virtual AP
- **MAC Address** : The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here.
- **Status** : Indicate the Status of the respective Virtual AP. **The Primary AP always on.**
- **Security Type** : Indicate an used security type of the respective Virtual AP.
- **MAC Filter** : Indicate an used MAC filter of the respective Virtual AP.
- **Edit** : Click **Edit** button to configure Virtual AP's settings, including security type and MAC Filter.

3.2.3.2 Virtual AP Setup

For each Virtual AP, administrators can configure SSID, VLAN tag(ID), SSID broadcasting, Maximum number of client associations, security type settings.

Click **Edit** button on the Edit column, and then a Virtual AP setup page appears.

VAP 1 Setup

Security

Enable AP : Enable Disable

ESSID :

Client Isolation : Enable Disable

Hidden SSID : Enable Disable

Maximum Clients :

VLAN Tag(ID) : Enable Disable (1-4094)

Security Type :

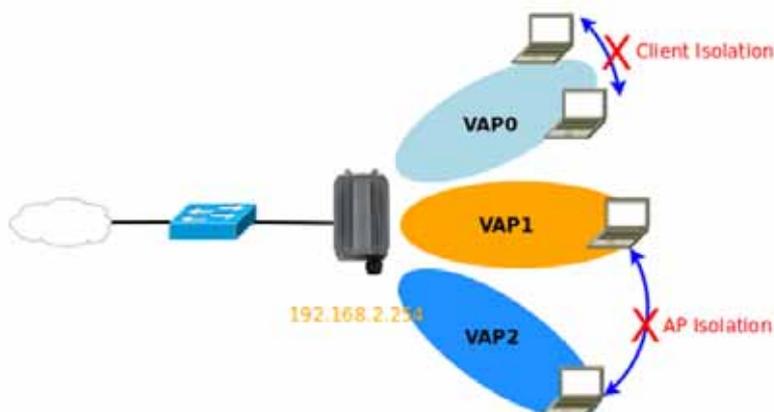
MAC Filter

Action :

- **Enable AP** : By default, it's "**Disable**" for VAP1 ~ VAP6. **The Primary AP always enabled.**

Select "**Enable**" to activate VAP or click "**Disable**" to deactivate this function

- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified VAP.
- **Client Isolation** : Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients. Below Figures depict Client Isolation and AP Isolation



- **Hidden SSID** : By default, it's "**Disable**".

Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.

- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.

- **VLAN Tag(ID)** : By default, it's selected "**Disable**".

This system supports tagged Virtual LAN(VLAN). A valid number of **1** to **4094** can be entered after it's enabled. If your network utilize VLANs you could tie a VLAN Tag to a specific SSID, and packets from/to wireless clients belonging to that SSID will be tagged with that VLAN Tag. This enables security of wireless applications by applying VLAN Tag.

- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
 - ➔ **Disable** : Data are unencrypted during transmission when this option is selected.
 - ➔ **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

- **Authentication Method** : Enable the desire option among **OPEN**, **SHARED** or **WEPAUTO**.

- ➔ **Key Index** : Key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ➔ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite** : By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.



Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period** : By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- ➔ **WPA-Enterprise (or WPA2-Enterprise)**: The RADIUS authentication and encryption will be both enabled if this is selected.

WPA General

Cipher Suite :

Group Key Update Period : seconds

PMK Cache Period : minute

Pre-Authentication : Disable Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.



PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X** : When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

802.1x WEP

Dynamic WEP : Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **Radius Server Settings :**

- **IP Address** : Enter the IP address of the Authentication RADIUS server.
- **Port** : By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret** : A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout** : The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

3.2.4 Wireless MAC Filter Setup

Continue **3.2.3.2 Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.

- **MAC Filter Setup** : By default, it's "**Disable**". Options are **Disable**, **Only Deny List MAC** or **Only Allow List MAC**.

Two ways to set MAC filter rules :

→ **Only Allow List MAC.**

The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

→ **Only Deny List MAC.**

The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Click **Reboot** button to activate your changes



MAC Access Control is the weakest security approach. WPA and WPA2 security method is highly recommended.

3.3 Wireless Network Expansion

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.**



Please click on **Wireless -> WDS Setup** and follow the below setting.

WDS Setup

Security

Security Type: Disable

WDS MAC List

| Enable | WDS Peer's MAC Address | Description |
|--------------------------|--|--|
| <input type="checkbox"/> | 01 <input style="width: 40px;" type="text"/> | <input style="width: 95%;" type="text"/> |
| <input type="checkbox"/> | 02 <input style="width: 40px;" type="text"/> | <input style="width: 95%;" type="text"/> |
| <input type="checkbox"/> | 03 <input style="width: 40px;" type="text"/> | <input style="width: 95%;" type="text"/> |
| <input type="checkbox"/> | 04 <input style="width: 40px;" type="text"/> | <input style="width: 95%;" type="text"/> |

- **Security Type** : Option is “Disable”, “WEP”, “TKIP” or “AES” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
 - ➔ **WEP Key** : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
 - ➔ **TKIP Key** : Enter **8 to 63 ASCII** or **64 HEX** format TKIP key.
 - ➔ **AES Key** : Enter **8 to 63 ASCII** or **64 HEX** format AES key.
- **WDS MAC List**
 - ➔ **Enable** : Click **Enable** to create WDS link.
 - ➔ **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
 - ➔ **Description** : Description of WDS link.



The WDS link needs to be set at same **Channel** and with same **Security Type**.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

3.4 System Management

3.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - ➔ **Enable HTTP** : Check to select HTTP Service.
 - ➔ **HTTP Port** : The default is **80** and the range is between 1 ~ 65535.
 - ➔ **Enable HTTPS** : Check to select HTTPS Service
 - ➔ **HTTPS Port** : The default is **443** and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

- ➔ **Enable Telnet** : Check to select Telnet Service
- ➔ **Telnet Port** : The default is **23** and the range is between 1 ~ 65535.
- ➔ **Enable SSH** : Check to select SSH Service
- ➔ **SSH Port** : Please The default is **22** and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

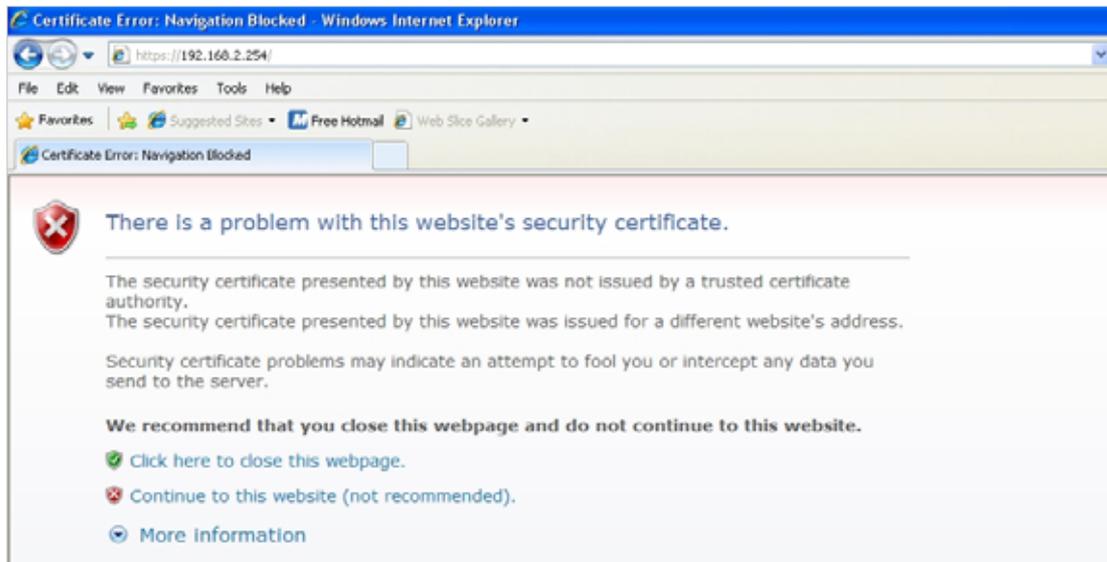
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

 - ➔ **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
 - ➔ **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
 - ➔ **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
 - ➔ **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
 - ➔ **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

3.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

Save

- **Local Time** : Display the current system time.

- **NTP Client** : To synchronize the system time with NTP server.
 - ➔ **Enable** : Check to select NTP client.
 - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
 - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
 - ➔ **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

3.4.3 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable:** Check to enable SNMP v2c.

- ➔ **ro community :** Set a community string to authorize read-only access.
- ➔ **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

- ➔ **SNMP ro user :** Set a community string to authorize read-only access.
- ➔ **SNMP ro password :** Set a password to authorize read-only access.
- ➔ **SNMP rw user :** Set a community string to authorize read/write access.
- ➔ **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

- **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

3.4.4 Backup / Restore and Reset to Factory

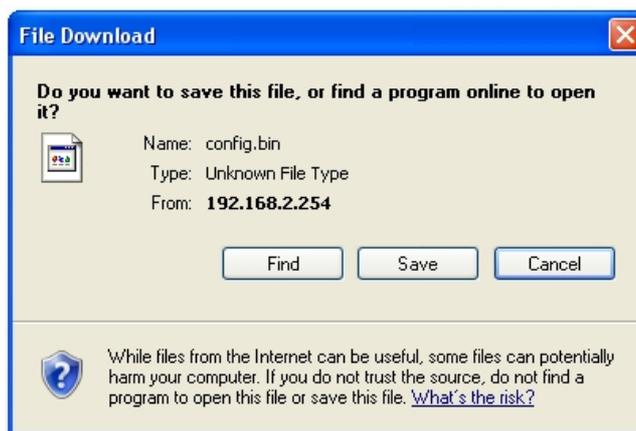
Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings To PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

3.4.5 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Infomation

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27

Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

3.4.6 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

Network Utility

Ping

Destination IP/Domain: Count:

Traceroute

Destination Host: MAX Hop:

Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.

 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click **Stop** button to stopped test

 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

3.4.7 Reboot

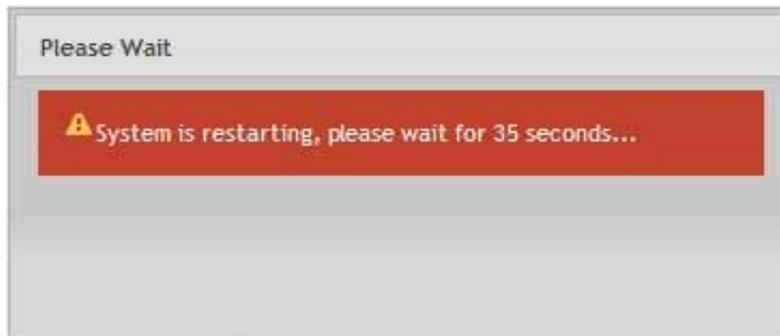
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

Reboot

 You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Reboot

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

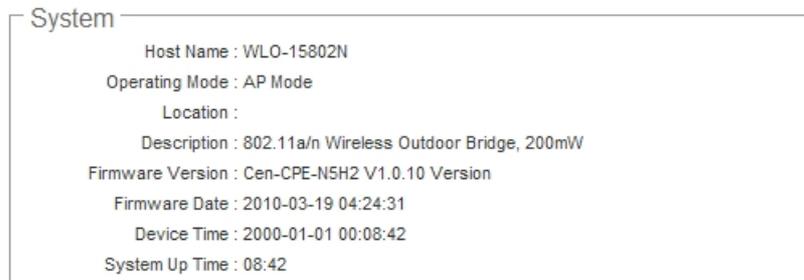
3.5 System Status

This section breaks down into subsections of **System Overview**, **Associated Clients Status**, **WDS Link Status**, **Extra Information** and **Event Log**.

3.5.1 System Overview

Display detailed information of **System**, **Network**, **LAN and Wireless** in the System Overview page.

- **System** : Display the information of the system.



- **System Name** : The name of the system.
- **Operating Mode** : The mode currently in service.
- **Location** : Deployed geographical location.
- **Description** : A description of the system.
- **Firmware Version** : The current installed firmware version.
- **Firmware Date** : The build time of installed firmware.
- **Device Time** : The current time of the system.
- **System Up Time** : The time period that system has been in service since last reboot.

- **Network Information** : Supports Static or Dynamic modes on the LAN interface.



- **IP Address** : The management IP of system. By default, it's 192.168.2.254.
- **IP Netmask** : The network mask. By default, it's 255.255.255.0.
- **IP Gateway** : The gateway IP address and by default, it's 192.168.2.1.
- **Primary DNS** : The primary DNS server in service.
- **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.

| LAN Information | |
|--------------------|-------------------|
| MAC Address : | 00:1A:50:00:47:B0 |
| Receive Bytes : | 23282 |
| Receive Packets : | 174 |
| Transmit Bytes : | 13388 |
| Transmit Packets : | 126 |

- **MAC Address** : The MAC address of the LAN port.
- **Receive bytes** : The total received packets in bytes on the LAN port.
- **Receive packets** : The total received packets of the LAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display total received and transmitted statistics on available Virtual AP.

| Wireless Information | |
|----------------------|-------------------|
| MAC Address : | 00:1A:50:00:47:A8 |
| Receive Bytes : | 0 |
| Receive Packets : | 0 |
| Transmit Bytes : | 3261 |
| Transmit Packets : | 16 |

- **MAC Address** : The MAC address of the Wireless port.
- **Channel** : The current channel on the Wireless port.
- **Rate** : The current Bit Rate on the Wireless port.
- **Receive bytes** : The total received packets in bytes on the Wireless port.
- **Receive packets** : The total received packets on the Wireless port.
- **Transmit bytes** : The total transmitted packets in bytes on the Wireless port.
- **Transmit packets** : The total transmitted packets on the Wireless port.

3.5.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with all Virtual AP.

Wireless Clients

| VAP Information | | | | | Primary AP Clients | | | | | |
|-----------------|---------|-------|---------------|---------|--------------------|-------------------------|-------------------------|-----------|--------------|-----------------|
| VAP | ESSID | State | Security Type | Clients | MAC | Signal Strength ANT0 | Signal Strength ANT1 | Bandwidth | Idle Time | Connect Time |
| Primary AP | Main_AP | On | Disable | 1 | 00:90:CC:0F:51:38 | 100%(0dBm) | 100%(0dBm) | 20MHz | 2 | 2 |
| VAP1 | | Off | Disable | 0 | | | | | | |
| VAP2 | | Off | Disable | 0 | | | | | | |
| VAP3 | | Off | Disable | 0 | | | | | | |
| VAP4 | | Off | Disable | 0 | | | | | | |
| VAP5 | | Off | Disable | 0 | | | | | | |
| VAP6 | | Off | Disable | 0 | | | | | | |

- **VAP Information** : Highlights key VAP information.
 - **VAP** : Available VAP from Primary AP to VAP6.
 - **ESSID** : Display name of ESSID for each VAP.
 - **MAC Address** : Display MAC address for each VAP.
 - **Status** : On/Off
 - **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
 - **Clients** : Display total number of wireless connections for each VAP.

- **VAP Clients** : Display all associated clients on each Virtual AP.
 - **MAC Address** : MAC address of associated clients
 - **Signal Strength ANT0/ANT1** : Signal Strength of from associated clients.
 - **Bandwidth** : Channel bandwidth of from associated clients
 - **Idle Time** : Last inactive time period in seconds for a wireless connection.
 - **Connect Time** : Total connection time period in seconds for a wireless connection.
 - **Disconnect** : Click "**Delete**" button to manually disconnect a wireless client in a Virtual AP.

3.5.3 Show WDS Link Status

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.

WDS Information

| WDS Link Status | | | | | | |
|-------------------|-------------------------|-------------------------|-------------|-----------|-----|-----|
| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | Phy Mode | BandWidth | MCS | SGI |
| 00:1A:50:0A:7B:F2 | 100% (-5 dBm) | 100% (-6 dBm) | HTMIX | 40M | 15 | 1 |

- **MAC Address** : Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1** : Indicate the signal strength of the respective WDS links.
- **Phy Mode** : Indicate the phy mode of the respective WDS linked.
- **BandWidth** : Indicate the channel bandwidth of the respective WDS linked.
- **MCS** : Indicate the MCS of the respective WDS linked.
- **SGI** : Indicate the SGI (Short Guard Interval) of the respective WDS linked. "1" indicate the Short Guard Interval, "0" indicate the Long Guard Interval.



*If display "no signal" Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address, Channel and Security type**. Also, adjust antenna angle and Tx Power.*

3.5.4 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
Information: Route Information

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | bre0 |

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | bre0 |

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

| IP Address | HW Type | Flags | HW Address | Mask | Device |
|--------------|---------|-------|-------------------|------|--------|
| 192.168.2.22 | 0x1 | 0x2 | 00:1A:92:9F:A4:9B | * | bre0 |

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0~ra6 and wds0~wds3).

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-------------|
| bre0 | 8000.000c432880b0 | no | eth2 ra0 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be dropped.

Bridge MACs Information

| Port | MAC Address | Local | Ageing Timer |
|-----------|-------------------|-------|--------------|
| PrimaryAP | 00:1A:50:13:35:ef | no | 157.50 |
| WDS0 | 00:1A:50:0a:7b:f1 | no | 2.05 |
| LAN | 00:1A:50:0a:7b:f9 | yes | 0.00 |
| PrimaryAP | 00:1A:50:0a:7b:fa | yes | 0.00 |
| LAN | 00:1A:50:9f:a4:9b | no | 0.10 |

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

Bridge STP Information

| bre0 | | | |
|-----------------------|-------------------|----------------------|------------|
| bridge id | 8000.000c43288008 | | |
| designated root | 8000.000c43288008 | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 0.84 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 2.83 |
| flags | | | |
| eth2 (1) | | | |
| port id | 8001 | state | forwarding |
| designated root | 8000.000c43288008 | path cost | 100 |
| designated bridge | 8000.000c43288008 | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.85 |
| flags | | | |
| ra0 (2) | | | |
| port id | 8002 | state | forwarding |
| designated root | 8000.000c43288008 | path cost | 100 |
| designated bridge | 8000.000c43288008 | message age timer | 0.00 |
| designated port | 8002 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.85 |
| flags | | | |

3.5.5 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|---|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 4. WDS Mode Configuration

Please refer to illustrations of the section 1.3 for possible applications in the WDS mode. This section provides detailed explanation for users to configure in the WDS mode with help of illustrations. In the WDS mode, functions listed in the table below are also available from the Web-based GUI interface.

| Option | System | Wireless | Utilities | Status |
|-----------|----------------|----------------|-------------------|-----------------|
| Functions | Operating Mode | General Setup | Profiles Settings | System Overview |
| | LAN | Advanced Setup | Firmware Upgrade | WDS Status |
| | Management | WDS Setup | Network Utility | Extra Info |
| | Time Server | | Reboot | Event Log |
| | SNMP | | | |

Table 4-1: WDS Mode Functions

4.1 External Network Connection

4.1.1 Network Requirement

You could expand your Ethernet network via WDS link. In this mode, the WLO-15814N / WLO-15802N connects directly to a wired LAN, and wirelessly bridges to a remote access point via a WDS link as shown in Figure 4-1. In the mode, it can't associate with any wireless clients.



Figure 4-1 Point to Point network Configuration

4.1.2 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

LAN Setup

Ethernet Connection Type
Mode : Static IP Dynamic IP

Static IP
IP Address : 192.168.2.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.2.1

DNS
DNS : No Default DNS Server Specify DNS Server IP
Primary :
Secondary :

Save

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
 - ➔ **Static IP** : The administrator can manually setup the LAN IP address when static IP is available/ preferred.
 - ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
 - ➔ **Dynamic IP** : This configuration type is applicable when the WLO-15814N / WLO-15802N is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

Dynamic IP
Hostname :

- ✓ **Hostname** : The Hostname of the LAN port
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.2 Wireless Network Expansion

The network manager can configure related wireless settings, **General Settings**, **Advanced Settings** and **WDS Settings**.

4.2.1 General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

General Setup

MAC Address: 00 1A 50 0A 7B FA

Band Mode: 802.11 a/n mixed mode

Country: NONE

Channel: 44

Tx Power: 10 %

HT Physical Mode

Operating Mode: Mixed Mode Green Field

Channel Bandwidth: 20 20/40

Guard Interval: Long Auto

MCS: Auto

Reverse Direction Grant (RDG): Disable Enable

A-MSDU: Disable Enable

Auto Block ACK: Disable Enable

Decline BA Request: Disable Enable

HT Other

HT TxStream: 2

HT RxStream: 2

- **MAC Address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Channel/Frequency** : The channel range will be changed by selecting different country code. Below depicts the channel range for different **Country**.

| Country | Channel |
|---------|---|
| US | 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 |
| ETSI | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 |
| JP | 36, 40, 44, 48 |
| NONE | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161 |

- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between **1** to **100** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput)** settings should be hidden immediately.

- **HT TxStream/RxStream** : By default, it's 2.
- **Operating Mode** : By default, it's Mixed mode
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "20/40" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "Auto" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG)** : Disable or enable reserve direction grant. Default is enabled.
- **A-MSDU** : Aggregated Mac Service Data Unit . Select **Enable** to allow aggregation for multiple MSDUs in one MPDU Default is disabled.
- **Auto Block ACK** : Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request** : Disable or enable decline BA request. Default is disabled.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **all WDS Links**.

4.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Short Slot : Enable Disable

Extra Slot Time : us

ACK Timeout : us

Beacon Interval : ms

DTIM Interval : ms

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

Pkt_Aggregate : Enable Disable

IEEE 802.11H(DFS) : Enable Disable

WMM : Enable Disable

Save

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time** : Slot time is in the range of **1~255** and set in unit of **microsecond**. The default value is **9** microsecond.



When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout** : ACK timeout is in the range of **1~255** and set in unit of *microsecond*. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.
- **RTS Threshold** : TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble** : By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
- **Pkt_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.
- **IEEE802.11H (DFS)** : By default, it's "**Enable**". To **Disable** is to deactivate IEEE802.11H(DFS)

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

| | |
|---------------------|--|
| DFS Channels | 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140 |
|---------------------|--|

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.



*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When WLO-15814N / WLO-15802N detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

| WMM Parameters of Access Point | | | | | | |
|--------------------------------|-------|-------|-------|------|--------------------------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
| AC_BE | 3 | 15 | 63 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VI | 1 | 7 | 15 | 94 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VO | 1 | 3 | 7 | 47 | <input type="checkbox"/> | <input type="checkbox"/> |

| WMM Parameters of Station | | | | | |
|---------------------------|-------|-------|-------|------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM |
| AC_BE | 3 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_VI | 2 | 7 | 15 | 94 | <input type="checkbox"/> |
| AC_VO | 2 | 3 | 7 | 47 | <input type="checkbox"/> |



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

→ **WMM Parameters of Access Point** : This affects traffic flowing from the access point to the client station

| Queue | Data Transmitted AP to Clients | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : *This affects traffic flowing from the client station to the access point.*

| Queue | Data Transmitted Clients to AP | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until

either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".

- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **all WDS Links**.

4.2.3 WDS Setup

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.**

WDS Setup

| Enable | WDS Peer's MAC Address | Description |
|--------------------------|-------------------------|----------------------|
| <input type="checkbox"/> | 01 <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | 02 <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | 03 <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | 04 <input type="text"/> | <input type="text"/> |

- **Security Type** : Option is “Disable”, “WEP”, “TKIP” or “AES” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
 - **WEP Key** : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
 - **TKIP Key** : Enter **8 to 63 ASCII** or **64 HEX** format TKIP key.
 - **AES Key** : Enter **8 to 63 ASCII** or **64 HEX** format AES key.

- **WDS MAC List**
 - **Enable** : Click **Enable** to create WDS link.
 - **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
 - **Description** : Description of WDS link.



The WDS link needs to be set at same **Channel** and **Security Type** between WDS link.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.3 System Management

4.3.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - ➔ **Enable HTTP** : Check to select HTTP Service.
 - ➔ **HTTP Port** : The default is 80 and the range is between 1 ~ 65535.
 - ➔ **Enable HTTPS** : Check to select HTTPS Service
 - ➔ **HTTPS Port** : The default is 443 and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

- ➔ **Enable Telnet** : Check to select Telnet Service
- ➔ **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- ➔ **Enable SSH** : Check to select SSH Service
- ➔ **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

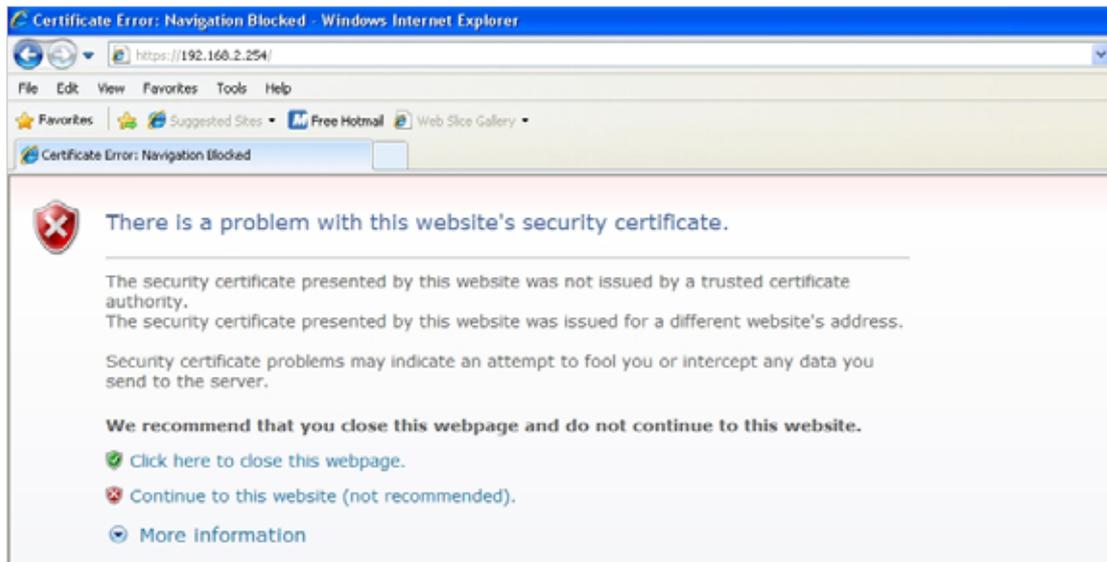
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

 - ➔ **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
 - ➔ **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
 - ➔ **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
 - ➔ **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
 - ➔ **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254/>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

4.3.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

Save

- **Local Time** : Display the current system time.
- **NTP Client** : To synchronize the system time with NTP server.
 - **Enable** : Check to select NTP client.
 - **Default NTP Server** : Select the NTP Server from the drop-down list.
 - **Time Zone** : Select a desired time zone from the drop-down list.
 - **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

4.3.3 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable** : Check to enable SNMP v2c.

- ➔ **ro community** : Set a community string to authorize read-only access.
- ➔ **rw community** : Set a community string to authorize read/write access.

- **SNMP v3 Enable**: Check to enable **SNMP v3**.

SNMPv3 supports the highest level SNMP security.

- ➔ **SNMP ro user** : Set a community string to authorize read-only access.
- ➔ **SNMP ro password** : Set a password to authorize read-only access.
- ➔ **SNMP rw user** : Set a community string to authorize read/write access.
- ➔ **SNMP rw password** : Set a password to authorize read/write access.

- **SNMP Trap** : Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

- **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

4.3.4 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

Profile Save

Save Settings To PC :

Load Settings From PC :

Reset To Factory Default :

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

4.3.5 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27

Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding.
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

4.3.6 Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

Network Utility

Ping

Destination IP/Domain: Count

Traceroute

Destination Host: MAX Hop

Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.

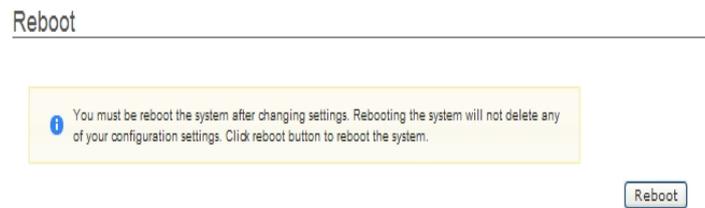
 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test

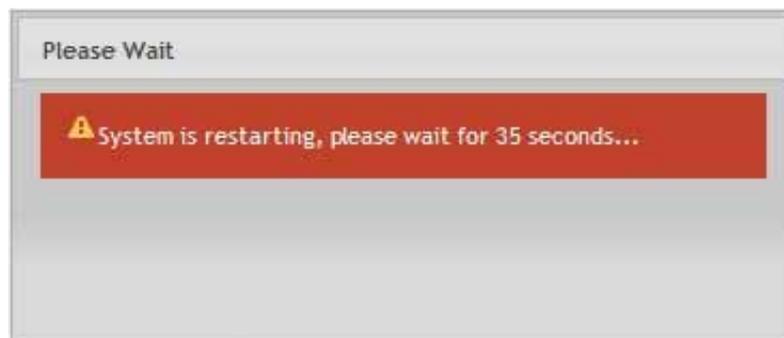
 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

4.3.7 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

4.4 System Status

This section breaks down into subsections of **System Overview**, **WDS Link Status**, **Extra Information** and **Event Log**.

4.4.1 System Overview

Detailed information on **System**, **Network**, **LAN Information** and **Wireless Information** can be reviewed via this page.

- **System** : Display the information of the system.

```

System
  Host Name : WLO-15802N
  Operating Mode : WDS Mode
  Location :
  Description : 802.11a/n Wireless Outdoor Bridge, 200mW
  Firmware Version : Cen-CPE-N5H2 V1.0.10 Version
  Firmware Date : 2010-03-19 04:24:31
  Device Time : 2000-01-01 00:03:53
  System Up Time : 03:53
  
```

- **System Name** : The name of the system.
- **Operating Mode** : The mode currently in service.
- **Location** : The reminding note on the geographical location of the system.
- **Description** : The reminding note of the system.
- **Firmware Version** : The current firmware version installed.
- **Firmware Date** : The build time of the firmware installed.
- **Device Time** : The current time of the system.
- **System Up Time** : The time period that system has been in service since last reboot.

- **Network Information** : Display the information of the Network.

```

Network
  Mode : Static Mode
  IP Address : 192.168.2.254
  IP Netmask : 255.255.255.0
  IP Gateway : 192.168.2.1
  Primary DNS :
  Secondary DNS :
  
```

- **Mode** : Supports Static or Dynamic modes on the LAN interface.
- **IP Address** : The management IP of system. By default, it's 192.168.2.254.
- **IP Netmask** : The network mask. By default, it's 255.255.255.0.
- **IP Gateway** : The gateway IP address and by default, it's 192.168.2.1.
- **Primary DNS** : The primary DNS server in service.
- **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.

| LAN Information | |
|--------------------|-------------------|
| MAC Address : | 00:1A:50:28:60:30 |
| Receive Bytes : | 2888 |
| Receive Packets : | 22 |
| Transmit Bytes : | 3610 |
| Transmit Packets : | 22 |

- **MAC Address** : The MAC address of the LAN port.
- **Receive bytes** : The total received packets in bytes on the LAN port.
- **Receive packets** : The total received packets of the LAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display the detailed receive and transmit statistics of Wireless interface.

| Wireless Information | |
|----------------------|-------------------|
| MAC Address : | 00:1A:50:0A:7B:FA |
| Channel : | 44 |
| Rate : | 300 Mb/s |
| Receive Bytes : | 167110 |
| Receive Packets : | 706 |
| Transmit Bytes : | 15373 |
| Transmit Packets : | 104 |

- **MAC Address** : The MAC address of the Wireless port.
- **Channel** : The current channel on the Wireless port.
- **Rate** : The current Bit Rate on the Wireless port.
- **Receive bytes** : The total received packets in bytes on the Wireless port.
- **Receive packets** : The total received packets of the Wireless port.
- **Transmit bytes** : The total transmitted packets in bytes of the Wireless port.
- **Transmit packets** : The total transmitted packets of the Wireless port.

