

Ubiquiti Networks Inc.

# **INSTANT OUTDOOR HOTSPOT**

## User Manual



© 2006 Ubiquiti, Inc No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system without written consent. Information in this manual is subject to change without notice, and does not represent a commitment on the part of Ubiquiti.

Ubiquiti shall not be liable for incidental or consequential damages resulting from the furnishing, performance, or use of this manual.

All brand names used in this manual are the registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not constitute an endorsement by the trademark holder.



# Table of Contents

1.Product Overview .....	9
1.1 Compatibility and Requirements.....	9
1.2 AP-ONE HotSpot Manager Features.....	9
1.3 AP-ONE Features.....	9
1.4 AP-ONE HotSpot Manager Installation Guide .....	10
2.AP-ONE HotSpot Manager .....	11
2.1 Overview of AP-ONE HotSpot MS Interface .....	11
2.1.1AP-ONE HotSpot Manager Main Menu .....	13
2.1.2Network Topology Tab Information Panes.....	14
2.1.3Node Shortcut Menu .....	15
2.2 Getting Started with AP-ONE HotSpot MS .....	17
2.2.1Auto-Discovering Nodes .....	17
2.2.2Configuring a New Node.....	18
2.2.3Moving and Resizing Icons .....	20
2.2.4Adding Background Map Images .....	20
2.2.5Saving and Loading Profiles.....	22
2.2.6Using the Node Shortcut Menu.....	22
3. IP Networking .....	30
3.1 Using the Network Interfaces Tree.....	31
3.2 Configuring Basic IP Settings .....	31
3.2.1IP Address .....	31
3.2.2Subnet .....	31
3.2.3Enable/Disable Selected Interface .....	31
3.2.4PTP IP Address.....	32
3.2.5MAC Address .....	32
3.2.6MAC Spoofing .....	32
3.2.7STP Enable.....	32
3.3 Configuring Global Settings .....	32
3.3.1Default Gateway .....	32
3.3.2IP Forwarding .....	32
3.3.3DNS1 and DNS2.....	33
3.4 Using Table view .....	33
4. Static IP Routing.....	34
4.1 Configuring Routing Tables and Entries .....	35
4.1.1Adding a New Routing Table .....	35
4.1.2Remove an Existing Routing Table.....	36
4.1.3Adding Static Routing Entries.....	36
4.1.4Removing Static Routing Entries .....	37
4.1.5Modifying Static Routing Entries.....	37
4.1.6Repositioning Static Routing Entries .....	37
4.2Configuring Static Rules .....	37
4.2.1Adding Rule Entries .....	38
4.2.2Removing Rule Entries.....	39
4.2.3Modifying Rule Entries .....	39
4.2.4Repositioning Rule Entries .....	39

5. Wireless .....	40
5.1 Setting Operational Modes .....	41
5.1.1 Selected Operational Mode .....	41
5.1.2 Configuring AP-ONE as an Access Point .....	42
5.1.3 Configuring AP-ONE as a WDS Mode .....	45
5.1.4 Using Site Survey Operation .....	46
5.2 Configuring Radio Settings .....	47
5.2.1 Selecting Physical Layer Options .....	48
5.2.2 Setting Channels and Frequencies .....	48
5.2.3 Setting Transmission Rates .....	48
5.2.4 Setting the MAC Address .....	49
5.2.5 Setting Frag .....	49
5.2.6 Setting RTS .....	49
5.2.7 Selecting Diversity Options .....	49
5.2.8 Selecting Antenna Options .....	49
5.2.9 Setting Transmitted Power .....	49
5.3 Configuring Security Settings .....	50
5.3.1 Setting Wired Equivalent Privacy (WEP) .....	50
5.3.2 Setting Wi-Fi Protected Access (WPA) .....	50
5.3.3 Configuring Access Control Lists (ACL) .....	52
5.4 Configuring Atheros Advanced Capabilities .....	53
6. Firewall and NAT .....	57
6.1 Firewall and NAT Chains .....	57
6.1.1 Firewall Chains .....	57
6.1.2 NAT Chains .....	57
6.2 Configuring Firewall Rules .....	58
6.2.1 Configuring Firewall Matching Fields .....	59
6.3 Configuring NAT Rules .....	64
6.3.1 Configuring NAT Matching fields .....	65
6.3.2 Examples .....	68
7. DHCP .....	72
7.1 Configuring a DHCP SERVER .....	72
7.1.1 Setting DHCP Server Fields .....	73
7.1.2 Lease Time Strategies .....	75
7.2 Configuring a DHCP CLIENT .....	76
7.3 Configuring a DHCP Relay .....	77
8. Quality of Service .....	79
8.1 The QoS window tab .....	79
8.1.1 Traffic Classes .....	80
8.1.2 Traffic Policies .....	81
8.1.3 Network Interfaces .....	81
8.2 Differentiating network traffic .....	82
8.3 Guarantees and Limitations .....	83
8.3.1 Committed Information Rate (CIR) .....	84
8.3.2 Peak Information Rate (PIR) .....	84
8.3.3 Excess Burst Size (EBS) .....	84
8.3.4 Committed Burst Size (CBS) .....	85
8.3.5 Priority .....	85
8.4 Example: Bandwidth reservation for FTP Servers .....	86
8.4.1 Single Class per Policy .....	87
8.4.2 Parallel Classes .....	89
8.4.3 Class Hierarchy .....	91

8.5 Example: Elimination of P2P Traffic.....	93
8.5.1 Shared Policies .....	95
8.6 Example: Access Point Bandwidth Sharing .....	95
8.6.1 New QoS Entry .....	95
8.6.2 QoS Statistics .....	95
8.7 Design Guidelines and Limitations .....	96
8.7.1 Destination/Source MAC match type .....	97
8.7.2 Application match type .....	97
8.7.3 Child to Parent class relation .....	97
8.7.4 PIR on parallel classes .....	97
8.7.5 Efficiency considerations .....	98
8.8 Frequently Asked Questions.....	98
8.8.1 Submit, Apply Changes: I'm confused! .....	98
9. System Services .....	99
9.1 Configuring SNMP Settings .....	100
9.2 Configuring HTTP Settings .....	101
9.3 Configuring SSH Settings .....	102
9.4 Configuring NTP Settings.....	103
9.5 Setting the Administrator Password .....	104
10. Monitoring and Statistics.....	107
10.1 Using the Status Info Dialog Box .....	107
10.2 Using the Current Throughput Graph .....	107
10.3 Viewing Packet Statistics .....	108
10.4 Viewing the ARP table .....	109
10.5 Viewing the Open Connections List .....	110
10.6 Using Monitor Utilities .....	111
12.6.1 Pinging (ICMP Utility).....	111
12.6.2 Using Traceroute.....	112
10.7 Viewing System Properties.....	114
11. MRTG Support .....	115
11.1 Using MRTG .....	116
12. Appendix 1: Zero Configuration .....	117
12.1 Operation .....	117
12.2 Physical Distribution.....	119
12.3 HotSpot Configuration .....	123
12.3.1 Blackhaul Interface Settings .....	124
12.3.2 Ethernet Settings .....	125
12.3.3 Hot Spot .....	126
12.3.4 Statistics .....	127
12.4 Design Guidelines .....	127
12.4.1 Stability Considerations.....	128
12.4.2 Performance Considerations.....	128
12.4.3 Security Considerations.....	130
12.4.4 Deployment Considerations .....	133
12.4.5 Security Considerations.....	134
12.5 Limitations.....	135
12.5.1 Roaming .....	135
12.6 HotSpot Wizard .....	135
12.6.1 HotSpot Main Tab.....	135
12.6.2 Using the HotSpot Wizard.....	138

12.6.3 HotSpot Configuration Example .....	146
13. Index .....	155





# 1. Product Overview

---

The **AP-ONE Hotspot Management System (AP-ONE HMS)** is used to configure and manage wireless networks of **AP-ONE HotSpot** nodes. AP-ONE HMS has been designed to provide network administrators with a comprehensive and simple way to control and configure their network nodes.

## 1.1 Compatibility and Requirements

The AP-ONE HMS software operates on any PC or Mac supported by Java. That is any version of Microsoft Windows (98/ME/2000/NT/XP) or GNU/Linux.

## 1.2 AP-ONE HotSpot Manager Features

- Optimized communication protocol between AP-ONE's software and AP-ONE HMS featuring high levels of interactivity. Additionally an advanced encryption scheme can guarantee secure configuration and monitoring of AP-ONE nodes.
- New graph-based statistics providing real time bandwidth utilization per network interface.
- New robust network topology display.
- Built-in Multi Router Traffic Grapher (MRTG) support

## 1.3 AP-ONE Features

- Advanced fault tolerant mechanisms guaranteeing node stability.
- DHCP leases information added.
- Wireless Functionality
  - Advanced Wireless Security (WPA, 802.1x)
  - Best Channel Selection Algorithm
  - Country Code Selection (+ out of band modes)
  - Wireless to wireless traffic filtering
  - Mac Address Spoofing
  - Advanced Firewall functionality
  - NTP (Network Time Protocol) service

## 1.4 AP-ONE HotSpot Manager Installation Guide

For a Windows installation, double-click the `AP-ONE_HotSpotManager_setup_vX.exe` installer and follow the prompts. The installer comes bundled with jre 1.4, so you do not have to pre-install it.

For a Linux or Macintosh installation, unzip the `AP-ONE_HotSpotManagervX_jars.zip` file and launch the application as `java -jar AP-ONE_HotSpotManagervX.jar` from the current directory. JRE (v1.4) must be preinstalled.

## 2. AP-ONE HotSpot Manager

If your goal is to deploy several wireless access points in one system, central management is recommended. Even if you plan to begin with a smaller network, but expect to expand in the future, a centrally managed system should be considered. The AP-ONE HotSpot Network Management System (AP-ONE HMS) provides an effective, turnkey management solution that covers the needs of most users.

Using **AP-ONE HotSpot Manager** you can:

- Manage access points and devices on the wireless network
- Configure network nodes, polling settings, and other parameters
- Load and save network configurations
- Configure and view network topology
- Auto-discover available nodes
- Analyze network traffic using the Multi Router Traffic Grapher (MRTG)

### 2.1 Overview of AP-ONE HotSpot MS Interface

The user interface utilizes typical drop down menus, short cut menus (right click) and tabbed/sub-tabbed panes inside the main window.

#### AP-ONE HotSpot Manager Main Window

The AP-ONE HMS window is a graphical user interface that facilitates viewing, configuring and monitoring your wireless network. The interface includes a typical main menu, tabbed panes containing graphical and textual information and shortcut menus that allow you to navigate to other windows, tabs and dialog boxes.

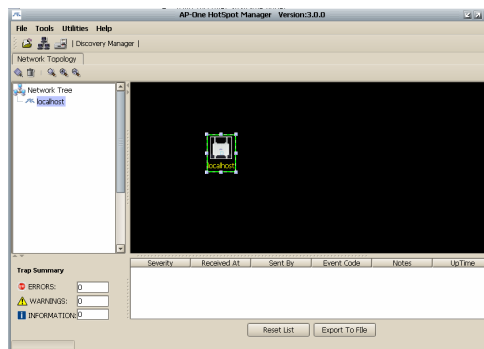


Figure 1. AP-ONE HotSpot Manager Main Window

## Main Menu

The **AP-ONE HMS** window features a menu system with four main menu headings: **File**, **Tools**, **Utilities** and **Help**.

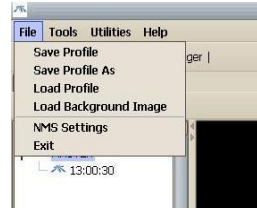


Figure 2. AP-ONE HMS Main Menu System

## Tabbed Panes

The main body of the AP-ONE HMS window displays information in tabbed panes. When AP-ONE HMS starts the **Network Topology** tab is available. This tab contains three information panes: the **Topology Map**, the **Registered Node List** and the **Node Status** pane.

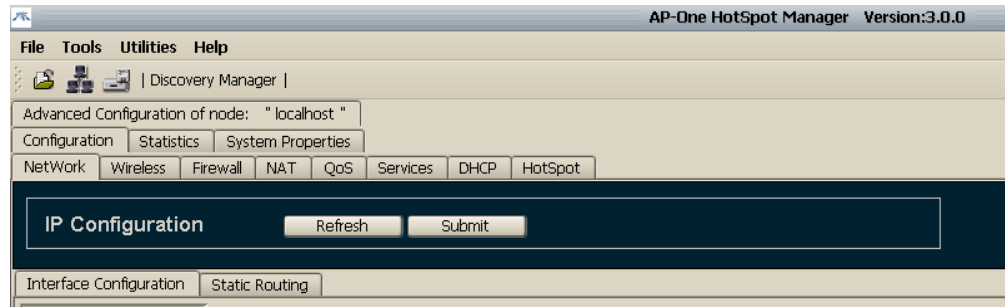


Figure 3. AP-ONE HMS Tabbed Panes

## Node Shortcut Menu

Many other functions are accessible via the **Node Shortcut Menu**, which includes the following items: **Basic Configuration**, **GUI-Node Connectivity Settings**, **System Status Window**, **Advanced Node Configuration**, **Current Throughput**, **Remove Node** and **System**. From the Node Shortcut Menu you can access additional tabbed windows used in configuring and monitoring the network.

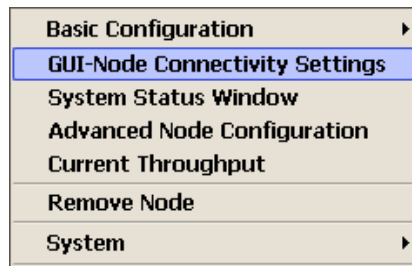


Figure 4. Node Shortcut Menu

### 2.1.1 AP-ONE HotSpot Manager Main Menu

Using AP-ONE HMS menus you can manage system profiles, implement tools to discover, add and view nodes, launch utilities and access help information. Menu on the top of AP-ONE HMS include:

#### File

- **Save Profile** – Save the current AP-ONE HMS profile
- **Save Profile as** – Save the profile with a different name
- **Load Profile** – Load a previously saved AP-ONE HMS profile
- **Load Background Image** – Load a background image (typically a map) to be displayed in the Topology Map
- **NMS Settings** – Set polling interval and polling port values
- **Exit** – Exit AP-ONE HMS

#### Tools

- **View Topology** – Display the Topology Map tab
- **Add New Node** – Open the Insert New Node dialog box
- **License Manager** – Display the License Manager tab
- **Discovery Manager** – Open the Auto Discovery dialog box

#### Utilities

- **MRTG** – Open the MRTG window

#### Help

- **Home Page** – Access the Ubiquiti Inc website
- **About** – Display the AP-ONE introductory window

## 2.1.2 Network Topology Tab Information Panes

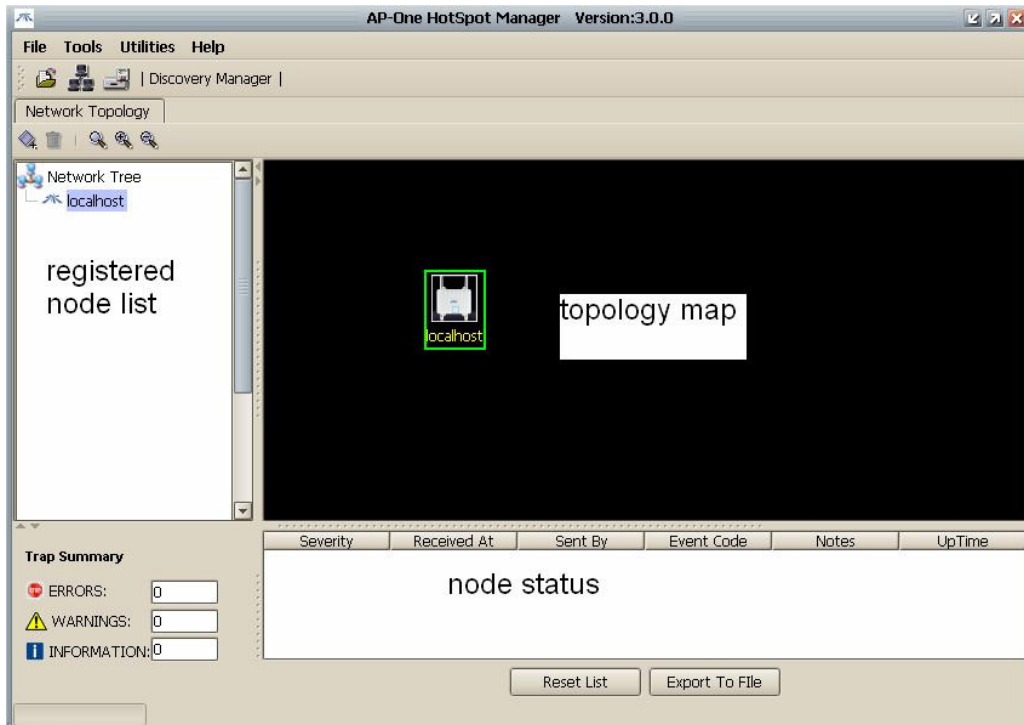


Figure 5. The AP-ONE NMS Window

### Topology Map

Located in the center pane, the **Topology Map** displays icons representing network nodes and connection information describing the layout of the network. It also can display a map graphic in the background.

### Registered Node List

Located in the left pane, the **Registered Node List** displays all registered nodes on the network

### Node Status

Located in the bottom pane, the **Node Status** area displays the following information on the currently selected node

- **Trap Summary** – Presents the number of ERRORS, WARNINGS and INFORMATION available during the auto-configuration of the HotSpot network.
- **Detailed Table containing information regarding the status of Backhaul interface during configuration** – For each message

produced during configuration the following columns are available: Severity, Received At, Sent By, Event Code, Notes, Up Time.

- **Reset List, Export To File Buttons:** The user has the option either to reset the list of messages or to export it to a file for future reference.

All panes are resizable and can be adjusted according to user preferences.

### 2.1.3 Node Shortcut Menu

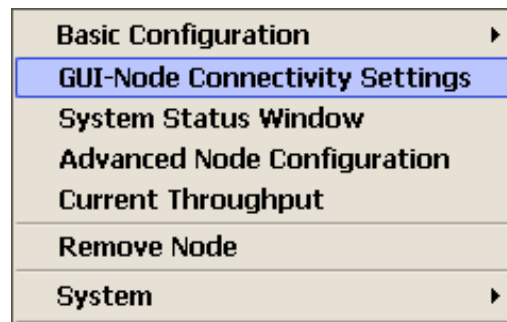


Figure 6. Node Shortcut Menu

#### Basic Configuration

The **Basic Configuration** menu option allows you to **Detect/Update Adjacent Nodes**, retrieve **Node Configuration/Info**, getting information about **Backhaul Encryption**, and **Remove inactive connections**.

#### GUI-Node Connectivity Settings

The **GUI-Node Connectivity Settings** menu option allows you to access the **Node Connectivity Settings** dialog box (for the currently selected node).

#### System Status Window

The **System Status Window** menu option allows you to access the **Status** dialog box, which contains the **FW Version**, **Key Level**, **Up Time** and **Host Name** fields.

#### Advanced Node Configuration

The **Advanced Node Configuration** menu option allows you to retrieve information from the selected node. A new pane is displayed containing a main tab (**Advanced Configuration of node: [node name]**). Under this tab three sub-tabs are displayed: **Configuration**, **Statistics** and **System Properties**. Each of these tabs contains several additional sub-tabs used in the configuration process.

## Current Throughput

The **Current Throughput** menu option allows you to display a real-time graphical display of traffic transmitted and received of the network interface.

## Remove Node

The **Remove** menu option allows you to remove the currently selected node from the **Topology Map** and **Registered Node List**.

## System

The **System** menu option has four options:

**i) Save Configuration:** This option allows you to permanently save the configuration for the current node.

***Note:** After the base station is configured, the configuration parameters are stored in RAM (volatile memory). If the base station is powered down the configuration will be lost unless you Save Configuration to the base station's permanent memory.*

**ii) Back up:** This menu option allows you to back up and restore the configuration settings for the selected node via **Retrieve / Restore Configuration** options.

**iii) FW Upgrade:** This menu option allows you to access the **Select** dialog box, from which you can select the firmware image file to be loaded into the node.

**iv) Reboot:** This menu option allows you to reboot the node.



## 2.2 Getting Started with AP-ONE HotSpot MS

Starting from the menus and windows mentioned above, you can auto-discover and insert new nodes, display maps and graphics of your wireless network, save and load profiles and access multi-tabbed windows used for advanced configuration of nodes.

### 2.2.1 Auto-Discovering Nodes

**Discovery Manager** allows you to discover nodes and insert them into the **Topology Map**. A custom polling protocol is used to detect AP-ONE nodes in the specified subnet. Discovered nodes are displayed in a tabular format.

To use **Discovery Manager**:

- In the **Tools** menu, select **Discovery Manager**. The **Auto Discovery** dialog box appears.

The screenshot shows the 'Auto Discovery' dialog box. It features a title bar with a close button. The main area contains the following elements:

- Network Subnet:** A text box containing '192.168.1.0' followed by a dropdown menu showing '/24'. To the right is an unchecked checkbox labeled 'Enable Broadcast Discovery'.
- Timeout:** A text box containing '2' followed by 'secs'.
- Discovery Results:** A section with a label and a text box above a table.
- Table:** A table with four columns: IP, Host Name, Include to topology, and Password. It contains one row with the values: 192.168.1.3, localhost, a checked checkbox, and an empty field.
- Buttons:** Three buttons labeled 'Start', 'Submit', and 'Cancel' are located at the bottom of the dialog.

Figure 7. Auto Discovery Dialog Box

### Network Subnet

In the **Network Subnet** field, type the subnet address. (AP-ONE NMS will detect nodes in which the first three segments, or 24 bits, of their IP address match the first three segments of the subnet address.)

### Enable Broadcast Discovery

Select the **Enable Broadcast Discovery** checkbox. (AP-ONE NMS uses a UDP broadcast message to detect any nodes on the network.)

## Timeout

In the **Timeout** field, type a timeout value in seconds (default: 10 seconds)

## Discovery Results

Click **Start** to initiate a discovery poll. The **Discovery Results** bar graph displays the progress of the poll. When complete, the table displays the **IP Address**, **Host Name** and **Password** (if used) of discovered node. The checkbox under **Include to Topology** is automatically selected.

## Include to Topology

To display a node in the **Topology Map**, leave the **Include to Topology** checkbox selected.

## Submit

Click the **Submit** button to insert the nodes into the **Topology Map**.

## Cancel

Click the **Cancel** button to exit the **Auto Discovery** dialog box.


Icons for each node should be visible in the **Topology Map**, labeled with the hostname. If two nodes have the same default hostname, AP-ONE NMS will label one with the hostname and the other with its IP address. (The label can be changed to an Alias using the **GUI-Node Connectivity Settings** dialog box, accessible from the **Node Shortcut Menu**.)

## 2.2.2 Configuring a New Node

Network nodes can be configured manually using the **Insert New Node** dialog box.

1. Use any one of the following three methods to configure a new node:
  - Right click anywhere in the topology pane, then click the **Insert new node** button that appears

or

- Click the  icon

or

- On the **Tools** menu, click **Add New Node**. The **Insert New Node** dialog box appears.

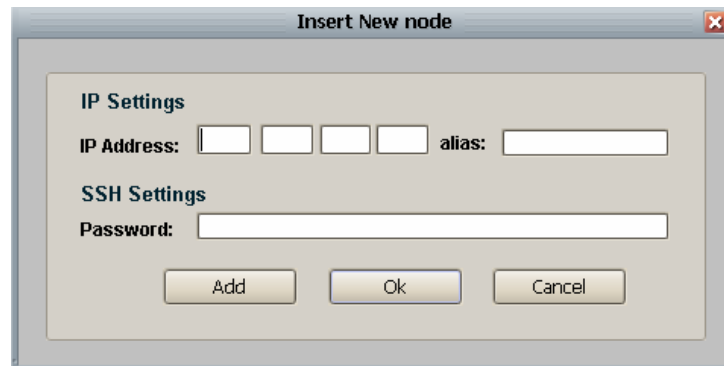


Figure 8. Insert New Node Dialog Box

2. Type the **IP address**, **Alias** (optional) and **SSH Settings Password**. (Typically a new node is given the default password *admin*)

The **Displayed Icon** to represent the node is the following.



Figure 9. Displayed Icon

**Note:** Though optional, adding **Alias** provides an enhanced visual representation of the nodes. This becomes especially useful when working with middle to large scale networks.

3. Click the **Add** button. The icon will appear in the topology pane. All topology panes are updated with the new insertion information.

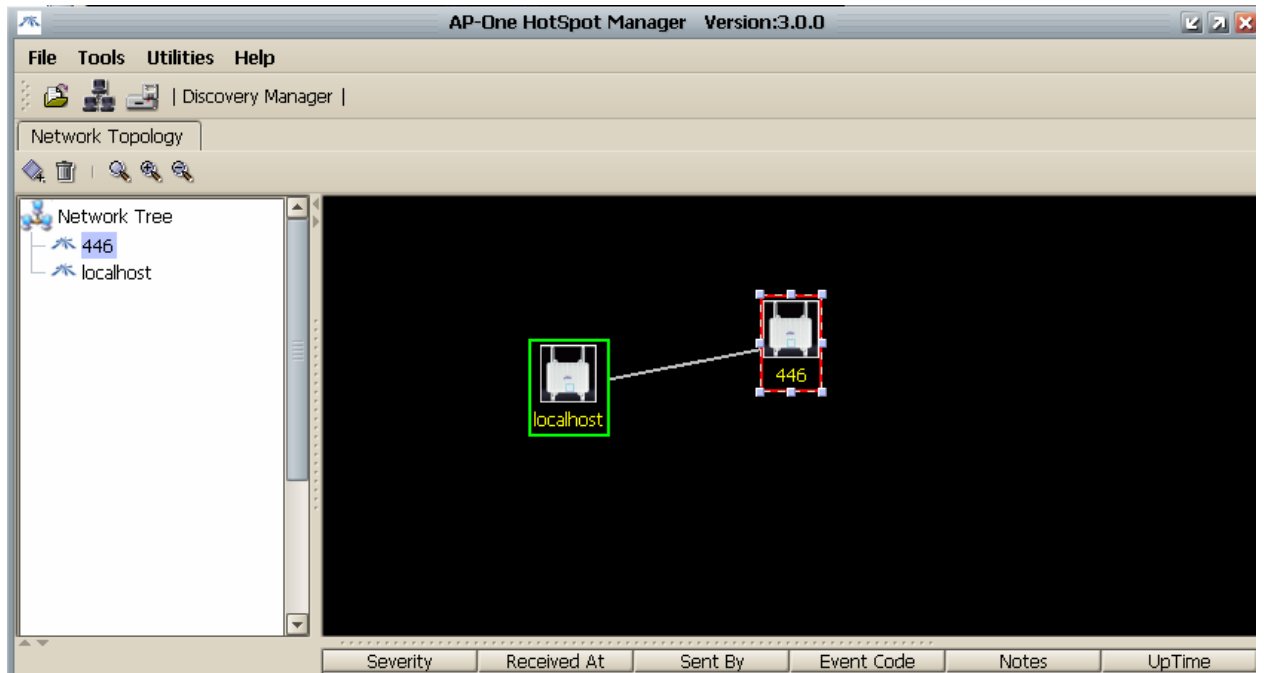



Figure 10. Node Insertion

If the newly inserted node has successfully responded to a network probe,

a green outline appears around the icon. A red outline  indicates the node is not responding.

### 2.2.3 Moving and Resizing Icons

- To move a node icon, drag it to the desired location in the pane.
- To resize a node icon, select the icon, then drag one of its handles.

### 2.2.4 Adding Background Map Images

**Topology Map** can be further enhanced by loading a background image to indicate the geographical location of the nodes. To add a background image:

1. On the **File** menu, click **Load Background Image**. The **Load Background Image** dialog appears.

2. Browse to the image file you wish to load, select it and click the **Load Background Image** button.

**Note:** .gif or .jpg formats may be used for background images

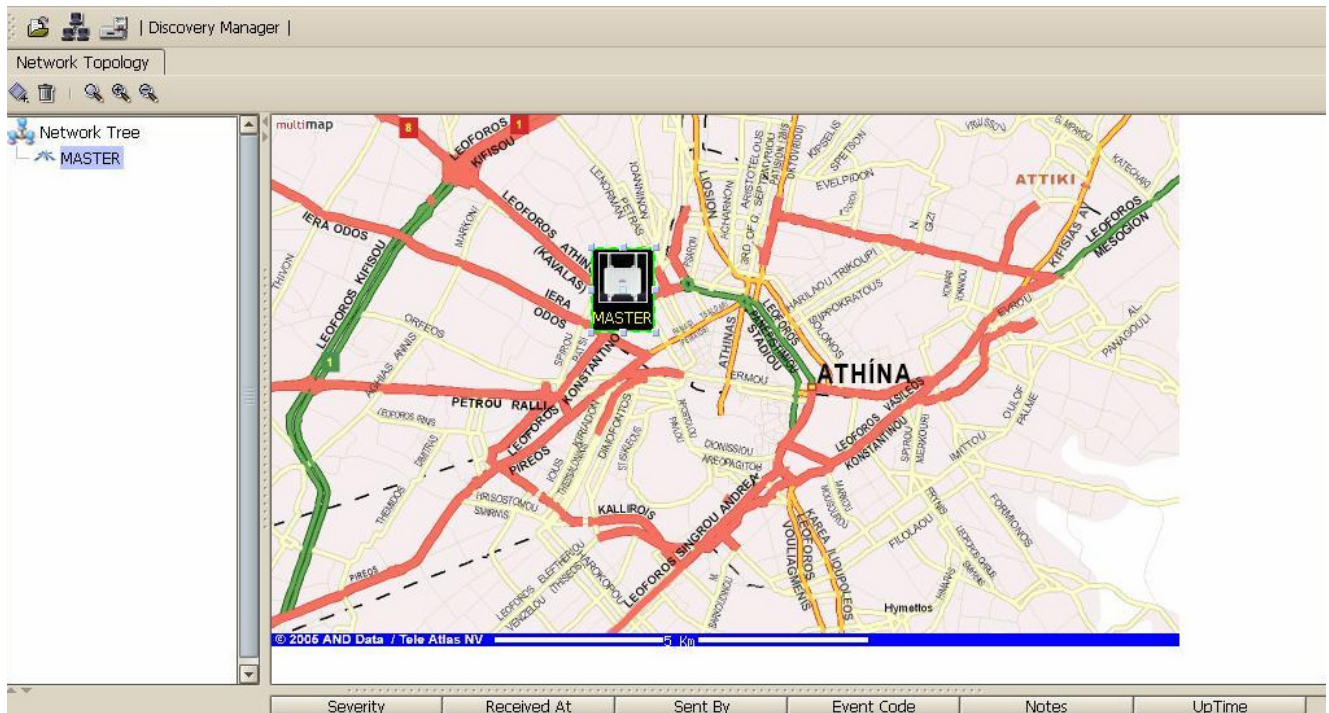





Figure 11. Customized Topology Map

3. Adjust the magnification level of the background image using the following zoom buttons located above the **Registered Node List**:

-  Zoom In
-  Zoom Out
-  Restore to default.

4. Create arrows indicating a connection between nodes by clicking in the center of the *source* node (a hand cursor will appear), and dragging to the center of the *destination* node. A line with arrowhead will appear between the nodes.

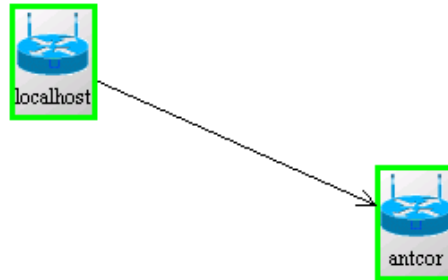


Figure 12. Network Nodes Showing Connection

## 2.2.5 Saving and Loading Profiles

1. To save a **Topology Profile**, on the **File** menu, click **Save Profile**.
2. To load a **Topology Profile**, on the **File** menu, click **Load Profile**.