4.4.2 WDS List

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.

WDS Information

| WDS Link Status | | | | | | |
|-------------------|-------------------------|-------------------------|-------------|-----------|-----|-----|
| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | Phy Mode | BandWidth | MCS | SGI |
| 00:1A:50:0A:7B:F2 | 100% (-5 dBm) | 100% (-6 dBm) | HTMIX | 40M | 15 | 1 |

- **MAC Address** : Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1** : Indicate the signal strength of the respective WDS links.
- **Phy Mode** : Indicate the phy mode of the respective WDS linked.
- **BandWidth** : Indicate the channel bandwidth of the respective WDS linked.
- **MCS** : Indicate the MCS of the respective WDS linked.
- **SGI** : Indicate the SGI (Short Guard Interval) of the respective WDS linked. "1" indicate the Short Guard Interval, "0" indicate the Long Guard Interval.



*If display "no signal" Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address, Channel and Security type**. Also, adjust antenna angle and Tx Power.*

4.4.3 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
Information: Route Information

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | bre0 |

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | bre0 |

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

| IP Address | HW Type | Flags | HW Address | Mask | Device |
|--------------|---------|-------|-------------------|------|--------|
| 192.168.2.22 | 0x1 | 0x2 | 00:1A:92:9F:A4:9B | * | bre0 |

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces (e.g. eth2, ra0 and wds0~wds3).

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-------------|
| bre0 | 8000.000c432880b0 | no | eth2 ra0 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

| Port | MAC Address | Local | Ageing Timer |
|------|--------------------|-------|--------------|
| WDS0 | 00:1A:50:0A:7B:F1 | no | 1.69 |
| LAN | 00:1A:50:0A:7B:F9 | yes | 0.00 |
| LAN | 00:1A:50:51:EA:27 | no | 68.68 |
| LAN | 00:1A:50:33:32:6B | no | 15.71 |
| LAN | 00:1A:50:1E:E5:15 | no | 273.04 |
| LAN | 00:1A:50::9F:A4:9B | no | 0.19 |
| LAN | 00:1A:50:DF:D9:31 | no | 24.29 |

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

| | | | |
|-----------------------|-------------------|----------------------|------------|
| bre0 | | | |
| bridge id | 8000.000c43288008 | | |
| designated root | 8000.000c43288008 | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 0.84 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 2.83 |
| flags | | | |
| eth2 (1) | | | |
| port id | 8001 | state | forwarding |
| designated root | 8000.000c43288008 | path cost | 100 |
| designated bridge | 8000.000c43288008 | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.85 |
| flags | | | |
| ra0 (2) | | | |
| port id | 8002 | state | forwarding |
| designated root | 8000.000c43288008 | path cost | 100 |
| designated bridge | 8000.000c43288008 | message age timer | 0.00 |
| designated port | 8002 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.85 |
| flags | | | |

4.4.4 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|---|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 5. CPE Mode Configuration

When CPE mode is chosen, the system can be configured as a Customer Premises Equipment(CPE). This section provides detailed explanation for users to configure in the CPE mode with help of illustrations. In the CPE mode, functions listed in the table below are also available from the Web-based GUI interface.

| OPTION | System | Wireless | Advance | Utilities | Status |
|-----------|----------------|------------------|------------------|-------------------|--------------------|
| Functions | Operating Mode | General Setup | DMZ | Profiles Settings | System Overview |
| | WAN | Wireless Profile | IP Filter | Firmware Upgrade | Station Statistics |
| | LAN | Site Survey | MAC Filter | Network Utility | Extra Info |
| | DDNS | | Virtual Server | Reboot | QoS Plot |
| | Management | | Parental Control | | Event Log |
| | Time Server | | QoS | | |
| | UPNP | | | | |
| | SNMP | | | | |

Table 5-1: CPE Mode Functions

5.1 External Network Connection

5.1.1 Network Requirement

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE mode, WLO-15814N / WLO-15802N is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to WLO-15814N / WLO-15802N are in **different** subnet from those connected to Main Base Station, and, in CPE mode, it **does not** accept wireless association from wireless clients.

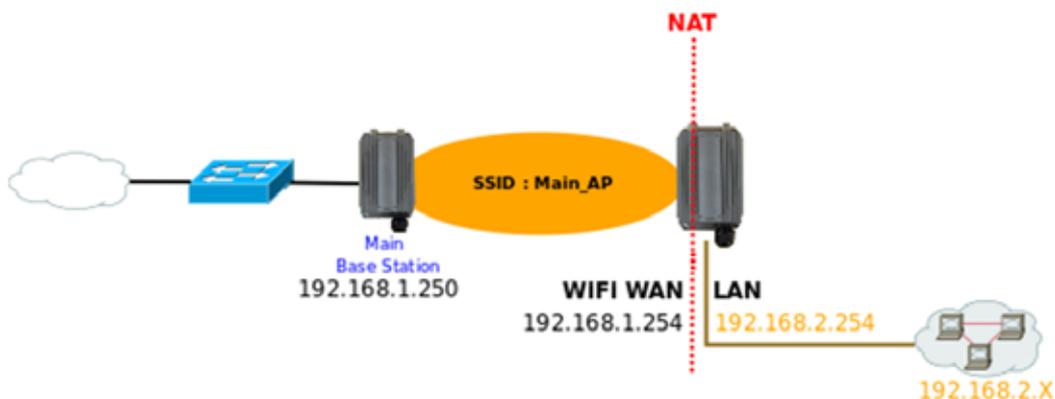


Figure 5-1 CPE mode network configuration

5.1.2 Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**.

Please click on **System** -> **WAN** and follow the below setting.

WAN Setup

Internet Connection Type
Mode : Static IP Dynamic IP PPPoE PPTP

Static IP
IP Address :
IP Netmask :
IP Gateway :

DNS
DNS : No Default DNS Server Specify DNS Server IP
Primary :
Secondary :

MAC Clone
 Keep Default MAC Address
 Clone MAC Address: 00:1A:92:9F:A4:9B
 Manual MAC Address:



In CPE mode, the WAN Port is the Wireless interface.

- **Mode** : By default, it's "**Static IP**". Check "Static IP", "Dynamic IP", "PPPoE" or "PPTP" to set up system WAN IP.
 - ➔ **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.
 - ✓ **IP Address** : The IP address of the WAN port; default IP address is 192.168.1.254
 - ✓ **IP Netmask** : The Subnet mask of the WAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the WAN port; default Gateway is 192.168.1.1
 - ➔ **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click **Release** button to release IP address and click **Renew** button to renew IP address again.

Dynamic IP
Hostname :

- ✓ **Hostname** : The Hostname of the WAN port

- ➔ **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.

PPPoE
User name :
Password :
Reconnect Mode : Always On On Demand Manual
Idle Time : minutes
MTU :

- ✓ **User Name** : Enter User Name for PPPoE connection
- ✓ **Password** : Enter Password for PPPoE connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
 - ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
 - ✓ **MTU** : By default, it’s **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ➔ **PPTP** : The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

PPTP

IP Address :

IP Netmask :

PPTP Server IP Address :

User name :

Password :

Reconnect Mode : Always On On Demand Manual

Idle Time : minutes

MTU :

MPPE Encryption : MPPE-40 MPPE-128

- ✓ **IP Address** : The IP address of the WAN port
- ✓ **IP Netmask** : The Subnet mask of the WAN port
- ✓ **PPTP Server IP Address** : The IP address of the PPTP server
- ✓ **User Name** : Enter User Name for PPTP connection
- ✓ **Password** : Enter Password for PPTP connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
- ✓ **MTU** : By default, it’s **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ✓ **MPPE Encryption** : Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
- **DNS** : Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.
- **MAC Clone** : The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC. (CPE+AP Mode does not support MAC Clone function)

MAC Clone

Keep Default MAC Address
 Clone MAC Address: 00:1A:92:9F:A4:9B
 Manual MAC Address: : : : : :

- ➔ **Keep Default MAC Address** : Keep the default MAC address of WAN port on the system.
- ➔ **Clone MAC Address** : If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.



The Clone MAC Address field will display MAC address of the PC connected to system. Click “Save” button can make clone MAC effective.

- ➔ **Manual MAC Address** : Enter the MAC address registered with your ISP.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.1.3 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

Please click on **System -> DDNS Setup** and follow the below setting.

Dynamic DNS Setup

DDNS

Enable : Enable Disable

Service Provider :

Hostname : .

User Name :

Password :

Save

- **Enabled:** By default, it's "**Disable**". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.1.4 Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System** -> **LAN** and follow the below setting.

LAN Setup

- **LAN IP** : The administrator can manually setup the LAN IP address.
 - ➔ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ➔ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

- ➔ **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- ➔ **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain** : Enter the domain name for this network.
- ➔ **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.2 Access Point Association

5.2.1 Configure Wireless General Setting

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between **1** to **100** (the unit is %) for your environment. If you are not sure of which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput) Physical Mode** and **11n Configuration** settings should be hidden immediately.

- **Operating Mode** : By default, it's Mixed Mode.
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "**Auto**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **MPDU Enable** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **A-MPDU** : A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select “Manual” to set “MPDU Density”
- **MPDU Density** : Minimum separation of MPDUs in an A-MPDU.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------------|------|------|------|------|------|------|-------|
| No Restriction | ¼ µs | ½ µs | 1 µs | 2 µs | 4 µs | 8 µs | 16 µs |

- **A-MSDU** : Aggregated Mac Service Data Unit, A-MSDU. Select **Enable** to allows aggregation for multiple MSDUs in one MPDU. Default is disabled.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

5.2.2 Configure Wireless Advanced Setting

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

WMM : Enable Disable

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.
- **RTS Threshold** : RTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble** : By default, it's "**Auto**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
- **WMM** : By default, it's "**Disable**". Select Enable, the packets with QoS WMM will have higher priority.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

5.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.

Station Site Survey

Scan Result

| ESSID | MAC Address | Signal | Channel | Security | Band | Network Type | Select |
|-------------|-------------------|--------|---------|--------------|-------|----------------|------------------------|
| Main_AP | 00:1A:50:0A:7C:3A | 50% | 44 | NONE | 11a/n | Infrastructure | Select |
| Main_AP-253 | 00:1A:50:0A:7B:F2 | 100% | 44 | NONE | 11a/n | Infrastructure | Select |
| 253AP1 | 00:1A:50:0A:7B:F3 | 100% | 44 | WEP | 11a/n | Infrastructure | Select |
| 253AP2 | 00:1A:50:0A:7B:F4 | 100% | 44 | WPAPSK/AES | 11a/n | Infrastructure | Select |
| 253AP3 | 00:1A:50:0A:7B:F5 | 100% | 44 | WPAPSK/TKIP | 11a/n | Infrastructure | Select |
| 253AP4 | 00:1A:50:0A:7B:F6 | 100% | 44 | WPA2PSK/AES | 11a/n | Infrastructure | Select |
| 253AP5 | 00:1A:50:0A:7B:F7 | 100% | 44 | WPA2PSK/TKIP | 11a/n | Infrastructure | Select |

- **ESSID** : Available Extend Service Set ID of surrounding Access Points.
- **MAC Address** : MAC addresses of surrounding Access Points.
- **Signal** : Received signal strength of all found Access Points.
- **Channel** : Channel numbers used by all found Access Points.
- **Security** : Security type by all found Access Points.
- **Band** : Wireless band used by all found Access Points.
- **Network Type** : Network type used by all found Access Points.
- **Select** : Click "**Select**" to configure settings and associate with chosen AP.



While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless Profile Setup. However, more settings are needed including Security Key.

5.2.4 Create Wireless Profile

The administrator can configure station profiles via this page.

Please click on **Wireless -> Wireless Profile** and follow the below setting.

Station Profile

- **MAC Address** : The MAC address of the Wireless Station is displayed here.
 - **Profile Name** : Set different profiles for quick connection uses.
 - **ESSID** : Assign Service Set ID for the wireless system.
 - **Security Type** : Select an appropriate security type for association, the Security Type can be selected in **“NONE”**, **“OPEN”**, **“SHARED”**, **“WPA-PSK”**, or **“WPA2-PSK”** from drop-down list; the type needs to be the same as that associated access point.
- ➔ **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.

- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**
- ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.

- **Profile List** : The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List

Profile List

| Active | # | Profile Name | ESSID | Security Type | Delete | Edit |
|----------------------------------|---|--------------|---------|---------------|------------------------|----------------------|
| <input type="radio"/> | 1 | Profile0 | default | NONE | Delete | Edit |
| <input checked="" type="radio"/> | 2 | Profile-Test | 253AP1 | OPEN | Delete | Edit |

- ➔ Click "**Edit**" an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click "**Save**" button to save the profile.
- ➔ Click "**Delete**" to remove profile.
- ➔ Click and Select a profile from list, then click the "**Connect**" button to connecting to the wireless network with the profile setting. After clicking "Connect" button, you can verify connecting status on Station Statistic Page

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.3 System Management

5.3.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - ➔ **Enable HTTP** : Check to select HTTP Service.
 - ➔ **HTTP Port** : The default is 80 and the range is between 1 ~ 65535.
 - ➔ **Enable HTTPS** : Check to select HTTPS Service
 - ➔ **HTTPS Port** : The default is 443 and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

- ➔ **Enable Telnet** : Check to select Telnet Service
- ➔ **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- ➔ **Enable SSH** : Check to select SSH Service
- ➔ **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

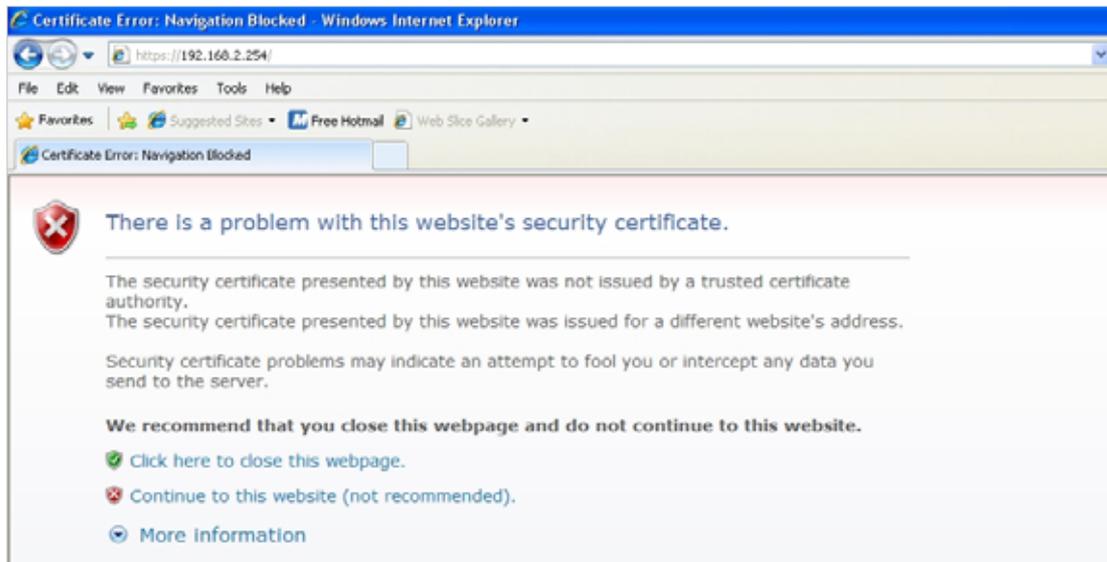
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

- ➔ **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
- ➔ **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- ➔ **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
- ➔ **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- ➔ **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254/>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

5.3.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

- **Local Time** : Display the current system time.
- **NTP Client** : To synchronize the system time with NTP server.
 - **Enable** : Check to select NTP client.
 - **Default NTP Server** : Select the NTP Server from the drop-down list.
 - **Time Zone** : Select a desired time zone from the drop-down list.
 - **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

5.3.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.



- **UPnP** : By default, it's "**Disable**". Select "**Enable**" or "**Disable**" of UPnP Service.

Click **Save** button to save changes and click **Reboot** button to activate changes

For UPnP to work in Windows XP, the "WLO-15814N / WLO-15802N" must be available in "**My Network Places**", as shown here: (your specific model may vary)



If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to **Appendix E. Using UPnP on Windows XP**

5.3.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable:** Check to enable SNMP v2c.

- **ro community :** Set a community string to authorize read-only access.
- **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

- **SNMP ro user :** Set a community string to authorize read-only access.
- **SNMP ro password :** Set a password to authorize read-only access.
- **SNMP rw user :** Set a community string to authorize read/write access.
- **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

SNMP Trap

Enable :

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

5.3.5 Backup / Restore and Reset to Factory

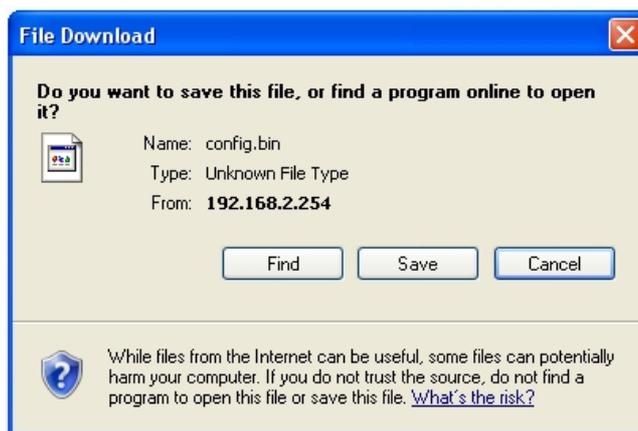
Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

5.3.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27

Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding.
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

5.3.7 Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting

Network Utility

Ping

Destination IP/Domain: Count:

Traceroute

Destination Host: MAX Hop:

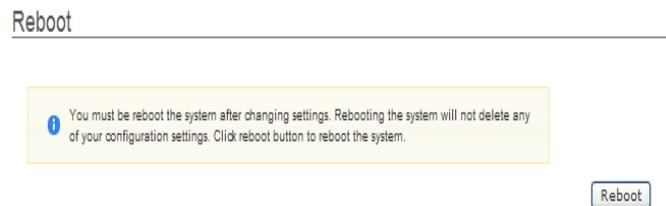
Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

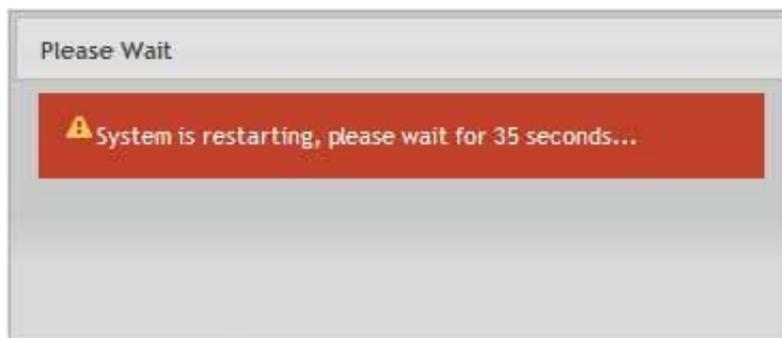
- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

5.3.8 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.



A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

5.4 Access Control List

5.4.1 IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.

IP Filter Setup

| # | Source Address/Mask | Port | Destination Address/Mask | Port | In/Out | Protocol | Listen | Action | Interface | Delete | Edit |
|-------------------------|---------------------|------|--------------------------|------|--------|----------|--------|--------|-----------|--------|------|
| No IP Rule in the List! | | | | | | | | | | | |

- **Source Address/Mask** : Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **Destination Address/Mask** : Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **In/Out** : Applies to Ingress or egress packets
- **Protocol** : Supports **TCP**, **UDP** or **ICMP**.
- **Listen** : Click **Yes** radial button to match TCP packets only with the SYN flag.
- **Active** : **Deny** to drop and **Pass** to allow per filter rules
- **Interface** : The interface that a filter rule applies



All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

- **Example 1** : Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | Pass | LAN |
| 2 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |

- **Example 2** : All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |
| 2 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | pass | LAN |

5.4.2 MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.

MAC Filter Setup

- **MAC Filter Rule** : By default, it's "**Disable**". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click **Save** button to save your change.

Two ways to set the MAC Filter List:

➔ **Only Allow List MAC.**

The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

➔ **Only Deny List MAC.**

The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.



If there does not have any MAC address in MAC Filter List, the MAC filter function deactivated

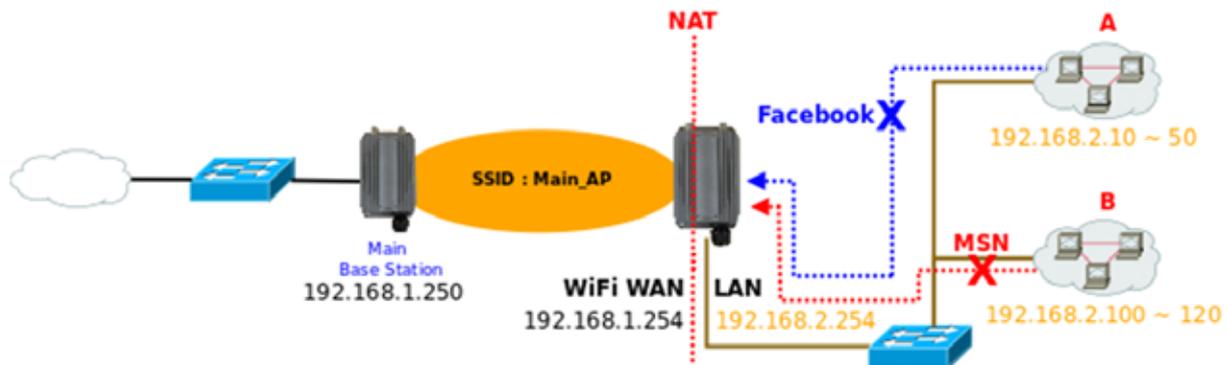
- **MAC Address** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons.

Click **Reboot** button to activate your changes

5.4.3 Parental Control Setup

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.



Please click on **Advance** -> **Parental Control** and follow the below setting.

Parental Control

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

Protocol:

Local Port:

Destination Port:

Active: Enable Disable

Parental Control List

| # | Comment | Active | Delete | Edit |
|----------------------|---------|--------|--------|------|
| | Rule | | | |
| No Rule in the List! | | | | |

- **Rules** : control can be managed by a rule. Use the settings on this screen to establish an access policy.
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click **"Add"** button to add in the MAC group of each rule. Click **"Remove"** button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
 - ➔ **Protocol** : Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **URL Blocking** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application**, the Local(LAN)/ Destination Port can not used.

If you want to block websites with specific URL address or using specific keywords, enter each URL or keywords in the “**URL Blocking**” field and click “**Add**” button to add in the URL Blocking list of each rule. Click “**Remove**” button can remove URL or keywords.

URL Blocking :

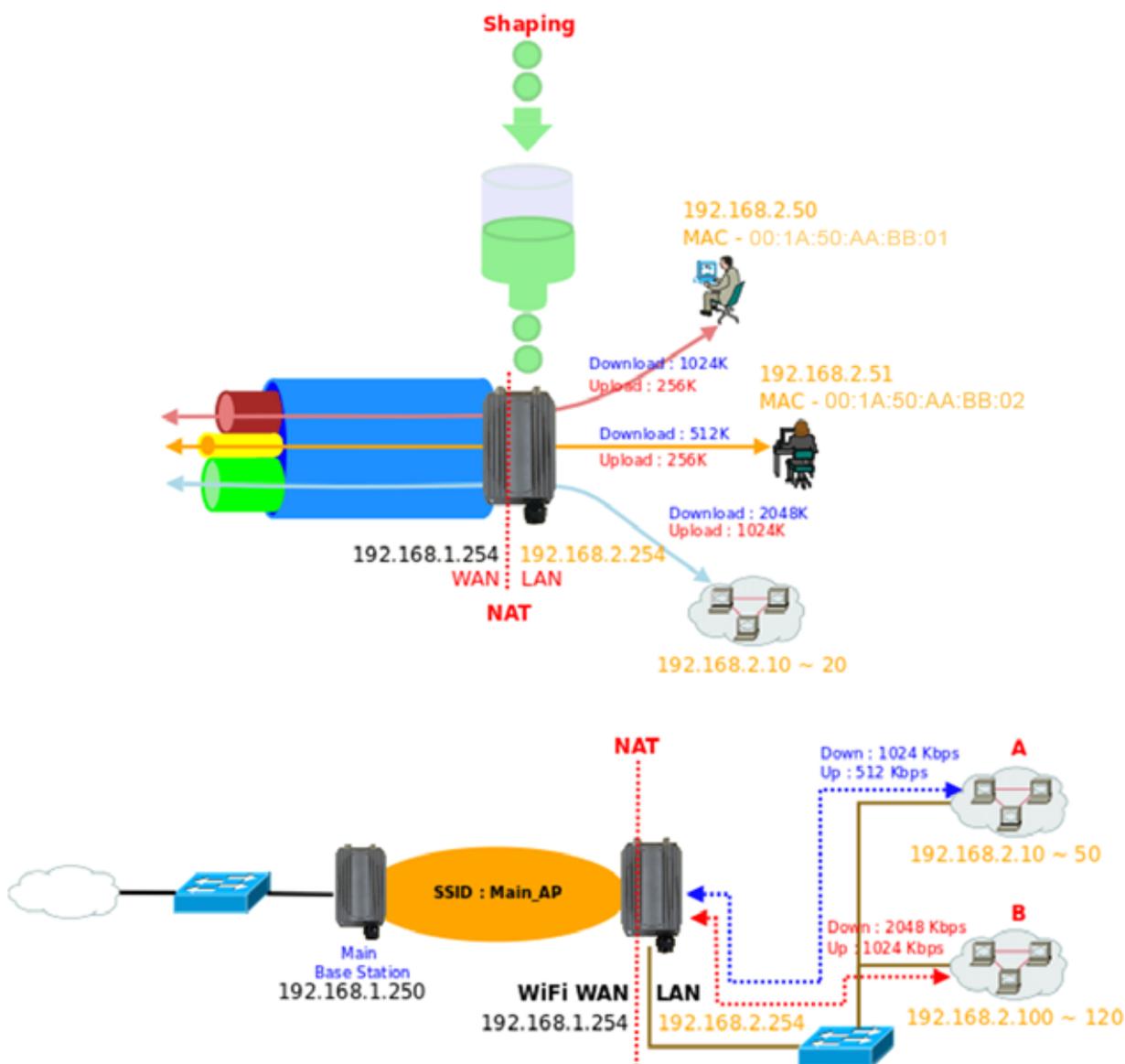
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Active** : Check **Enable** button to activate this rule, and **Disable** to deactivate.

Click “**Add**” button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

5.4.4 QoS Setup

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.



Please click on **Advance** -> **QoS** and follow the below setting.

QoS Setup

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

DSCP Class:

Protocol:

Local Port:

Destination Port:

QoS List

| # | Comment | Remark DSCP | Bandwidth(U/D) | Delete | Edit |
|--------------------------|---------|-------------|----------------|--------|------|
| No QoS Rule in the List! | | | | | |

Action

Remark DSCP:

Bandwidth: Enable Disable

Upload: Kbits

Download: Kbits

- **Rules** : Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click “**Add**” button to add in the MAC group of each rule. Click “**Remove**” button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
 - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list. The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.
 - ✓ **BE** : *Default* PHB, which is typically best-effort traffic
 - ✓ **EF** : *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
 - ✓ **AF** : *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

| DROP Precedence | Class 1 | Class 2 | Class 3 | Class 4 |
|-----------------|---------|---------|---------|---------|
| Low Drop | AF11 | AF21 | AF31 | AF41 |
| Medium Drop | AF12 | AF22 | AF32 | AF42 |
| High Drop | AF13 | AF23 | AF33 | AF43 |

- **Protocol** : Select **Any** or specify protocol(**TCP, UDP, ICMP, Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local/ Destination Port can not used.
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Action** : After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
 - **Remark DSCP** : Specify a new DSCP class, if you want to replace or remark the DSCP
 - **Bandwidth** : Click "**Enable**" to activate function, and click "**Disable**" to deactivate function
 - **Upload / Download** : Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click "**Add**" button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- **Example 1** : On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |
| 2 | | | ANY | ANY | NO | 512/512 |

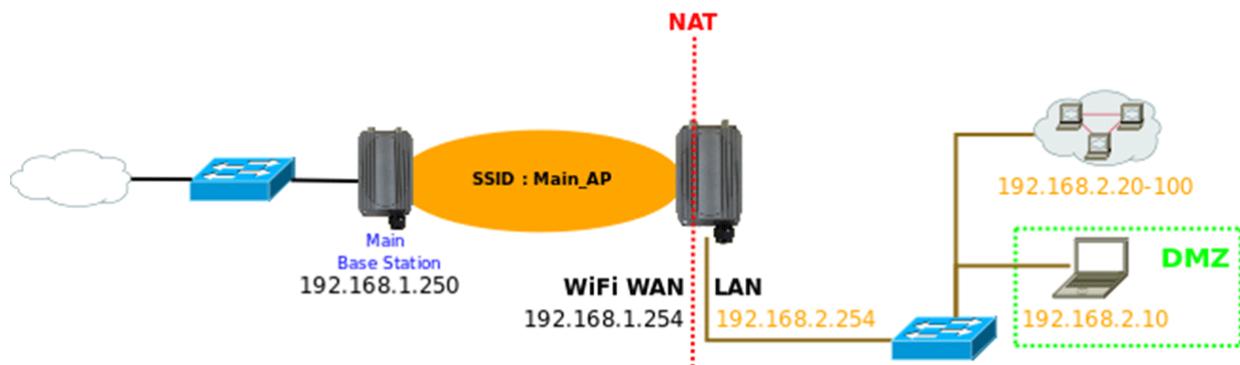
- **Example 2** : On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | | | ANY | ANY | NO | 512/512 |
| 2 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |

5.5 Resource Sharing

5.5.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.



Please click on **Advance** -> **DMZ** and follow the below setting.

DMZ Setup

DMZ

DMZ: Enable Disable

IP Address:

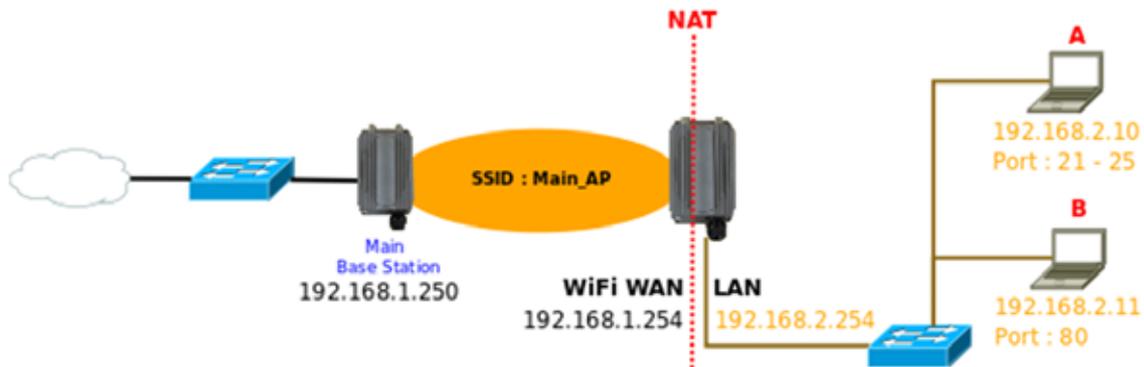
- **DMZ** : By default, it's "**Disable**". Check **Enable** radial button to enable DMZ.
- **IP Address** : Enter IP address of DMZ host and only one DMZ host is supported.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

5.5.2 Virtual Server (Port Forwarding)

“Virtual Server” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



Please click on **Advance** -> **Virtual Server** and follow the below setting.

Virtual Server Setup

Virtual Server

Virtual Server: Enable Disable

Description:

Private IP:

Protocol Type: TCP UDP

Private Port:

Public Port:

Virtual Server List

| # | Status | Description | Protocol | Private IP | Public Port | Private Port | Delete | Edit |
|----------------------|--------|-------------|----------|------------|-------------|--------------|--------|------|
| No Rule in the List! | | | | | | | | |

- **Virtual Server** : By Default, It's "**Disable**". Check **Enable** radial button to enable Virtual Server.
- **Description** : Enter appropriate message for resource sharing via Virtual Server.
- **Private IP** : Enter corresponding IP address of internal resource to share.
- **Protocol Type** : Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80
- **Public Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80



The Private Port and Public Port can be different. However, total number of ports need to be the same. Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click "**Add**" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP **20~80** will be redirected to port TCP **20~80** of **192.168.2.11**

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.10 | 22 | 22 |
| 2 | TCP | 192.168.2.11 | 20:80 | 20:80 |

- **Example 2** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port **20~80** will be redirected to port **20~80** of **192.168.2.11**. The rule 2 won't take effect.

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.11 | 20:80 | 20:80 |
| 2 | TCP | 192.168.2.10 | 22 | 22 |

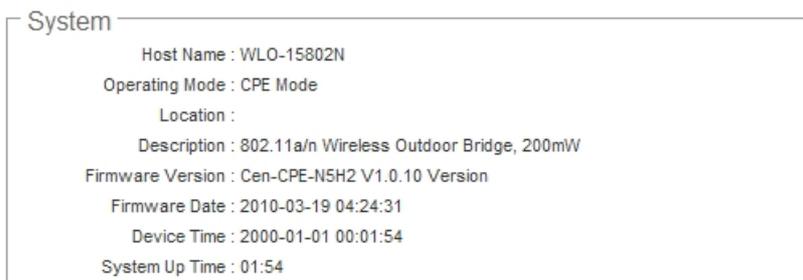
5.6 System Status

This section breaks down into subsections of **System Overview**, **Station Statistics**, **Extra Information** and **Event Log**.

5.6.1 Overview

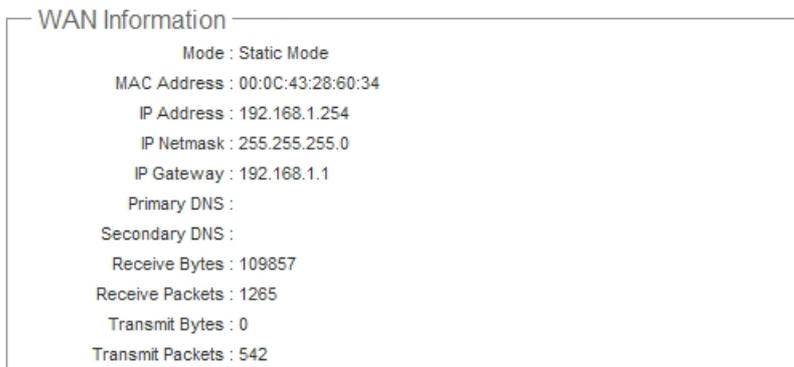
Detailed information on **System**, **WAN Information**, **LAN Information** and **DHCP Server Status** can be reviewed via this page.

- **System** : Display the information of the system.



- **System Name** : The name of the system.
- **Operating Mode** : The mode currently in service.
- **Location** : The reminding note on the geographical location of the system.
- **Description** : The reminding note of the system.
- **Firmware Version** : The current firmware version installed.
- **Firmware Date** : The build time of the firmware installed.
- **Device Time** : The current time of the system.
- **System Up Time** : The time period that system has been in service since last reboot.

- **WAN Information** : Display the information of the WAN interface.



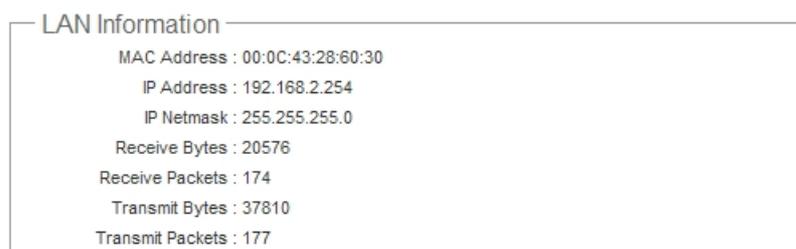
The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.



The WAN port specified **PPPoE** or **PPTP**, and the **Connect** and **DisConnect** button will be show up. Click “**Connect**” button to assigned IP address from PPPoE or PPTP server, “**DisConnect**” button to release IP address of WAN port.



- **Mode** : Supports Static, Dynamic, PPPoE and PPTP modes.
 - **Reconnect Mode** : The current reconnect mode of the PPPoE or PPTP.
 - **MAC Address** : The MAC address of the WAN port.
 - **IP Address** : The IP address of the WAN port.
 - **IP Netmask** : The IP netmask of the WAN port.
 - **IP Gateway** : The gateway IP address of the WAN port.
 - **Primary DNS** : The primary DNS server in service.
 - **Secondary DNS** : The secondary DNS server in service.
 - **Receive bytes** : The total received packets in bytes on the WAN port.
 - **Receive packets** : The total received packets of the WAN port.
 - **Transmit bytes** : The total transmitted packets in bytes of the WAN port.
 - **Transmit packets** : The total transmitted packets of the WAN port.
- **LAN Information** : Display total received and transmitted statistics on the LAN interface.



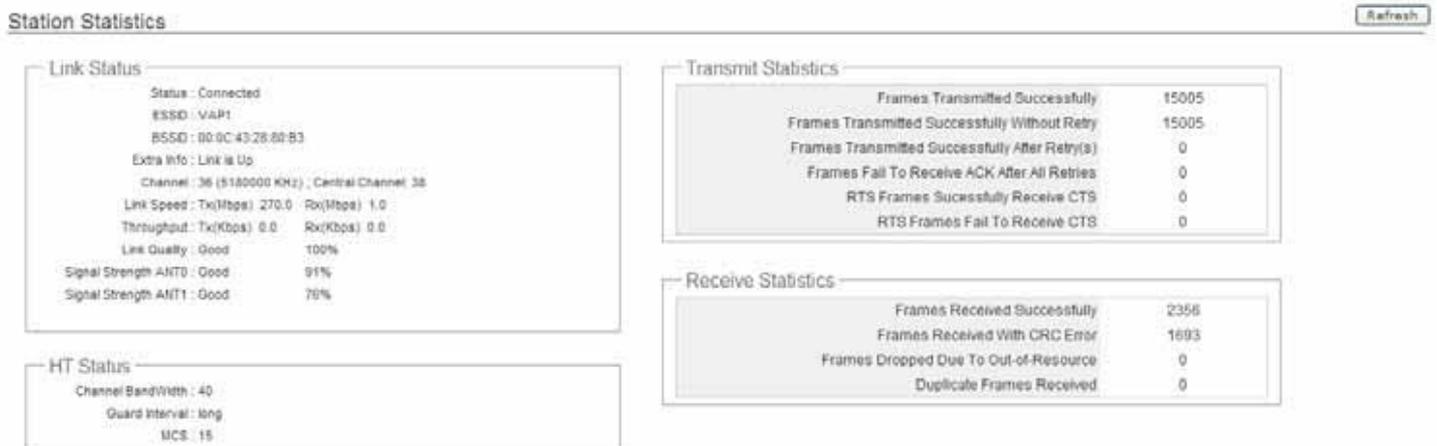
- **MAC Address** : The MAC address of the LAN port.
 - **IP Address** : The IP address of the LAN port.
 - **IP Netmask** : The IP netmask of the LAN port.
 - **Receive bytes** : The total received packets in bytes on the LAN port.
 - **Receive packets** : The total received packets of the LAN port.
 - **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
 - **Transmit packets** : The total transmitted packets of the LAN port.
- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.

| DHCP Server Status | | |
|-------------------------|-------------|------------|
| DHCP : Enable | | |
| Start IP : 192.168.2.10 | | |
| End IP : 192.168.2.70 | | |
| DNS1 IP : 192.168.2.1 | | |
| DNS2 IP : | | |
| WINS IP : | | |
| Domain : | | |
| Lease Time : 86400 | | |
| IP Address | MAC Address | Expired In |
| | none | |

- **IP Address** : IP addresses to LAN devices by DHCP server.
- **MAC Address** : MAC addresses of LAN devices.
- **Expired In** : Shows how long the leased IP address will expire.

5.6.2 Station Statistics

Link information, Transmit and Receive Statistics for the connection with AP, Below depicts an example for Station Statistics.



■ Link Status :

- ➔ **Status** : Shows the current link status. It should be “**Connected**” or “**Disconnected**”.
- ➔ **ESSID** : Shows the current SSID, which must be the same on the wireless client and AP in order for communication to be established.
- ➔ **BSSID** : Shows the associated BSSID, which can be used to identify the wireless access point.
- ➔ **Extra Info** : Shows the current link status of extra information. It should be “**Link is Up**” or “**Link is Down**”.
- ➔ **Channel** : Shows current channel and central channel, its corresponding frequency.
- ➔ **Link Speed(Mbps)** : The data transfer speed adopted by this network. (measured in Mbits per second)
- ➔ **Link Quality** : Shows the link quality of the system with an access point.
- ➔ **Signal Strength ANT0/ANT1** : Shows the wireless signal strength of the connection between system and an access point.

■ HT Status :

- ➔ **Channel BandWidth** : Shows the current channel bandwidth used for communication. It should be “**20**” or “**40**”
- ➔ **Guard Interval** : Shows the current GI used for communication. It should be “**short**” or “**long**”.
- ➔ **MCS** : Shows the current GI used for communication. It should be between **0** to **15** or **32**.

■ Transmit Statistics

- ➔ **Frames Transmitted Successfully**: The number of successfully transmitted frames.
- ➔ **Frames Transmitted Successfully Without Retry**: The number of successfully transmitted frames without any retry.
- ➔ **Frames Transmitted Successfully After Retry(s)**: The number of successfully transmitted frames with one or more retries.

- **Frames Fail To Receive ACK After All Retries:** The number of unsuccessfully transmitted frame with many retries.
 - **RTS Frames Successfully Receive CTS:** The number of successful received CTS (Clear To Send) response after this WLO-15814N / WLO-15802N sends out the RTS (Request To Send) message.
 - **RTS Frames Fail To Receive CTS:** The number of unsuccessful received CTS response after this WLO-15814N / WLO-15802N sends out the RTS message.
- **Receive Statistics**
- **Frames Received Successfully:** The number of successful received frames.
 - **Frames Received With CRC Error:** The number of received frames with CRC (Cyclical Redundancy Checking) error.
 - **Frames Dropped Due To Out-of-Resource:** The number of dropped frames.
 - **Duplicate Frames Received:** The number of duplicate frames.

5.6.3 Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
Information: Netstat Information

Netstat Information

| Protocol | LiveTime | Status | SrcIP | SrcPort | DstIP | DstPort |
|----------|----------|-------------|--------------|---------|---------------|---------|
| tcp | 119 | TIME_WAIT | 192.168.2.22 | 3423 | 192.168.2.254 | 80 |
| tcp | 113 | TIME_WAIT | 192.168.2.22 | 3419 | 192.168.2.254 | 80 |
| udp | 5 | | 192.168.2.22 | 138 | 192.168.2.255 | 138 |
| tcp | 118 | TIME_WAIT | 192.168.2.22 | 3421 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3413 | 192.168.2.254 | 80 |
| tcp | 431999 | ESTABLISHED | 192.168.2.22 | 3425 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3415 | 192.168.2.254 | 80 |
| tcp | 91 | TIME_WAIT | 192.168.2.22 | 3417 | 192.168.2.254 | 80 |

- **Netstat Information** : Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status*, *Source/Destination IP address* and *Port*.

- **Route table information** : Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

Route Information

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | ra0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.1.1 | 0.0.0.0 | UG | 0 | 0 | 0 | ra0 |

- **ARP table Information** : Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

ARP Table Information

| IP Address | HW Type | Flags | HW Address | Mask | Device |
|--------------|---------|-------|-------------------|------|--------|
| 192.168.2.22 | 0x1 | 0x2 | 00:1A:92:9F:A4:9B | * | bre0 |

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces.

Bridge Table Information

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-----------|
| bre0 | 8000.000c43288008 | no | eth2 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

Bridge MACs Information

| Port No | MAC Address | Local | Ageing Timer |
|---------|-------------------|-------|--------------|
| 1 | 00:0c:43:28:80:08 | yes | 0.00 |
| 1 | 00:1a:92:9f:a4:9b | no | 0.04 |

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

Bridge STP Information

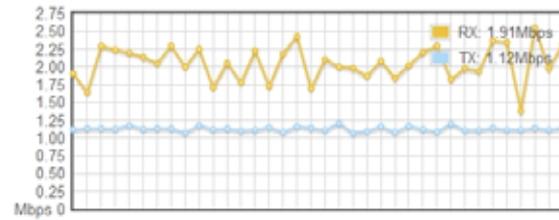
| | | | |
|-----------------------|-------------------|----------------------|------------|
| bre0 | | | |
| bridge id | 8000.000c43288008 | | |
| designated root | 8000.000c43288008 | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 1.93 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 3.92 |
| flags | | | |
| eth2 (1) | | | |
| port id | 8001 | state | forwarding |
| designated root | 8000.000c43288008 | path cost | 100 |
| designated bridge | 8000.000c43288008 | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |

5.6.4 QoS Plot

The QoS Plot show graphs which continuously represents the current data traffic on each QoS rule. The chart scale and throughput dimension (bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically every **5** seconds. The throughput statistics of QoS can be updated manually using the **Refresh** button.

QoS Plot

| QoS List | | | |
|----------|---------|-------------|--------------------|
| # | Comment | Remark DSCP | Bandwidth(U/D)kbps |
| 1 | FTP | NO | 1024/2048 |



5.6.5 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|---|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 6. CPE + AP Mode Configuration

When CPE+AP mode is chosen, the system can be configured as a Customer Premises Equipment(CPE). This section provides detailed explanation for users to configure in the CPE+AP mode with help of illustrations. In the CPE+AP mode, functions listed in the table below are also available from the Web-based GUI interface.

| OPTION | System | Wireless | Advance | Utilities | Status |
|-----------|----------------|-------------------|------------------|-------------------|--------------------|
| Functions | Operating Mode | General Setup | DMZ | Profiles Settings | System Overview |
| | WAN | Advanced Setup | IP Filter | Firmware Upgrade | Station Statistics |
| | LAN | Repeater AP Setup | MAC Filter | Network Utility | Extra Info |
| | DDNS | Wireless Profile | Virtual Server | Reboot | QoS Plot |
| | Management | Site Survey | Parental Control | | Event Log |
| | Time Server | | QoS | | |
| | UPNP | | | | |
| | SNMP | | | | |

Table 6-1: CPE+AP Mode Functions

6.1 External Network Connection

6.1.1 Network Requirement

It can be used as an Outdoor Customer Premises Equipment (CPE) to receive and repeat wireless signal over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers. In the CPE+AP mode, WLO-15814N / WLO-15802N is a gateway enabled with NAT and DHCP Server functions. The wired and wireless clients connected to WLO-15814N / WLO-15802N are in **different** subnet from those connected to Main Base Station, and, in CPE+AP mode, it **accepts** wireless connections from wireless client devices.

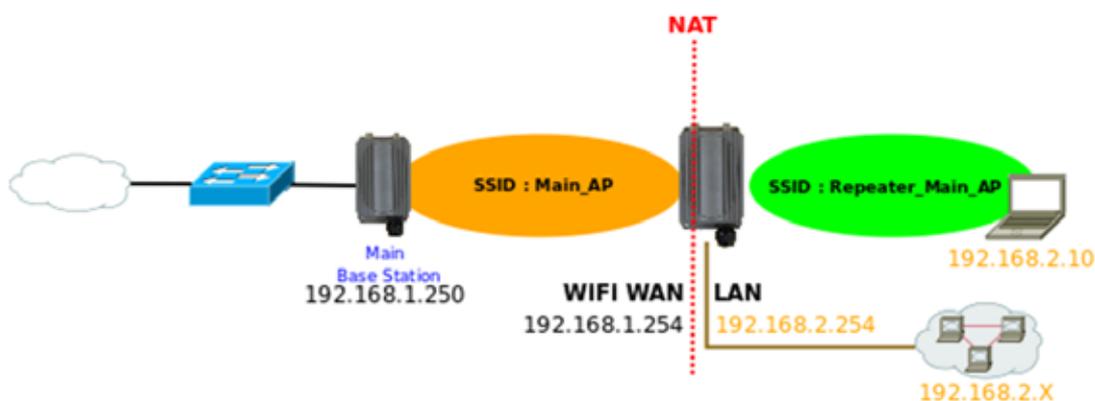


Figure 6-1 CPE+AP mode network configuration



When the WLO-15814N / WLO-15802N configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between WLO-15814N / WLO-15802N to Main Base Station and wireless client to WLO-15814N / WLO-15802N, but security type can be different.

6.1.2 Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**,

Please click on **System -> WAN** and follow the below setting.

 *In CPE mode, the WAN Port is the Wireless interface.*

- **Mode** : By default, it's "**Static IP**". Check "Static IP", "Dynamic IP", "PPPoE" or "PPTP" to set up system WAN IP.
 - ➔ **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.
 - ✓ **IP Address** : The IP address of the WAN port; default IP address is 192.168.1.254
 - ✓ **IP Netmask** : The Subnet mask of the WAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the WAN port; default Gateway is 192.168.1.1
 - ➔ **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click **Release** button to release IP address and click **Renew**

button to renew IP address again.

- ✓ **Hostname** : The Hostname of the WAN port

- ➔ **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.

- ✓ **User Name** : Enter User Name for PPPoE connection
- ✓ **Password** : Enter Password for PPPoE connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
 - ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
 - ✓ **MTU** : By default, it’s **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ➔ **PPTP** : The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

PPTP

IP Address :

IP Netmask :

PPTP Server IP Address :

User name :

Password :

Reconnect Mode : Always On On Demand Manual

Idle Time : minutes

MTU :

MPPE Encryption : MPPE-40 MPPE-128

- ✓ **IP Address** : The IP address of the WAN port
- ✓ **IP Netmask** : The Subnet mask of the WAN port
- ✓ **PPTP Server IP Address** : The IP address of the PPTP server
- ✓ **User Name** : Enter User Name for PPTP connection
- ✓ **Password** : Enter Password for PPTP connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “**0**”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
- ✓ **MTU** : By default, it’s **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ✓ **MPPE Encryption** : Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
- **DNS** : Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.



In this mode, the system does not support MAC Clone function.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.3 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

Please click on **System -> DDNS Setup** and follow the below setting.

Dynamic DNS Setup

DDNS

Enable: Enable Disable

Service Provider:

Hostname: .

User Name:

Password:

- **Enabled:** By default, it's "**Disable**". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.1.4 Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System** -> **LAN** and follow the below setting.

LAN Setup

- **LAN IP** : The administrator can manually setup the LAN IP address.
 - ➔ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ➔ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

- ➔ **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- ➔ **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain** : Enter the domain name for this network.
- ➔ **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.2 Access Point Association

6.2.1 Configure Wireless General Setting

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

The screenshot shows the 'Wireless Setup' configuration interface. It is organized into three main panels:

- General Setup:**
 - Band Mode: 802.11 a/n mixed mode (dropdown)
 - Country: NONE (dropdown)
 - Tx Power: 100 % (input field)
- HT Other:**
 - HT TxStream: 2 (dropdown)
 - HT RxStream: 2 (dropdown)
- HT Physical Mode:**
 - Operating Mode: Mixed Mode, Green Field
 - Channel BandWidth: 20, 20/40
 - Guard Interval: Long, Auto
 - MCS: Auto (dropdown)
 - Reverse Direction Grant (RDG): Disable, Enable
 - A-MSDU: Disable, Enable
 - Auto Block ACK: Disable, Enable
 - Decline BA Request: Disable, Enable

A 'Save' button is located at the bottom center of the HT Physical Mode panel.

- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54** Mbps for **802.11a**
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between **1** to **100** (the unit is %) for your environment. If you are not sure of which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput) Physical Mode** and **11n Configuration** settings should be hidden immediately.

- **Operating Mode** : By default, it's Mixed Mode.
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "**Auto**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **MPDU Enable** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **A-MPDU** : A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select "Manual" to set "MPDU Density"
- **MPDU Density** : Minimum separation of MPDUs in an A-MPDU.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------------|------|------|------|------|------|------|-------|
| No Restriction | ¼ µs | ½ µs | 1 µs | 2 µs | 4 µs | 8 µs | 16 µs |

- **A-MSDU** : Aggregated Mac Service Data Unit, A-MSDU. Select **Enable** to allows aggregation for multiple MSDUs in one MPDU. Default is disabled.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Short Slot : Enable Disable

Extra Slot Time : us

ACK Timeout : us

Beacon Interval : ms

DTIM Interval : ms

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

Pkt_Aggregate : Enable Disable

IEEE 802.11H(DFS) : Enable Disable

WMM : Enable Disable

Save

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time** : Slot time is in the range of **1~255** and set in unit of **microsecond**. The default value is **9** microsecond.



When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout** : ACK timeout is in the range of **1~255** and set in unit of *microsecond*. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.
- **RTS Threshold** : TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble** : By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
- **Pkt_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.
- **IEEE802.11H (DFS)** : By default, it's "**Enable**". To **Disable** is to deactivate IEEE802.11H(DFS)

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

| | |
|---------------------|--|
| DFS Channels | 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140 |
|---------------------|--|

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.



*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When WLO-15814N / WLO-15802N detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

| WMM Parameters of Access Point | | | | | | |
|--------------------------------|-------|-------|-------|------|--------------------------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
| AC_BE | 3 | 15 | 63 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VI | 1 | 7 | 15 | 94 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VO | 1 | 3 | 7 | 47 | <input type="checkbox"/> | <input type="checkbox"/> |

| WMM Parameters of Station | | | | | |
|---------------------------|-------|-------|-------|------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM |
| AC_BE | 3 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_VI | 2 | 7 | 15 | 94 | <input type="checkbox"/> |
| AC_VO | 2 | 3 | 7 | 47 | <input type="checkbox"/> |



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

WMM Parameters of Access Point : This affects traffic flowing from the access point to the client station

| Queue | Data Transmitted AP to Clients | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : This affects traffic flowing from the client station to the access point.

| Queue | Data Transmitted Clients to AP | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is

the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".

- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **Repeater AP**.

6.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.

Station Site Survey

| Scan Result | | | | | | | |
|-------------|-------------------|--------|---------|--------------|-------|----------------|------------------------|
| ESSID | MAC Address | Signal | Channel | Security | Band | Network Type | Select |
| Main_AP | 00:1A:50:0A:7C:3A | 50% | 44 | NONE | 11a/n | Infrastructure | Select |
| Main_AP-253 | 00:1A:50:0A:7B:F2 | 100% | 44 | NONE | 11a/n | Infrastructure | Select |
| 253AP1 | 00:1A:50:0A:7B:F3 | 100% | 44 | WEP | 11a/n | Infrastructure | Select |
| 253AP2 | 00:1A:50:0A:7B:F4 | 100% | 44 | WPAPSK/AES | 11a/n | Infrastructure | Select |
| 253AP3 | 00:1A:50:0A:7B:F5 | 100% | 44 | WPAPSK/TKIP | 11a/n | Infrastructure | Select |
| 253AP4 | 00:1A:50:0A:7B:F6 | 100% | 44 | WPA2PSK/AES | 11a/n | Infrastructure | Select |
| 253AP5 | 00:1A:50:0A:7B:F7 | 100% | 44 | WPA2PSK/TKIP | 11a/n | Infrastructure | Select |

- **ESSID** : Available Extend Service Set ID of surrounding Access Points.
- **MAC Address** : MAC addresses of surrounding Access Points.
- **Signal** : Received signal strength of all found Access Points.
- **Channel** : Channel numbers used by all found Access Points.
- **Security** : Security type by all found Access Points.
- **Band** : Wireless band used by all found Access Points.
- **Network Type** : Network type used by all found Access Points.
- **Select** : Click "**Select**" to configure settings and associate with chosen AP.



While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless Profile Setup. However, more settings are needed including Security Key.

6.2.4 Create Wireless Profile

The administrator can configure station profiles via this page.

Please click on **Wireless -> Wireless Profile** and follow the below setting.

Station Profile

- **MAC Address** : The MAC address of the Wireless Station is displayed here.
 - **Profile Name** : Set different profiles for quick connection uses.
 - **ESSID** : Assign Service Set ID for the wireless system.
 - **Lock to AP MAC** : This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.
 - **Channel/Frequency** : Select the desired channel range.
 - **Security Type** : Select the desired security type from the drop-down list; the options are "NONE" "OPEN", "SHARED", "WPA-PSK" and "WPA2-PSK".
- ➔ **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.

- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

WPA

Cipher Suite :

Pre-shared Key :

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**
 - ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.
- **Profile List** : The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List

Profile List

| Active | # | Profile Name | ESSID | MAC Address | Channel | Security Type | Delete | Edit |
|----------------------------------|---|--------------|---------|-------------------|---------|---------------|------------------------|----------------------|
| <input type="radio"/> | 1 | AP_Profile0 | default | | 44 | NONE | Delete | Edit |
| <input checked="" type="radio"/> | 2 | Profile-Test | 253AP1 | 00:1A:50:0A:7B:F3 | 44 | OPEN | Delete | Edit |

- ➔ Click “**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.
- ➔ Click “**Delete**” to remove profile.
- ➔ Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting. After clicking “Connect” button, you can verify connecting status on Remote AP Page



*If tuen on IEEE802.11H and WLO-15814N / WLO-15802N connect AP with DFS channel 52-150, WLO-15814N / WLO-15802N Will have **60** sec to do channel available check, and will not send beacon and can not be connect.*

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.3 Wireless LAN Network Creation

The network manager can configure related wireless settings, **Repeater AP Setup**, **Security Settings**, and **MAC Filter Settings**.

6.3.1 Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.

Repeater AP Setup

- **Enable Repeater AP** : By default, it's "**Enable**" for repeater AP. Select "**Enable**" to activate Repeater AP or click "**Disable**" to deactivate this function
- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified AP.
- **Client Isolation** : By default, it's "**Disable**".
Select "**Enable**", all clients will be isolated from each other, which means they can't reach each other.
- **Hidden SSID** : By default, it's "**Disable**".
Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP's clients could make to associate to it.
- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this Repeater AP.
- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
 - ➔ **Disable** : Data are unencrypted during transmission when this option is selected.
 - ➔ **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

WEP

Authentication Type : OPEN SHARED WEPAUTO

Key Index : 1

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- ✓ **Authentication Method** : Enable the desired option among **OPEN**, **SHARED** or **WEPAUTO**.
- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

WPA General

Cipher Suite : AES

Pre-shared Key :

Group Key Update Period : 3600 seconds

- ✓ **Cipher Suite** : By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.



Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period** : By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- ➔ **WPA-Enterprise (or WPA2-Enterprise)**: The RADIUS authentication and encryption will be both enabled if this is selected.

WPA General

Cipher Suite : ▼

Group Key Update Period : seconds

PMK Cache Period : minute

Pre-Authentication : Disable Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.



PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X** : When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

The screenshot displays two configuration panels. The top panel, titled "802.1x WEP", contains a single text field with the value "Dynamic WEP : Enable". The bottom panel, titled "Authentication RADIUS Server", contains four text fields: "Authentication Server" (empty), "Port" (containing "1812"), "Shared Secret" (empty), and "Session Timeout" (containing "0").

✓ **Radius Server Settings :**

- **IP Address** : Enter the IP address of the Authentication RADIUS server.
- **Port** : By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret** : A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout** : The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.3.2 Wireless MAC Filter Setup

Continue **6.3.1 Repeater AP Setup** section, the administrator can allow or reject clients to access Repeater AP.

- **MAC Filter Setup** : By default, it's "**Disable**". Options are **Disable**, **Only Deny List MAC** or **Only Allow List MAC**.

Two ways to set MAC filter rules :

→ **Only Allow List MAC.**

The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

→ **Only Deny List MAC.**

The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Click **Reboot** button to activate your changes



MAC Access Control is the weakest security approach. WPA or WPA2 security method is highly recommended.

6.4 System Management

6.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

The screenshot shows the Management Setup configuration page with the following fields and options:

- System Information:**
 - System Name: WLO-15802N
 - Description: 802.11a/n Wireless Outdoor Bridge, 20
 - Location: (empty field)
- Root Password:**
 - New Root Password: (empty field)
 - Check Root Password: (empty field)
- Admin Password:**
 - New Admin Password: (empty field)
 - Check New Password: (empty field)
- Admin Login Methods:**
 - Enable HTTP: Port: 80
 - Enable HTTPS: Port: 443
 - Enable Telnet: Port: 23
 - Enable SSH: Port: 22
 - Host Key Fingerprint: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgwi
- Ping Watchdog:**
 - Ping Watchdog: Enable Disable
 - IP Address To Ping: (empty field)
 - Ping Interval: 300 Seconds
 - Startup Delay: 300 Seconds
 - Failure Count To Reboot: 3

A button is located at the bottom center of the form.

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - **Enable HTTP** : Check to select HTTP Service.
 - **HTTP Port** : The default is 80 and the range is between 1 ~ 65535.
 - **Enable HTTPS** : Check to select HTTPS Service
 - **HTTPS Port** : The default is 443 and the range is between 1 ~ 65535.



If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.

- **Enable Telnet** : Check to select Telnet Service
- **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- **Enable SSH** : Check to select SSH Service
- **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.

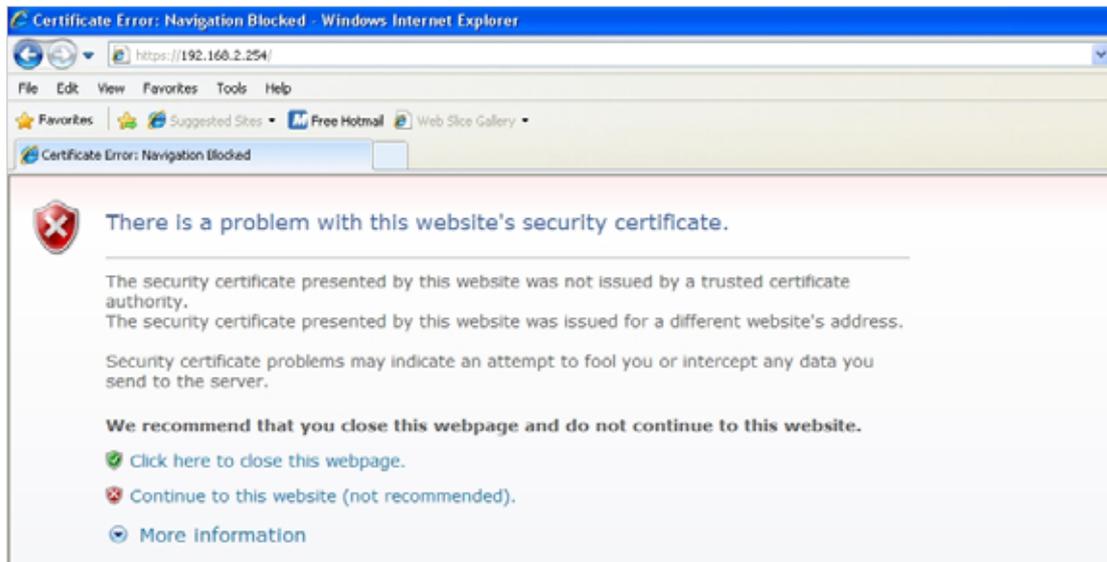
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

- **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
- **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
- **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254/>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

6.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

- **Local Time** : Display the current system time.