## 2.2.6 Using the Node Shortcut Menu

You can manage and configure a variety of operating parameters of network nodes from the **Node Shortcut Menu**, which can be accessed using either of the following methods:

- Double click any node name shown in the **Node List**
- or
- Right click any node in the **Topology Map**

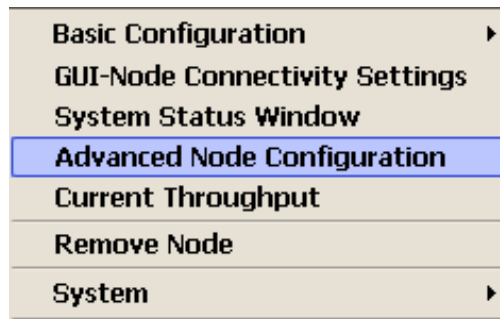


Figure 13. Node Shortcut Menu

## Basic Configuration

Click this option for either **Detect/Update Adjacent Nodes** to Backhaul Interface, get **Node Configuration/Info**, set **Backhaul Encryption** or **Remove inactive connections** (see picture 14).

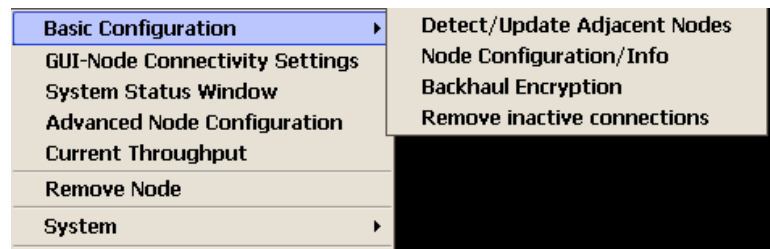


Figure 14. Node-Backhaul Shortcut Menu

In case we choose **Node Configuration/Info** we are permitted to change **Backhaul Settings**, **Ethernet Settings**, **HotSpot** or view **Statistics** regarding the node has been selected. In case we choose **Backhaul Encryption**, we can either enable or disable encryption for the backhaul network (5Ghz) (**For more information see chapter 12.3**).

## GUI-Node Connectivity Settings

Click this option to display the **Node Connectivity Settings** dialog box. This box contains the **IP Address** and **Alias** assigned to the selected icon. If an Alias has not been assigned, the Alias field will contain the Hostname of the node.

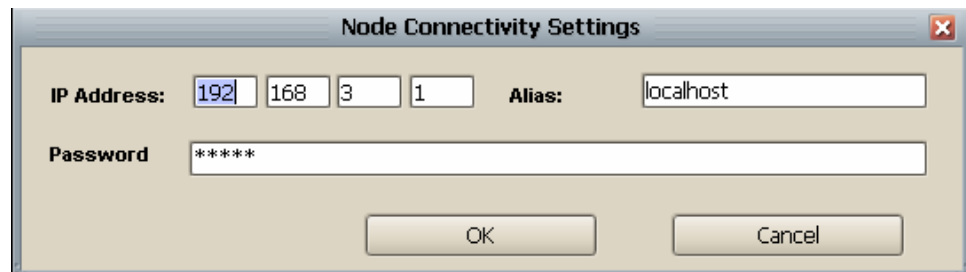


Figure 15. GUI-Node Connectivity Settings Dialog Box

## IP Address

When AP-ONE NMS scans the network it looks for the **IP Address** listed in this dialog. If it makes a connection, the border around the icon turns green. If not, the border is red.

## Alias

To change the **Alias**, type the new name into the Alias text box.

## Password

Type the password (default: *admin*) into the **Password** field. (This step is required to allow access to **Advanced Node Configuration** described later in this section.)

## Ok

Click the **Ok** button to add the node to the Topology Map and keep the dialog box open

**NOTE:** Changing the IP Address, Alias or Password, specifies the parameters assigned to the currently selected node icon. The IP address and password will be used when AP-ONE HotSpot Manager scans the network. Changing the IP address of the icon does not change the IP address of the node. If the IP address of the icon is changed to an address not present on the network, the border of the associated icon will turn red indicating no connection has been made.

## System Status Window

Click this option to access the **Status** dialog box, which contains the **FW (Firmware) Version, Key Level, Up Time** and **Host Name** fields. (The FW Version, Key Level and Up Time fields also are displayed in the **Node Status** pane of the **Topology Map** tab.)

- The **FW Version** field contains the version number of the firmware residing in the currently selected node.
- **Up Time** – The length of time the node has been operating
- **Host Name** – The name of the currently selected node



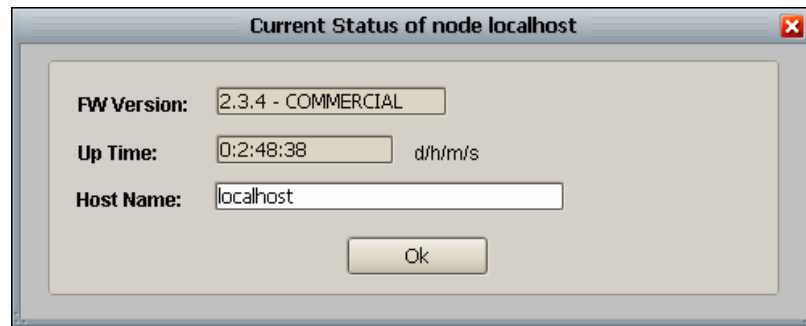


Figure 16. Current Status Dialog Box

## Advanced Node Configuration

Click this option to retrieve information from the selected node and open the **Advanced Configuration of Node** tab.

**NOTE:** To access the Advanced Node Configuration you must first access the GUI-Node Connectivity Settings via the Node Shortcut Menu and enter the password, then click **OK** or **Submit**.

The **Advanced Configuration of Node** tab contains three sub-tabs: **Configuration**, **Statistics** and **System Properties**.



Figure 17. Advanced Node Configuration Tab with Sub-Tabs

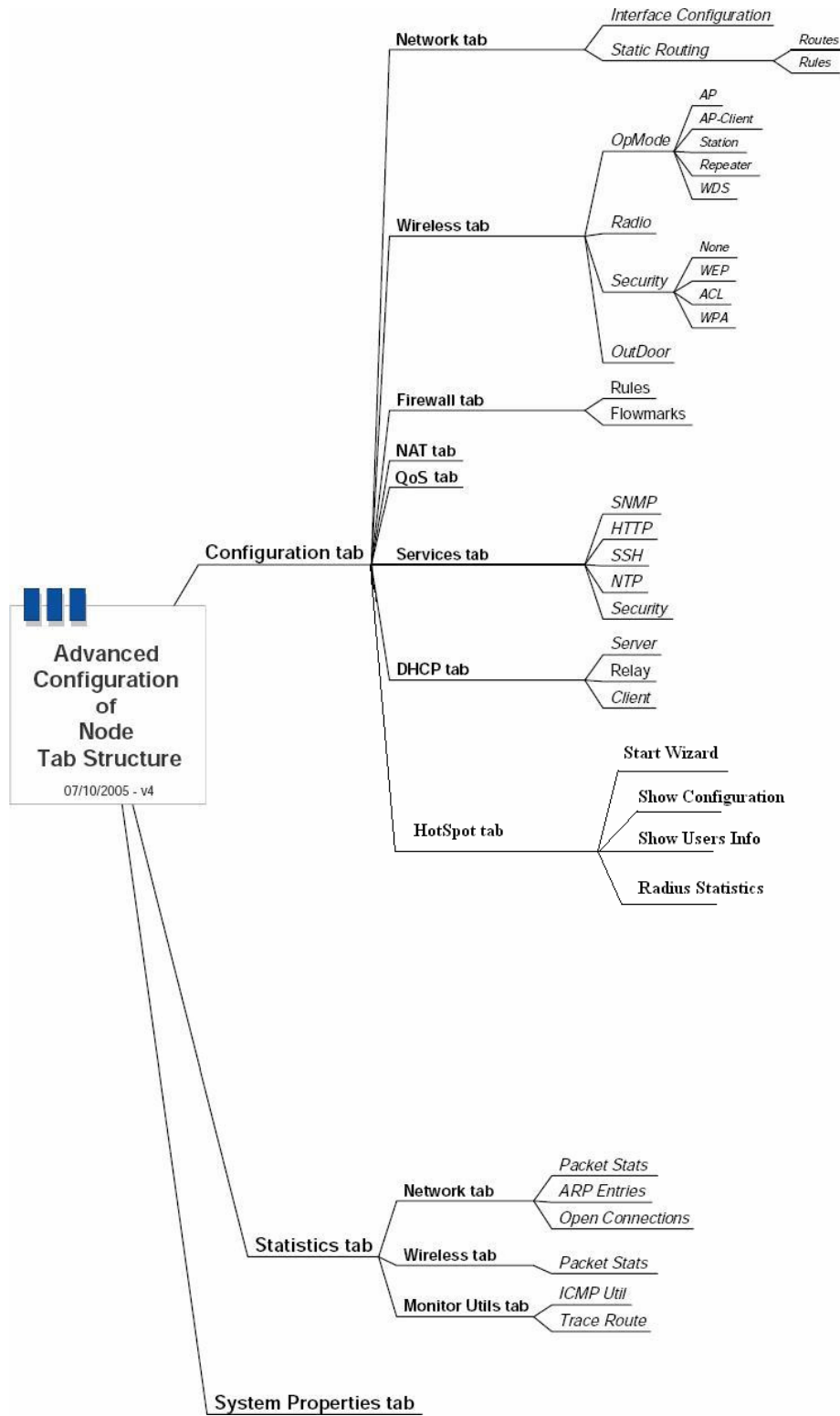
Each tab contains several additional tabs. The mind map below shows the hierarchy of advanced configuration tabs and sub-tabs used. The table indicates the chapter where descriptions and configuration procedures for each tab are located.

<b>Tab</b>	<b>Chapter</b>
Network	2, 3, 4
Wireless	5
Firewall	6
NAT	6
QoS	8
Services	9
DHCP	7

*Figure 18. Tab/Chapter List*

The table above indicates the chapters where descriptions and configuration procedures for each tab are located.

### **Advanced Configuration Tab Hierarchy**



Picture 1. Mind Map of Advanced Configuration Tabs and Sub-tabs

## Current Throughput

Click this option to display a real-time graphical display of transmit and receive traffic of the network interface.

## Remove Node

Click this option to remove the currently selected node from the **Topology Map** and **Registered Node List**

## System

Click this option and you will be allowed either to:

### i) Save Configuration

Click this option to permanently save the configuration for the current node.

**Note:** After the base station is configured, the configuration parameters are stored in RAM (volatile memory). If the base station is powered down the configuration will be lost unless you Save Configuration to the base station's permanent memory.

### ii) Back Up

Click this option and select

- **Retrieve Configuration** to Retrieve the last saved node configuration
- or
- **Restore Configuration** to Restore the node configuration from a file

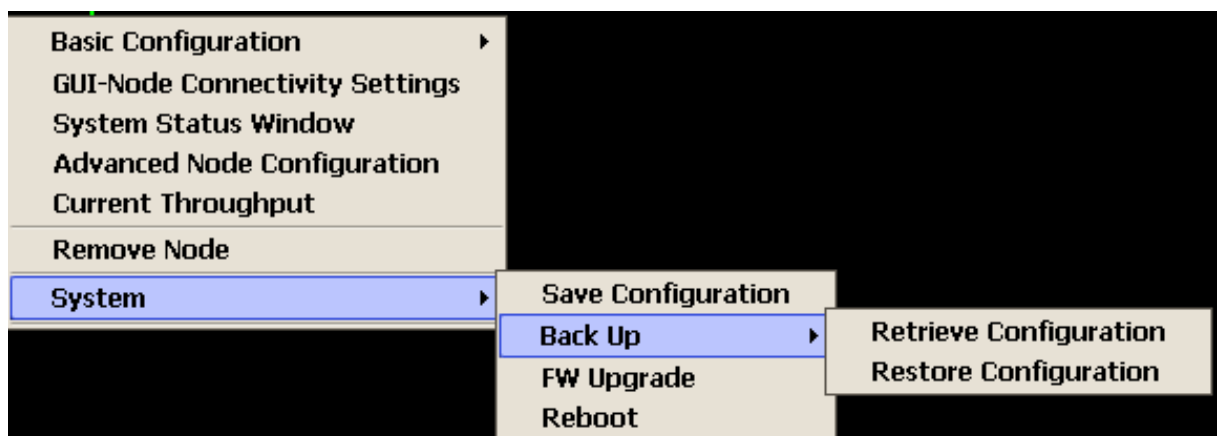


Figure 19. Back up Menu Options

### iii) FW Upgrade

Click this option to access the **Select** dialog box, from which you can select the firmware image file to be loaded into the node.

### iv) Reboot

Click this option to reboot the node. An **Alert** dialog box appears with the question: **Should system save its configuration before reboot.** Click **Yes** if you want to save the configuration.

## 3. IP Networking

This section describes **IP Networking** settings and configuration procedures for your AP-ONE node.

To configure **IP Networking**, select the **Interface Configuration** tab, located under the **Advanced Configuration of Node, Configuration, Network** tabs.

*See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.*

The **Interface Configuration** tab features four panes:

- **Network Interfaces Tree** (left pane)
- **IP Configuration** (center left pane)
- **Interface Configuration** (center right pane)

Two buttons are located at the top of the IP Configuration tab:

- **Refresh** – Click Refresh to retrieve setting from the selected node.
- **Submit** – Click Submit to upload the configuration to the node.

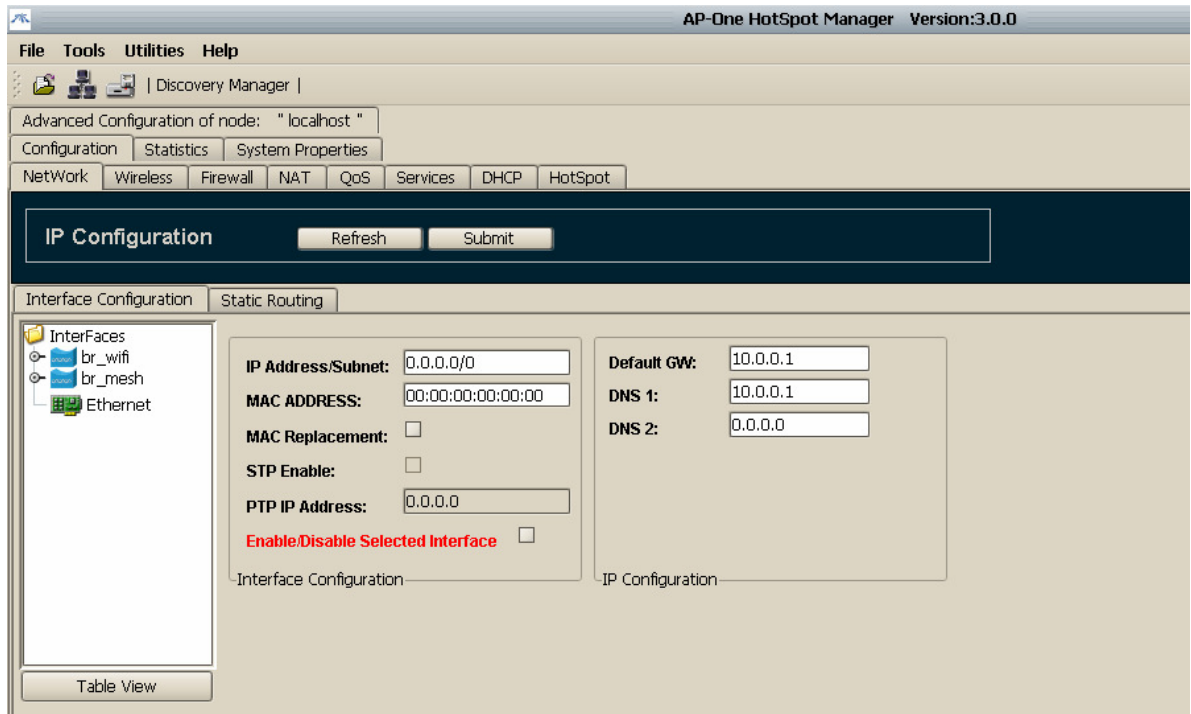


Figure 19. Network Configuration Tab

## 3.1 Using the Network Interfaces Tree

The left pane of the **Interface Configuration** tab contains the **Network Interfaces Tree**, a representation of all available network interfaces of the selected node. The tree view can be expanded or collapsed by left clicking on any master interface. When an interface is selected, data fields in the other panes display the parameters associated with the selected interface and changes can be made.