- **NTP Client** : To synchronize the system time with NTP server.
 - ➔ **Enable** : Check to select NTP client.
 - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
 - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
 - ➔ **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

6.4.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

UPNP Setup

UPNP

UPNP: Enable Disable

Save

- **UPnP** : By default, it's "**Disable**". Select "**Enable**" or "**Disable**" of UPnP Service.

Click **Save** button to save changes and click **Reboot** button to activate changes

For UPnP to work in Windows XP, the "WLO-15814N / WLO-15802N" must be available in "**My Network Places**", as shown here: (your specific model may vary)



If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to **Appendix E. Using UPnP on Windows XP**

6.4.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable:** Check to enable SNMP v2c.

- **ro community :** Set a community string to authorize read-only access.
- **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

- **SNMP ro user :** Set a community string to authorize read-only access.
- **SNMP ro password :** Set a password to authorize read-only access.
- **SNMP rw user :** Set a community string to authorize read/write access.
- **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

SNMP Trap

Enable :

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

6.4.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

Profile Save

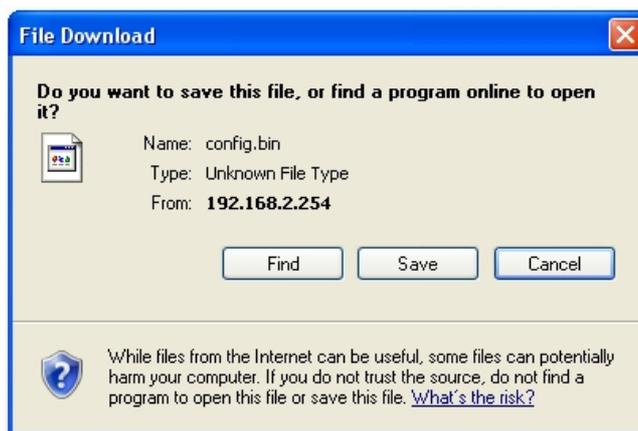
Save Settings To PC :

Load Settings From PC :

Reset To Factory Default :

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

6.4.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27
Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding.
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

6.4.7 Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting

Network Utility

Ping

Destination IP/Domain: Count:

Traceroute

Destination Host: MAX Hop:

Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.

 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test

 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

6.4.8 Reboot

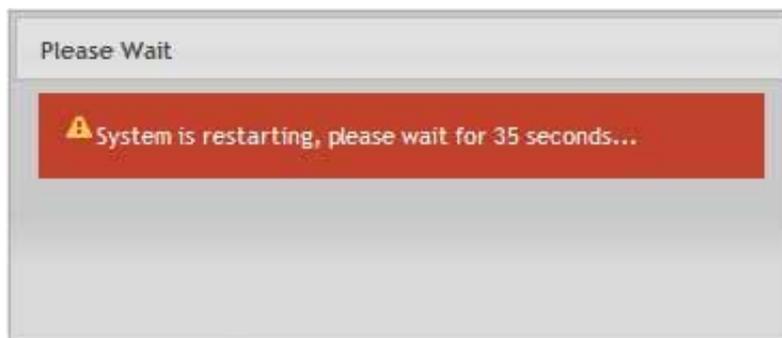
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

Reboot

 You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Reboot

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

6.5 Access Control List

6.5.1 IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.

IP Filter Setup

IP Rules

Source Address/Mask:

Source Port:

Destination Address/Mask:

Destination Port:

In/Out: In Out

Protocol: TCP UDP ICMP

Listen: Yes No

Action: Deny Pass

Interface: LAN WAN Both

IP Filter List

| # | Source Address/Mask | Port | Destination Address/Mask | Port | In/Out | Protocol | Listen | Action | Interface | Delete | Edit |
|-------------------------|---------------------|------|--------------------------|------|--------|----------|--------|--------|-----------|--------|------|
| No IP Rule in the List! | | | | | | | | | | | |

- **Source Address/Mask** : Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **Destination Address/Mask** : Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **In/Out** : Applies to Ingress or egress packets
- **Protocol** : Supports **TCP**, **UDP** or **ICMP**.
- **Listen** : Click **Yes** radial button to match TCP packets only with the SYN flag.
- **Active** : **Deny** to drop and **Pass** to allow per filter rules
- **Interface** : The interface that a filter rule applies



All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

- **Example 1** : Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | Pass | LAN |
| 2 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |

- **Example 2** : All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |
| 2 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | pass | LAN |

6.5.2 MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.

MAC Filter Setup

The screenshot shows two main sections: 'MAC Rules' and 'MAC Filter List'.
 In the 'MAC Rules' section, there is a dropdown menu for 'Action' currently set to 'Disabled', a 'Save' button, and a text input field for 'MAC Address' with an 'Add' button.
 In the 'MAC Filter List' section, there is a table with the following structure:

| # | MAC Address | Delete | # | MAC Address | Delete |
|--------------------------|-------------|--------|---|-------------|--------|
| No MAC Rule in the List! | | | | | |

- **MAC Filter Rule** : By default, it's "**Disable**". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click **Save** button to save your change.

Two ways to set the MAC Filter List:

➔ **Only Allow List MAC.**

The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

➔ **Only Deny List MAC.**

The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

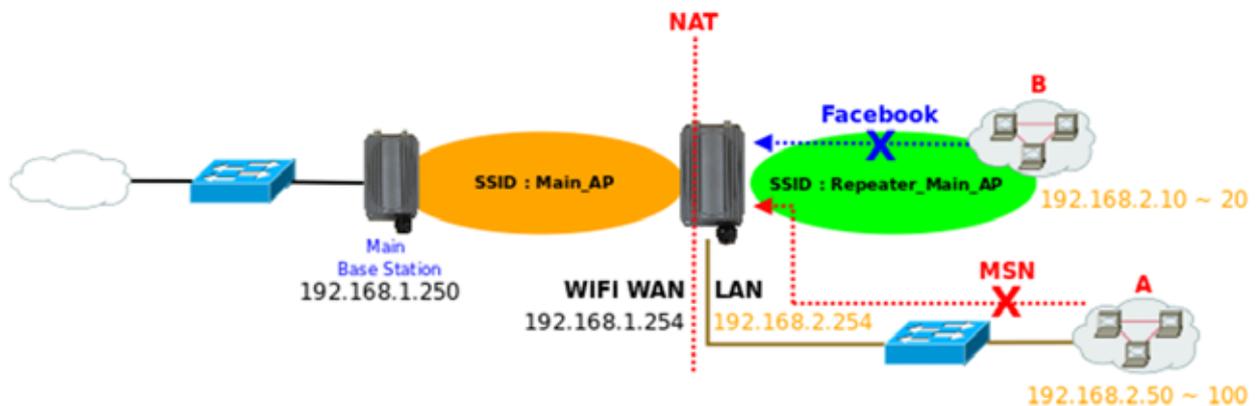
- **MAC Address** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons.

Click **Reboot** button to activate your changes

6.5.3 Parental Control Setup

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.



Please click on **Advance -> Parental Control** and follow the below setting.

Parental Control

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

Protocol:

Local Port:

Destination Port:

Active: Enable Disable

Parental Control List

| # | Comment | Active | Delete | Edit |
|----------------------|---------|--------|--------|------|
| No Rule in the List! | | | | |

- **Rules** : control can be managed by a rule. Use the settings on this screen to establish an access policy.
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click **"Add"** button to add in the MAC group of each rule. Click **"Remove"** button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.

→ **Protocol** : Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **URL Blocking** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local(LAN)/ Destination Port can not used.

If you want to block websites with specific URL address or using specific keywords, enter each URL or keywords in the “**URL Blocking**” field and click “**Add**” button to add in the URL Blocking list of each rule. Click “**Remove**” button can remove URL or keywords.

URL Blocking :

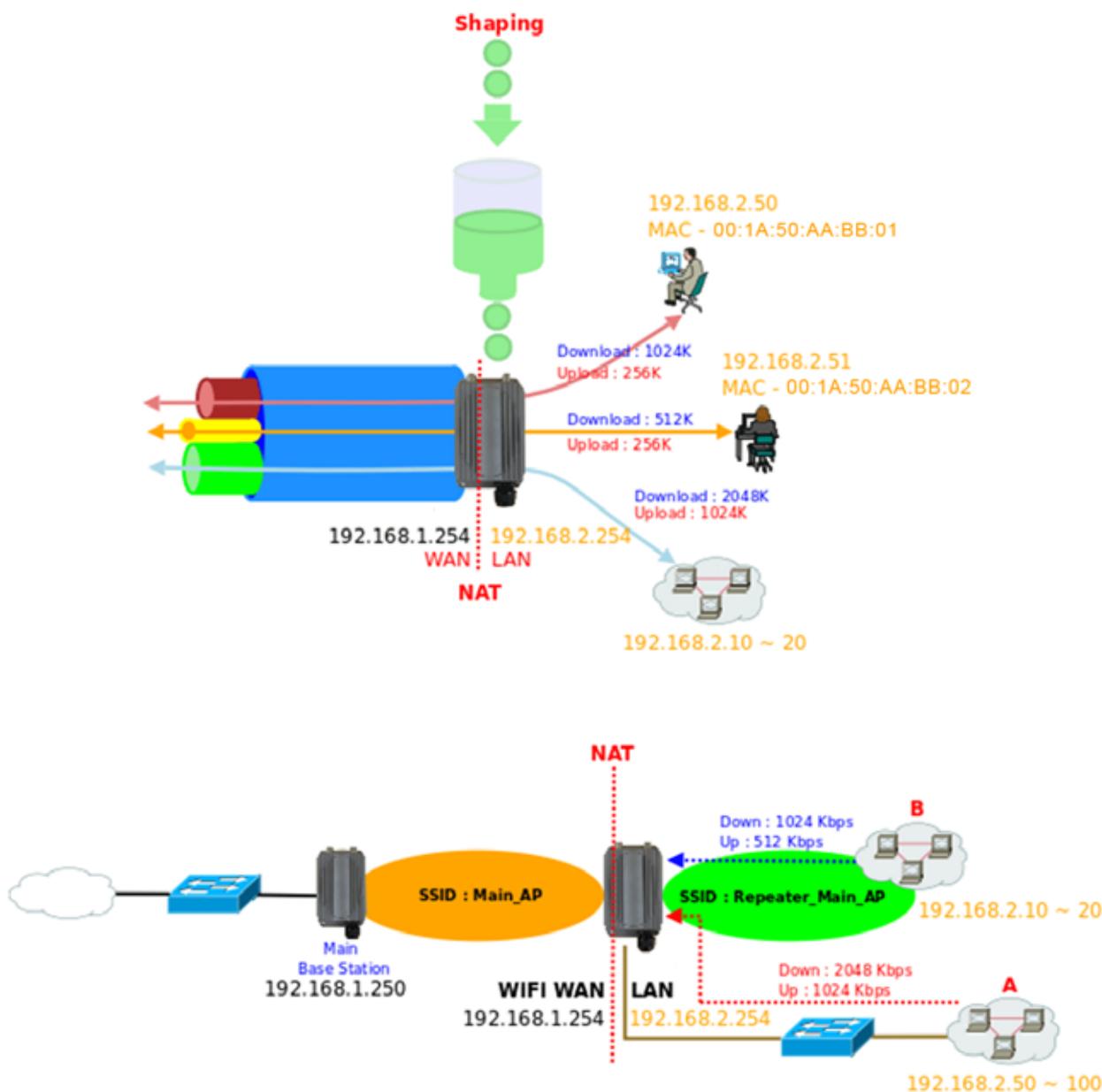
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Active** : Check **Enable** button to activate this rule, and **Disable** to deactivate.

Click “**Add**” button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

6.5.4 QoS Setup

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.



Please click on **Advance** -> **QoS** and follow the below setting.

QoS Setup

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

DSCP Class:

Protocol:

Local Port:

Destination Port:

QoS List

| # | Comment | Remark DSCP | Bandwidth(U/D) | Delete | Edit |
|--------------------------|---------|-------------|----------------|--------|------|
| No QoS Rule in the List! | | | | | |

Action

Remark DSCP:

Bandwidth: Enable Disable

Upload: Kbits

Download: Kbits

- **Rules** : Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click “**Add**” button to add in the MAC group of each rule. Click “**Remove**” button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
 - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list. The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.
 - ✓ **BE** : *Default* PHB, which is typically best-effort traffic
 - ✓ **EF** : *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
 - ✓ **AF** : *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

| DROP Precedence | Class 1 | Class 2 | Class 3 | Class 4 |
|-----------------|---------|---------|---------|---------|
| Low Drop | AF11 | AF21 | AF31 | AF41 |
| Medium Drop | AF12 | AF22 | AF32 | AF42 |
| High Drop | AF13 | AF23 | AF33 | AF43 |

- **Protocol** : Select **Any** or specify protocol from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Source/ Destination Port can not used.
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Action** : After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
 - **Remark DSCP** : Specify a new DSCP class, if you want to replace or remark the DSCP
 - **Bandwidth** : Click "**Enable**" to activate function, and click "**Disable**" to deactivate function
 - **Upload / Download** : Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click "**Add**" button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- **Example 1** : On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |
| 2 | | | ANY | ANY | NO | 512/512 |

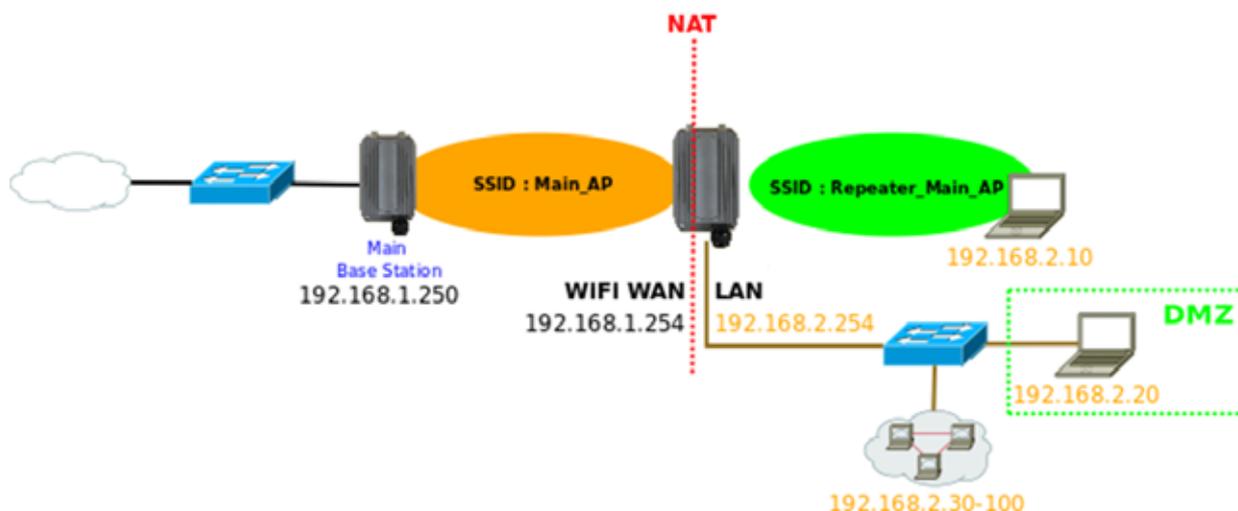
- **Example 2** : On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | | | ANY | ANY | NO | 512/512 |
| 2 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |

6.6 Resource Sharing

6.6.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.



Please click on **Advance** -> **DMZ** and follow the below setting.

DMZ Setup

DMZ

DMZ : Enable Disable

IP Address :

Save

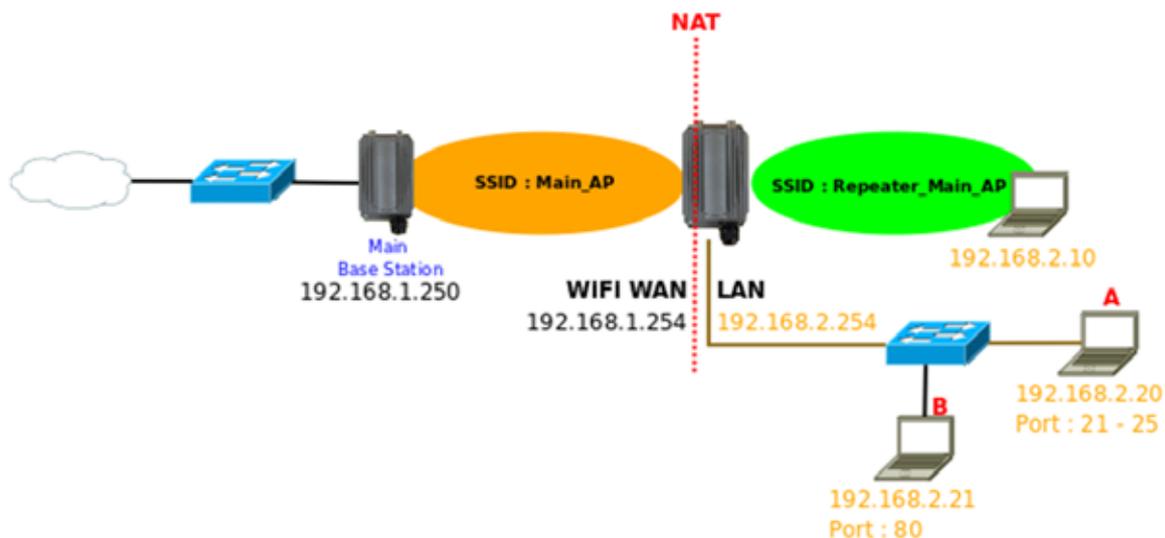
- **DMZ** : By default, it's "**Disable**". Check **Enable** radial button to enable DMZ.
- **IP Address** : Enter IP address of DMZ host and only one DMZ host is supported.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

6.6.2 Virtual Server (Port Forwarding)

“Virtual Server” can also be referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



Please click on **Advance** -> **Virtual Server** and follow the below setting.

Virtual Server Setup

Virtual Server

Virtual Server: Enable Disable

Description:

Private IP:

Protocol Type: TCP UDP

Private Port:

Public Port:

Virtual Server List

| # | Status | Description | Protocol | Private IP | Public Port | Private Port | Delete | Edit |
|---------------------|--------|-------------|----------|------------|-------------|--------------|--------|------|
| No Rule in the List | | | | | | | | |

- **Virtual Server** : By Default, It's "**Disable**". Check **Enable** radial button to enable Virtual Server.
- **Description** : Enter appropriate message for resource sharing via Virtual Server.
- **Private IP** : Enter corresponding IP address of internal resource to share.
- **Protocol Type** : Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80
- **Public Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80



The Private Port and Public Port can be different. However, total number of ports need to be the same.
Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click "**Add**" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP **20~80** will be redirected to port TCP **20~80** of **192.168.2.11**

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.10 | 22 | 22 |
| 2 | TCP | 192.168.2.11 | 20:80 | 20:80 |

- **Example 2** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port **20~80** will be redirected to port **20~80** of **192.168.2.11**. The rule 2 won't take effect.

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.11 | 20:80 | 20:80 |
| 2 | TCP | 192.168.2.10 | 22 | 22 |

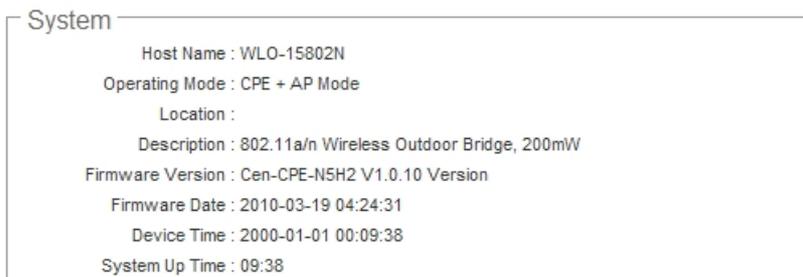
6.7 System Status

This section breaks down into subsections of **System Overview**, **Associated Clients Status**, **Remote AP**, **Extra Information** and **Event Log**.

6.7.1 Overview

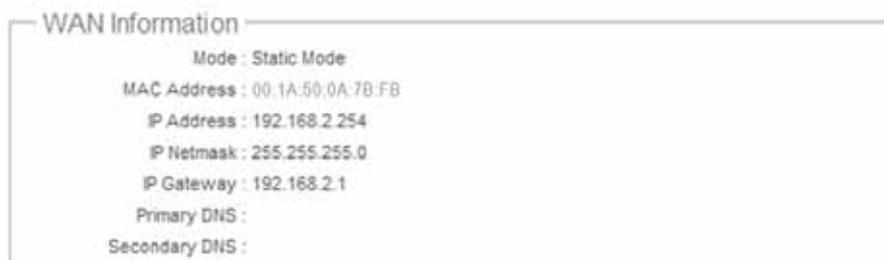
Detailed information on **System**, **WAN Information**, **LAN Information**, **Wireless Information** and **DHCP Server Status** can be reviewed via this page.

- **System** : Display the information of the system.



- ➔ **System Name** : The name of the system.
- ➔ **Operating Mode** : The mode currently in service.
- ➔ **Location** : The reminding note on the geographical location of the system.
- ➔ **Description** : The reminding note of the system.
- ➔ **Firmware Version** : The current firmware version installed.
- ➔ **Firmware Date** : The build time of the firmware installed.
- ➔ **Device Time** : The current time of the system.
- ➔ **System Up Time** : The time period that system has been in service since last reboot.

- **WAN Information** : Display the information of the WAN interface.



The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.

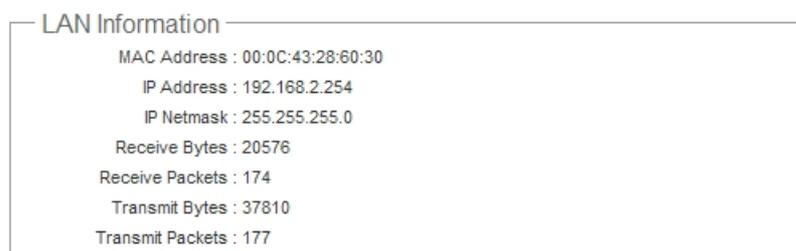


The WAN port specified **PPPoE** or **PPTP**, and the **Connect** and **DisConnect** button will be show up. Click “**Connect**” button to assigned IP address from PPPoE or PPTP server, “**DisConnect**” button to release IP address of WAN port.



- **Mode** : Supports Static, Dynamic, PPPoE and PPTP modes.
- **Reconnect Mode** : The current reconnect mode of the PPPoE or PPTP.
- **MAC Address** : The MAC address of the WAN port.
- **IP Address** : The IP address of the WAN port.
- **IP Netmask** : The IP netmask of the WAN port.
- **IP Gateway** : The gateway IP address of the WAN port.
- **Primary DNS** : The primary DNS server in service.
- **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.



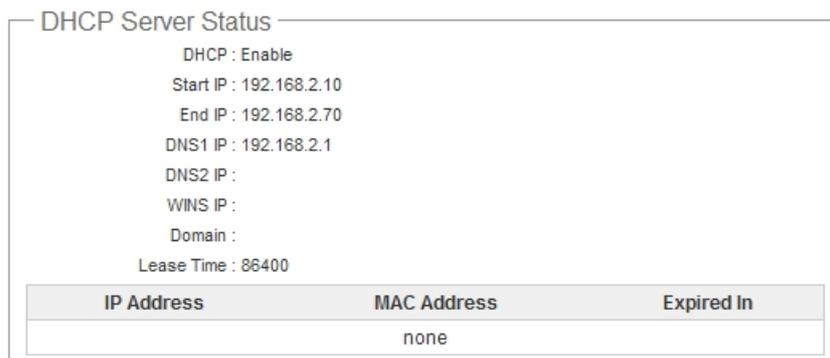
- **MAC Address** : The MAC address of the LAN port.
- **IP Address** : The IP address of the LAN port.
- **IP Netmask** : The IP netmask of the LAN port.
- **Receive bytes** : The total received packets in bytes on the LAN port.
- **Receive packets** : The total received packets of the LAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display the detailed receive and transmit statistics of Wireless interface.



- **AP MAC Address** : The MAC address of the Repeater AP.
- **Station MAC Address** : The MAC address of the Wireless Client Station.
- **Channel** : The current channel on the Wireless port.
- **AP Rate** : The current Bit Rate on the Repeater AP.
- **Station Rate** : The current Bit Rate on the Wireless Client Station.
- **Receive bytes** :The total received packets in bytes on the Wireless port.
- **Receive packets** : The total received packets on the Wireless port.
- **Transmit bytes** : The total transmitted packets in bytes on the Wireless port.
- **Transmit packets** : The total transmitted packets on the Wireless port.

- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.



- **IP Address** : IP addresses to LAN devices by DHCP server.
- **MAC Address** : MAC addresses of LAN devices.
- **Expired In** : Shows how long the leased IP address will expire.

6.7.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with Repeater AP.

Wireless Clients Refresh

| AP Information | | | | | |
|----------------|------------------|-------------------|-------|---------------|---------|
| AP | ESSID | MAC Address | State | Security Type | Clients |
| Repeater AP | Main_AP_Repeater | 00:1A:50:0A:7B:FA | On | Disable | 1 |

| Repeater AP Clients | | | | | | |
|---------------------|----------------------|----------------------|-----------|-----------|--------------|------------|
| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | BandWidth | Idle Time | Connect Time | Disconnect |
| 00:1A:50:0A:7B:FA | 100%(-32dBm) | 100%(-40dBm) | 20MHz | 8 | 57 | Delete |

- **AP Information** : Highlights key Repeater AP information.
 - **AP** : Available Repeater AP.
 - **ESSID** : Display name of ESSID for Repeater AP.
 - **MAC Address** : Display MAC address for Repeater AP.
 - **Status** : On/Off
 - **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
 - **Clients** : Display total number of wireless connections on Repeater AP.

- **Repeater AP Clients** : Display all associated clients.
 - **MAC Address** : MAC address of associated clients
 - **Signal Strength ANT0/ANT1** : Signal Strength of from associated clients.
 - **Bandwidth** : Channel bandwidth of from associated clients
 - **Idle Time** : Last inactive time period in seconds for a wireless connection.
 - **Connect Time** : Total connection time period in seconds for a wireless connection.
 - **Disconnect** : Click **"Delete"** button to manually disconnect a wireless client in a Repeater AP.

6.7.3 Remote AP

SSID, MAC address, antenna 0/1 received signal strength and channel bandwidth for associated AP are available.

Remote AP

| Connection Information | | | | |
|------------------------|-------------------|----------------------|----------------------|-----------|
| ESSID | MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | BandWidth |
| Main_AP-253 | 00:1A:50:0A:7B:F2 | 100%(-39dBm) | 100%(-42dBm) | 40MHz |

- **ESSID** : Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.
- **MAC Address** : Display MAC address of associated AP.
- **Signal Strength ANT0/ANT1** : Shows the wireless signal strength of the connection between system and an access point.
- **BandWidth** : Shows the current channel bandwidth used for communication. It should be "20" or "40"



*If display "**No Connection API!**", you need check Wireless configuration. Things to verify are **Channel** and **Security type**. Also, adjust antenna angle and Tx Power.*

6.7.4 Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
 Information: Netstat Information

Netstat Information

| Protocol | LiveTime | Status | SrcIP | SrcPort | DstIP | DstPort |
|----------|----------|-------------|--------------|---------|---------------|---------|
| tcp | 119 | TIME_WAIT | 192.168.2.22 | 3423 | 192.168.2.254 | 80 |
| tcp | 113 | TIME_WAIT | 192.168.2.22 | 3419 | 192.168.2.254 | 80 |
| udp | 5 | | 192.168.2.22 | 138 | 192.168.2.255 | 138 |
| tcp | 118 | TIME_WAIT | 192.168.2.22 | 3421 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3413 | 192.168.2.254 | 80 |
| tcp | 431999 | ESTABLISHED | 192.168.2.22 | 3425 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3415 | 192.168.2.254 | 80 |
| tcp | 91 | TIME_WAIT | 192.168.2.22 | 3417 | 192.168.2.254 | 80 |

- **Netstat Information** : Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

NetStatus will show all connection track on the system, the information include *Protocol*, *Live Time*, *Status*, *Source/Destination IP address* and *Port*.

- **Route table information** : Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

Route Information

| Destination | Gateway | Netmask | Interface |
|-------------|-------------|---------------|-----------|
| 192.168.3.0 | 0.0.0.0 | 255.255.255.0 | bre0 |
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | apcli0 |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | apcli0 |

- **ARP table Information** : Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

ARP Table Information

| IP Address | MAC Address | Interface |
|--------------|-------------------|-----------|
| 192.168.2.1 | 00:1A:50:AE:38:81 | apcli0 |
| 192.168.3.27 | 00:1A:92:9F:A4:9B | bre0 |

- **Bridge table information** : Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces.

Bridge Table Information

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-----------------------|
| bre0 | 8000.000c43286010 | no | eth2 ra0 apcli0 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

Bridge MACs Information

| Port | MAC Address | Local | Ageing Timer |
|-------------|-------------------|-------|--------------|
| LAN | 00:1A:50:0A:7B:F0 | yes | 0.00 |
| Repeater-AP | 00:1A:50:0A:7B:FA | yes | 0.00 |
| LAN | 00:1a:92:9fa4:9b | no | 0.09 |

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

Bridge STP Information

bre0

| | | | |
|-----------------------|-------------------|----------------------|-------|
| bridge id | 8000.000c43286010 | | |
| designated root | 8000.000c43286010 | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 1.36 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 3.36 |
| flags | | | |

eth2 (1)

| | | | |
|-------------------|-------------------|---------------------|------------|
| port id | 8001 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |

ra0 (2)

| | | | |
|-------------------|-------------------|---------------------|------------|
| port id | 8002 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8002 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |

apcli0 (3)

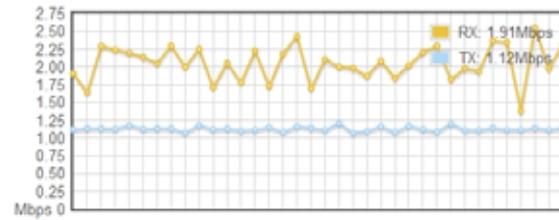
| | | | |
|-------------------|-------------------|---------------------|------------|
| port id | 8003 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8003 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |

6.7.5 QoS Plot

The QoS Plot show graphs which continuously represents the current data traffic on each QoS rule. The chart scale and throughput dimension (bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically every **5** seconds. The throughput statistics of QoS can be updated manually using the **Refresh** button.

QoS Plot

| QoS List | | | |
|----------|---------|-------------|--------------------|
| # | Comment | Remark DSCP | Bandwidth(U/D)kbps |
| 1 | FTP | NO | 1024/2048 |



6.7.6 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|---|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 7. Client Bridge + Universal Repeater Configuration

When Client Bridge+Universal Repeater mode is activated, the system can be configured as an **Access Point** and **Client Station** simultaneously. This section provides information in configuring the Client Bridge+Universal Repeater mode with graphical illustrations. WLO-15814N / WLO-15802N provides functions as stated below where they can be configured via a user-friendly web based interface.

| Option | System | Wireless | Utilities | Status |
|-----------|----------------|-------------------|-------------------|-----------------|
| Functions | Operating Mode | General Setup | Profiles Settings | System Overview |
| | LAN | Advanced Setup | Firmware Upgrade | Clients |
| | Management | Repeater AP Setup | Network Utility | Remote AP |
| | Time Server | Wireless Profile | Reboot | Extra Info |
| | SNMP | Site Survey | | Event Log |

Table 7-1: Client Bridge+Universal Repeater Mode Functions

7.1 External Network Connection

7.1.1 Network Requirement

It can be used as an Client Bridge or Universal Repeater to receive and repeat wireless signal over last mile applications, helping WISPs deliver wireless broadband Internet service to new residential and business customers. In this mode, WLO-15814N / WLO-15802N is enabled with DHCP Server functions. The wired clients of WLO-15814N / WLO-15802N are in **the same** subnet from Main Base Station and it **accepts** wireless connections from wireless client devices.