## 3.2 Configuring Basic IP Settings

The center-left pane of the **Interface Configuration** tab contains all **Basic Interface Configuration** fields for the interface selected in the Network Interfaces Tree.

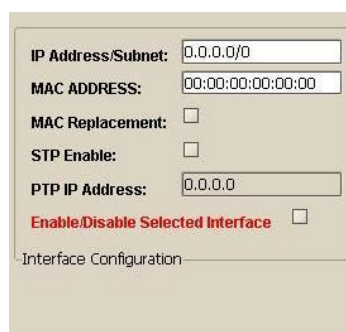
The image shows a configuration window titled "Interface Configuration". It contains several fields and checkboxes: "IP Address/Subnet:" with a text box containing "0.0.0.0/0"; "MAC ADDRESS:" with a text box containing "00:00:00:00:00:00"; "MAC Replacement:" with an unchecked checkbox; "STP Enable:" with an unchecked checkbox; "PTP IP Address:" with a text box containing "0.0.0.0"; and "Enable/Disable Selected Interface" with an unchecked checkbox. The text "Interface Configuration" is also visible at the bottom left of the window.

Figure 20. IP Interface Settings

The following section describes the fields used to configure IP settings.

### 3.2.1 IP Address

The **IP Address** field contains the IP address of the selected interface. To change the IP address of the interface, type the new address into this field and click the **Submit** button.

### 3.2.2 MAC Address

The **MAC Address** field displays the interface's Media Access Control (MAC) address in hex format. This field is readable for any kind of interface and writeable only for physical interfaces. To change the MAC address of a physical interface the **MAC Spoofing** check box must be selected.

### 3.2.3 MAC Replacement

When the **MAC Replacement** check box is selected an alternate MAC address (for physical interfaces only) can be typed into the **MAC Address** field.

### 3.2.4 STP Enable

The **STP Enable** check box enables the use of Spanning Tree Protocol,

**Note:** Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure

### 3.2.5 PTP IP Address

If there is a PPP connection (from a PPPoE client or a PPTP client), the remote peer IP address is displayed in the **PTP IP Address** field. Otherwise this field is blank. This is a read-only field.

### 3.2.6 Enable/Disable Selected Interface

The **Enable/Disable Selected Interface** box indicates whether the interface is enabled. If this box is not checked the interface will maintain the desired configuration but it will remain disabled.

## 3.3 Configuring Global Settings

The right-center pane of the Interface Configuration tab contains **IP Configuration**. These fields apply to all network interfaces.

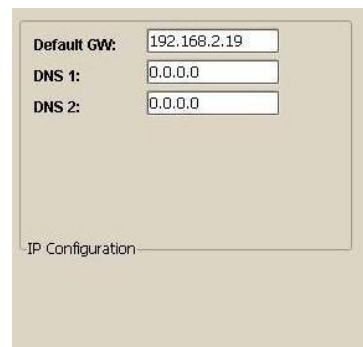
A screenshot of a web-based configuration interface for IP settings. It features three input fields: 'Default GW:' with the value '192.168.2.19', 'DNS 1:' with the value '0.0.0.0', and 'DNS 2:' with the value '0.0.0.0'. Below these fields is a label 'IP Configuration'.

Figure 21. IP Configuration Settings

### 3.3.1 Default Gateway

Every IP packet with an unknown destination will be forwarded through the default gateway IP address. Set this address statically by typing it into the **Default GW** field. It also can be set dynamically from another application such as a DHCP client, a PPPoE client, or a PPTP client.

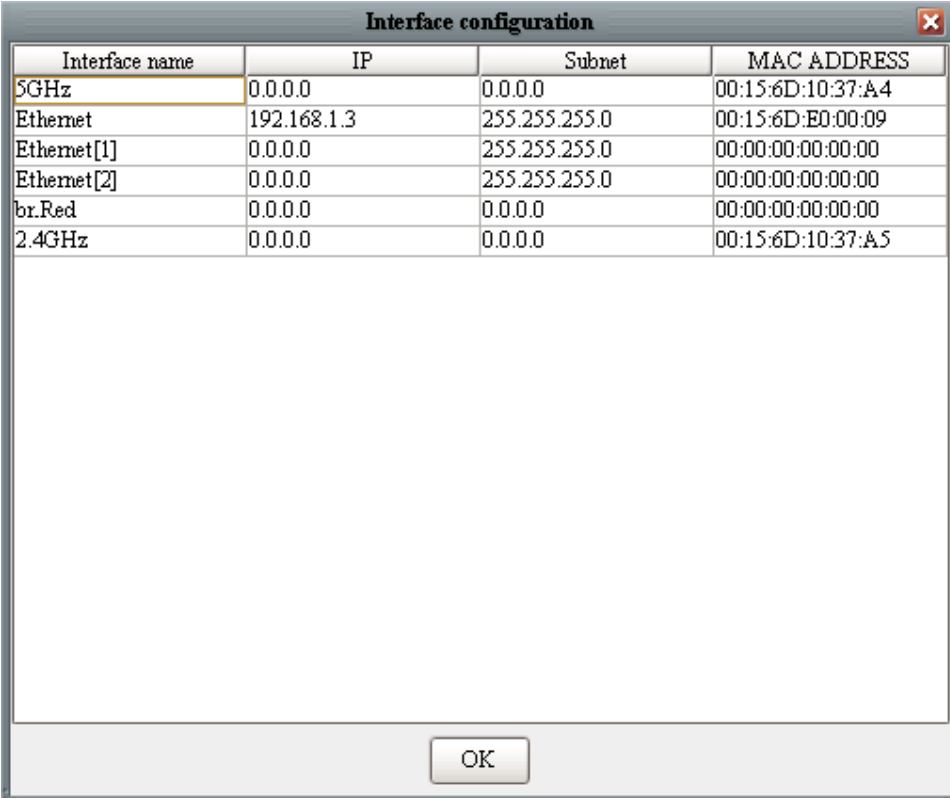


### 3.3.2 DNS1 and DNS2

You can set DNS1 and DNS2 addresses statically by typing them in or they can be set dynamically from another application such as a DHCP client, a PPPoE client, or a PPTP client.

## 3.4 Using Table View

The **Table View** option is a feature that further enhances the controllability of interface IP settings. This feature allows you to browse and edit the basic settings of all available interfaces. To access this option, click the **Table View** button located below Network Interface Tree pane. The **Interface Configuration** dialog appears.



Interface name	IP	Subnet	MAC ADDRESS
5GHz	0.0.0.0	0.0.0.0	00:15:6D:10:37:A4
Ethernet	192.168.1.3	255.255.255.0	00:15:6D:E0:00:09
Ethernet[1]	0.0.0.0	255.255.255.0	00:00:00:00:00:00
Ethernet[2]	0.0.0.0	255.255.255.0	00:00:00:00:00:00
br.Red	0.0.0.0	0.0.0.0	00:00:00:00:00:00
2.4GHz	0.0.0.0	0.0.0.0	00:15:6D:10:37:A5

OK

Figure 22. Interface Table View

## 4. Static IP Routing

Static routing is the manual method used to set up routing. An administrator enters routes into the router using configuration commands. This method has the advantage of being predictable and simple to set up. It is useful in managing small networks but becomes somewhat unwieldy on larger networks. AP-ONE HotSpot Manager provides management tools for manipulating any of the routing tables and configuring rules.

To configure **Static IP Routing**, select the **Static Routing** tab, located under the **Advanced Configuration of Node, Configuration, Network** tabs. In the **Static Routing** tab you can select the **Routes** tab or the **Rules** tab.

*See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.*

In the **Routes** tab you can:

- Add, delete and select routing tables
- Add, delete, modify and prioritize routes

In the **Rules** tab you can:

- Add, delete and select rules

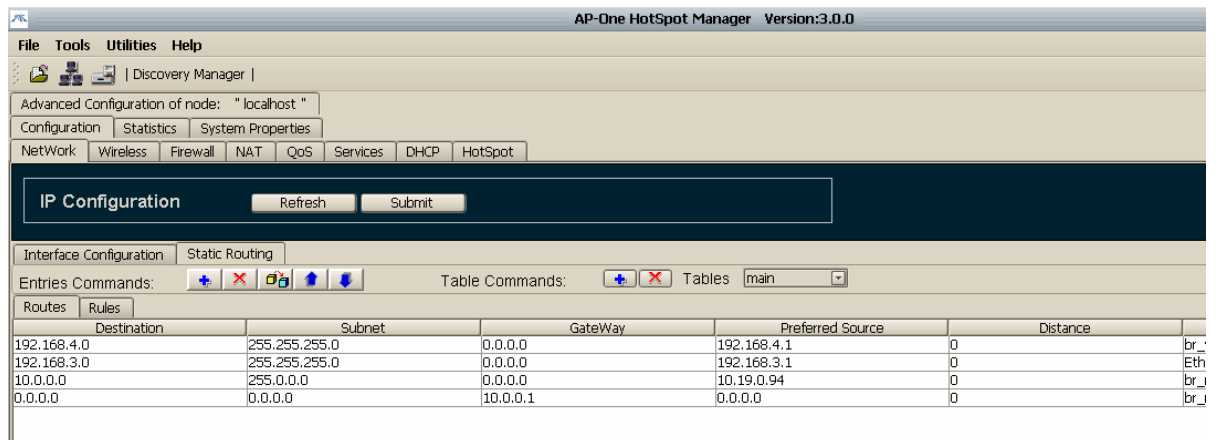


Figure 23. Routing Table Handling

The bar across the top of the **Static Routing** tab contains the following options:

- **Entries Commands** buttons






Button	Command
	Insert New Route
	Delete Route
	Modify Route
	Move Up
	Move Down

Figure 24. Route Entries Commands

- **Table Commands** buttons



Button	Command
	Insert New Route
	Delete Route

Figure 25. Route Table Commands

- **Tables** drop down list

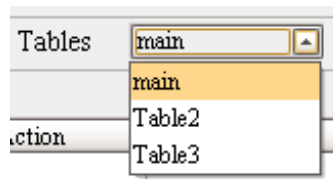



Figure 26. Routing Tables Drop Down List

## 4.1 Configuring Routing Tables and Entries

AP-ONE provides a multiple routing table system with a flexible infrastructure and the ability to implement policy routing. In addition to the local and main routing tables, AP-ONE supports up to 252 additional routing tables.


### 4.1.1 Adding a New Routing Table

To create a new routing table that will be integrated in the multiple routing table system

1. Click the **Table Commands**  button. The **Insert New Routing Table** dialog appears.
2. Type the name into the **Routing Table** box, and then click **Submit**. The table name is stored in the drop down list for future use.

### 4.1.2 Remove an Existing Routing Table


To delete an existing routing table

1. Select the table name from the Main drop down list.
2. Click the Table Commands  button.

*CAUTION: The user has to be careful not to delete the main routing table, as this action can lead to connectivity problems.*

### 4.1.3 Adding Static Routing Entries

To add a new static route

1. Select the **Routes** tab
2. Click the **Entries Commands**  button. The **Insert New Route** dialog box appears.

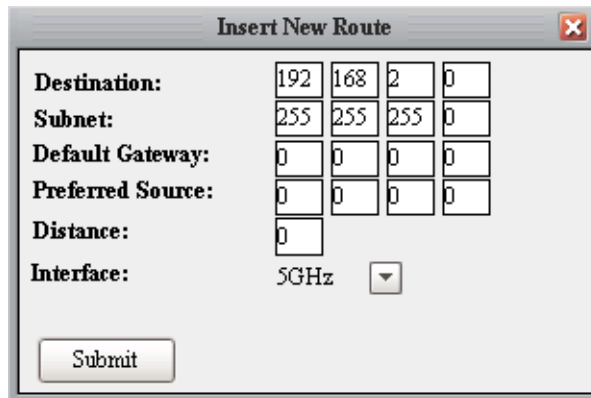



Figure 27. Insert New Route


*In the above example all the traffic with destination addresses that belong to subnet 192.168.2.0/24 will be forwarded via interface 5GHz.*

3. In the **Destination** boxes, type the destination network or destination host address.
4. In the **Subnet** boxes, type the netmask for the destination net. (255.255.255.255 for a host destination and 0.0.0.0 for the default route)
5. In the **Default Gateway** boxes, type the gateway address (if required).
6. In the **Preferred Source** boxes, type the preferred source address for communicating to that destination.
7. In the **Distance** box, type the distance to the target, usually counted in hops. (This field is not used by recent kernels, but may be needed by routing daemons.)
8. In the **Interface** drop down list, select the interface to which packets for this route will be sent.
9. To accept your settings, click the **Insert New Route** dialog **Submit** button, then click the **IP Configuration** pane **Submit** button to complete the process.



#### 4.1.4 Removing Static Routing Entries

To remove a specific routing entry, select the table row of that entry, then click the **Entries Commands**  button.

#### 4.1.5 Modifying Static Routing Entries

To edit a specific routing entry, select the table row of that entry, then click the **Entries Commands**  button.

#### 4.1.6 Repositioning Static Routing Entries

Routing entries allocated in each routing table are parsed by the OS kernel in a serial manner. To modify the series (priority) of allocated entries, select the table row of the entry to be moved, and then click the **Entries Commands**  button to move the entry upward or the  button to move it downward in the list.

## 4.2 Configuring Static Rules

A rule is a method for implementing Access Control Lists (ACL) for routes. Rules allow you to specify the filters that match packets to select a route structure when the filter does match.


Using a rule you can perform the most common Policy Routing function: route by source address. The rule can specify the selection of a packet if the source address of the packet falls within a designated address range, and which route structure to use or other destination to choose if there is no match. However, on a system with only one routing table, a rule set is usable only under limited conditions.

Figure 28. New Routing Rule Insertion

### 4.2.1 Adding Rule Entries


To add a new rule entry

1. Select the **Rules** tab


2. Click the **Entries Commands**  button. The **Insert New Rule** dialog appears.
3. In the **Source Address** boxes, type the address of the source network or source host.
4. In the Source Address **Subnet** boxes, type the netmask for the source net. Type 255.255.255.255 for a host source.
5. In the **Destination Address** boxes, type the destination network or destination host.
6. In the Destination Address **Subnet** boxes, type the netmask for the destination net. Type 255.255.255.255 for a host destination.
7. In the **Interface** drop down list, select the interface that packets are received from. The interface can be one of the available physical interfaces or can be set to **All**.

8. In the **Action** drop down list, select one of the following:
  - a) **LookUp** to cause the routing subsystem to look up the routing table selected in the **Table** drop down list. (Default: Main table)
  - b) **Unreachable** to drop the received packet and send an ICMP packet to the source indicating the destination was unreachable.
  - c) **Drop** to silently drop packets with matching frames.
9. In the **Table** drop down list, select the routing table you wish to use with the **LookUp** option described above.



### 4.2.2 Removing Rule Entries

To remove a specific rule entry, select the table row of that entry, then click the **Entries Commands**  button.

### 4.2.3 Modifying Rule Entries

To edit a specific rule entry, select the table row of that entry, then click the **Entries Commands**  button. The **Insert New Rule** dialog appears with the fields for the selected rule filled in. Modify as required, then click **Submit**.

### 4.2.4 Repositioning Rule Entries

Rules entries allocated in each routing table are parsed by the OS kernel in a serial manner. To modify the series (priority) of allocated entries, select the table row of the entry to be moved, then click the **Entries Commands**  button to move the entry upward or the  button to move it downward in the list.

# 5. Wireless

AP-ONE HotSpot Manager allows you to configure all wireless settings for nodes on your wireless network, including:

- **Link Distance**
- **Transmitter Power**
- **Operational Modes**
- **Radio Settings**
- **Security Settings**
- **Outdoor Settings**
- **Country Code Settings**
- **Site Survey Operation**

To configure **Wireless** settings, select the **Wireless** tab, located under the **Advanced Configuration of Node, Configuration** tabs. In the **Wireless** tab you can select the **OpMode, Radio, Security** or **Outdoor** sub-tabs.