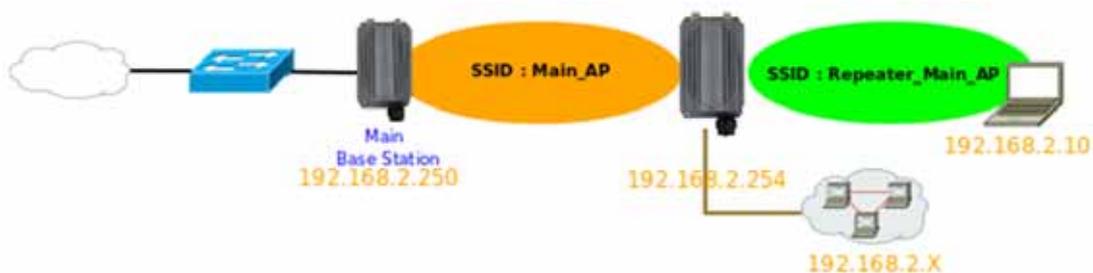


Figure 7-1 Client Bridge + Universal Repeater mode network Configuration



When the WLO-15814N / WLO-15802N configured as an Access Point and Client Station simultaneously, the Wireless General and Advanced Setup also used simultaneously. But the Security Type can be different. In the other word, the channel or other settings will be the same between WLO-15814N / WLO-15802N to Main Base Station and wireless client to WLO-15814N / WLO-15802N, but security type can be different.

7.1.2 Configure LAN IP

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

LAN Setup

Ethernet Connection Type
Mode : Static IP Dynamic IP

Static IP
IP Address : 192.168.2.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.2.1

DNS
DNS : No Default DNS Server Specify DNS Server IP
Primary :
Secondary :

DHCP Server
DHCP : Enable Disable

- **Mode** : Check either “Static IP” or “Dynamic IP” button as desired to set up the system IP of LAN port .
 - ➔ **Static IP** : The administrator can manually setup the LAN IP address when static IP is available/ preferred.
 - ✓ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ✓ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the LAN port; default Gateway is 192.168.2.1
 - ➔ **Dynamic IP** : This configuration type is applicable when the WLO-15814N / WLO-15802N is connected to a network with the presence of a DHCP server; all related IP information will be provided by the DHCP server automatically.

Dynamic IP
Hostname :

- **Hostname** : The Hostname of the LAN port
- **DNS** : Check either “No Default DNS Server” or “Specify DNS Server IP” button as desired to set up the system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.
- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

DHCP Server
DHCP : Enable Disable
Start IP : 192.168.2.10
End IP : 192.168.2.70
DNS1 IP :
DNS2 IP :
WINS IP :
Domain :
Lease Time :

- **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- **Domain** : Enter the domain name for this network.
- **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

7.2 Access Point Association

7.2.1 Configure Wireless General Setting

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

The screenshot shows the 'Wireless Setup' configuration interface. It is organized into three main panels:

- General Setup:**
 - Band Mode: 802.11 a/n mixed mode (dropdown)
 - Country: NONE (dropdown)
 - Tx Power: 100 % (input field)
- HT Other:**
 - HT TxStream: 2 (dropdown)
 - HT RxStream: 2 (dropdown)
- HT Physical Mode:**
 - Operating Mode: Mixed Mode, Green Field
 - Channel BandWidth: 20, 20/40
 - Guard Interval: Long, Auto
 - MCS: Auto (dropdown)
 - Reverse Direction Grant (RDG): Disable, Enable
 - A-MSDU: Disable, Enable
 - Auto Block ACK: Disable, Enable
 - Decline BA Request: Disable, Enable

A 'Save' button is located at the bottom center of the HT Physical Mode panel.

- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54** Mbps for **802.11a**
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit number between **1** to **100** (the unit is %) for your environment. If you are not sure of which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput) Physical Mode** and **11n Configuration** settings should be hidden immediately.

- **Operating Mode** : By default, it's Mixed Mode
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "**Auto**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **MPDU Enable** : Check **Enable** button to activate this function, and **Disable** to deactivate.
- **A-MPDU** : A-MPDU (Aggregated Mac Protocol Data Unit) allows the transmissions of multiple Ethernet frames to a single location as burst of up to 64kbytes This is performed on the hardware itself. Select "Manual" to set "MPDU Density"
- **MPDU Density** : Minimum separation of MPDUs in an A-MPDU.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------------|------|------|------|------|------|------|-------|
| No Restriction | ¼ µs | ½ µs | 1 µs | 2 µs | 4 µs | 8 µs | 16 µs |

- **A-MSDU** : Aggregated Mac Service Data Unit, A-MSDU. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU. Default is disabled.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **Repeater AP**

7.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Short Slot : Enable Disable

Extra Slot Time : us

ACK Timeout : us

Beacon Interval : ms

DTIM Interval : ms

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

Pkt_Aggregate : Enable Disable

IEEE 802.11H(DFS) : Enable Disable

WMM : Enable Disable

Save

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time** : Slot time is in the range of **1~255** and set in unit of **microsecond**. The default value is **9** microsecond.



When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout** : ACK timeout is in the range of **1~255** and set in unit of *microsecond*. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.
- **RTS Threshold** : TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble** : By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
- **Pkt_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.
- **IEEE802.11H (DFS)** : By default, it's "**Enable**". To **Disable** is to deactivate IEEE802.11H(DFS)

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

| | |
|---------------------|--|
| DFS Channels | 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140 |
|---------------------|--|

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.



*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When WLO-15814N / WLO-15802N detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

WMM Parameters of Access Point

| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
|-------|-------|-------|-------|------|--------------------------|--------------------------|
| AC_BE | 3 | 15 | 63 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VI | 1 | 7 | 15 | 94 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VO | 1 | 3 | 7 | 47 | <input type="checkbox"/> | <input type="checkbox"/> |

WMM Parameters of Station

| | Aifsn | CWMin | CWMax | Txop | ACM |
|-------|-------|-------|-------|------|--------------------------|
| AC_BE | 3 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_VI | 2 | 7 | 15 | 94 | <input type="checkbox"/> |
| AC_VO | 2 | 3 | 7 | 47 | <input type="checkbox"/> |



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

WMM Parameters of Access Point : This affects traffic flowing from the access point to the client station

| Queue | Data Transmitted AP to Clients | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : This affects traffic flowing from the client station to the access point.

| Queue | Data Transmitted Clients to AP | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is

the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".

- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **Repeater AP**.

7.2.3 Site Survey

Use this tool to scan and locate WISP Access Points and select one to associate with.

Please click on **Wireless -> Site Survey**. Below depicts an example for site survey.

Station Site Survey

| Scan Result | | | | | | | |
|-------------|-------------------|--------|---------|--------------|-------|----------------|------------------------|
| ESSID | MAC Address | Signal | Channel | Security | Band | Network Type | Select |
| Main_AP | 00:1A:50:0A:7C:3A | 50% | 44 | NONE | 11a/n | Infrastructure | Select |
| Main_AP-253 | 00:1A:50:0A:7B:F2 | 100% | 44 | NONE | 11a/n | Infrastructure | Select |
| 253AP1 | 00:1A:50:0A:7B:F3 | 100% | 44 | WEP | 11a/n | Infrastructure | Select |
| 253AP2 | 00:1A:50:0A:7B:F4 | 100% | 44 | WPAPSK/AES | 11a/n | Infrastructure | Select |
| 253AP3 | 00:1A:50:0A:7B:F5 | 100% | 44 | WPAPSK/TKIP | 11a/n | Infrastructure | Select |
| 253AP4 | 00:1A:50:0A:7B:F6 | 100% | 44 | WPA2PSK/AES | 11a/n | Infrastructure | Select |
| 253AP5 | 00:1A:50:0A:7B:F7 | 100% | 44 | WPA2PSK/TKIP | 11a/n | Infrastructure | Select |

- **ESSID** : Available Extend Service Set ID of surrounding Access Points.
- **MAC Address** : MAC addresses of surrounding Access Points.
- **Signal** : Received signal strength of all found Access Points.
- **Channel** : Channel numbers used by all found Access Points.
- **Security** : Security type by all found Access Points.
- **Band** : Wireless band used by all found Access Points.
- **Network Type** : Network type used by all found Access Points.
- **Select** : Click "**Select**" to configure settings and associate with chosen AP.



While clicking "Select" button in the Site Survey Table, the "**ESSID**" and "**Security Type**" will apply in the Wireless General Setup. However, more settings are needed including Security Key.

7.2.4 Create Wireless Profile

The administrator can configure station profiles via this page.

Please click on **Wireless -> Wireless Profile** and follow the below setting.

- **MAC Address** : The MAC address of the Wireless Station is displayed here.
- **Profile Name** : Set different profiles for quick connection uses.
- **ESSID** : Assign Service Set ID for the wireless system.
- **Lock to AP MAC** : This allows the station to always maintain connection to a particular AP with a specific MAC address. This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.
- **Channel/Frequency** : Select the desired channel range.
- **Security Type** : Select the desired security type from the drop-down list; the options are “NONE” “OPEN”, “SHARED”, “WPA-PSK” and “WPA2-PSK”.
 - ➔ **OPEN / SHARED** : OPEN and SHARED require the user to set a WEP key to exchange data.

- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

WPA

Cipher Suite : AES

Pre-shared Key :

- ✓ **Cipher Suite** : Select the desired cipher suite from the drop-down list; the options are **AES** and **TKIP**
 - ✓ **Pre-shared Key** : Enter the information for pre-shared key; the key can be either entered as a 256-bit secret in **64 HEX** digits format, or **8 to 63 ASCII** characters.
- **Profile List** : The user can manage the created profiles for home, work or public areas. Below depict an example for Profile List

| Active | # | Profile Name | ESSID | MAC Address | Channel | Security Type | Delete | Edit |
|----------------------------------|---|--------------|---------|-------------------|---------|---------------|--------|------|
| <input type="radio"/> | 1 | AP_Profile0 | default | | 44 | NONE | Delete | Edit |
| <input checked="" type="radio"/> | 2 | Profile-Test | 253AP1 | 00:1A:50:0A:7B:F3 | 44 | OPEN | Delete | Edit |

Connect

- Click “**Edit**” an exist profile on the Profile List. The field of System Configuration and Security Policy will display profile's content. Edit profile's content and then click “**Save**” button to save the profile.
- Click “**Delete**” to remove profile.
- Click and Select a profile from list, then click the “**Connect**” button to connecting to the wireless network with the profile setting. After clicking “Connect” button, you can verify connecting status on Remote AP Page



*If tuen on IEEE802.11H and WLO-15814N / WLO-15802N connect AP with DFS channel 52-150, WLO-15814N / WLO-15802N Will have **60** sec to do channel available check, and will not send beacon and can not be connect.*

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes

7.3 Wireless LAN Network Creation

The network manager can configure related wireless settings, **Repeater AP Setup**, **Security Settings**, and **MAC Filter Settings**.

7.3.1 Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings.

Repeater AP Setup

- **Enable Repeater AP** : By default, it's "**Enable**" for repeater AP. Select "**Enable**" to activate Repeater AP or click "**Disable**" to deactivate this function
- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified AP.
- **Client Isolation** : By default, it's "**Disable**".
Select "**Enable**", all clients will be isolated from each other, which means they can't reach each other.
- **Hidden SSID** : By default, it's "**Disable**".
Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP's clients could make to associate to it.
- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this Repeater AP.
- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
 - ➔ **Disable** : Data are unencrypted during transmission when this option is selected.
 - ➔ **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

WEP

Authentication Type : OPEN SHARED WEPAUTO

Key Index :

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- ✓ **Authentication Method** : Enable the desired option among **OPEN**, **SHARED** or **WEPAUTO**.
- ✓ **Key Index** : key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
- ✓ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

WPA General

Cipher Suite :

Pre-shared Key :

Group Key Update Period : seconds

- ✓ **Cipher Suite** : By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.



Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period** : By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- ➔ **WPA-Enterprise (or WPA2-Enterprise)**: The RADIUS authentication and encryption will be both enabled if this is selected.

WPA General

Cipher Suite : ▼

Group Key Update Period : seconds

PMK Cache Period : minute

Pre-Authentication : Disable Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.



PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X** : When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

| | |
|------------------------------|-----------------------------------|
| 802.1x WEP | |
| Dynamic WEP : Enable | |
| Authentication RADIUS Server | |
| Authentication Server : | <input type="text"/> |
| Port : | <input type="text" value="1812"/> |
| Shared Secret : | <input type="text"/> |
| Session Timeout : | <input type="text" value="0"/> |

✓ **Radius Server Settings :**

- **IP Address** : Enter the IP address of the Authentication RADIUS server.
- **Port** : By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret** : A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout** : The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

7.3.2 Wireless MAC Filter Setup

Continue **7.3.1 Repeater AP Setup** section, the administrator can allow or reject clients to access Repeater AP.

- **MAC Filter Setup** : By default, it's "**Disable**". Options are **Disable**, **Only Deny List MAC** or **Only Allow List MAC**.

Two ways to set MAC filter rules :

→ **Only Allow List MAC.**

The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

→ **Only Deny List MAC.**

The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Click **Reboot** button to activate your changes



MAC Access Control is the weakest security approach. WPA or WPA2 security method is highly recommended.

7.4 System Management

7.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - **Enable HTTP** : Check to select HTTP Service.
 - **HTTP Port** : The default is **80** and the range is between 1 ~ 65535.
 - **Enable HTTPS** : Check to select HTTPS Service
 - **HTTPS Port** : The default is **443** and the range is between 1 ~ 65535.



*If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.*

- **Enable Telnet** : Check to select Telnet Service
- **Telnet Port** : The default is **23** and the range is between 1 ~ 65535.
- **Enable SSH** : Check to select SSH Service
- **SSH Port** : Please The default is **22** and the range is between 1 ~ 65535.



*Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.*

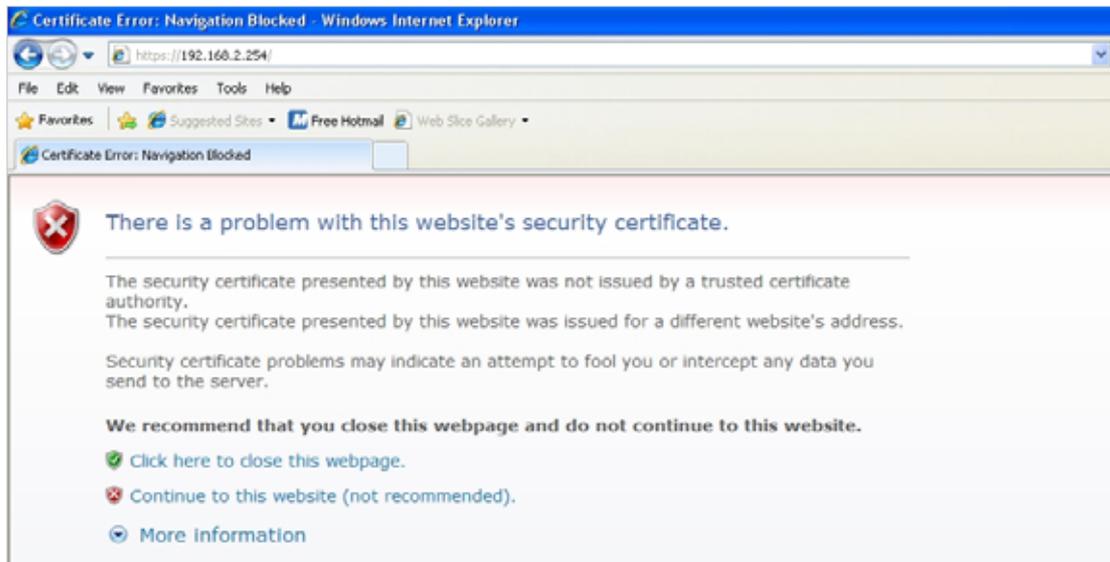
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

- **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
- **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
- **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254/>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

7.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

Save

- **Local Time** : Display the current system time.

- **NTP Client** : To synchronize the system time with NTP server.
 - ➔ **Enable** : Check to select NTP client.
 - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
 - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
 - ➔ **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

7.4.3 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP manager and agent. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable:** Check to enable SNMP v2c.

- **ro community** : Set a community string to authorize read-only access.
- **rw community** : Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

- **SNMP ro user** : Set a community string to authorize read-only access.
- **SNMP ro password** : Set a password to authorize read-only access.
- **SNMP rw user** : Set a community string to authorize read/write access.
- **SNMP rw password** : Set a password to authorize read/write access.

- **SNMP Trap** : Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

SNMP Trap

Enable :

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

7.4.4 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

Profile Save

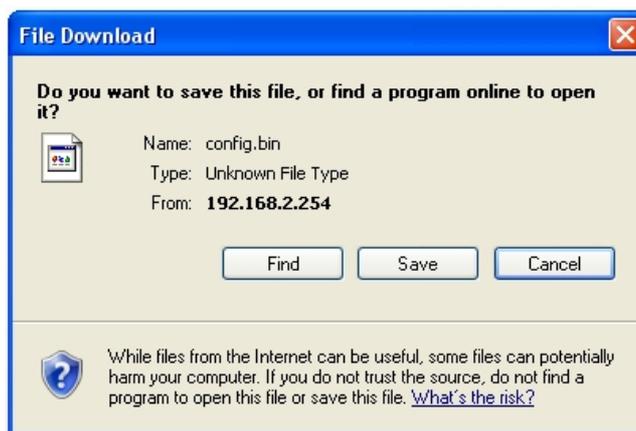
Save Settings To PC :

Load Settings From PC :

Reset To Factory Default :

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings To PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

7.4.5 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-N5H2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27

Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

7.4.6 Network Utility

The administrator can diagnose network connectivity via the PING utility.

Please click on **Utilities -> Network Utility** and follow the below setting.

Network Utility

Ping

Destination IP/Domain: Count

Traceroute

Destination Host: MAX Hop

Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.

 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

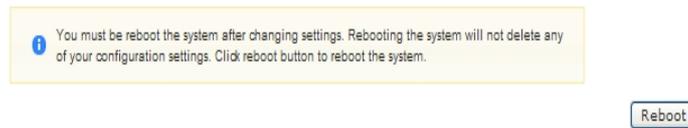
- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test

 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

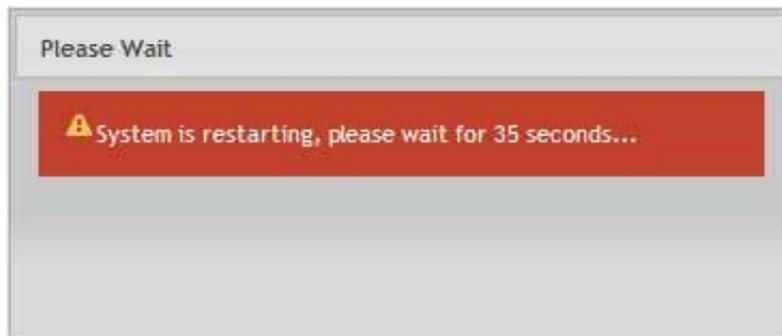
7.4.7 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

Reboot



A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

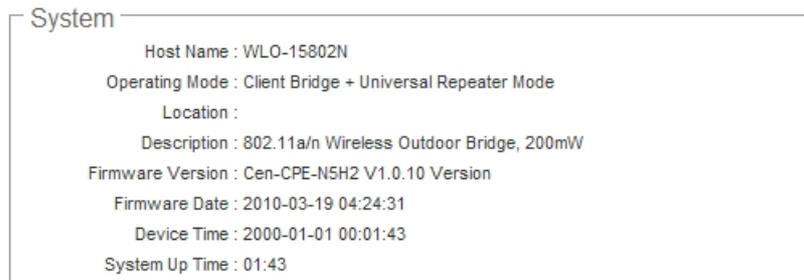
7.5 System Status

This section breaks down into subsections of **System Overview**, **Associated Clients Status**, **Remote AP**, **Extra Information** and **Event Log**.

7.5.1 System Overview

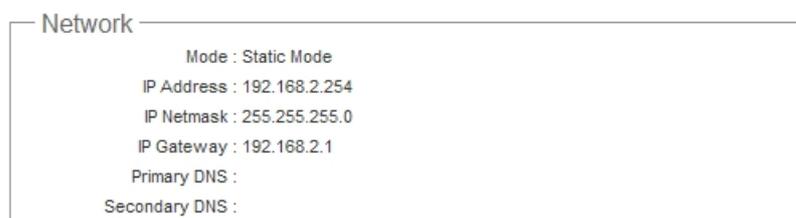
Display detailed information of **System**, **Network**, **LAN and Wireless** in the System Overview page.

- **System** : Display the information of the system.



- **System Name** : The name of the system.
- **Operating Mode** : The mode currently in service.
- **Location** : The reminding note on the geographical location of the system.
- **Description** : The reminding note of the system.
- **Firmware Version** : The current firmware version installed.
- **Firmware Date** : The build time of the firmware installed.
- **Device Time** : The current time of the system.
- **System Up Time** : The time period that system has been in service since last reboot.

- **Network Information** : Display the information of the Network.



- **Mode** : Supports Static or Dynamic modes on the LAN interface.
- **IP Address** : The management IP of system. By default, it's 192.168.2.254.
- **IP Netmask** : The network mask. By default, it's 255.255.255.0.
- **IP Gateway** : The gateway IP address and by default, it's 192.168.2.1.
- **Primary DNS** : The primary DNS server in service.
- **Secondary DNS** : The secondary DNS server in service.

- **LAN Information** : Display the detailed receive and transmit statistics of LAN interface.

```
LAN Information
MAC Address : 00:1A:50:28:60:30
Receive Bytes : 75821
Receive Packets : 585
Transmit Bytes : 113309
Transmit Packets : 375
```

- **MAC Address** : The MAC address of the LAN port.
- **Receive bytes** : The total received packets in bytes on the LAN port.
- **Receive packets** : The total received packets of the LAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display the detailed receive and transmit statistics of Wireless interface.

```
Wireless Information
AP MAC Address : 00:1A:50:0A:7B:FA
Station MAC Address : 00:1A:50:0A:7B:FB
Channel : 44
AP Rate : 300 Mb/s
Station Rate : 300 Mb/s
Receive Bytes : 113126
Receive Packets : 526
Transmit Bytes : 2708
Transmit Packets : 88
```

- **AP MAC Address** : The MAC address of the repeater AP.
- **Station MAC Address** : The MAC address of the Wireless Client Station.
- **Channel** : The current channel on the Wireless port.
- **AP Rate** : The current Bit Rate on the Repeater AP.
- **Station Rate** : The current Bit Rate on the Wireless Client Station.
- **Receive bytes** : The total received packets in bytes on the Wireless port.
- **Receive packets** : The total received packets on the Wireless port.
- **Transmit bytes** : The total transmitted packets in bytes on the Wireless port.
- **Transmit packets** : The total transmitted packets on the Wireless port.

- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.

| DHCP Server Status | | |
|-------------------------|-------------|------------|
| DHCP : Enable | | |
| Start IP : 192.168.2.10 | | |
| End IP : 192.168.2.70 | | |
| DNS1 IP : 192.168.2.1 | | |
| DNS2 IP : | | |
| WINS IP : | | |
| Domain : | | |
| Lease Time : 86400 | | |
| IP Address | MAC Address | Expired In |
| | none | |

- ➔ **IP Address** : IP addresses to LAN devices by DHCP server.
- ➔ **MAC Address** : MAC addresses of LAN devices.
- ➔ **Expired In** : Shows how long the leased IP address will expire.

7.5.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with Repeater AP.

Wireless Clients Refresh

| AP Information | | | | | |
|----------------|------------------|-------------------|-------|---------------|---------|
| AP | ESSID | MAC Address | State | Security Type | Clients |
| Repeater AP | Main_AP_Repeater | 00 1A 50 5A 7B FA | On | Disable | 1 |

| Repeater AP Clients | | | | | | |
|---------------------|----------------------|----------------------|-----------|-----------|--------------|------------|
| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | BandWidth | Idle Time | Connect Time | Disconnect |
| 00:1A:50:13:35:EF | 100%(-32dBm) | 100%(-40dBm) | 20MHz | 8 | 67 | Delete |

- **AP Information** : Highlights key Repeater AP information.
 - **AP** : Available Repeater AP.
 - **ESSID** : Display name of ESSID for Repeater AP.
 - **MAC Address** : Display MAC address for Repeater AP.
 - **Status** : On/Off
 - **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
 - **Clients** : Display total number of wireless connections on Repeater AP.

- **Repeater AP Clients** : Display all associated clients.
 - **MAC Address** : MAC address of associated clients
 - **Signal Strength ANT0/ANT1** : Signal Strength of from associated clients.
 - **Bandwidth** : Channel bandwidth of from associated clients
 - **Idle Time** : Last inactive time period in seconds for a wireless connection.
 - **Connect Time** : Total connection time period in seconds for a wireless connection.
 - **Disconnect** : Click **"Delete"** button to manually disconnect a wireless client in a Repeater AP.

7.5.3 Remote AP

SSID, MAC address, antenna 0/1 received signal strength and channel bandwidth for associated AP are available.

Remote AP

| Connection Information | | | | |
|------------------------|-------------------|----------------------|----------------------|-----------|
| ESSID | MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | BandWidth |
| Main_AP-253 | 00:1A:50:0A:7B:F2 | 100%(-39dBm) | 100%(-42dBm) | 40MHz |

- **ESSID** : Shows the current ESSID, which must be the same on the wireless client and AP in order for communication to be established.
- **MAC Address** : Display MAC address of associated AP.
- **Signal Strength ANT0/ANT1** : Shows the wireless signal strength of the connection between system and an access point.
- **BandWidth** : Shows the current channel bandwidth used for communication. It should be “20” or “40”



*If display “**No Connection API!**”, you need check Wireless configuration. Things to verify are **Channel** and **Security type**. Also, adjust antenna angle and Tx Power.*

7.5.4 Extra Information

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
Information: Netstat Information

| Protocol | LiveTime | Status | SrcIP | SrcPort | DstIP | DstPort |
|----------|----------|-------------|--------------|---------|---------------|---------|
| tcp | 119 | TIME_WAIT | 192.168.2.22 | 3423 | 192.168.2.254 | 80 |
| tcp | 113 | TIME_WAIT | 192.168.2.22 | 3419 | 192.168.2.254 | 80 |
| udp | 5 | | 192.168.2.22 | 138 | 192.168.2.255 | 138 |
| tcp | 118 | TIME_WAIT | 192.168.2.22 | 3421 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3413 | 192.168.2.254 | 80 |
| tcp | 431999 | ESTABLISHED | 192.168.2.22 | 3425 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3415 | 192.168.2.254 | 80 |
| tcp | 91 | TIME_WAIT | 192.168.2.22 | 3417 | 192.168.2.254 | 80 |

- **Route table information :** Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-------------|---------------|-------|--------|-----|-----|-------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | bre0 |
| 127.0.0.0 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | lo |
| 0.0.0.0 | 192.168.2.1 | 0.0.0.0 | UG | 0 | 0 | 0 | bre0 |

- **ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

| IP Address | HW Type | Flags | HW Address | Mask | Device |
|--------------|---------|-------|-------------------|------|--------|
| 192.168.2.22 | 0x1 | 0x2 | 00:1A:92:9F:A4:9B | * | bre0 |

- **Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces. (e.g. eth2, ra0 and apcli0).

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-----------------------|
| bre0 | 8000.000c43286010 | no | eth2 ra0 apcli0 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

| Port | MAC Address | Local | Ageing Timer |
|-------------|-------------------|-------|--------------|
| Repeater-AP | 00:1A:50:13:35:EF | no | 0.09 |
| WLAN-Client | 00:1A:50:0A:7B:F1 | no | 2.80 |
| LAN | 00:1A:50:0A:7B:F9 | yes | 0.00 |
| Repeater-AP | 00:1A:50:0A:7B:FA | yes | 0.00 |
| WLAN-Client | 00:1A:50:0A:7B:FB | yes | 0.00 |
| LAN | 00:1A:50:9F:A4:9B | no | 0.10 |
| WLAN-Client | 00:1A:50:3E:7B:FB | no | 65.92 |

- Bridge STP Information :** Select **"Bridge STP Information"** on the drop-down list to display a list of bridge STP information.

| | | | |
|-----------------------|-------------------|----------------------|------------|
| bre0 | | | |
| bridge id | 8000.000c43286010 | | |
| designated root | 8000.000c43286010 | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 1.36 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 3.36 |
| flags | | | |
| eth2 (1) | | | |
| port id | 8001 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |
| ra0 (2) | | | |
| port id | 8002 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8002 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |
| apcli0 (3) | | | |
| port id | 8003 | state | forwarding |
| designated root | 8000.000c43286010 | path cost | 100 |
| designated bridge | 8000.000c43286010 | message age timer | 0.00 |
| designated port | 8003 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.00 |
| flags | | | |

7.5.5 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|--|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

Chapter 8. Router AP Mode Configuration

When Router AP mode is chosen, the system can be configured as a Router with Access Point and WDS function. This section provides detailed explanation for users to configure in the Router AP mode with help of illustrations. In the Router AP mode, functions listed in the table below are also available from the Web-based GUI interface.

| OPTION | System | Wireless | Advance | Utilities | Status |
|-----------|----------------|------------------|------------------|-------------------|--------------------|
| Functions | Operating Mode | General Setup | DMZ | Profiles Settings | System Overview |
| | WAN | Advanced Setup | IP Filter | Firmware Upgrade | Station Statistics |
| | LAN | Virtual AP Setup | MAC Filter | Network Utility | Extra Info |
| | DDNS | WDS Setup | Virtual Server | Reboot | QoS Plot |
| | Management | | Parental Control | | Event Log |
| | Time Server | | QoS | | |
| | UPNP | | | | |
| | SNMP | | | | |

Table 8-1: Router AP Mode Functions

8.1 External Network Connection

8.1.1 Network Requirement

It can be used as an Router AP with WDS function. In this mode, WLO-15814N / WLO-15802N is a gateway enabled with NAT and DHCP Server functions. The wireless clients connected to WLO-15814N / WLO-15802N are in **different** subnet from those connected to Internet.

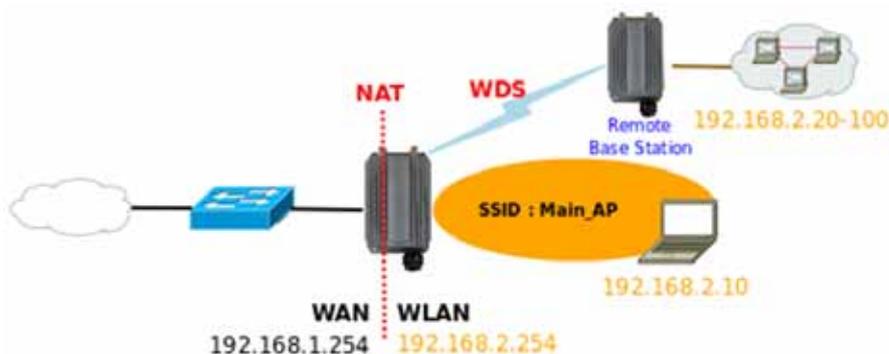


Figure 8-1 Router AP mode network configuration

8.1.2 Configure WAN Setup

There are three connection types for the WAN port : **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**.