*See picture 1 for a diagram showing Advanced Configuration tabs and sub-tabs.*

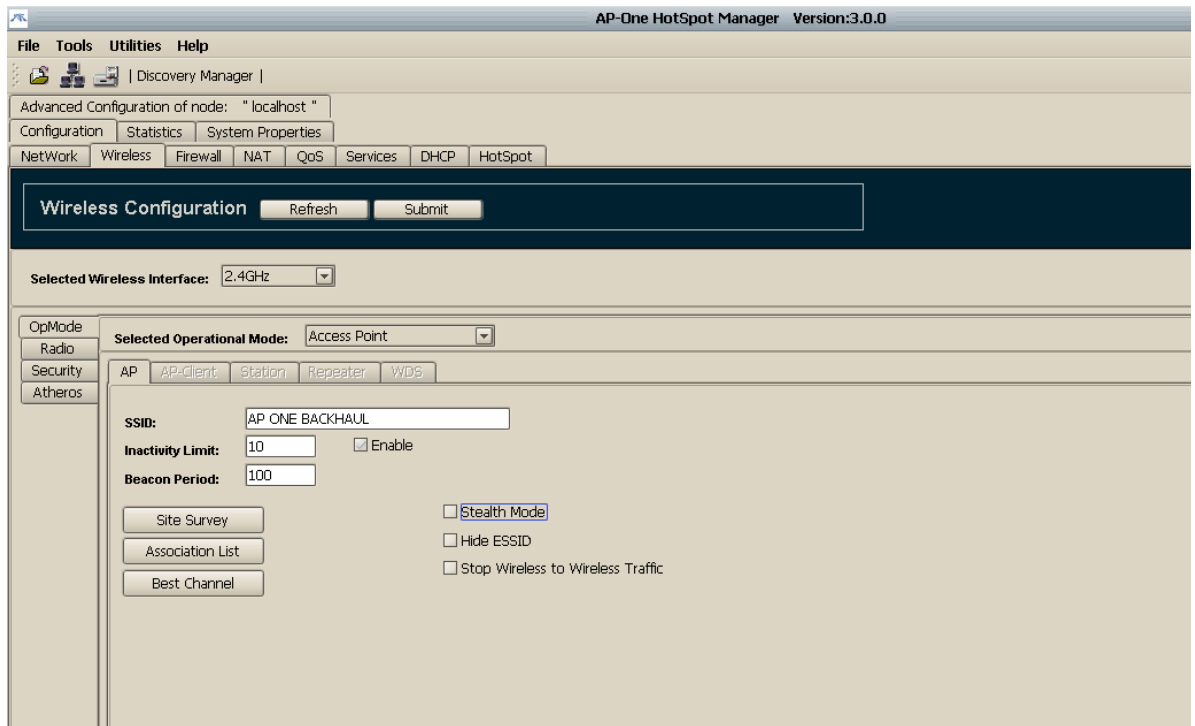


Figure 29. Wireless Configuration Panel



Three buttons and two drop down lists are located at the top of the **Wireless** tab:

- **Refresh** – Click **Refresh** to retrieve setting from the selected node.
- **Submit** – Click **Submit** to upload the configuration to the node.
- **Set CC** – Click **Set CC** to accept the country code specified in the CC drop down list
- **CC List** – Select the required country code from the list and then click Set CC. The software will perform all the appropriate checks of the available radio chipsets in the system in the background. If any of them does not support the specified country code a possible violation could occur. If that occurs, AP-ONE HotSpot Manager warns you with a popup alert. This protects you from choosing an unsupported country code which might cause a loss of connection with the wireless interface after setting the specific country code.
- **Selected Wireless Interface list** – Select the wireless interface to be configured. If there are multiple wireless interfaces available, this drop down a list is populated. If the selected interface is not active a red warning message is shown next to the interface.

## 5.1 Setting Operational Modes

An AP-ONE node has the ability to operate in the following modes:

- **Access Point**
- **WDS** (Wireless Distribution System)

### Site Survey

The **Site Survey** button is accessible in all **OpMode** tabs. **Site Survey** scans all available frequencies associated with the IEEE 802.11a, b and g physical layer. When the scan is complete the **Site Survey** dialog box appears, indicating any possible sources of interference by other nearby access points. **For more information on Site Survey settings, see Section 5.1.4.**

### 5.1.1 Selected Operational Mode

The **Selected Operational Mode** drop down list is populated with all available operational modes an AP-ONE node can adopt. Selecting an operational mode from the drop down list makes the corresponding pane available in the **OpMode** tab.

## 5.1.2 Configuring AP-ONE node as an Access Point

To configure the node as an access point (AP), select **Access Point** in the **Selected Operational Mode** drop down list. The **AP** tab becomes available. Several parameters must be configured as follows:

The screenshot shows a configuration window for a wireless interface. At the top, 'Selected Wireless Interface' is set to '5GHz'. Below that, 'Selected Operational Mode' is set to 'Access Point'. The 'AP' tab is active, showing the following settings:

- SSID:** An empty text input field.
- Inactivity Limit:** An empty text input field with an 'Enable' checkbox to its right.
- Beacon Period:** A text input field containing the value '100'.
- Buttons:** 'Site Survey', 'Association List', and 'Best Channel' are located on the left side.
- Checkboxes:** 'Stealth Mode', 'Hide ESSID', and 'Stop Wireless to Wireless Traffic' are located on the right side.

Figure 30. Wireless Operational Mode Settings

### SSID (Service Set Identifier)

This field contains the string which is published as ESSID by the access point. To create a name for the service set identifier (SSID), type the name in the **SSID** box.

### Inactivity Limit

If a station associated with the AP-ONE access point is idle for a period of time defined by the **Inactivity Limit** field, the AP-ONE access point sends a disassociation frame to the station to inform it that it had been disassociated due to inactivity timeout. To configure the **Inactivity Limit**, type the inactivity threshold, in minutes, in this box.

### Beacon Period

This field represents the desirable time interval between two consecutive beacons. To configure the **Beacon Period**, type the number of seconds in this box. (Default: 100)

### Association List

To access a list of information for all nodes associated with the AP, click the **Association List** button. The **Associated stations for wireless interface** dialog box appears.

Alias	MAC Address	IP address	Signal Level	Fade Margin	Noise Level	Rate	Idle Time	Type	Action
	00:0C:F1:27:...	UNKNOWN	-227 dbm	29 dbm	-0 dbm	65	0:0:0.0 d/h/m/s	CLIENT	Not Set

Figure 31. Association List

A description for each field in the Association List follows:

### Alias

An **Alias** is a special name you can create to identify a client on the AP. When the configuration is saved, all aliases are saved on the device.

### MAC Address

The **MAC Address** field contains the MAC address of each client associated with the AP.

### IP Address

The **IP Address** field contains the IP address of each client that exchanges network traffic with the AP

*Note: A client can be seen with multiple IP addresses if transparent bridging is being used. To see a list of the IP addresses, click Expand with the desired client selected.*

### Signal Level

The **Signal Level** field displays the signal level for each associated client based on Received Signal Strength Indication (RSSI).

### Fade Margin

The **Fade Margin** field displays the actual difference between Signal Level and Noise Level.

### Noise Level

The **Noise Level** field displays the noise level of the chip according to transmit rate and physical layer standard

### Rate

The **Rate** field displays the transmission rate the AP uses to exchange data with each client.

## Idle Time

The **Idle Time** field displays the time that has passed since a formerly associated client was disassociated.

## Type

The **Type** field indicates the type of the node listed. It can contain the following values:

- AP Mode\_Type
- WDS\_Type

*NOTE: Every client that has ever been associated to the AP is included to this list, which is automatically saved when you click **Save Configuration**.*

## Action

- The **Action** field is a drop down list that allows you to perform several different actions on the selected node. You can:
  - Select **Set Alias** to set an Alias for a specific node.
  - Select **Remove** to remove an idle node from the list.
  - Select **Disassociate** to disassociate a client which is associated with the AP.
  - Select **Permanent Disassociation** to disassociate a client which is associated to the AP and simultaneously add its MAC to an Access Control List to deny access.

## Best Channel

**Best Channel** selection is an extra feature of access point mode. To enable best channel selection (BCS) click the **Best Channel** button. The system calculates the best available frequency based on the BCS algorithm and configures the AP to transmit on the appropriate channel to achieve better performance.

## Stealth Mode

**Stealth Mode** is another enhancement of Access Point mode. When Stealth Mode is enabled the AP does not transmit beacons and hides its SSID in transmitted probe responses, which makes the AP essentially invisible. No other node can discover it unless that node already has the AP's settings. In addition, a custom polling protocol is implemented, which is compatible with links between AP-ONE APs and AP-ONE clients. When using this protocol AP-ONE clients are able to detect AP-ONE Stealth APs.

To implement this feature, select the **Stealth Mode** checkbox.

## Hide ESSID

Hiding the AP's ESSID prevents outside users from joining the network because they cannot detect the network identifier. To stop the AP from publishing its ESSID in its beacon transmissions, select the **Hide ESSID** check box.

## Stop Wireless To Wireless Traffic

To prevent traffic between two wireless stations that are both associated with an AP-ONE AP, select the **Stop Wireless to Wireless Traffic** check box.

**NOTE:** AP-ONE has the ability to support Address 4 traffic. However it is necessary to put the wireless interface (the one that operates as an access point) under a Network Bridge (check IP Network configuration) if you intend to enable Address 4 support.

### 5.1.3 Configuring an AP-One as a WDS Mode

An AP-ONE node can operate as an access point WDS node. This gives you the opportunity to configure a Wireless Distribution System Network by setting up a number of AP-ONE WDS nodes, each one taking part in the network. All the features and settings described in the access point section are supported for WDS mode. In addition, WDS Mode features a WDS List which contains the MAC addresses of all WDS nodes included in the network.

To configure the currently selected node for Wireless Distribution System (WDS) mode, select **WDS** in the **Selected Operation Mode** drop down list. The **WDS** tab becomes available. **SSID**, **Inactivity Limit**, **Beacon Period**, **Site Survey**, **Stealth Mode**, **Hide ESSID** and **Stop Wireless to Wireless Traffic** fields are configured the same as for Access Point Mode. The WDS tab also features an **Association List** button and a list of **Registered WDS Nodes**.

The screenshot shows the configuration interface for WDS Mode. At the top, 'Selected Wireless Interface' is set to '2.4GHz'. Below that, 'Selected Operational Mode' is set to 'WDS'. The 'WDS' tab is selected, showing the following settings:

- SSID:** My\_Hotspot
- Inactivity Limit:** [ ]  Enable
- Beacon Period:** [ ]
- Site Survey:** [ ]
- Stealth Mode:**
- Hide ESSID:**
- Stop Wireless to Wireless Traffic:**

On the right, there is a table titled 'Registered WDS nodes' with 10 rows, each containing a MAC address field and a checkbox.

Figure 32. Wireless WDS Mode Settings

In the **Registered WDS nodes** list, type the MAC addresses of the nodes to be configured. Select the check box next to the MAC address field to enable it as part of the WDS network topology. (The enable feature can be helpful when WDS nodes change behavior. You can maintain the nodes' MAC addresses in the list and enable or disable as necessary.)

### 5.1.4 Using Site Survey Operation

The **Site Survey** button is available on all **OpMode** tabs. If an AP-ONE node acts as an access point or WDS, Site Survey can be used to scan and monitor adjacent frequencies to detect interference from other access points.

When you click the Site Survey button, the Site Survey dialog box appears. Rows in the dialog box display all the available information for every node scanned.

After the scan is complete and the dialog box list is populated, the status bar at the bottom of AP-ONE NMS window displays the message **Site survey list retrieved successfully**.

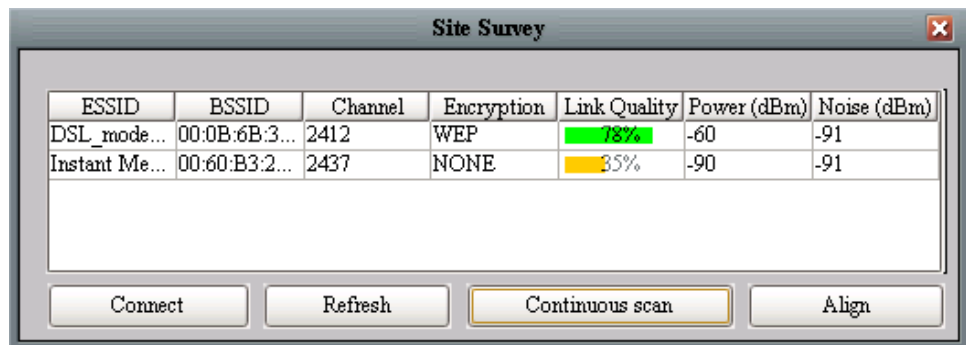


Figure 33. Site Survey Operation

At the bottom of the Site Survey dialog box four buttons are available:

#### Connect:

Select a node in the list and click **Connect** to connect to that node.

#### Refresh

Click the Refresh button to re-scan and update the Site Survey list.

#### Continuous Scan

Click **Continuous Scan** to enable consecutive scanning. The button remains depressed until clicked a second time. While in Continuous Scan

mode, the Site Survey list is updated dynamically, merging all the possible unique entries.

## Align

The **Align** option allows you to achieve the best possible alignment for a distant point-to-point link. Click the **Align** button. The **Site Survey Align** dialog box appears. This dialog box displays **BSSID**, **SSID**, **Channel Number**, **Link Quality** and **Signal Level** fields. Using this dialog you can monitor signal strength and quality value statistics through consecutive polling. Polling occurs at a high frequency to provide an up-to-date representation of the link. While monitoring these statistics you can adjust your antenna to achieve maximum performance. When optimal antenna position and polarity are achieved, click the **Quit** button to return to the Site Survey panel.

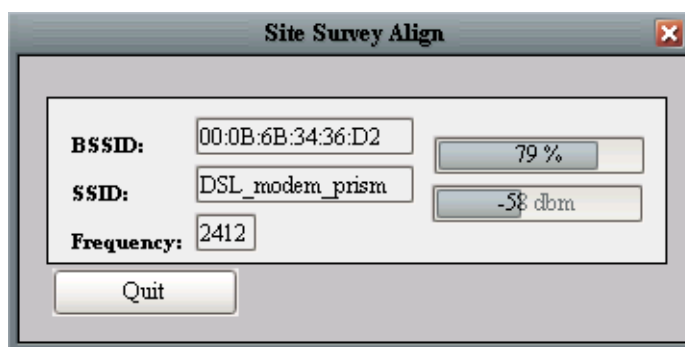


Figure 34. Site Survey Align

## 5.2 Configuring Radio Settings

To configure the radio settings of the selected wireless interface, select the **Radio** tab on the left side of the **Wireless** pane. From the Radio tab you can:

- select the **Physical** layer options (IEEE 802.11 a,b and g)
- select the **Channel** number
- select whether the Channel is expressed as a number or **Frequency**
- select the **TxRate** (data transmission rate)
- set and enable the **Frag** value
- set and enable the **RTS** parameter
- enable **Spoofing**
- configure the **MAC Address**

- enable **Diversity** operation
- select the **Antenna** connector

Figure 35. Wireless Radio Settings

### 5.2.1 Selecting Physical Layer Options

The **Physical** drop down list contains all physical layer options that are available for the specific hardware you are using. If your hardware supports IEEE 802.11 a, b and g standards the **Physical** drop down list will contain **AUTO**, **802.11A**, **802.11B**, **802.11B-G**, **Turbo A** and **Turbo G** options. (If the hardware does not support a physical layer standard AP-ONE HotSpot Manager returns a warning dialog indicating the NIC cannot be configured in the selected physical layer standard.)

### 5.2.2 Setting Channels and Frequencies

The **Channel** drop down list displays the currently selected radio channel using the standard IEEE channel numbering convention. To convert the Channel field to display the actual frequency, click the **Frequency** button.

### 5.2.3 Setting Transmission Rates

The **TxRate** drop down list allows you to select a standard transmission rate based on the available rates associated with the selected physical layer standard. You also can select **Auto** mode. In Auto mode AP-ONE will be auto-configured to support the optimal TxRate for each related node. This can be very useful in environments sensitive to retries. In Auto mode an auto-rate fallback algorithm, which runs on the background, tries to maximize the data transfer rate.

**Note:** Management and Control frames are always transmitted at the lowest available rate of the selected physical layer standard.



## 5.2.4 Setting the MAC Address

The **MAC Address** field contains the MAC address of the configured radio card/hardware that has been selected in the **Selected Wireless Interface** field. However, you can enable spoofing functionality by selecting the **Enable Spoofing** checkbox and typing a new MAC address into the MAC Address field.

## 5.2.5 Setting Frag

The **Frag** field allows you to implement fragmentation of packets, a technique that improves network performance in the presence of RF interference. You can set the fragment size by typing in the frame size threshold (in bytes). If a frame exceeds this value it will be fragmented. The fragmentation range is 256 to 2048 bytes. Setting the fragmentation threshold to 2048 effectively disables fragmentation.

To implement fragmentation, type the threshold value into the **Frag** box and select the Enable check box.

## 5.2.6 Setting RTS

The RTS field allows you to implement RTS/CTS handshaking between an AP-ONE node and another station on the wireless network. RTS/CTS handshaking helps minimize collisions among hidden stations on a wireless network. An RTS/CTS handshake involves the originating node sending a *Ready To Send* frame to its destination, then waiting for the destination to return a *Clear To Send* frame. The originating node will then send its data. RTS/CTS operation adds to overhead but can help avoid collisions. When implementing RTS on an AP-ONE access point RTS operation is initiated if a packet exceeds the threshold configured in the **RTS** field. The valid range is 0 to 2347 bytes. (If RTS is enabled a starting value of 500 is recommended.)

To implement **RTS**, type the threshold value into the **RTS** box and select the Enable check box.

## 5.2.7 Selecting Diversity Options

The **Diversity** field allows you to enable the use of two antennae for diversity operation, if two are used for the same radio.

## 5.2.8 Selecting Antenna Options

The **Antenna** drop down list allows you to select the **Right** or **Left** antenna, if two are used.

## 5.2.9 Setting Transmitted Power

The transmitted power of the node can be set by selecting preset values between 5 and 30. This is a custom scale (with no defined units) which

simply represents minimum and maximum Transmitted Power of the currently selected wireless interface. To set transmitted power, select a value in the **Tx Power** drop down list.

## 5.3 Configuring Security Settings

From the **Security** tab you can configure the security settings of the Selected Wireless Interface. From this tab you can set up

- **None** (no security)
- **WEP** (Wired Equivalent Privacy)
- **WPA** (Wi-Fi Protected Access)
- **ACL** (Access Control List)

### 5.3.1 Setting Wired Equivalent Privacy (WEP)

Through the **WEP** tab you can configure an AP-ONE node to encrypt/decrypt data with keys based on the WEP protocol. To implement WEP, select **WEP** in the **Selected Encryption Mode** drop down list.

To implement 64-bit encryption, select **WEP-64** in the **WEP Type** drop down list.

To implement 128-bit encryption, select **WEP-128** in the **WEP Type** drop down list.

Four text boxes (**WEP Key #1**, **#2**, **#3** and **#4**) with adjacent option buttons allow you to maintain four different encryption keys, while using one of them. Type one or more encryption key into the text boxes, then select the option button of the one to be used.



Figure 36. Wireless WEP Settings

### 5.3.2 Setting Wi-Fi Protected Access (WPA)

In the **WPA** tab you can configure an AP-ONE node to encrypt/decrypt data with keys based on WPA protocol. To implement WPA, select **WPA** in the **Selected Encryption Mode** drop down list.

## Setting WPA Mode

To set the **WPA Mode**, select either the **WPA** or **RSN(WPA 2)** option button.

Figure 37. Wireless WPA Settings

## Setting Key Management Mode

To configure the **Key Management** field, select **PSK** (Pre-Shared Key) or **EAP** (Extensible Authentication Protocol) in the **Key Management Mode** drop down list. This selection determines the type of fields that appear in the area in the right side of the pane.

### EAP

When EAP is selected, several text boxes appear on the right side of the panel. These fields are required in order to force an AP-ONE access point to authenticate clients on a Back-End Authentication Server. They include

- the **Server IP** address
- the **Server Port** number, used for EAP-TLS packet transactions (usually 1812)
- a **Server Secret** phrase which is used for the AP-ONE node authenticator to be accepted by the Back-End Authentication Server.

*EAP-TLS is by default the supported protocol for EAP. The AP-ONE node uses 802-1X authentication to authenticate its clients. If the AP-ONE node is configured as a client, in the case of EAP-TLS usage, you should upload the appropriate certificates on AP-ONE station. This can be done by clicking the **Server** and **Client Certificate** buttons on the right pane.*

Figure 38. EAP Settings

## PSK

When **PSK** is selected in the **Key Management Mode**, drop down list, the **Pass Phrase** text box appears on the right side of the pane. This is the initial value on which negotiated WPA keys are created. To configure the **Pass Phrase** field, type the pass phrase.

The screenshot shows a configuration interface for PSK settings. It includes a 'WPA Mode' section with radio buttons for 'WPA' (selected) and 'RSH (WPA 2)'. Below this is a 'Key Management Mode' dropdown menu currently showing 'PSK'. To the right of these is a 'Pass Phrase' text input field. At the bottom, there are two more dropdown menus for 'Pairwise Cipher' and 'Group Cipher'.

Figure 39. PSK Settings

## Pairwise Cipher

The **Pairwise Cipher** field provides three options for the encryption mechanism of an AP-ONE node.

- **TKIP** (Temporal Key Integrity Protocol)
- **AES(CCMP)** (Advanced Encryption Standard-Counter Mode CBC-MAC Protocol)
- **BOTH** (selected if an AP-ONE node is configured as an access point)

## Group Cipher

(Group Cipher is not functional in AP-ONE NMS version 1.1.3)

### 5.3.3 Configuring Access Control Lists (ACL)

When the **Selected Operational Mode** has been set to **Access Point** or **WDS**, the **ACL** sub-tab in the **Security** tab is available for selection. You have the option of setting an **Access Control List** to manage clients trying to connect to the access point. To configure Access Control List functions, click the **ACL** tab, then select the **Enable** checkbox.

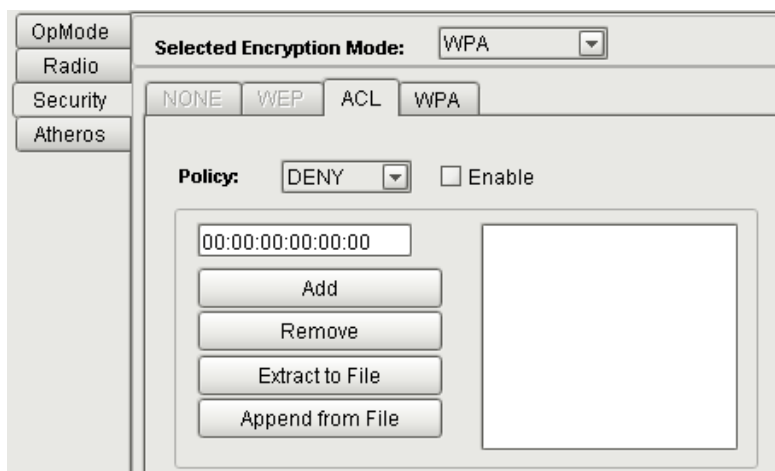


Figure 40. Access Control List Settings

## Denying Access

To deny specified clients access to the node, select **DENY** in the **Policy** drop down list. Clients with MAC addresses matching MAC addresses registered in the ACL will be denied access. All other addresses will be allowed

## Allowing Access

To allow specified clients access to the node, select **ALLOW** in the **Policy** drop down list. Clients with MAC addresses matching MAC addresses registered in the ACL will be allowed access. All other addresses will be denied.

## Setting up Access Control Lists

There are two methods to set up an Access Control List.

- Type in the MAC addresses manually, using the **Add** button, and remove selected MAC addresses using the **Remove** button.
- Load a text file containing the MAC addresses using the **Append from File** button.

## Extracting Access Control Lists

To save an existing ACL, click **Extract to File** and name/save the file. This can be a useful feature if you need to submit the same MAC list to another access point.

## 5.4 Configuring Atheros Advanced Capabilities

The Atheros tab is useful in optimizing the operation of distant AP-ONE nodes.

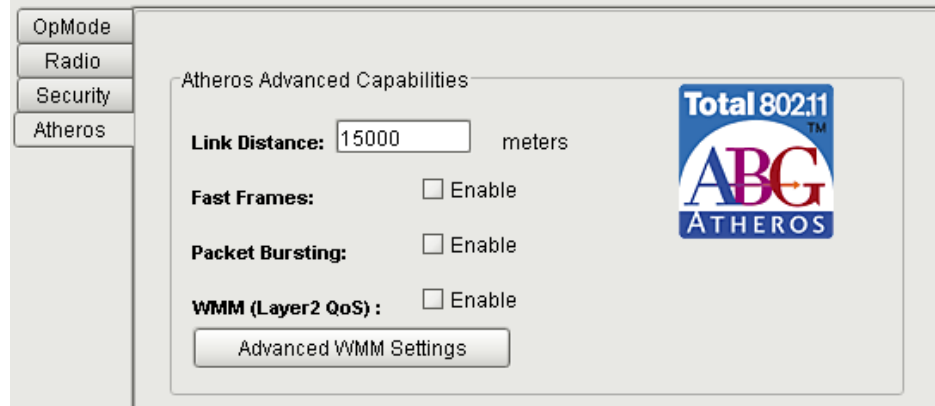


Figure 41. Atheros Settings

## Link Distance

Setting the Link Distance can be effective in optimizing operation of a node. When Link Distance is defined, the acknowledge timeout is configured according to the distance. In lossy environments, where many retries occur, acknowledge timeout should be configured accordingly to the distance between the nodes. To set this parameter, type the distance (in meters) into the **Link Distance** text box.

## Fast Frames

**Fast Frames** is a feature of Atheros-based technologies that utilizes *frame aggregation* and timing modifications to increase the data throughput rate of the system. It increases throughput by transmitting more data per frame and removing inter-frame pauses. To implement fast frames, select the **Fast Frames** check box.

## Packet Bursting

**Packet Bursting** is another technique used by Atheros-based technologies to increase throughput by decreasing overhead and sending more data frames per given period of time. To implement packet bursting, select the **Packet Bursting** check box.

## WMM (Layer 2 QoS) / Advanced WMM Settings

WMM (Wi-Fi Multimedia) is a priority-based Quality of Service method used in implementing Voice over WLANs. To implement WMM, select the **WMM (Layer QoS)** check box, then click the **Advanced WMM Settings** checkbox to access the **Advanced WMM Parameters** dialog Box.

Advanced WMM Parameters				
AP EDCA Parameters				
	AIFs	cw...	cwMax	Max.Burst
VOICE:	2	3	3	6016
VIDEO:	2	3	3	3264
BEST EFFORT:	7	3	7	0
BACKGROUND:	3	3	7	0
Station EDCA Parameters				
	AIFs	cw...	cwMax	Max.Burst
VOICE:	2	3	3	6016
VIDEO:	2	3	3	3264
BEST EFFORT:	7	3	7	0
BACKGROUND:	3	3	7	0

Submit Cancel

Figure 42. Advanced WMM Parameters

## WMM QUEUES (TRAFFIC PRIORITIES)

There are the four queues that h/w uses to organize and prioritized the packets

### **AC\_BK= Background Access Category**

(Lowest Priority for bulk data that require maximum throughput and there is not any time sensitivity related such as FTP for example)

### **AC\_BE= Best Effort Access Category**

(medium priority, traditional IP data via this queue)

### **AC\_VI= Video Access Category**

(High Priority lower than VOICE, video data sent to this)

### **AC\_VO= Voice Access Category**

(High priority, VOIP data and streaming media)

*NOTE1 :: On behalf of the AP these fields are advertised in the Beacon and the CLIENT or STATION on the other side are informed via this in order to be aware of the policy of the AP. On the other hand AP knows the policy of each Client.*

*NOTE2 :: AP EDCA parameters affect traffic flowing from AP to the client or station (On the other hand STA EDCA control the upstream form client or Station to AP)*

## CONFIGURABLE FIELDS (per queue)

a. **CWmin** = Minimum Value of Contention Window

b. **CWmax** = Maximum Value of Contention Window

b. **AIFsn** = Arbitrary Interframe Space

d. **TXOP** = Length of TXOP

### **CWmin**

Input to the algorithm that specifies the initial random backoff wait time (window as known) for retry transmission. This value is the upper limit in msec of a range from which initial random backoff wait time is determined.

### **CWmax**

This value is the upper limit in msec for the doubling random backoff value. This doubling continues until either the data frames is sent or the Max Contention Window is reached

### **AIFs**

The Arbitration Inter-Frame Spacing specifies a wait time for data frames

### **TXOP**

This is an interval of time when a **WMM** station or client has the right to initiate transmissions onto the wireless medium.



## 6. Firewall and NAT

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. A network system in order to support firewall functionality must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

To configure **Firewall** settings, select the **Firewall** tab, located under the **Advanced Configuration of Node, Configuration** tabs.

To configure **NAT** settings, select the **NAT** tab, located under the **Advanced Configuration of Node, Configuration** tabs.

*See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.*

### 6.1 Firewall and NAT Chains

AP-ONE supports advanced firewall and NAT (Network Address Translation) functionality and features an easy management and monitoring interface, providing a turnkey solution for advanced and novice network administrators. However, a firewall mis-configuration may result in denial of service even for the administrator, outlining a high risk configuration.

AP-ONE's Firewall and NAT subsystems consist of four firewall and two NAT queue chains.

#### 6.1.1 Firewall Chains

- **Input firewall** - All incoming traffic is tested against the input firewall rules prior to being accepted.
- **Output firewall** - All outgoing traffic is tested against the output firewall rules prior to being sent.
- **Forwarding firewall** - All traffic that is being forwarded through the operating system is tested against the forwarding firewall rules prior to being forwarded.
- **Flowmark** - All incoming traffic that matches the corresponding criteria is marked.

#### 6.1.2 NAT Chains

- **DNAT** - Used to alter destination attributes of a packet (to redirect them).

- **SNAT** - Used to alter source attributes of a packet (to hide sender's address and properties).

The following image displays the way data packets flow through Firewall and NAT chains:

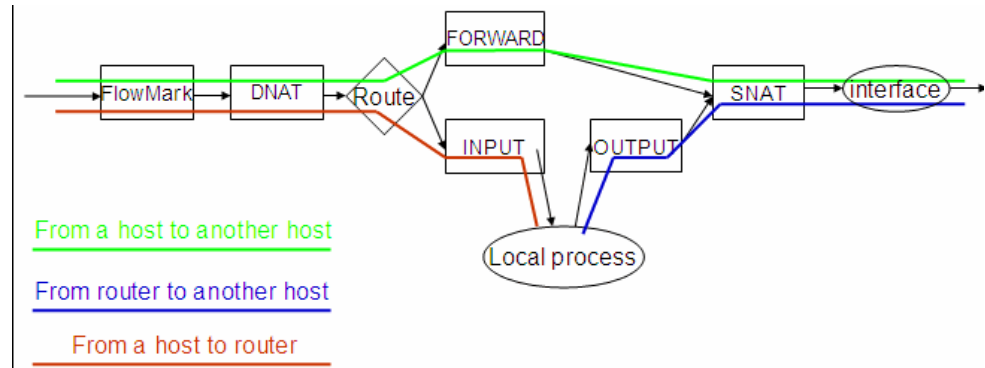


Figure 43. Packet flow diagram

## 6.2 Configuring Firewall Rules

Rules are entries in a chain consisting of several fields (criteria) that can be used to match a data packet. If all criteria are met, the rule is matched and the packet leaves the chain, launching the action of the matching rule.