Please click on **System -> WAN** and follow the below setting.

WAN Setup

Internet Connection Type

Mode : Static IP Dynamic IP PPPoE PPTP

Static IP

IP Address :

IP Netmask :

IP Gateway :

DNS

DNS : No Default DNS Server Specify DNS Server IP

Primary :

Secondary :

MAC Clone

Keep Default MAC Address

Clone MAC Address: 00:1A:92:9F:A4:9B

Manual MAC Address:

 *In Router AP mode, the WAN Port is the wired interface.*

- **Mode** : By default, it's "**Static IP**". Check "Static IP", "Dynamic IP", "PPPoE" or "PPTP" to set up system WAN IP.
 - ➔ **Static IP** : Users can manually setup the WAN IP address with a static IP provided by WISP.
 - ✓ **IP Address** : The IP address of the WAN port; default IP address is 192.168.1.254
 - ✓ **IP Netmask** : The Subnet mask of the WAN port; default Netmask is 255.255.255.0
 - ✓ **IP Gateway** : The default gateway of the WAN port; default Gateway is 192.168.1.1
 - ➔ **Dynamic IP** : Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings including DNS can be available from DHCP server. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click **Release** button to release IP address and click **Renew**

button to renew IP address again.

Dynamic IP

Hostname :

- ✓ **Hostname** : The Hostname of the WAN port

- ➔ **PPPoE** : To create wireless PPPoE WAN connection to a PPPoE server in network.

PPPoE

User name :

Password :

Reconnect Mode : Always On On Demand Manual

Idle Time : minutes

MTU :

- ✓ **User Name** : Enter User Name for PPPoE connection
- ✓ **Password** : Enter Password for PPPoE connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
 - ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
 - ✓ **MTU** : By default, it’s **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ➔ **PPTP** : The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

PPTP

IP Address :

IP Netmask :

PPTP Server IP Address :

User name :

Password :

Reconnect Mode : Always On On Demand Manual

Idle Time : minutes

MTU :

MPPE Encryption : MPPE-40 MPPE-128

- ✓ **IP Address** : The IP address of the WAN port
- ✓ **IP Netmask** : The Subnet mask of the WAN port
- ✓ **PPTP Server IP Address** : The IP address of the PPTP server
- ✓ **User Name** : Enter User Name for PPTP connection
- ✓ **Password** : Enter Password for PPTP connection
- ✓ **Reconnect Mode** :
 - **Always on** – A connection to Internet is always maintained.
 - **On Demand** – A connection to Internet is made as needed.



When **Time Server** is enabled at the “On Demand” mode, the “Reconnect Mode” will turn out “Always on”.

- **Manual** – Click the “**Connect**” button on “**WAN Information**” in the Overview page to connect to the Internet.
- ✓ **Idle Time** : Time to last before disconnecting PPPoE session when it is idle. Enter preferred Idle Time in minutes. Default is “0”, indicates disabled. When Idle time is disabled, the “**Reconnect Mode**” will turn out “**Always on**”
- ✓ **MTU** : By default, it’s **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- ✓ **MPPE Encryption** : Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol(PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections. **128-bit** key (strong) and **40-bit** key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
- **DNS** : Check “No Default DNS Server” or “Specify DNS Server IP” radial button as desired to set up system DNS.
 - ➔ **Primary** : The IP address of the primary DNS server.
 - ➔ **Secondary** : The IP address of the secondary DNS server.
- **MAC Clone** : The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.

MAC Clone

Keep Default MAC Address
 Clone MAC Address: 00:1A:92:9F:A4:9B
 Manual MAC Address: : : : : :

- ➔ **Keep Default MAC Address** : Keep the default MAC address of WAN port on the system.
- ➔ **Clone MAC Address** : If you want to clone the MAC address of the PC, then click the **Clone MAC Address** button. The system will automatically detect your PC's MAC address.



The Clone MAC Address field will display MAC address of the PC connected to system. Click “Save” button can make clone MAC effective.

- ➔ **Manual MAC Address** : Enter the MAC address registered with your ISP.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.1.3 Configure DDNS Setup

Dynamic DNS allows you to map domain name to dynamic IP address.

Please click on **System -> DDNS Setup** and follow the below setting.

Dynamic DNS Setup



The screenshot shows a web form titled "DDNS" with the following fields and options:

- Enable: Enable Disable
- Service Provider: A dropdown menu with "dyndns" selected.
- Hostname: Two adjacent text input fields.
- User Name: A text input field.
- Password: A text input field.

Save

- **Enabled:** By default, it's "**Disable**". The mapping domain name won't change when dynamic IP changes. The beauty of it is no need to remember the dynamic WAP IP while accessing to it.
- **Service Provider:** Select the preferred Service Provider from the drop-down list including *dyndns*, *dhs*, *ods* and *tzo*
- **Hostname:** Host Name that you register to Dynamic-DNS service and export.
- **User Name & Password:** User Name and Password are used to login DDNS service.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.1.4 Configure LAN Setup

Here are the instructions for how to setup the local IP Address and Netmask.

Please click on **System -> LAN** and follow the below setting.

LAN Setup

- **LAN IP** : The administrator can manually setup the LAN IP address.
 - ➔ **IP Address** : The IP address of the LAN port; default IP address is 192.168.2.254
 - ➔ **IP Netmask** : The Subnet mask of the LAN port; default Netmask is 255.255.255.0

- **DHCP Setup** : Devices connected to the system can obtain an IP address automatically when this service is enabled.

- ➔ **DHCP** : Check **Enable** button to activate this function or **Disable** to deactivate this service.
- ➔ **Start IP / End IP**: Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0
- ➔ **DNS1 IP** : Enter IP address of the first DNS server; this field is required.
- ➔ **DNS2 IP** : Enter IP address of the second DNS server; this is optional.
- ➔ **WINS IP** : Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.
- ➔ **Domain** : Enter the domain name for this network.
- ➔ **Lease Time** : The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is **86400** seconds

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.2 Wireless LAN Network Creation

The network manager can configure related wireless settings, **General Settings**, **Advanced Settings**, **Virtual AP(VAP) Setting**, **Security Settings**, and **MAC Filter Settings**.

8.2.1 Wireless General Setup

The administrator can change the data transmission, channel and output power settings for the system. Please click on **Wireless -> General Setup** and follow the below setting.

Wireless Setup

- **MAC Address** : The MAC address of the Wireless interface is displayed here.
- **Band Mode** : Select an appropriate wireless band; bands available are **801.11a** or **802.11a/n mixed mode**.
- **AP Isolation** : Select **Enable**, all clients will be isolated from each VAP, that means different VAP's clients can not reach to each other.
- **Transmit Rate Control** : Select the desired rate from the drop-down list; the options are auto or ranging from **6** to **54Mbps** only for **802.11a** mode.
- **Country** : Select the desired country code from the drop-down list; the options are **US**, **ETSI**, **JP** and **NONE**.
- **Channel/Frequency** : The channel range will be changed by selecting different country code. Below depicts the channel range for different **Country**.

| Country | Channel |
|---------|---|
| US | 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 |
| ETSI | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 |
| JP | 36, 40, 44, 48 |
| NONE | 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161 |

- **Tx Power** : You can adjust the output power of the system to get the appropriate coverage for your wireless network. Specify digit numbers between **1** to **100** (the unit is %) for your environment. If you are not sure which setting to choose, then keep the default setting, **100%**.

When **Band Mode** select in **802.11a only mode**, the **HT(High Throughput)** settings should be hidden immediately.

- **HT TxStream/RxStream** : By default, it's **2**.
- **Operating Mode** : By default, it's **Mixed Mode**.
 - ➔ **Mixed Mode** : In this mode packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In this mode the receiver shall be able to decode both the Mixed Mode packets and legacy packets.
 - ➔ **Green Field** : In this mode high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth** : The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Guard Interval** : Using "**Auto**" option can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **MCS** : This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary. (Refer to **Appendix C. MCS Data Rate**)
- **Reverse Direction Grant(RDG)** : Disable or enable reserve direction grant. Default is enabled.
- **A-MSDU** : Aggregated Mac Service Data Unit. Select **Enable** to allow aggregation for multiple MSDUs in one MPDU. Default is disabled.
- **Auto Block ACK** : Disable or enable auto block ACK. Default is enabled.
- **Decline BA Request** : Disable or enable decline BA request. Default is disabled.

Change these settings as described here and click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF general settings and will be applied to **all VAPs** and **WDS Links**.

8.2.2 Wireless Advanced Setup

To achieve optimal wireless performance, it is necessary to tweak advance setting per requirements properly, not necessary higher the better or lower.

The administrator can change the RTS threshold and fragmentation threshold settings for the system. Please click on **Wireless -> Advanced Setup** and follow the below setting.

Wireless Setup

Advanced Setup

Short Slot : Enable Disable

Extra Slot Time : us

ACK Timeout : us

Beacon Interval : ms

DTIM Interval : ms

Fragment Threshold :

RTS Threshold :

Short Preamble : Enable Disable

Tx Burst : Enable Disable

Pkt_Aggregate : Enable Disable

IEEE 802.11H(DFS) : Enable Disable

WMM : Enable Disable

Save

- **Short Slot** : By default, it's "**Enable**" for educing the slot time from the standard **20 microseconds** to the **9 microsecond** short slot time

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. For a sender and receiver own right of the channel the shorter slot time help manage shorter wait time to re-transmit from collision because of hidden wireless clients or other causes. When collision sources can be removed sooner and other senders attempting to send are listening the channel(CSMA/CA) the owner of the channel should continue ownership and finish their transmission and release the channel. Then, following ownership of the channel will be sooner for the new pair due to shorter slot time. However, when long duration of existing collision sources and shorter slot time exist the owners might experience subsequent collisions. When adjustment to longer slot time can't improve performance then RTS/CTS could supplement and help improve performance.

- **Extra Slot Time** : Slot time is in the range of **1~255** and set in unit of **microsecond**. The default value is **9** microsecond.



When you enable Short Slot and set Extra Slot time to "10", the actual Slot Time=9+10 us.
When you disable Short Slot and set Extra Slot time to "10", the actual Slot Time=20+10 us.

- **ACK Timeout** : ACK timeout is in the range of **1~255** and set in unit of *microsecond*. The default value is **32** microsecond.

All data transmission in 802.11b/g request an “Acknowledgement” (ACK) send by receiving radio. The transmitter will resend the original packet if correspondent ACK failed to arrive within specific time interval, also refer to as “ACK Timeout”.

ACK Timeout is adjustable due to the fact that distance between two radio links may vary in different deployment. ACK Timeout makes significant influence in performance of long distance radio link. If ACK Timeout is set too short, transmitter will start to “Resend” packet before ACK is received, and throughputs become low due to excessively high re-transmission.

ACK Timeout is best determined by distance between the radios, data rate of average environment. The Timeout value is calculated based on round-trip time of packet with a little tolerance, So, if experiencing re-transmissions or poor performance the ACK Timeout could be made longer to accommodate.



Slot Time and ACK Timeout settings are for long distance links. It is important to tweak settings to achieve the optimal result based on requirement.

- **Beacon Interval** : Beacon Interval is in the range of **20~1024** and set in unit of *millisecond*. The default value is **100** msec.

Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called “Beacon”. Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate.

All the radio stations received beacon recognizes the existence of such AP, and may proceed next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis, the time interval can be adjusted.

By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.

- **DTIM Interval** : The DTIM interval is in the range of **1~255**. The default is **1**.

DTIM is defined as *Delivery Traffic Indication Message*. It is used to notify the wireless stations, which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

- **Fragment Threshold** : The Fragment Threshold is in the range of **256~2346** byte. The default is **2346** byte.

Each Wi-Fi packet can be divided into smaller packets, marked with a sequential fragment number and re-assemble in the receiving ends. The purpose is to make a short frame, instead of long frame, transmitting by radio in a heavy noisy environment. Because of sending smaller frames, corruptions are much less likely to occur. The pros is obvious, the cons is the overhead for transmission. So, in a clean environment, higher fragment threshold can be an option to increase throughput.

Fragmentation will be triggered by setting the Fragment Threshold, usually in Byte-length. Only when the frame size is over the Threshold, fragmentation will take place automatically.
- **RTS Threshold** : TRTS Threshold is in the range of **1~2347** byte. The default is **2347** byte.

The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.
- **Short Preamble** : By default, it's "**Enable**". To **Disable** is to use Long 128-bit Preamble Synchronization field.

The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.
- **Tx Burst** : By default, it's "**Enable**". To **Disable** is to deactivate Tx Burst.

With TX burst enabled, AP will send many packets in a burst, without collision detection and RTS/CTS for each packet. TX Burst have better throughput but cause interference with other APs in channel.
- **Pkt_Aggregate** : By default, it's "**Enable**"

Increase efficiency by aggregating multiple packets of application data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost of just a single frame.
- **IEEE802.11H (DFS)** : By default, it's "**Enable**". To **Disable** is to deactivate IEEE802.11H(DFS)

With DFS(Dynamic Frequency Selection) enabled, radio is operating on one of the following channels, the wireless device uses DFS to monitor the operating frequency and switch to another frequency or reduce power as necessary:

| | |
|---------------------|--|
| DFS Channels | 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 136, 140 |
|---------------------|--|

The maximum legal transmit power is greater for some 5 GHz channels than for others. When the wireless device randomly selects a 5 GHz channel on which power is restricted, the wireless device automatically reduces transmit power to comply with power limits for that channel in that regulatory domain.



*The Channel **52-140** is DFS channel. If tuen on IEEE802.11H, AP Will have **60** sec to do channel available check, and will not send beacon and can not be connect. When WLO-15814N / WLO-15802N detect radar(5GHz) signal, the AP will switch channel and stop beacon trasmit between **15** sec.*

- **WMM** : By default, it's "**Disable**". To **Enable** is to use WMM and the WMM parameters should appears.

| WMM Parameters of Access Point | | | | | | |
|--------------------------------|-------|-------|-------|------|--------------------------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM | AckPolicy |
| AC_BE | 3 | 15 | 63 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VI | 1 | 7 | 15 | 94 | <input type="checkbox"/> | <input type="checkbox"/> |
| AC_VO | 1 | 3 | 7 | 47 | <input type="checkbox"/> | <input type="checkbox"/> |

| WMM Parameters of Station | | | | | |
|---------------------------|-------|-------|-------|------|--------------------------|
| | Aifsn | CWMin | CWMax | Txop | ACM |
| AC_BE | 3 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_BK | 7 | 15 | 1023 | 0 | <input type="checkbox"/> |
| AC_VI | 2 | 7 | 15 | 94 | <input type="checkbox"/> |
| AC_VO | 2 | 3 | 7 | 47 | <input type="checkbox"/> |



When you enable WMM, the "Tx Burst" will be Disabled automatically by system.

→ **WMM Parameters of Access Point** : This affects traffic flowing from the access point to the client station

| Queue | Data Transmitted AP to Clients | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".
- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.
- ✓ **AckPolicy** : Acknowledgment Policy, WMM defines two ACK policies: **Normal ACK** and **No ACK**. Click "Checkbox" indicates "No ACK"

When the no acknowledgment (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient.

When the Normal ACK policy is used, the recipient acknowledges each received unicast packet.

➔ **WMM Parameters of Station** : *This affects traffic flowing from the client station to the access point.*

| Queue | Data Transmitted Clients to AP | Priority | Description |
|-------|--------------------------------|----------|--|
| AC_BK | Background. | Low | High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). |
| AC_BE | Best Effort | Medium | Medium throughput and delay. Most traditional IP data is sent to this queue |
| AC_VI | Video | High | Minimum delay. Time-sensitive video data is automatically sent to this queue |
| AC_VO | Voice | High | Time-sensitive data like VoIP and streaming media are automatically sent to this queue |

- ✓ **Aifsn** : The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames
- ✓ **CWmin** : Minimum Contention Window. This parameter is input to the algorithm that determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.
- ✓ **CWmax** : Maximum Contention Window. The value specified here in the Maximum Contention Window is

the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".

- ✓ **Txop** : Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (Txop) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.
- ✓ **ACM** : Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes. The items in this page are for AP's RF advanced settings and will be applied to **all VAPs** and **WDS Links**.

8.2.3 Create Virtual AP (VAP)

The WLO-15814N / WLO-15802N support broadcasting multiple SSIDs, allowing the creation of Virtual Access Points, partitioning a single physical access point into **7** logical access points, each of which can have a different set of security and network settings. **Figure 8-2** shows multiple SSIDs with security type settings.

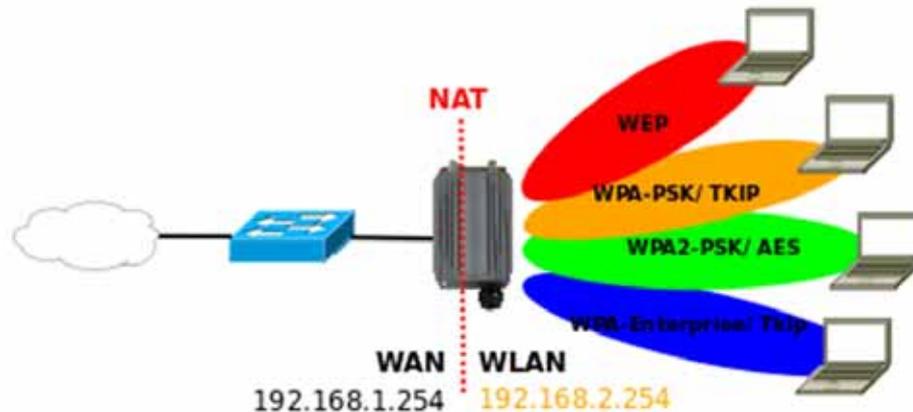


Figure 8-2 Multiple SSIDs with different Security Type

8.2.3.1 Virtual AP Overview

The administrator can view all of the Virtual AP's settings via this page.

Please click on **Wireless -> Virtual AP Setup** and the Virtual AP Overview Page appears.

Virtual AP Overview

| VAP | ESSID | MAC Address | Status | Security Type | MAC Filter | Edit |
|------------|---------|-------------------|--------|---------------|------------|----------------------|
| Primary AP | Main_AP | 00:1A:50:01:C6:92 | On | Disable | Disable | Edit |
| VAP1 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP2 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP3 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP4 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP5 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |
| VAP6 | | 00:00:00:00:00:00 | Off | Disable | Disable | Edit |

- **VAP** : Indicate the system's Virtual AP.
- **ESSID** : Indicate the ESSID of the respective Virtual AP
- **MAC Address** : The MAC address of the VAP Interface is displayed here. When you enable AP and reboot system, the MAC address will display here.
- **Status** : Indicate the Status of the respective Virtual AP. **The Primary AP always on.**
- **Security Type** : Indicate an used security type of the respective Virtual AP.
- **MAC Filter** : Indicate an used MAC filter of the respective Virtual AP.
- **Edit** : Click **Edit** button to configure Virtual AP's settings, including security type and MAC Filter.

8.2.3.2 Virtual AP Setup

For each Virtual AP, administrators can configure SSID, SSID broadcasting, Maximum number of client associations, security type settings.

Click **Edit** button on the Edit column, and then a Virtual AP setup page appears.

VAP 1 Setup

Security

Enable AP : Enable Disable

ESSID :

Client Isolation : Enable Disable

Hidden SSID : Enable Disable

Maximum Clients :

VLAN Tag(D) : Enable Disable (1-4094)

Security Type :

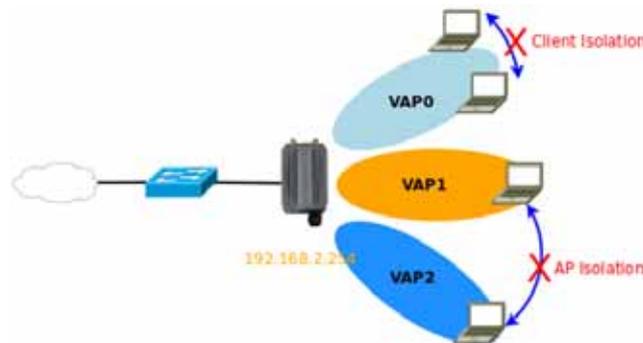
MAC Filter

Action :

- **Enable AP** : By default, it's "**Disable**" for VAP1 ~ VAP6. **The Primary AP always enabled.**

Select "**Enable**" to activate VAP or click "**Disable**" to deactivate this function

- **ESSID** : Extended Service Set ID, When clients are browsing for available wireless networks, this is the SSID that will appear in the list. ESSID will determine the service type available to AP's clients associated with the specified VAP.
- **Client Isolation** : Select **Enable**, all clients will be isolated from each other, that means all clients can not reach to other clients. Below Figures depict Client Isolation and AP Isolation



- **Hidden SSID** : By default, it's "**Disable**".

Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced. It's suggested to enable it after AP security settings are archived and setting of AP clients could make to associate to it.

- **Maximum Clients** : The default value is **32**. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.



In this mode, the system does not support VLAN Tag(ID) function.

- **Security Type** : Select the desired security type from the drop-down list; the options are **Disable**, **WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA-Enterprise**, **WPA2-Enterprise** and **WEP 802.1X**.
 - ➔ **Disable** : Data are unencrypted during transmission when this option is selected.
 - ➔ **WEP** : Wired Equivalent Privacy(WEP) is a data encryption mechanism based on a 64-bit or 128-bit shared key.

WEP

Authentication Type : OPEN SHARED WEPAUTO

Key Index :

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

- **Authentication Method** : Enable the desire option among **OPEN**, **SHARED** or **WEPAUTO**.
 - ➔ **Key Index** : Key index is used to designate the WEP key during data transmission. 4 different WEP keys can be entered at the same time, but only one is chosen.
 - ➔ **WEP Key #** : Enter **HEX** or **ASCII** format WEP key value; the system supports up to 4 sets of WEP keys.

| Key Length | Hex | ASCII |
|------------|---------------|---------------|
| 64-bit | 10 characters | 5 characters |
| 128-bit | 26 characters | 13 characters |

- ➔ **WPA-PSK (or WPA2-PSK)** : WPA (or WPA2) Algorithms, allows the system accessing the network by using the WPA-PSK protected access.

WPA General

Cipher Suite :

Pre-shared Key :

Group Key Update Period : seconds

- ✓ **Cipher Suite** : By default, it is **AES**. Select either AES or TKIP cipher suites
- ✓ **Pre-shared Key** : Enter the pre-shared key; the format shall go with the selected key type.



Pre-shared key can be entered with either a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

- ✓ **Group Key Update Period** : By default, it is **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.

- **WPA-Enterprise (or WPA2-Enterprise):** The RADIUS authentication and encryption will be both enabled if this is selected.

WPA General

Cipher Suite :

Group Key Update Period : seconds

PMK Cache Period : minute

Pre-Authentication : Disable Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **WPA General Settings :**

- **Cipher Suite :** By default, it is AES. Select either AES or TKIP cipher suites
- **Group Key Update Period :** By default, it's **3600** seconds. This time interval for rekeying GTK, broadcast/multicast encryption keys, in seconds. Entering the time-length is required.
- **PMK Cache Period :** By default, it's 10 minutes. Set **WPA2** PMKID cache timeout period, after time out, the cached key will be deleted.
- **Pre-Authentication :** By default, it's "Disable". To Enable is use to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.



PMK Cache Period and Pre-Authentication is used in WPA2-Enterprise

✓ **Radius Server Settings :**

- **IP Address :** Enter the IP address of the Authentication RADIUS server.
- **Port :** By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret :** A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout :** The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

- **WEP 802.1X** : When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete configuration.

802.1x WEP

Dynamic WEP : Enable

Authentication RADIUS Server

Authentication Server :

Port :

Shared Secret :

Session Timeout :

✓ **Radius Server Settings :**

- **IP Address** : Enter the IP address of the Authentication RADIUS server.
- **Port** : By default, it's **1812**. The port number used to communicate with RADIUS server.
- **Shared secret** : A secret key used between system and RADIUS server. Supports **8** to **64** characters.
- **Session Timeout** : The Session timeout is in the range of **0~60 seconds**. The default is **0** to disable re-authenticate service.

Amount of time before a client will be required to re-authenticate.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.2.4 Wireless MAC Filter Setup

Continue **8.2.3.2 Virtual AP Setup** section. For each Virtual AP setting, the administrator can allow or reject clients to access each Virtual AP.

- **MAC Filter Setup** : By default, it's "**Disable**". Options are **Disable**, **Only Deny List MAC** or **Only Allow List MAC**.

Two ways to set MAC filter rules :

→ **Only Allow List MAC.**

The wireless clients in the "**Enable**" list will be **allowed** to access the Access Point; All others or clients in the "**Disable**" list will be **denied**.

→ **Only Deny List MAC.**

The wireless clients in the "**Enable**" list will be **denied** to access the Access Point; All others or clients in the "**Disable**" list will be **allowed**.

- **Add a station MAC** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the "**Enable**" List.

There are a maximum of **20** clients allowed in this "Enable" List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Click **Reboot** button to activate your changes



MAC Access Control is the weakest security approach. WPA and WPA2 security method is highly recommended.

8.3 Wireless Network Expansion

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings.**



Please click on **Wireless -> WDS Setup** and follow the below setting.

WDS Setup

Security

Security Type: Disable

WDS MAC List

| Enable | WDS Peer's MAC Address | Description |
|--------------------------|--|--|
| <input type="checkbox"/> | 01 <input style="width: 20px;" type="text"/> | <input style="width: 80%;" type="text"/> |
| <input type="checkbox"/> | 02 <input style="width: 20px;" type="text"/> | <input style="width: 80%;" type="text"/> |
| <input type="checkbox"/> | 03 <input style="width: 20px;" type="text"/> | <input style="width: 80%;" type="text"/> |
| <input type="checkbox"/> | 04 <input style="width: 20px;" type="text"/> | <input style="width: 80%;" type="text"/> |

- **Security Type** : Option is “Disable”, “WEP”, “TKIP” or “AES” from drop-down list. Needs the same type to build WDS links. Security type takes effect when WDS is enabled.
 - ➔ **WEP Key** : Enter **5 / 13 ASCII** or **10 / 26 HEX** format WEP key.
 - ➔ **TKIP Key** : Enter **8 to 63 ASCII** or **64 HEX** format TKIP key.
 - ➔ **AES Key** : Enter **8 to 63 ASCII** or **64 HEX** format AES key.
- **WDS MAC List**
 - ➔ **Enable** : Click **Enable** to create WDS link.
 - ➔ **WDS Peer's MAC Address** : Enter the MAC address of WDS peer.
 - ➔ **Description** : Description of WDS link.



The WDS link needs to be set at same **Channel** and with same **Security Type**.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.4 System Management

8.4.1 Configure Management

Administrator could specify geographical location of the system via instructions in this page. Administrator could also enter new Root and Admin passwords and allow multiple login methods.

Please click **System -> Management** and follow the below settings.

Management Setup

■ System Information

- ➔ **System Name** : Enter a desired name or use the default one.
- ➔ **Description** : Provide description of the system.
- ➔ **Location** : Enter geographical location information of the system. It helps administrator to locate the system easier.

The system supports **two** management accounts, root and admin. The network manager is assigned with full administrative privileges, when logging in as **root** user, to manage the system in all aspects. While logging in as an **admin** user, only subset of privileges is granted such as basic maintenance. For example, root user can change passwords for both root and admin account, and admin user can only manage its own. For more information about covered privileges for these two accounts, please refer to **Appendix D. Network manager Privileges**.

■ Root Password : Log in as a root user and is allowed to change its own, plus admin user's password.

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

■ Admin Password : Log in as a admin user and is allowed to change its own,

- ➔ **New Password** : Enter a new password if desired
- ➔ **Check New Password** : Enter the same new password again to check.

- **Admin Login Methods** : Only **root** user can enable or disable system login methods and change services port.
 - **Enable HTTP** : Check to select HTTP Service.
 - **HTTP Port** : The default is 80 and the range is between 1 ~ 65535.
 - **Enable HTTPS** : Check to select HTTPS Service
 - **HTTPS Port** : The default is 443 and the range is between 1 ~ 65535.



If you already have an SSL Certificate, please click "**UploadKey**" button to select the file and upload it.

- **Enable Telnet** : Check to select Telnet Service
- **Telnet Port** : The default is 23 and the range is between 1 ~ 65535.
- **Enable SSH** : Check to select SSH Service
- **SSH Port** : Please The default is 22 and the range is between 1 ~ 65535.



Click "**GenerateKey**" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.

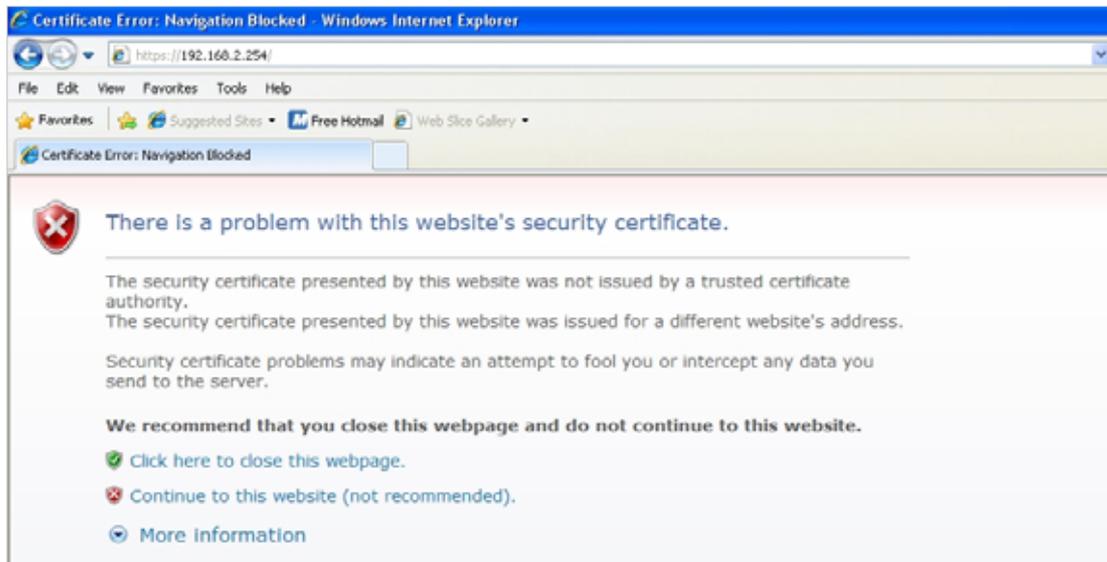
- **Ping Watchdog** : The ping watchdog sets the WLO-15814N / WLO-15802N Device to continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, the WLO-15814N / WLO-15802N device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. If the defined number of replies is not received, the tool reboots the device.

- **Enable Ping Watchdog** : control will enable Ping Watchdog Tool.
- **IP Address To Ping** : specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- **Ping Interval** : specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. Default is **300** seconds.
- **Startup Delay** : specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least **60** seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted. Default is **300** seconds.
- **Failure Count To Reboot** : specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (<https://192.168.2.254/>). There will be a "Certificate Error", because the browser treats system as an illegal website.



Click

"Continue to this website" to access the system's WMI. The system's Overview page will appear.

8.4.2 Configure System Time

System time can be configured via this page, and manual setting or via a NTP server is supported.

Please click on **System -> Time Server** and follow the below setting.