From the Firewall tab you can

- **Select Chains**
- **Set up Policy**
- Add, delete and manage Firewall **Rules** and **Flowmarks**
- **Write** rules to the active list
- **Refresh** the displayed information

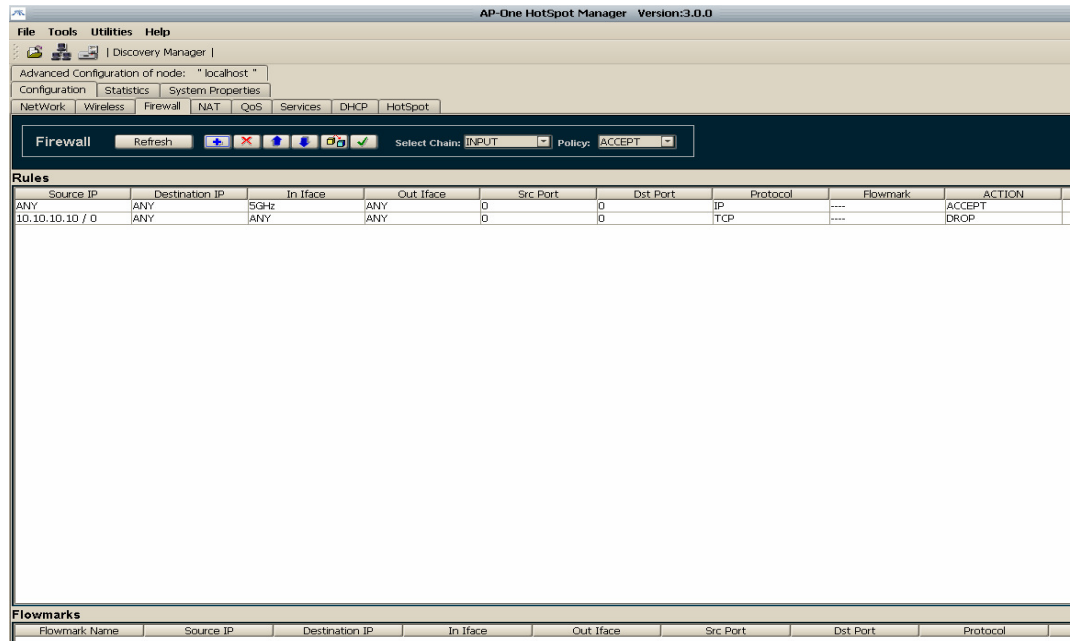


Figure 44. Firewall Chains

Before configuring a rule, you must **Select Chain** and set the **Policy**.

### Select Chain

In the **Select Chain** drop down list, select **Input**, **Output** or **Forward**.


### Policy

In the **Policy** drop down list, select **Accept** or **Drop**.

**ACCEPT** - The packet will flow to the next chain, leaving the current chain at this rule (no further rules in this chain are further examined),

**DROP** - The packet stops flowing, is discarded, without notifying the sender.

## 6.2.1 Configuring Firewall Matching Fields

Click the  button. The **Firewall Rule Configuration for [chain type] Chain** dialog box appears. This dialog box contains two tabs: **Basic** and **Advanced**.

### Not Check Boxes

In both tabs, several fields have a **Not** check box beside them. The Not field inverts the matching operation, causing a match to occur if the opposite of the rule is matched. For example, **Source IP**: is configured with the specific IP address. When the adjacent check box is selected the

rule will match all packets **except** the ones that have the specified Source IP address.

## Basic Rule Settings

Figure 45. Firewall Rule Configuration Dialog Box, Basic Tab

### Source IP

The **Source IP** field displays the Source IP address of the packet. The address can be expressed as a single IP address (e.g. 192.168.1.1/32), or as a whole IP subnet (e.g. 192.168.1.0/24). A match occurs if the source IP of the packet is exactly the same or belongs to the subnet configured.

Type the source IP address and number of subnet mask bits into the **Source IP** field.

### Destination IP

The **Destination IP** field displays the Destination IP address of the packet. The address can be expressed as a single IP address (e.g. 192.168.1.1/32), or as a whole IP subnet (e.g. 192.168.1.0/24). A match occurs if the destination IP of the packet is exactly the same or belongs to the subnet configured.

Type the destination IP address and number of subnet mask bits into the **Destination IP** field.

### Input Interface

The **Input Interface** field displays the interface from which the packet was delivered. A match occurs if the interface that the packet arrived from is the same as the configured interface (if the configured interface is a bridge, this also matches with interfaces under the bridge).

In the **Input Interface** drop down list, select a specific input interface, or select **ANY**.

## Output Interface

The **Output Interface** field displays the interface from which the packet is to be transmitted. A match occurs if the interface that the packet will be transmitted from is the same with the configured interface (in case the configured interface is a bridge, this also matches with interfaces under the bridge).

In the **Output Interface** drop down list, select a specific input interface, or select **ANY**.

## Existing Flowmark

The **Existing Flowmark** drop down list contains Flowmarks that already have been configured. Select a Flowmark from the list to configure a Flowmark as a firewall matching rule. A match occurs if the packet was marked by this mark when it flowed through the Flowmark chain.

## New Flowmark

The **New Flowmark** field is available if **Mark** is selected in the **Action** field. Type the name of the new flowmark in the **New Flowmark** box.

## Action

When a rule is matched, its action is performed. Firewall actions can be:

**ACCEPT** - The packet will flow to the next chain, leaving the current chain at this rule (no further rules in this chain are further examined),

**REJECT** - The packet stops flowing, is discarded, and a return ICMP packet (reason code UNREACHABLE) is sent back to the sender.

**DROP** - The packet stops flowing, is discarded, without notifying the sender.

**FORWARD** - (currently not in use)

**MARK** - The packet will flow to the next chain, leaving the current chain at this rule (no further rules in this chain are further examined). It will be marked as **New Flowmark**.

## Comment

The **Comment** field is used to enter a string consisting of at most 30 characters to describe the rule. This field is not used for matching.

## Advanced Rule Settings

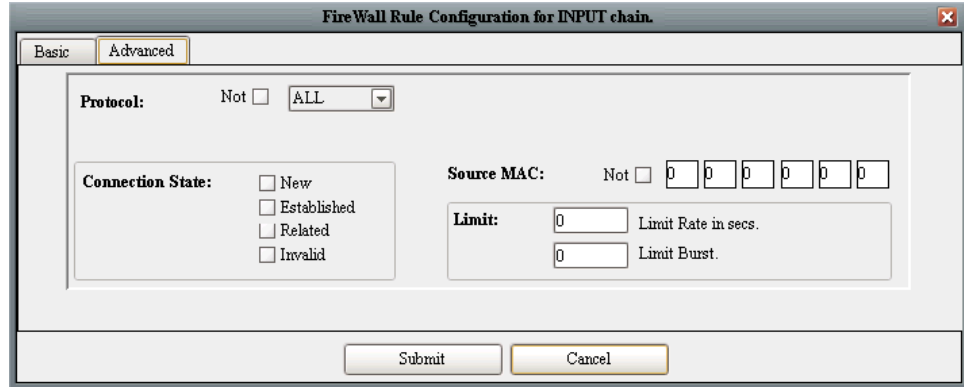


Figure 46. Firewall Rule Configuration Dialog Box, Advanced Tab

## Protocol

The **Protocol** drop down list contains a list of protocols that can be selected for matching. The contents of the dialog box changes depending on the protocol selected. The following selections may be configured in this field:

- **ALL** – A match always occurs.
- **TCP** – A match occurs if
  - the packet's protocol type is **TCP**

### AND

- the **SYN flag** of the packet matches based on which of the following is selected in the SYN flag drop down list:
  - **ALL** - matches always.
  - **SET** - A match occurs if the packet starts a new connection.
  - **NOT SET** - A match occurs if the packet is a member of a previously started connection.

### AND

- **Source Port** - Source port is entered as number (0-65535) where 0 indicates that all ports are matched.
- **Destination Port** - Destination port is entered as number (0-65535) where 0 indicates that all ports are matched.

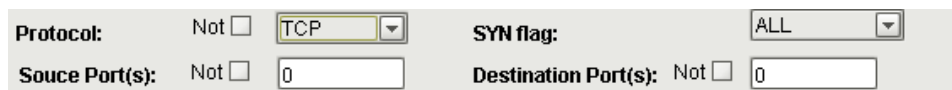


Figure 47. Advanced Firewall Rule, TCP

- **UDP** – A match occurs if
  - the packet's protocol type is **UDP****AND**
  - **Source Port** - Source port is entered as number (0-65535) where 0 indicates that all ports are matched.**AND**
  - **Destination Port** - Destination port is entered as number (0-65535) where 0 indicates that all ports are matched.
- **ICMP** – A match occurs if
  - the packet's protocol type is **ICMP****AND**
  - the **ICMP Type** matches based on which of the following is selected in the **ICMP Type** drop down list:
    - **ANY**: A match occurs always
    - **REQUEST**: A match occurs if the packet is an ICMP request.
    - **RESPONSE**: A match occurs if the packet is an ICMP response.
- **GRE** – A match occurs if the packet's protocol type is **GRE** (Generic Routing Encapsulation)
- **ESP** - A match occurs if the packet's protocol type is **ESP**
- **AH** – A match occurs if the packet's protocol type is **AH**

### **Connection State**

AP-ONE can perform firewall functions based on the connection state. The following selections may be configured in this field:

**New** - A match occurs if the packet starts a new connection (router has seen packets in one direction).

**Established** - A match occurs if the packet is a member of an existing connection (router has seen packets in both directions).

**Related** - A match occurs if the packet starts a new connection, but is also a member of an existing connection (router has seen packets in both directions).

**Invalid** - A match occurs if the packet is not a member of an existing connection, but also it does not start a connection (ambiguous packet).

## Source MAC


A match occurs if the packet's **Source MAC** address (in the Ethernet header) is the same as the address in this field. Type the **Source MAC** address in the **Source MAC** field

## Limit

The **Limit** fields contain settings related to the rate at which the packet is arriving.

**Limit Rate** - A match occurs if the configured rate has not been reached yet.

**Limit Burst** - A match occurs if the configured burst rate has not been reached yet.

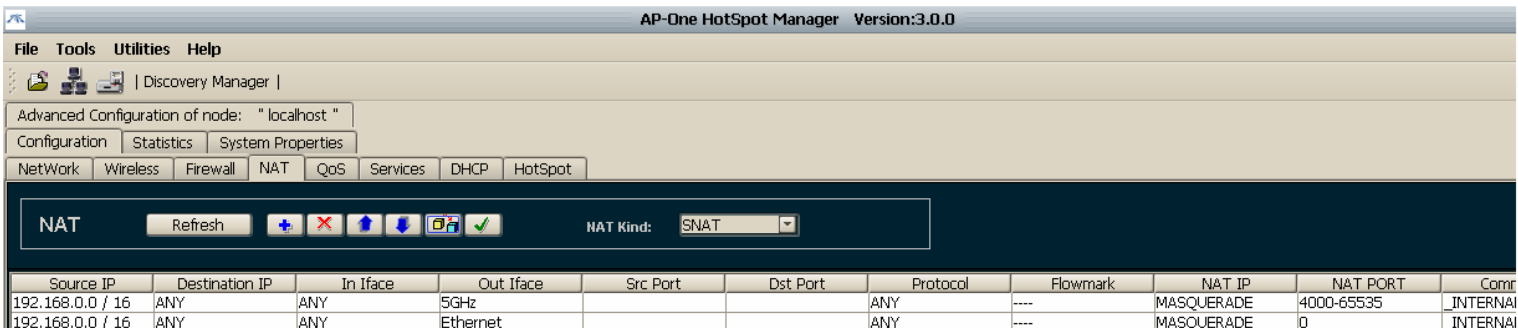
**Important:** To enable a Firewall rule (write it to the active list) you must click the  button.

## 6.3 Configuring NAT Rules

Rules are entries in a chain consisting of several fields (criteria) that can be used to match a data packet. If all criteria are met, then the rule is matched and the packet leaves the chain, launching the action of the matching rule.

From the NAT tab you can

- Select the **NAT Kind**
- Add, delete, edit and manage NAT rules
- Write NAT rules to the active list



Source IP	Destination IP	In Iface	Out Iface	Src Port	Dst Port	Protocol	Flowmark	NAT IP	NAT PORT	Conn
192.168.0.0 / 16	ANY	ANY	5GHz			ANY	----	MASQUERADE	4000-65535	_INTERNAL
192.168.0.0 / 16	ANY	ANY	Ethernet			ANY	----	MASQUERADE	0	_INTERNAL

Figure 48. NAT Chains




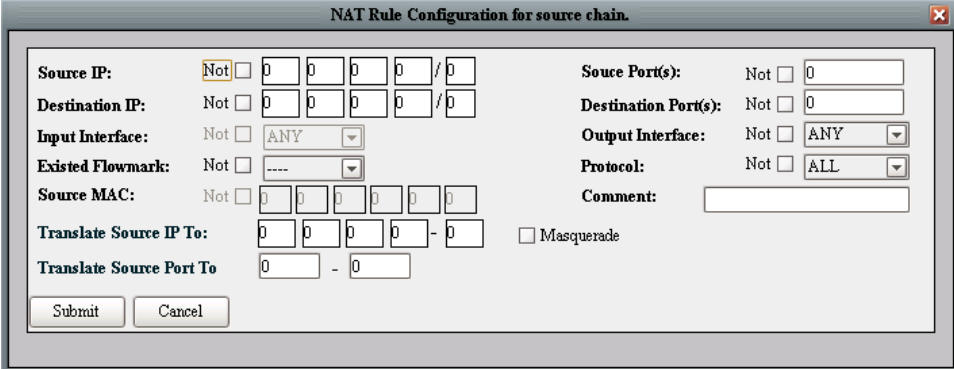
Before configuring rules you must select the **NAT Kind** drop down list.

## NAT Kind

In the **NAT Kind** drop down list, select **SNAT** or **DNAT**.

### 6.3.1 Configuring NAT Matching fields

To add a rule, click the  button. The **NAT Rule Configuration for [NAT Kind] Chain** dialog box appears.



The dialog box titled "NAT Rule Configuration for source chain" contains the following fields and controls:

- Source IP:** Not  [0][0][0][0] / [0]
- Destination IP:** Not  [0][0][0][0] / [0]
- Input Interface:** Not  ANY
- Existed Flowmark:** Not  ----
- Source MAC:** Not  [0][0][0][0][0][0]
- Translate Source IP To:** [0][0][0][0] - [0]  Masquerade
- Translate Source Port To:** [0] - [0]
- Source Port(s):** Not  [0]
- Destination Port(s):** Not  [0]
- Output Interface:** Not  ANY
- Protocol:** Not  ALL
- Comment:** [Text Field]

Buttons: Submit, Cancel

Figure 49. NAT Rule for Configuration for Source Chain Dialog Box

## SNAT/DNAT Common Fields

The following fields are common to SNAT and DNAT configuration dialog boxes.

### Not Check Boxes

Several fields have a **Not** check box beside them. The NOT field inverts the matching operation, causing a match to occur if the opposite of the rule is matched. For example, **Source MAC:** is configured with the specific MAC address. When the adjacent check box is selected the rule will match all packets **except** the ones that have the specified Source MAC address.

### Source IP

The **Source IP** field displays the Source IP address of the packet. The address can be expressed as a single IP address (e.g. 192.168.1.1/32), or as a whole IP subnet (e.g. 192.168.1.0/24). A match occurs if the source IP of the packet is exactly the same or belongs to the subnet configured.

Type the source IP address and number of subnet mask bits into the **Source IP** field.

### **Destination IP**

The **Destination IP** field displays the Destination IP address of the packet. The address can be expressed as a single IP address (e.g. 192.168.1.1/32), or as a whole IP subnet (e.g. 192.168.1.0/24). A match occurs if the destination IP of the packet is exactly the same or belongs to the subnet configured.

Type the destination IP address and number of subnet mask bits into the **Destination IP** field.

### **Source Port(s)**

The **Source Port(s)** field displays the port number of the source node. A match occurs if the source port number is the same as the number in this field.

Type the source port number into the **Source Port** field.

### **Destination Port(s)**

The **Destination Port(s)** field displays the port number of the destination node. A match occurs if the destination port number is the same as the number in this field.

Type the destination port number into the **Destination Port** field.

### **Input Interface**

The **Input Interface** field displays the interface from which the packet was delivered. A match occurs if the interface that the packet arrived from is the same as the configured interface (if the configured interface is a bridge, this also matches with interfaces under the bridge).

In the **Input Interface** drop down list, select a specific input interface, or select **ANY**.

### **Output Interface**

The **Output Interface** field displays the interface from which the packet is to be transmitted. A match occurs if the interface that the packet will be transmitted from is the same with the configured interface (in case the configured interface is a bridge, this also matches with interfaces under the bridge).

In the **Output Interface** drop down list, select a specific input interface, or select **ANY**.

### **Existing Flowmark**

The **Existing Flowmark** drop down list contains Flowmarks that already have been configured. Select a Flowmark from the list to configure a Flowmark as a firewall matching rule. A match occurs if the packet was marked by this mark when it flowed through the Flowmark chain.