Time Server Setup

System Time

Local Time : 2000/01/01 Sat 00:05:44

NTP Client

Enable :

Default NTP Server : time.stdtime.gov.tw (optional)

Time Zone : (GMT) Dublin, Edinburgh, Lisbon, London

Daylight saving time : Disable

Save

- **Local Time** : Display the current system time.

- **NTP Client** : To synchronize the system time with NTP server.
 - ➔ **Enable** : Check to select NTP client.
 - ➔ **Default NTP Server** : Select the NTP Server from the drop-down list.
 - ➔ **Time Zone** : Select a desired time zone from the drop-down list.
 - ➔ **Daylight saving time** : Enable or disable Daylight saving.



If the system time from NTP server seems incorrect, please verify your network settings, like default Gateway and DNS settings

Click **Save** button to save your changes. Click **Reboot** button to activate your changes

8.4.3 Configure UPnP

Universal Plug and Play(UPnP) is an architecture to enable pervasive peer-to-peer network connectivity between PCs, intelligent devices and appliances when UPnP is supported. UPnP works on TCP/IP network to enable UPnP devices to connect and access to each other, very well adopted in home networking environment.

UPNP Setup

UPNP

UPNP: Enable Disable

Save

- **UPnP** : By default, it's "**Disable**". Select "**Enable**" or "**Disable**" of UPnP Service.

Click **Save** button to save changes and click **Reboot** button to activate changes

For UPnP to work in Windows XP, the "WLO-15814N / WLO-15802N" must be available in "**My Network Places**", as shown here: (your specific model may vary)



If these devices are not available, you should verify that the correct components and services are loaded in Windows XP. Please refer to **Appendix E. Using UPnP on Windows XP**

8.4.4 Configure SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP Setup** and follow the below setting.

SNMP Setup

- **SNMP v2c Enable:** Check to enable SNMP v2c.

- **ro community :** Set a community string to authorize read-only access.
- **rw community :** Set a community string to authorize read/write access.

- **SNMP v3 Enable:** Check to enable SNMP v3.

SNMPv3 supports the highest level SNMP security.

- **SNMP ro user :** Set a community string to authorize read-only access.
- **SNMP ro password :** Set a password to authorize read-only access.
- **SNMP rw user :** Set a community string to authorize read/write access.
- **SNMP rw password :** Set a password to authorize read/write access.

- **SNMP Trap :** Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.

SNMP Trap

Enable :

Community :

IP 1 :

IP 2 :

IP 3 :

IP 4 :

- ➔ **Community** : Set a community string required by the remote host computer that will receive trap messages or notices send by the system.
- ➔ **IP** : Enter the IP addresses of the remote hosts to receive trap messages.

Click **Save** button to save changes and click **Reboot** button to activate.

8.4.5 Backup / Restore and Reset to Factory

Backup current configuration, restore prior configuration or reset back to factory default configuration can be executed via this page.

Please click on **Utilities -> Profile Setting** and follow the below setting.

Profile Save

i In this page, you can save your current configuration, restore a previously saved configuration, or reset all of the settings to the factory (default) settings.

- **Save Settings to PC** : Click **Save** button to save the current configuration to a local disk.



- **Load Settings from PC** : Click **Browse** button to locate a configuration file to restore, and then click **Upload** button to upload.
- **Reset To Factory Default** : Click **Default** button to reset back to the factory default settings and expect **Successful** loading message. Then, click **Reboot** button to activate.

8.4.6 Firmware Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or bugs fix. It takes around **2 minutes** to upgrade due to complexity of firmware. To upgrade system firmware, click **Browse** button to locate the new firmware, and then click **Upgrade** button to upgrade.

Firmware Upgrade

Firmware Information

Firmware Version : Cen-CPE-NSH2 V0.0.4 Beta Version
Firmware Date : 2009-09-03 09:26:27

Update Firmware :

 From time to time, the product may release new versions of the firmware. You can check and download up-to-date firmware and click Browser button to locate the file from your local harddisk.



1. To prevent data loss during firmware upgrade, please back up current settings before proceeding.
2. Do not interrupt during firmware upgrade including power on/off as this may damage system.
3. Never perform firmware upgrade over wireless connection or via remote access connection.

8.4.7 Network Utility

The administrator can diagnose network connectivity via the PING and TRACEROUTE utility.

Please click on **Utilities -> Network Utility** and follow the below setting

Network Utility

Ping

Destination IP/Domain: Count

Traceroute

Destination Host: MAX Hop

Result

- **Ping** : This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
 - ➔ **Destination IP/Domain** : Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click **ping** button to proceed. The ping result will be shown in the **Result** field.
 - ➔ **Count** : By default, it's 5 and the range is from 1 to 50. It indicates number of connectivity test.

- **Traceroute** : Allows tracing the hops from the WLO-15814N / WLO-15802N device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the **Start** button, click Stop button to stopped test
 - ➔ **Destination Host** : Specifies the Destination Host for the finding the route taken by ICMP packets across the network.
 - ➔ **MAX Hop** : Specifies the maximum number of hops(max time-to-live value) traceroute will probe.

8.4.8 Reboot

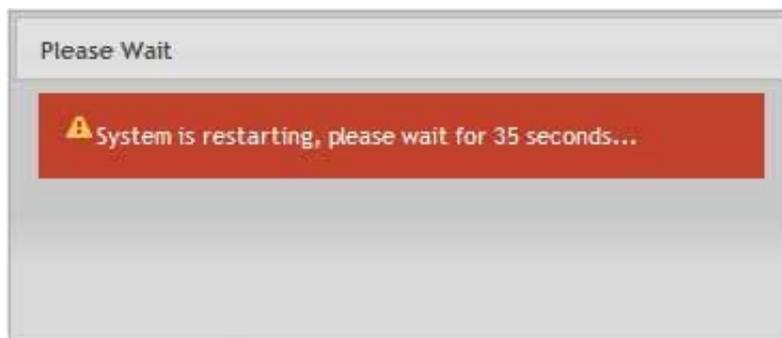
This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

Reboot

 You must be reboot the system after changing settings. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Reboot

A reminder will be available for remaining time to complete. If power cycle is necessary, please wait till completion of the reboot process.



The **System Overview** page appears upon the completion of reboot.

8.5 Access Control List

8.5.1 IP Filter Setup

Allows to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules.

Please click on **Advance -> IP Filter Setup** and follow the below setting.

IP Filter Setup

| # | Source Address/Mask | Port | Destination Address/Mask | Port | In/Out | Protocol | Listen | Action | Interface | Delete | Edit |
|-------------------------|---------------------|------|--------------------------|------|--------|----------|--------|--------|-----------|--------|------|
| No IP Rule in the List! | | | | | | | | | | | |

- **Source Address/Mask** : Enter desired source IP address and netmask; i.e. 192.168.2.10/32.
- **Source Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **Destination Address/Mask** : Enter desired destination IP address and netmask; i.e. 192.168.1.10/32
- **Destination Port** : Enter a port or a range of ports as **start:end**; i.e. port 20:80
- **In/Out** : Applies to Ingress or egress packets
- **Protocol** : Supports **TCP**, **UDP** or **ICMP**.
- **Listen** : Click **Yes** radial button to match TCP packets only with the SYN flag.
- **Active** : **Deny** to drop and **Pass** to allow per filter rules
- **Interface** : The interface that a filter rule applies



All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

- **Example 1** : Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | Pass | LAN |
| 2 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |

- **Example 2** : All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

| Rule | Source | | Destination | | In/Out | Protocol | Listen | Action | Side |
|------|----------------|------|------------------|------|--------|----------|--------|--------|------|
| | IP/Mask | Port | IP/Mask | Port | | | | | |
| 1 | 192.168.2.0/24 | | 192.168.2.254/32 | 22 | In | TCP | n | Deny | LAN |
| 2 | 192.168.2.2/32 | | 192.168.2.254/32 | 22 | In | TCP | n | pass | LAN |

8.5.2 MAC Filter Setup

Allows to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important to note that MAC filter rules have precedence over IP Filter rules.

Please click on **Advance -> MAC Filter Setup** and follow the below setting.

MAC Filter Setup

The screenshot shows two main sections: 'MAC Rules' and 'MAC Filter List'.
 In the 'MAC Rules' section, there is a dropdown menu for 'Action' currently set to 'Disabled', a 'Save' button, and a text input field for 'MAC Address' with an 'Add' button.
 The 'MAC Filter List' section displays a table with the following structure:
 - Header row: #, MAC Address, Delete, #, MAC Address, Delete
 - Content row: No MAC Rule in the List!

- **MAC Filter Rule** : By default, it's "**Disable**". Options are **Disabled**, **Only Deny List MAC** or **Only Allow List MAC**. Click **Save** button to save your change.

Two ways to set the MAC Filter List:

➔ **Only Allow List MAC.**

The wireless clients in the MAC Filter List will be **allowed** to access to Access Point; All others will be denied.

➔ **Only Deny List MAC.**

The wireless clients in the MAC Filter List will be **denied** to access to Access Point; All others will be allowed.

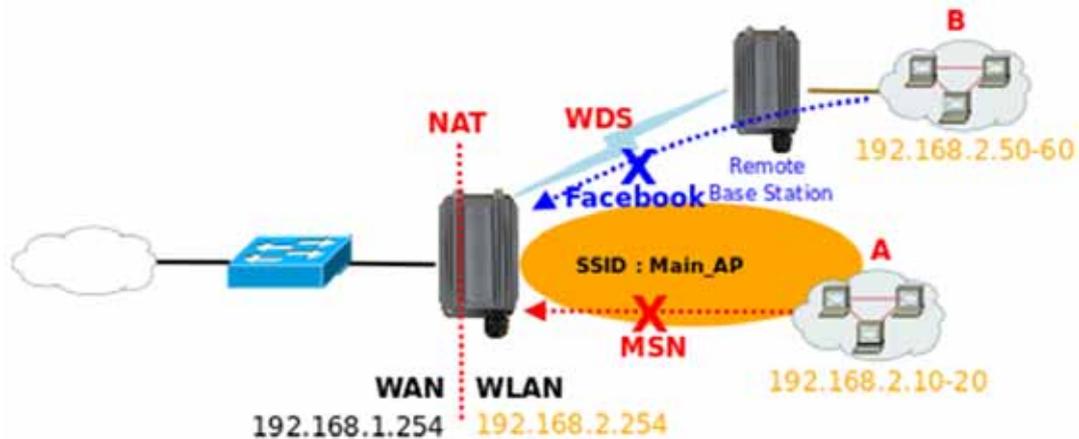
- **MAC Address** : Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.

There are a maximum of **20** clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Delete** buttons.

Click **Reboot** button to activate your changes

8.5.3 Parental Control Setup

Parental Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites.



Please click on **Advance -> Parental Control** and follow the below setting.

Parental Control

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

Protocol:

Local Port:

Destination Port:

Active: Enable Disable

Parental Control List

| # | Comment Rule | Active | Delete | Edit |
|----------------------|-----------------|--------|--------|------|
| No Rule in the List! | | | | |

- **Rules** : control can be managed by a rule. Use the settings on this screen to establish an access policy.
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click "**Add**" button to add in the MAC group of each rule. Click "**Remove**" button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.

→ **Protocol** : Select **Any** or specify protocol(**TCP**, **UDP**, **ICMP**, **URL Blocking** and **Application**) from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Local(LAN)/ Destination Port can not used.

If you want to block websites with specific URL address or using specific keywords, enter each URL or keywords in the “**URL Blocking**” field and click “**Add**” button to add in the URL Blocking list of each rule. Click “**Remove**” button can remove URL or keywords.

URL Blocking :

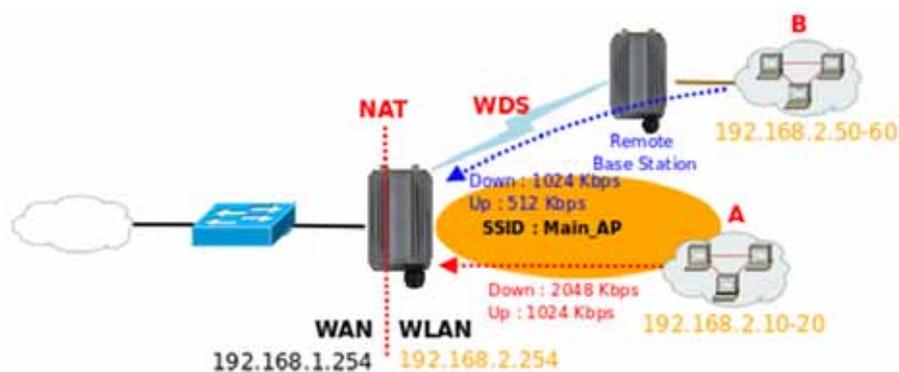
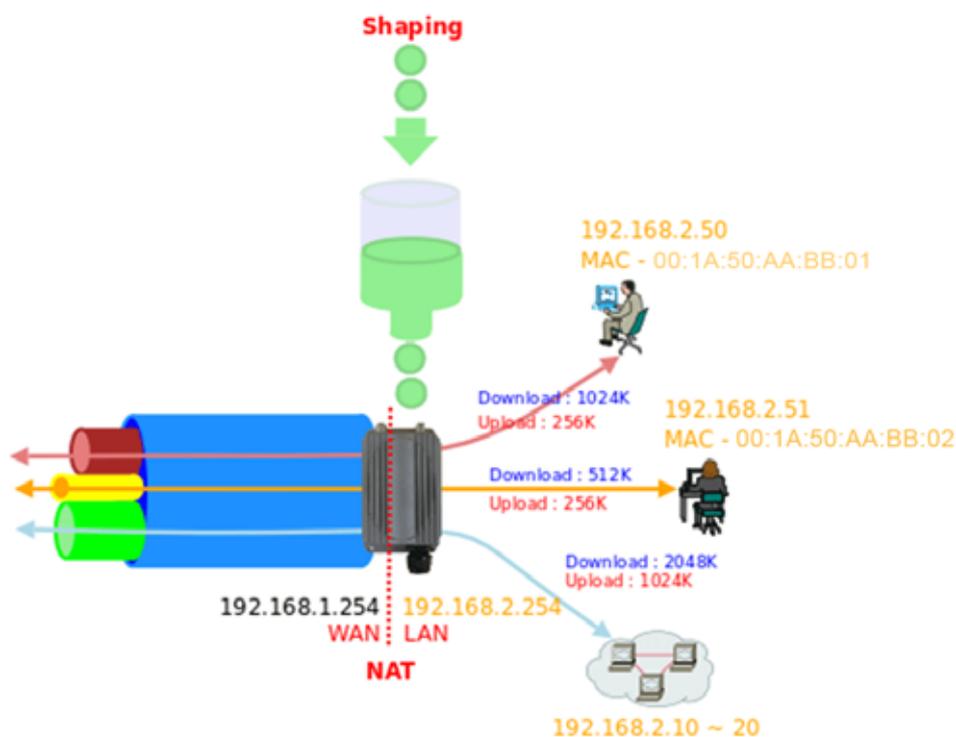
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Active** : Check **Enable** button to activate this rule, and **Disable** to deactivate.

Click “**Add**” button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

8.5.4 QoS Setup

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as FTP) to form a flow.



Please click on **Advance** -> **QoS** and follow the below setting.

QoS Setup

Rules

Comment:

MAC Address:

Local IP: -

Destination IP: -

DSCP Class:

Protocol:

Local Port:

Destination Port:

QoS List

| # | Comment | Remark DSCP | Bandwidth(U/D) | Delete | Edit |
|--------------------------|---------|-------------|----------------|--------|------|
| No QoS Rule in the List! | | | | | |

Action

Remark DSCP:

Bandwidth: Enable Disable

Upload: Kbits

Download: Kbits

- **Rules** : Use the rules to define the classifiers. After you define the rules, you can specify action to act upon the traffic that matches the rules
 - ➔ **Comment** : Enter a descriptive name for this rule for identifying purposes.
 - ➔ **MAC Address** : Enter MAC address in valid MAC address format(xx:xx:xx:xx:xx:xx) and click “**Add**” button to add in the MAC group of each rule. Click “**Remove**” button can remove MAC address in the group of each rule. There are **10** MAC address maximum allowed in each rule.
 - ➔ **Local / Destination IP** : Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.
 - ➔ **DSCP Class** : Differentiated services code point, DSCP. Select Any or specify classify traffic from drop-down list. The Per-Hop Behavior (PHB) is indicated by encoding a 6-bit value—called the Differentiated Services Code Point (DSCP)—into the 8-bit Differentiated Services (DS) field of the IP packet header. Below depicts class for DSCP.
 - ✓ **BE** : *Default* PHB, which is typically best-effort traffic
 - ✓ **EF** : *Expedited Forwarding* PHB, dedicated to low-loss, low-latency traffic
 - ✓ **AF** : *Assured Forwarding* PHB, which gives assurance of delivery under conditions. The AF behavior group defines four separate AF classes. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields twelve separate DSCP encodings from **AF11** through **AF43** (see table)

| DROP Precedence | Class 1 | Class 2 | Class 3 | Class 4 |
|-----------------|---------|---------|---------|---------|
| Low Drop | AF11 | AF21 | AF31 | AF41 |
| Medium Drop | AF12 | AF22 | AF32 | AF42 |
| High Drop | AF13 | AF23 | AF33 | AF43 |

- **Protocol** : Select **Any** or specify protocol from drop-down list. When you select **ICMP** or **Layer 7 Application** , the Source/ Destination Port can not used.
- **Local Port** : Specify local port(LAN port) range required for this rule
- **Destination Port** : Specify destination port range required for this rule
- **Action** : After configuring rule, a policy rule ensures that a traffic flow gets the requested treatment in the network.
 - **Remark DSCP** : Specify a new DSCP class, if you want to replace or remark the DSCP
 - **Bandwidth** : Click "**Enable**" to activate function, and click "**Disable**" to deactivate function
 - **Upload / Download** : Specify the bandwidth in kilobit per second (Kbps). Enter a number between **8** to **8192**, default upload is **128** Kbps, download is **1024** Kbps.

Click "**Add**" button to add QoS rule to List. There are **10** rules maximum allowed in this QoS List. All rules can be removed or edited on the List. Click **Reboot** button to activate your changes.

When you create rules on the QoS List, the previous rules have higher priority. . Below depict the examples for explaining priority of QoS setup.

- **Example 1** : On this setting, the FTP has **1024** Kbps upload and **8196** Kbps download on **192.168.2.10**. The remaining IP address and other remaining protocol of IP address 192.168.2.10 only can use total bandwidth **512** Kbps bandwidth. Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |
| 2 | | | ANY | ANY | NO | 512/512 |

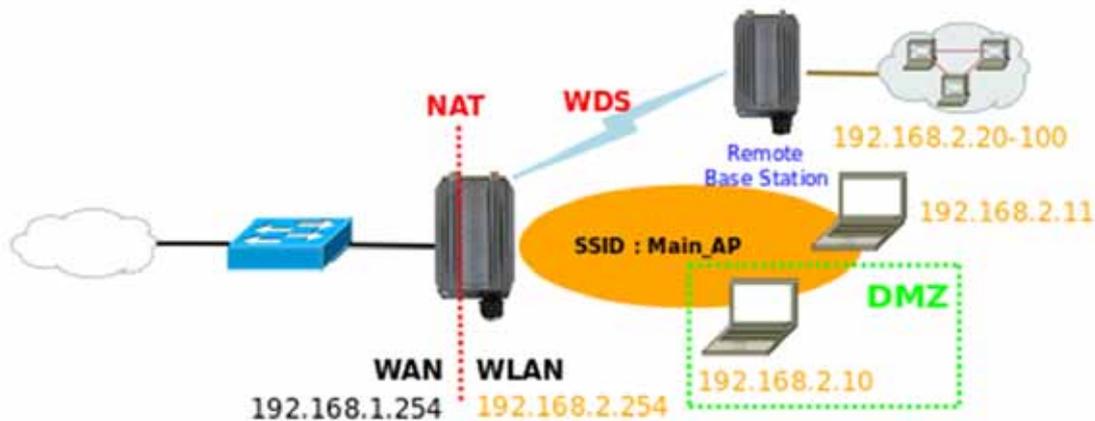
- **Example 2** : On this setting, the FTP has **512** Kbps upload and **512** Kbps download on **192.168.2.10** Because rule 1's priority is higher than rule 2

| Rule | Source IP | Destination IP | DSCP | Protocol | Remark DSCP | Bandwidth (Up/Down) |
|------|--------------|----------------|------|----------|-------------|---------------------|
| 1 | | | ANY | ANY | NO | 512/512 |
| 2 | 192.168.2.10 | | ANY | FTP | NO | 1024/8196 |

8.6 Resource Sharing

8.6.1 DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.



Please click on **Advance** -> **DMZ** and follow the below setting.

DMZ Setup

DMZ

DMZ: Enable Disable

IP Address:

Save

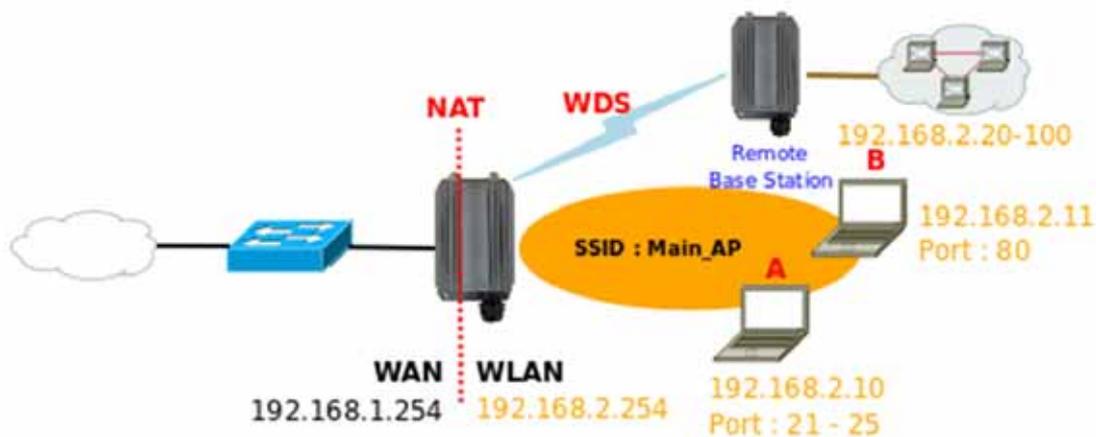
- **DMZ** : By default, it's "**Disable**". Check **Enable** radial button to enable DMZ.
- **IP Address** : Enter IP address of DMZ host and only one DMZ host is supported.

Click **Save** button to save your changes. Click **Reboot** button to activate your changes.

8.6.2 Virtual Server (Port Forwarding)

“Virtual Server” can also referred to as “Port Forward” as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.



Please click on **Advance** -> **Virtual Server** and follow the below setting.

Virtual Server Setup

Virtual Server

Virtual Server : Enable Disable

Description :

Private IP :

Protocol Type : TCP UDP

Private Port :

Public Port :

Virtual Server List

| # | Status | Description | Protocol | Private IP | Public Port | Private Port | Delete | Edit |
|----------------------|--------|-------------|----------|------------|-------------|--------------|--------|------|
| No Rule in the List! | | | | | | | | |

- **Virtual Server** : By Default, It's "**Disable**". Check **Enable** radial button to enable Virtual Server.
- **Description** : Enter appropriate message for resource sharing via Virtual Server.
- **Private IP** : Enter corresponding IP address of internal resource to share.
- **Protocol Type** : Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.
- **Private Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80
- **Public Port** : A port or a range of ports may be specified as **start:end**; i.e. port 20:80



The Private Port and Public Port can be different. However, total number of ports need to be the same. Example : Public Port is 11 to 20 and the Private Port can be a 10 ports range.

Click "**Add**" button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List. Click **Reboot** button to activate your changes.

While creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ one while both rules exist. Example 1 and 2 demonstrate proper usage of DMZ and Virtual Server rules.

- **Example 1** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all connections to TCP port 22 will be directed to TCP port 22 of 192.168.2.10 and remaining connections to port TCP **20~80** will be redirected to port TCP **20~80** of **192.168.2.11**

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.10 | 22 | 22 |
| 2 | TCP | 192.168.2.11 | 20:80 | 20:80 |

- **Example 2** : All connections should be redirected to **192.168.2.12** while DMZ is enabled. Since Virtual Server rules have precedence over the DMZ rule all other connections to TCP port **20~80** will be redirected to port **20~80** of **192.168.2.11**. The rule 2 won't take effect.

DMZ Enabled : 192.168.2.12

| Rule | Protocol | Private IP | Private Port | Public Port |
|------|----------|--------------|--------------|-------------|
| 1 | TCP | 192.168.2.11 | 20:80 | 20:80 |
| 2 | TCP | 192.168.2.10 | 22 | 22 |

8.7 System Status

This section breaks down into subsections of **System Overview**, **Associated Clients Status**, **WDS Link Status**, **Extra Information** and **Event Log**.

8.7.1 Overview

Detailed information on **System**, **WAN Information**, **LAN Information**, **Wireless Information** and **DHCP Server Status** can be reviewed via this page.

- **System** : Display the information of the system.

```

System
Host Name : WLO-15802N
Operating Mode : Router AP Mode
Location :
Description : 802.11a/n Wireless Outdoor Bridge, 200mW
Firmware Version : Cen-CPE-N5H2 V1.0.10 Version
Firmware Date : 2010-03-19 04:24:31
Device Time : 2000-01-01 00:04:06
System Up Time : 04:06
  
```

- **System Name** : The name of the system.
- **Operating Mode** : The mode currently in service.
- **Location** : The reminding note on the geographical location of the system.
- **Description** : The reminding note of the system.
- **Firmware Version** : The current firmware version installed.
- **Firmware Date** : The build time of the firmware installed.
- **Device Time** : The current time of the system.
- **System Up Time** : The time period that system has been in service since last reboot.

- **WAN Information** : Display the information of the WAN interface.

```

WAN Information
Mode : Static Mode
MAC Address : 00:1A:50:0A:7B:F9
IP Address : 192.168.1.254
IP Netmask : 255.255.255.0
IP Gateway : 192.168.1.1
Primary DNS :
Secondary DNS :
Receive Bytes : 31415
Receive Packets : 263
Transmit Bytes : 289764
Transmit Packets : 306
  
```

The WAN port specified **Dynamic IP**, the Release and Renew button will be show-up, click **Release** button to release IP address of WAN port, **Renew** button to renew IP address through DHCP server.

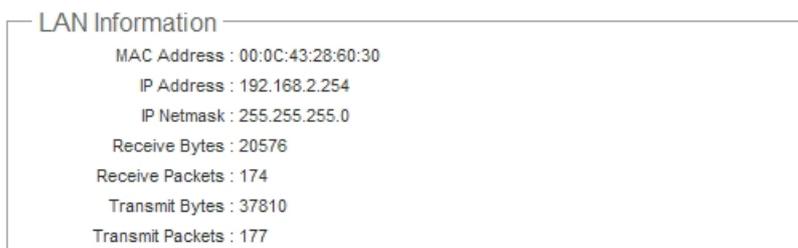


The WAN port specified **PPPoE** or **PPTP**, and the **Connect** and **DisConnect** button will be show up. Click “**Connect**” button to assigned IP address from PPPoE or PPTP server, “**DisConnect**” button to release IP address of WAN port.



- **Mode** : Supports Static, Dynamic, PPPoE and PPTP modes.
- **Reconnect Mode** : The current reconnect mode of the PPPoE or PPTP.
- **MAC Address** : The MAC address of the WAN port.
- **IP Address** : The IP address of the WAN port.
- **IP Netmask** : The IP netmask of the WAN port.
- **IP Gateway** : The gateway IP address of the WAN port.
- **Primary DNS** : The primary DNS server in service.
- **Secondary DNS** : The secondary DNS server in service.
- **Receive bytes** : The total received packets in bytes on the WAN port.
- **Receive packets** : The total received packets of the WAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the WAN port.
- **Transmit packets** : The total transmitted packets of the WAN port.

- **LAN Information** : Display total received and transmitted statistics on the LAN interface.



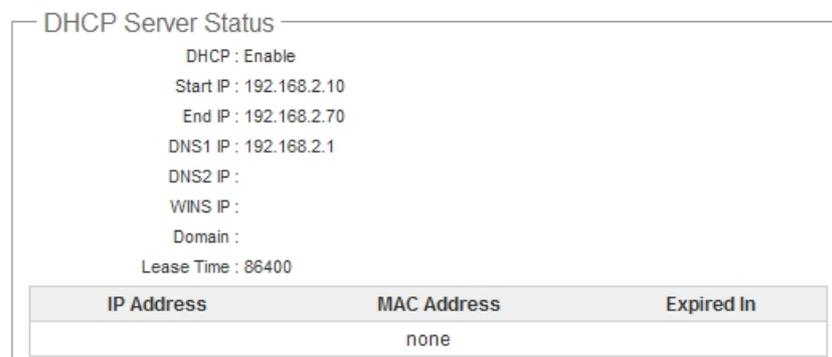
- **MAC Address** : The MAC address of the LAN port.
- **IP Address** : The IP address of the LAN port.
- **IP Netmask** : The IP netmask of the LAN port.
- **Receive bytes** : The total received packets in bytes on the LAN port.
- **Receive packets** : The total received packets of the LAN port.
- **Transmit bytes** : The total transmitted packets in bytes of the LAN port.
- **Transmit packets** : The total transmitted packets of the LAN port.

- **Wireless Information** : Display the detailed receive and transmit statistics of Wireless interface.



- **MAC Address** : The MAC address of the Wireless Port.
- **Channel** : The current channel on the Wireless port.
- **Rate** : The current Bit Rate on the Wireless port.
- **Receive bytes** :The total received packets in bytes on the Wireless port.
- **Receive packets** : The total received packets on the Wireless port.
- **Transmit bytes** : The total transmitted packets in bytes on the Wireless port.
- **Transmit packets** : The total transmitted packets on the Wireless port.

- **DHCP Server Status** : Users could retrieve DHCP server and DHCP clients' IP/MAC address via this field.



- **IP Address** : IP addresses to LAN devices by DHCP server.
- **MAC Address** : MAC addresses of LAN devices.
- **Expired In** : Shows how long the leased IP address will expire.

8.7.2 Associated Clients Status

It displays ESSID, on/off Status, Security Type, total number of wireless clients associated with all Virtual AP.

Wireless Clients Refresh

VAP Information

| VAP | ESSID | MAC Address | State | Security Type | Clients |
|------------|---------|-------------------|-------|---------------|---------|
| Primary AP | Main_AP | 00:1A:50:0A:7B:FA | On | Disable | 1 |
| VAP1 | | 00:00:00:00:00:00 | Off | Disable | 0 |
| VAP2 | | 00:00:00:00:00:00 | Off | Disable | 0 |
| VAP3 | | 00:00:00:00:00:00 | Off | Disable | 0 |
| VAP4 | | 00:00:00:00:00:00 | Off | Disable | 0 |
| VAP5 | | 00:00:00:00:00:00 | Off | Disable | 0 |
| VAP6 | | 00:00:00:00:00:00 | Off | Disable | 0 |

Primary AP Clients

| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | BandWidth | Idle Time | Connect Time | Disconnect |
|-------------------|----------------------|----------------------|-----------|-----------|--------------|------------|
| 00:1A:50:13:35:EF | 100%(-33dBm) | 100%(-38dBm) | 20MHz | 11 | 134 | Delete |

- **VAP Information** : Highlights key VAP information.
 - ➔ **VAP** : Available VAP from Primary AP to VAP6.
 - ➔ **ESSID** : Display name of ESSID for each VAP.
 - ➔ **MAC Address** : Display MAC address for each VAP.
 - ➔ **Status** : On/Off
 - ➔ **Security Type** : Display chosen security type; WEP, WPA/WPA2-PSK, WPA/WPA2-Enterprise.
 - ➔ **Clients** : Display total number of wireless connections for each VAP.

- **VAP Clients** : Display all associated clients on each Virtual AP.
 - ➔ **MAC Address** : MAC address of associated clients
 - ➔ **Signal Strength ANT0/ANT1** : Signal Strength of from associated clients.
 - ➔ **Bandwidth** : Channel bandwidth of from associated clients
 - ➔ **Idle Time** : Last inactive time period in seconds for a wireless connection.
 - ➔ **Connect Time** : Total connection time period in seconds for a wireless connection.
 - ➔ **Disconnect** : Click "Delete" button to manually disconnect a wireless client in a Virtual AP.

8.7.3 Show WDS Link Status

Peers MAC Address, antenna 0/1 received signal strength, phy mode and channel bandwidth for each WDS are available.

WDS Information

| WDS Link Status | | | | | | |
|-------------------|-------------------------|-------------------------|-------------|-----------|-----|-----|
| MAC Address | Signal Strength ANT0 | Signal Strength ANT1 | Phy Mode | BandWidth | MCS | SGI |
| 00:1A:50:0A:7B:F2 | 100% (-5 dBm) | 100% (-6 dBm) | HTMIX | 40M | 15 | 1 |

- **MAC Address** : Display MAC address of WDS peer.
- **Signal Strength ANT0/ANT1** : Indicate the signal strength of the respective WDS links.
- **Phy Mode** : Indicate the phy mode of the respective WDS linked.
- **BandWidth** : Indicate the channel bandwidth of the respective WDS linked.
- **MCS** : Indicate the MCS of the respective WDS linked.
- **SGI** : Indicate the SGI (Short Guard Interval) of the respective WDS linked. "1" indicate the Short Guard Interval, "0" indicate the Long Guard Interval.



*If display "no signal" Signal Strength ANT0/ANT1, you need check WDS configuration. Things to verify are **MAC Address, Channel and Security type**. Also, adjust antenna angle and Tx Power.*

8.7.4 Extra Info

Users could pull out information such as Route table, ARP table, MAC table, Bridge table or STP available in the drop-down list from system. The “Refresh” button is used to retrieve latest table information.

Extra Information Refresh

Extra Information
 Information: Netstat Information

Netstat Information

| Protocol | LiveTime | Status | SrcIP | SrcPort | DstIP | DstPort |
|----------|----------|-------------|--------------|---------|---------------|---------|
| tcp | 119 | TIME_WAIT | 192.168.2.22 | 3423 | 192.168.2.254 | 80 |
| tcp | 113 | TIME_WAIT | 192.168.2.22 | 3419 | 192.168.2.254 | 80 |
| udp | 5 | | 192.168.2.22 | 138 | 192.168.2.255 | 138 |
| tcp | 118 | TIME_WAIT | 192.168.2.22 | 3421 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3413 | 192.168.2.254 | 80 |
| tcp | 431999 | ESTABLISHED | 192.168.2.22 | 3425 | 192.168.2.254 | 80 |
| tcp | 90 | TIME_WAIT | 192.168.2.22 | 3415 | 192.168.2.254 | 80 |
| tcp | 91 | TIME_WAIT | 192.168.2.22 | 3417 | 192.168.2.254 | 80 |

- Netstat Information :** Select “**NetStatus Information**” on the drop-down list, the connection track list should show-up, the list can be updated using the Refresh button.

NetStatus will show all connection track on the system, the information include *Protocol, Live Time, Status, Source/Destination IP address and Port.*

- Route table information :** Select “**Route table information**” on the drop-down list to display route table.

WLO-15814N / WLO-15802N could be used as a L2 or L3 device. It doesn't support dynamic routing protocols such as RIP or OSPF. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of system's interfaces. When used as a L2 device, it could switch packets and, as L3 device, it's capable of being a gateway to route packets inward and outward.

Route Information

| Destination | Gateway | Netmask | Interface |
|-------------|-------------|---------------|-----------|
| 192.168.2.0 | 0.0.0.0 | 255.255.255.0 | bre0 |
| 192.168.1.0 | 0.0.0.0 | 255.255.255.0 | eth2 |
| 0.0.0.0 | 192.168.1.1 | 0.0.0.0 | eth2 |

- ARP table Information :** Select “**ARP Table Information**” on the drop-down list to display ARP table.

ARP associates each IP address to a unique hardware address (MAC) of a device. It is important to have a unique IP address as final destination to switch packets to.

ARP Table Information

| IP Address | MAC Address | Interface |
|--------------|-------------------|-----------|
| 192.168.2.26 | 00:1A:50:13:35:EF | bre0 |
| 192.168.1.27 | 00:1A:92:9F:A4:9B | eth2 |

- Bridge table information :** Select “**Bridge Table information**” on the drop-down list to display bridge table.

Bridge table will show Bridge ID and STP's Status on the each Ethernet bridge and its attached interfaces, the Bridge Port should be attached to some interfaces e.g. ra0 ~ra6 and wds0~wds3).

| Bridge Port | Bridge ID | STP Enabled | Interface |
|-------------|-------------------|-------------|-----------|
| bre0 | 8000.001A500a7bfa | no | ra0 |

- **Bridge MAC information :** Select “**Bridge MACs Information**” on the drop-down list to display MAC table.

This table displays local MAC addresses associated with wired or wireless interfaces, but also remember non-local MAC addresses learned from wired or wireless interfaces.

Ageing timers will be reset when existing MAC addresses in table are learned again or added when new MAC addresses are seen from wired or wireless interfaces as well. When time runs out for a particular entry, it will be pruned from the table. In that situation, switching packet to that particular MAC address will be discontinued.

| Port | MAC Address | Local | Ageing Timer |
|-----------|-------------------|-------|--------------|
| PrimaryAP | 00:1A:50:13:35:EF | no | 42.77 |
| PrimaryAP | 00:1A:50:0A:7B:FA | yes | 0.00 |

- **Bridge STP Information :** Select “**Bridge STP Information**” on the drop-down list to display a list of bridge STP information.

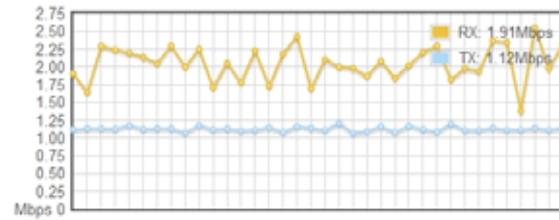
| | | | |
|-----------------------|-------------------|----------------------|------------|
| bre0 | | | |
| bridge id | 8000.001A500a7bfa | | |
| designated root | 8000.001A500a7bfa | | |
| root port | 0 | path cost | 0 |
| max age | 20.00 | bridge max age | 20.00 |
| hello time | 2.00 | bridge hello time | 2.00 |
| forward delay | 15.00 | bridge forward delay | 15.00 |
| ageing time | 300.00 | | |
| hello timer | 0.75 | tcn timer | 0.00 |
| topology change timer | 0.00 | gc timer | 0.75 |
| flags | | | |
| ra0 (1) | | | |
| port id | 8001 | state | forwarding |
| designated root | 8000.001A500a7bfa | path cost | 100 |
| designated bridge | 8000.001A500a7bfa | message age timer | 0.00 |
| designated port | 8001 | forward delay timer | 0.00 |
| designated cost | 0 | hold timer | 0.77 |
| flags | | | |

8.7.5 QoS Plot

The QoS Plot show graphs which continuously represents the current data traffic on each QoS rule. The chart scale and throughput dimension (bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics is updated automatically every 5 seconds. The throughput statistics of QoS can be updated manually using the **Refresh** button.

QoS Plot

| QoS List | | | |
|----------|---------|-------------|--------------------|
| # | Comment | Remark DSCP | Bandwidth(U/D)kbps |
| 1 | FTP | NO | 1024/2048 |



8.7.6 Event Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.

System Log

[Refresh](#) [Clear](#)

| Result | | | |
|---------------------|----------|----------|---|
| Time | Facility | Severity | Message |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: started, version 2.40 cachesize 150 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: compile time options: no-IPv6 GNU-getopt no-RTC no-MMU no-ISC-leasefile no-DBus no-I18N TFTP |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: reading /etc/resolv.conf |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: using nameserver 192.168.2.1#53 |
| 2000 Jan 1 00:00:11 | System | Info | dnsmasq[94]: cleared cache |
| 2000 Jan 1 00:00:38 | System | Info | Authentication successful for root from 192.168.2.22 |

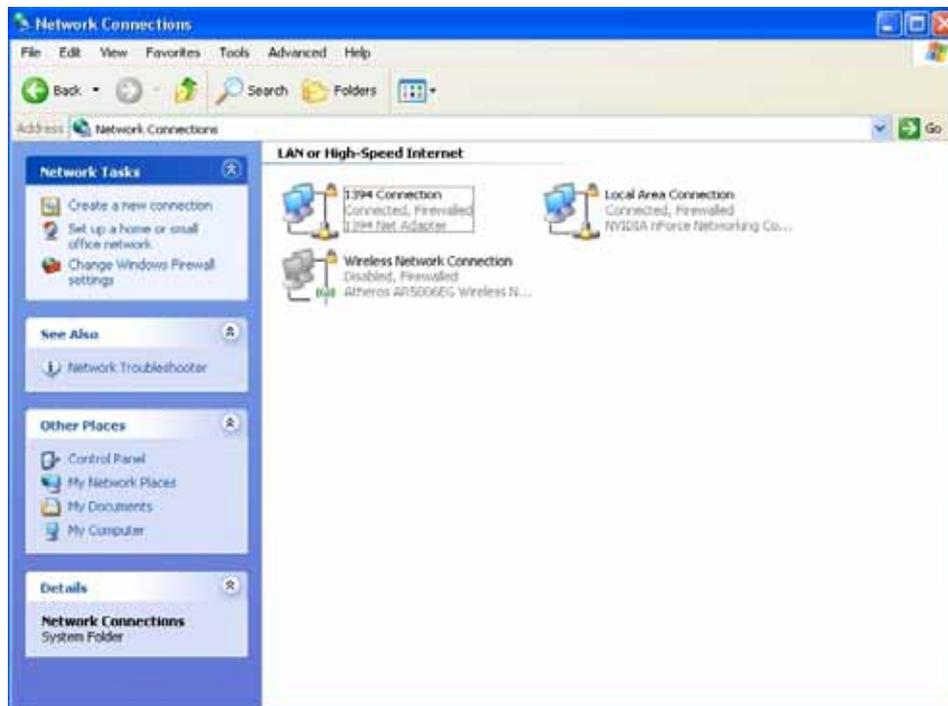
- **Time** : The date and time when the event occurred.
- **Facility** : It helps users to identify source of events such “System” or “User”
- **Severity** : Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message** : Description of the event.

Click **Refresh** button to renew the log, or click **Clear** button to clear all the record.

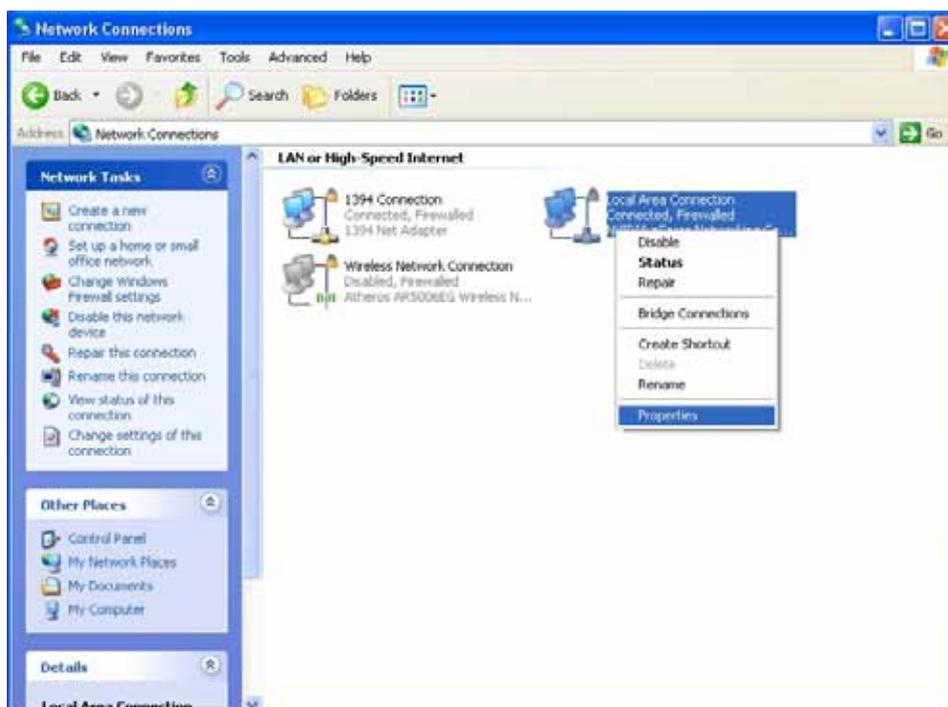
Appendix A. Windows TCP/IP Settings

■ Windows XP

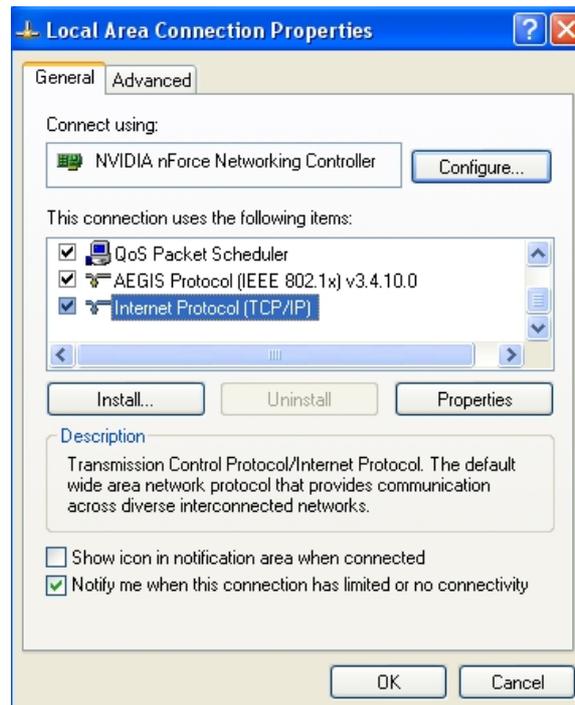
1. Click **Start -> Settings -> Control Panel**, and then “**Control Panel**” window appears. Click on “**Network Connections**”, and then “**Network Connections**” window appears.



2. Click right on “**Local Area Connection**”, and select **Properties**.



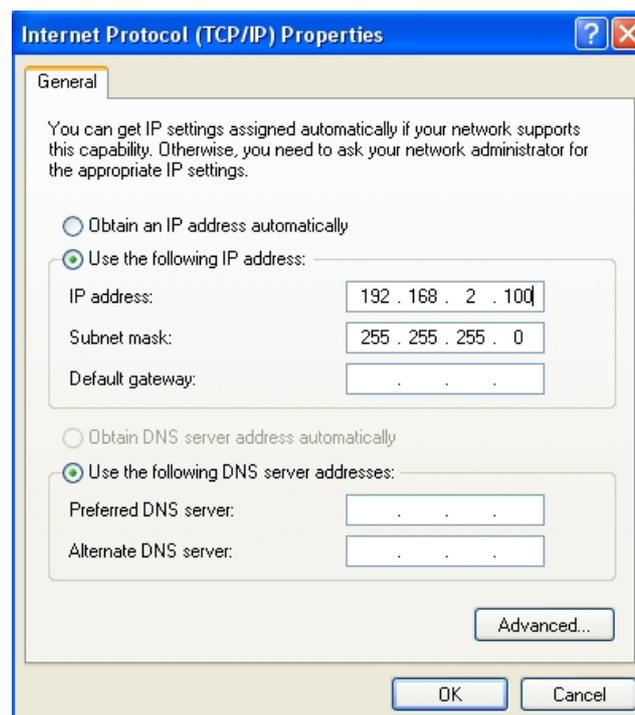
- In “**Local Area Connection Properties**” window, select “**Internet Protocol (TCP/IP)**” and click on **Properties** button.



- Select “Use the following IP address”, and type in

IP address : 192.168.2.100

Subnet mask : 255.255.255.0



Appendix B. WEB GUI Valid Characters

Table B WEB GUI Valid Characters

| Block | Field | Valid Characters |
|--------------------|--------------------|--|
| LAN | IP Address | IP Format; 1-254 |
| | IP Netmask | 128.0.0.0 ~ 255.255.255.252 |
| | IP Gateway | IP Format; 1-254 |
| | Primary DNS | IP Format; 1-254 |
| | Secondary DNS | IP Format; 1-254 |
| | Hostname | Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| WAN | Manual MAC Address | 12 HEX chars |
| | IP Address | IP Format; 1-254 |
| | IP Netmask | 128.0.0.0 ~ 255.255.255.252 |
| | IP Gateway | IP Format; 1-254 |
| | Hostname | Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | User name | Length : 32 0-9, A-Z, a-z |
| | Password | ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | MTU | 576 ~ 1492 for PPPoE; 1400 ~ 1460 for PPTP |
| | Idle Time | 0 ~ 60 minutes |
| | Primary DNS | IP Format; 1-254 |
| | Secondary DNS | IP Format; 1-254 |
| DDNS | Hostname | Length : 32 0-9, A-Z, a-z @ - _ . |
| | User Name | Length : 32 0-9, A-Z, a-z |
| | Password | ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| DHCP Server | Start IP | IP Format; 1-254 |
| | End IP | IP Format; 1-254 |
| | DNS1 IP | IP Format; 1-254 |
| | DNS2 IP | IP Format; 1-254 |
| | WINS IP | IP Format; 1-254 |
| | Domain | Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | Lease Time | 600 ~ 99999999 |

Table B WEB GUI Valid Characters (continued)

| Block | Field | Valid Characters |
|-------------------------|-----------------------|---|
| Management | System Name/ Location | Length : 32 0-9, A-Z, a-z Space ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | Description | 32 chars |
| | Password | Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | HTTP/ HTTPS Port | 1 ~ 65535 |
| | Telnet/ SSH Port | 1 ~ 65535 |
| SNMP | RO/RW community | Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] ; ` , . = |
| | RO/RW user | Length : 31 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] ; ` , . = |
| | RO/RW password | Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] ; ` , . = |
| | Community | Length : 32 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] ; ` , . = |
| | IP | IP Format; 1-254 |
| General Setup | Tx Power | 1-100 % |
| Wireless Profile | Profile Name | 32 chars |
| | ESSID | Length : 31 Space 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | WEP Key | 10, 26 HEX chars or 5, 13 ASCII chars |
| | Pre-shared Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| Advanced Setup | Beacon Interval | 20 ~ 1024 |
| | Date Beacon Rate | 1 ~ 255 |
| | Fragment Threshold | 256 ~ 2346 |
| | RTS Threshold | 1 ~ 2347 |

Table B WEB GUI Valid Characters (continued)

| Block | Field | Valid Characters |
|--------------------------|-------------------------|---|
| Virtual AP Setup | ESSID | Length : 31 Space 0-9, A-Z, a-z ~ ! @ # \$ % ^ * () _ + - { } : < > ? [] / ; ` , . = |
| | Maximum Clients | 1 ~ 32 |
| | VLAN ID | 1 ~ 4094 |
| | WEP Key | 10, 26 HEX chars or 5, 13 ASCII chars |
| | Group Key Update Period | >=60 seconds |
| | PMK Cache Period | > 0 minute |
| | Pre-Shared Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| | Radius Server IP | IP Format; 1-254 |
| | Radius Port | 1 ~ 65535 |
| | Shared Secret | 8 ~ 64 characters |
| | Session Timeout | >= 60 seconds; 0 is disable |
| WDS Setup | WEP Key | 10, 26 HEX chars or 5, 13 ASCII chars |
| | TKIP Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| | AES Key | 8 ~ 63 ASCII chars; 64 HEX chars |
| | Peer's MAC Address | 12 HEX chars |
| | Description | 32 chars |
| IP Filter | Source Address | IP Format; 1-254 |
| | Source Mask | 0 ~ 32 |
| | Source Port | 1 ~ 65535 |
| | Destination Address | IP Format; 1-254 |
| | Destination Mask | 0 ~ 32 |
| | Destination Port | 1 ~ 65535 |
| MAC Filter | MAC address | MAC Format; 12 HEX chars |
| Virtual Server | Description | 32 chars |
| | Private IP | IP Formate; 1-254 |
| | Private/ Public Port | 1 ~ 65535 |
| DMZ | IP Address | IP Format; 1-254 |
| QoS/ Parental Control | Comment | 32 chars |
| | MAC Address | MAC Format; 12 HEX chars |
| | Local/ Destination IP | IP Formate; 1-254 |

| Block | Field | Valid Characters |
|--------------|-------------------------|-------------------------|
| | Local/ Destination Port | 1 ~ 65535 |
| | Upload & Download | 8 ~ 8192 digital number |

Appendix C. MCS Data Rate

The table below shows the relationships between the variables that allow for the maximum data rate

Table C MCS Data Rate

| MCS Index | Modulation | Data Rate (Mb/s) | | | |
|-----------|------------|------------------------|----------------------|------------------------|----------------------|
| | | Channel Bandwidth = 20 | | Channel Bandwidth = 40 | |
| | | Long Guard Interval | Short Guard Interval | Long Guard Interval | Short Guard Interval |
| 0 | BPSK | 6.5 | 7.2 | 13.5 | 15.0 |
| 1 | QPSK | 13.0 | 14.4 | 27.0 | 30.0 |
| 2 | QPSK | 19.5 | 21.7 | 40.5 | 45.0 |
| 3 | 16-QAM | 26.0 | 28.9 | 54.0 | 60.0 |
| 4 | 16-QAM | 39.0 | 43.3 | 81.0 | 90.0 |
| 5 | 64-QAM | 52.0 | 57.8 | 108.0 | 120.0 |
| 6 | 64-QAM | 58.5 | 65.0 | 121.5 | 135.0 |
| 7 | 64-QAM | 65.0 | 72.2 | 135.0 | 157.5 |
| 8 | BPSK | 13.0 | 14.4 | 27.0 | 30.0 |
| 9 | QPSK | 26.0 | 28.9 | 54.0 | 60.0 |
| 10 | QPSK | 39.0 | 43.3 | 81.0 | 90.0 |
| 11 | 16-QAM | 52.0 | 57.8 | 108.0 | 120.0 |
| 12 | 16-QAM | 78.0 | 86.7 | 162.0 | 180.0 |
| 13 | 64-QAM | 104.0 | 115.6 | 216.0 | 240.0 |
| 14 | 64-QAM | 117.0 | 130.0 | 243.0 | 270.0 |
| 15 | 64-QAM | 130.0 | 114.4 | 270.0 | 300.0 |

Note :

- ✓ When MCS=32, only Short Guard Interval option is supported, Channel Bandwidth=20 is not supported. If Channel Bandwidth=40, the HT duplicate 6Mbps.
- ✓ When MCS=0~7(One Tx Stream), Guard Interval and Channel Bandwidth are supported
- ✓ When MCS=8~15(Two Tx Stream), Guard Interval and Channel Bandwidth are supported

Appendix D. System Manager Privileges

There are two system management accounts for maintaining the system; namely, the **root** and **admin** accounts are with different levels of privileges. The root manager account is empowered with full privilege to Read & Write while the admin manager account is Read only.

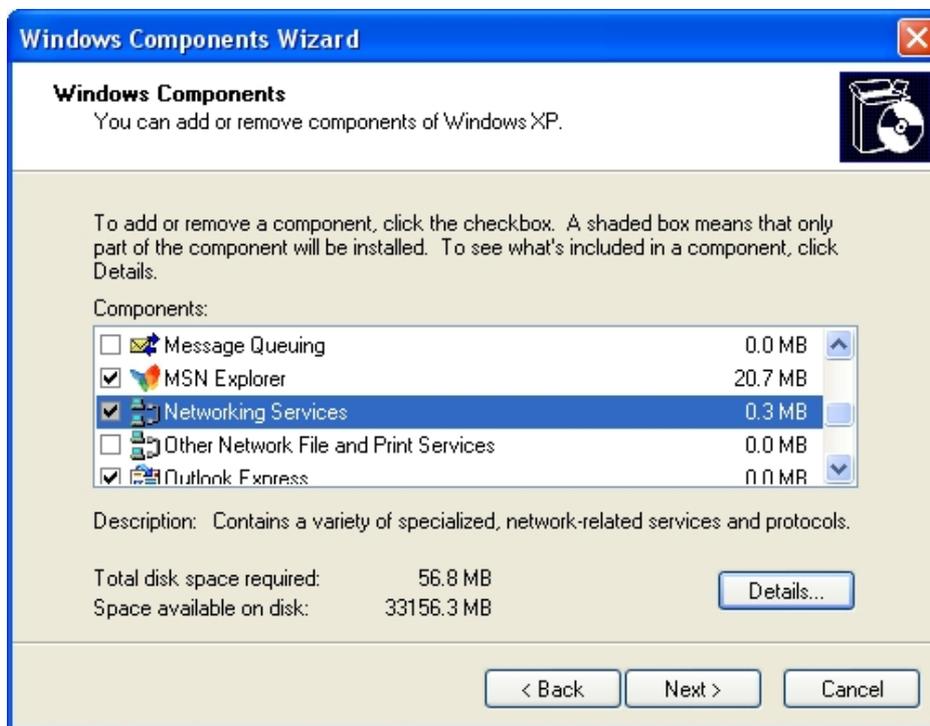
The following table display CPE admin account's privileges.

| Main Menu | Sub Menu | Group | Admin Privilege |
|----------------------|------------------|--------------------|-----------------|
| System | Operating Mode | | Read |
| | WAN | | Read |
| | LAN | | Read & Write |
| | DDNS | | Read & Write |
| | Time Server | | Read & Write |
| | UPNP | | Read & Write |
| | SNMP | | Read |
| Wireless | General | | Read |
| | Advanced | | Read |
| | Site Survey | | Read |
| Advance | DMZ | | Read |
| | IP Filter | | Read |
| | MAC Filter | | Read |
| | Virtual Server | | Read |
| | Parental Control | | Read |
| | QoS | | Read |
| Administrator | Management | System Information | Read |
| | | Root Password | Read |
| | | Admin Password | Read & Write |
| | | Login Methods | Read |
| | | Ping Watchdog | Read |
| | Profile Settings | Backup Settings | Read & Write |
| | | Restore Settings | Read |
| | | Reset to Default | Read |
| | System Upgrade | | Read |
| | Network Utility | | Read & Write |

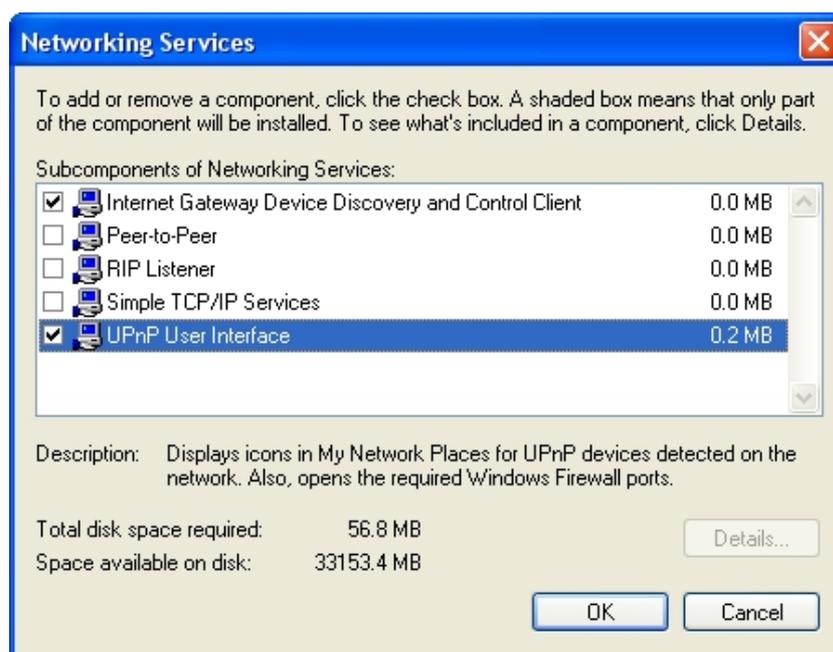
| | | | |
|--|--------|--|--------------|
| | Reboot | | Read & Write |
|--|--------|--|--------------|

Appendix E. Enabling UPnP in Windows XP

1. Open the “**Add/Remove Programs**” control panel, and then click on “**Add/Remove Windows Components**” in the sidebar. Scroll down and find “**Networking Services**”, highlight it, and then click **Details**.



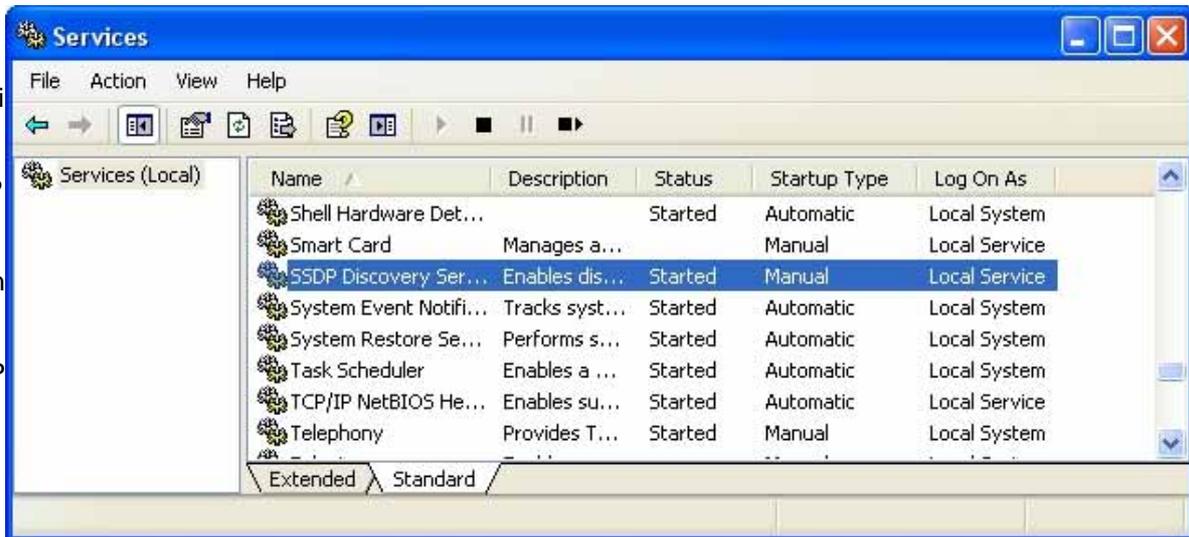
2. In the “**Networking Services**” window, ensure that the “**Internet Gateway Device**” and “**UPnP User Interface**” options are checked. If they are not, check it to enable them, as shown below, and click OK to continue.



3. Next, in the “**Control panel**”, open the “**Administrative Tools**” and then open “**Services**”. Scroll down until you find the “**SSDP Discovery Interface**”. If the Status is not **Started**, double-click on *SSDP Discovery Interface* to open the

service properties. Change the startup type to **Automatic**, then close the properties. Now, right-click on **SSDP Discovery Services**, and choose **Start** from the pop-up menu. The SSDP Discovery Service will then be running and start each time you boot.

4. After enabling UPnP and starting the SSDP Discovery Service, it



may take few minutes for the "Air Force One 5" to be discovered and appear in your "My Network Places".