## Protocol

The **Protocol** drop down list contains a list of protocols that can be selected for matching. The following selections may be configured in this field:

- **ALL** – A match always occurs.
- **TCP** – A match occurs if
  - The **Source port** is entered as a number from 0 to 65535, where 0 indicates that all ports are matched.
  - The **Destination port** is entered as a number from 0 to 65535, where 0 indicates that all ports are matched.
- **UDP** - A match occurs if packet's protocol type is UDP and,
  - The **Source port** is entered as a number from 0 to 65535, where 0 indicates that all ports are matched.
  - The **Destination port** is entered as a number from 0 to 65535, where 0 indicates that all ports are matched.
- **ICMP** - A match occurs if packet's protocol type is ICMP
- **GRE** - A match occurs if packet's protocol type is GRE
- **AH** - A match occurs if packet's protocol type is AH
- **ESP** - A match occurs if packet's protocol type is ESP

## Source MAC

This is the sender's MAC address. A match occurs if the packet's Source MAC address (in the Ethernet header) is the same.

## Comment

The **Comment** field is used to enter a string consisting of at most 30 characters to describe the rule. This field is not used for matching.

## SNAT Chain Specific Fields

The following fields are available in the SNAT configuration dialog box.

**Masquerade:** The IP address to be assigned to outgoing packets is dynamically retrieved by the current outgoing interface's IP address (does not need to explicitly configure the outgoing source IP address).

**Translate Source IP to:** The IP address (or range of IP addresses) that the source IP of the packet will change to. In case there is a range of IP addresses, a round robin algorithm is used to assign addresses.

**Translate Source Port to:** The range of the router's ports used to send NATed packets and track for responses.

## DNAT Chain Specific Fields

The following fields are available in the DNAT configuration dialog box.

**Redirect** – When a match occurs, the packet will be redirected to another port of the router.


**Translate Dest IP to** – The IP address (or range of IP addresses) that the destination IP of the packet will change to. In case there is a range of IP addresses, a round robin algorithm is used to assign addresses. This is used to **forward the packet to another host**.

**Translate Dest Port to** – The port that the packet will be sent to (in case there is a range of ports, a round robin algorithm is used).

The screenshot shows a dialog box titled "NAT Rule Configuration for destination chain." It contains the following fields and controls:

- Source IP:** Not  0 0 0 0 / 0
- Destination IP:** Not  0 0 0 0 / 0
- Input Interface:** Not  ANY (dropdown)
- Existed Flowmark:** Not  ---- (dropdown)
- Source MAC:** Not  0 0 0 0 0 0
- Translate Dest IP To:** 0 0 0 0 - 0
- Translate Dest Port To:** 0 - 0
- Source Port(s):** Not  0
- Destination Port(s):** Not  0
- Output Interface:** Not  ANY (dropdown)
- Protocol:** Not  ALL (dropdown)
- Comment:** [Text field]
- Redirect
- Buttons:** Submit, Cancel

Figure 50. NAT Rule for Configuration for Destination Chain Dialog Box

**Important:** To enable a NAT rule (write it to the active list) you must click the  button.

### 6.3.2 Examples

The following examples may be helpful in understanding how to configure Firewall and NAT rules.

#### Deny incoming SSH connections to your router from the internet.

SSH service by default runs on port 22. Assume that the router is connected to the internet through interface Ethernet0. To disallow incoming SSH connections from the internet, you can insert a rule in the Input chain of the Firewall system that will drop this kind of connection (because they are TCP connections, SYN flag will be set).

To accomplish this, configure the Firewall rules as follows:

#### In the Basic tab:

**Source IP:** 0.0.0.0/0 (any)

**Destination IP:** 0.0.0.0/0 (any)  
**Input interface:** Ethernet (the connection to internet)  
**Comment:** no\_SSH\_connect  
**ACTION:** DROP

**In the Advanced tab:**

**Protocol:** TCP  
**SYN Flag:** SET  
**Source Port:** 0(any)  
**Destination Port:** 22(SSH)

The screenshot shows the 'Basic' tab of the 'FireWall Rule Configuration for INPUT chain' dialog. The 'Source IP' field is set to '0.0.0.0/0' with 'Not' checked. The 'Destination IP' field is also set to '0.0.0.0/0' with 'Not' checked. The 'Existed Flowmark' is set to '---' with 'Not' checked. The 'Action' is set to 'REJECT'. The 'Input Interface' is set to 'Ethernet' with 'Not' checked. The 'Output Interface' is set to 'ANY' with 'Not' checked. The 'New Flowmark' and 'Comment' fields are empty. 'Submit' and 'Cancel' buttons are at the bottom.

Figure 51. Basic Rule Example Configuration

The screenshot shows the 'Advanced' tab of the 'FireWall Rule Configuration for INPUT chain' dialog. The 'Protocol' is set to 'TCP'. The 'SYN flag' is set to 'SET'. The 'Source Port(s)' is set to '0'. The 'Destination Port(s)' is set to '22'. The 'Connection State' section has four options: 'New', 'Established', 'Related', and 'Invalid', all of which are unchecked. The 'Source MAC' is set to '0.0.0.0.0.0.0' with 'Not' checked. The 'Limit' section has two fields: 'Limit Rate in secs.' and 'Limit Burst', both set to '0'. 'Submit' and 'Cancel' buttons are at the bottom.

Figure 52. Advanced Rule Example Configuration

Click **Submit** to add the rule to the list and apply it to the router.

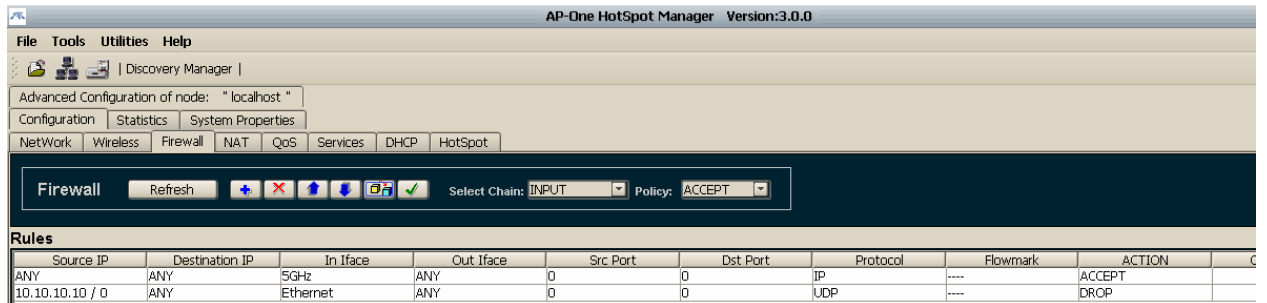


Figure 53. Example Firewall Tab

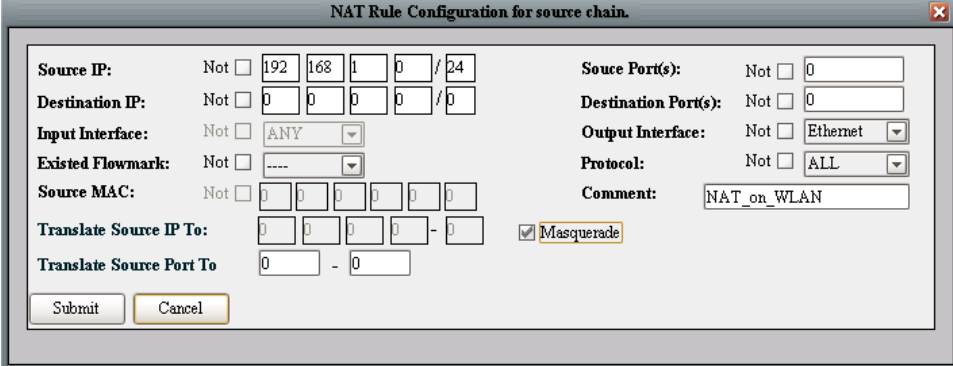
**NAT:** Having a single public IP address, allow whole local network to access the internet.

Assume that the router is connected to the internet through interface Ethernet0 and IP address 173.55.1.2/24. Your local network is connected to router's Ethernet1 interface with IP address 192.168.1.1/24. You should masquerade all outgoing traffic to the internet (interface Ethernet0) originated from your local network (interface Ethernet1).

Insert a rule to the SNAT chain as follows:

### Details

**Source IP:** 192.168.1.0/24 (local network)  
**Output Interface:** Ethernet0  
**Translate Source IP to:** 0.0.0.0-0 MASQUERADE (Ethernet0's IP address)  
**Comment:** NAT\_on\_WAN



**NAT Rule Configuration for source chain.**

Source IP: Not  192.168.1.0 / 24

Destination IP: Not  0.0.0.0 / 0

Input Interface: Not  ANY

Existed Flowmark: Not  ----

Source MAC: Not  0.0.0.0.0.0

Translate Source IP To:  0.0.0.0 -  0  Masquerade

Translate Source Port To: 0 - 0

Source Port(s): Not  0

Destination Port(s): Not  0

Output Interface: Not  Ethernet

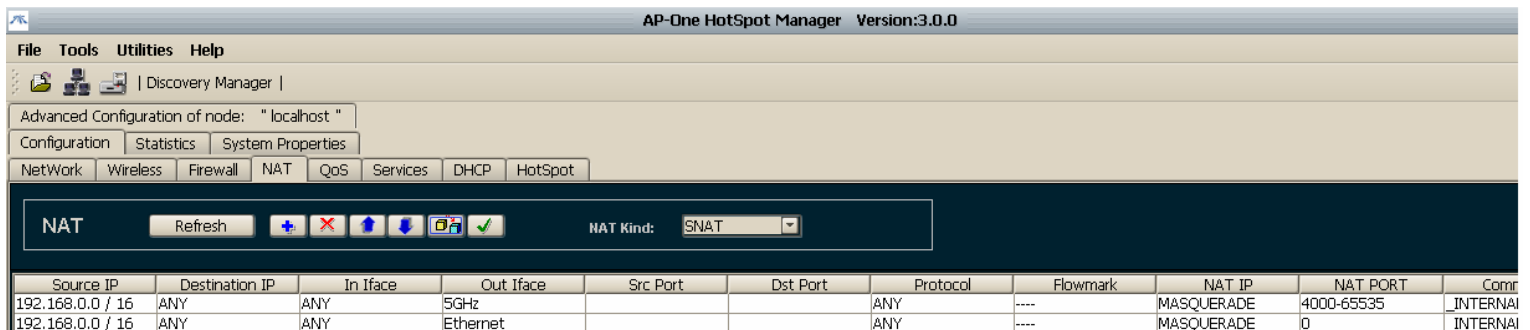
Protocol: Not  ALL

Comment: NAT\_on\_WLAN

Submit Cancel

Figure 54. NAT Configuration - Masquerade Example

Click **Submit** to add the rule to the list and apply it to the router.



AP-One HotSpot Manager Version:3.0.0

File Tools Utilities Help

Discovery Manager |

Advanced Configuration of node: "localhost"

Configuration Statistics System Properties


NetWork Wireless Firewall NAT QoS Services DHCP HotSpot

NAT Refresh + - Up Down Refresh Check HAT Kind: SNAT

Source IP	Destination IP	In Iface	Out Iface	Src Port	Dst Port	Protocol	Flowmark	NAT IP	NAT PORT	Comr
192.168.0.0 / 16	ANY	ANY	5GHz			ANY	----	MASQUERADE	4000-65535	_INTERNAL
192.168.0.0 / 16	ANY	ANY	Ethernet			ANY	----	MASQUERADE	0	_INTERNAL

Figure 55. NAT Tab - Masquerade Example

**HINT:** make sure IP Forwarding is enabled on the router (Interface settings Panel).

**Important:** To enable a NAT rule (write it to the active list) you must click the  button.

## 7. DHCP

---

The **Dynamic Host Configuration Protocol (DHCP)** provides configuration parameters to Internet hosts in a client-server model. [DHCP](#) server hosts allocate network addresses and deliver configuration parameters to other (client) hosts.

[DHCP](#) consists of two components: a protocol for delivering host-specific configuration parameters from a server to a host and a mechanism for allocation of network addresses to hosts.

To configure **DHCP** settings, select the **DHCP** tab, located under the **Advanced Configuration of Node, Configuration** tabs. The DHCP tab contains two sub-tabs: **Server** and **Client**, selected by clicking the corresponding option button.

*See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.*

### 7.1 Configuring a DHCP SERVER

The AP-ONE DHCP server provides an extended set of configuration parameters while at the same time being effective and low resource consuming.



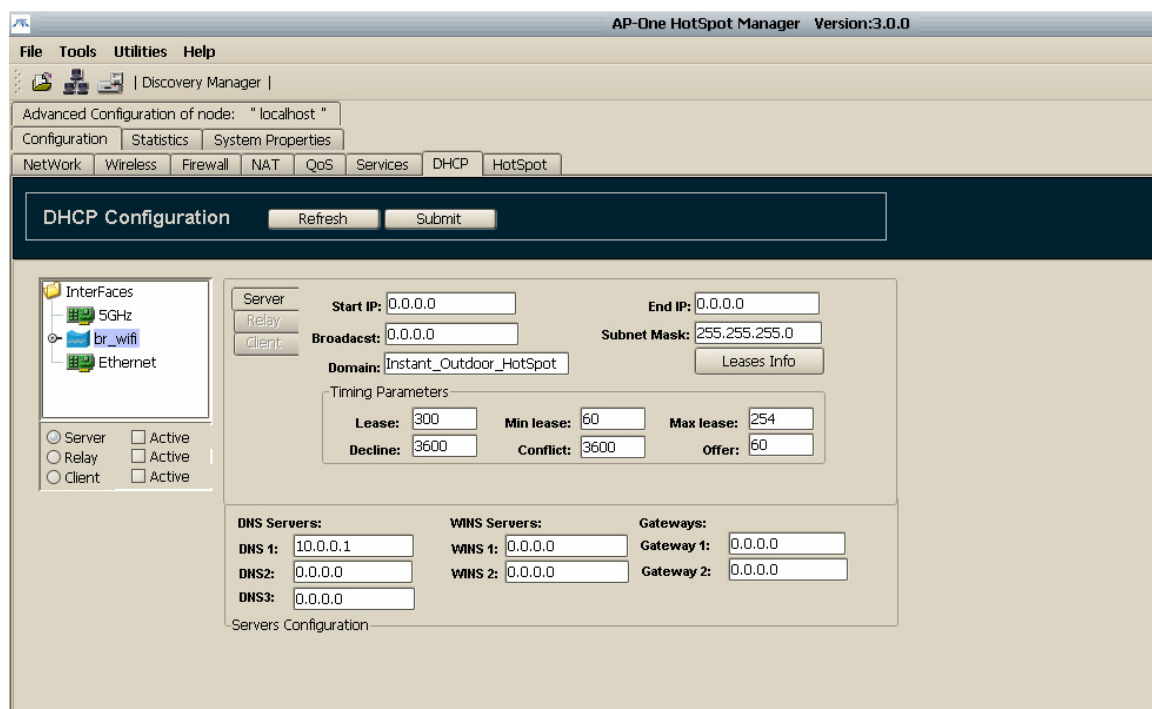


Figure 56. DHCP Server Configuration Dialog Box

To configure a **DHCP Server**, select the interface from the interface tree. Its background turns blue. Only clients in the same physical interface will be able to acquire IP addresses from this DHCP server. If clients from other physical interfaces must acquire their IP addresses from the same server a bridge should be created, and those interfaces should be added under that bridge. Then, select that bridge as the DHCP server interface.

**NOTE:** You cannot select an interface which is under a bridge as the DHCP server interface. Additionally the DHCP server interface should have already been configured with a valid IP address and subnet mask. Multiple DHCP servers on different interfaces are allowed.

### 7.1.1 Setting DHCP Server Fields

To configure DHCP server settings, select the **Server** option button and select the **Active** check box. The **Server** tab becomes available.

After completing the required fields, click the **Submit** button. This uploads the configuration to the node without starting the server.

#### Start IP and End IP

Type the appropriate IP addresses into the **Start IP** and **End IP** fields. These are the upper and lower limits for the DHCP server address pool.

## Broadcast

Type the appropriate IP address into the **Broadcast** field. This field contains the IP address clients will use. Broadcast IP should be one of the addresses the Subnet Mask permits.

## Subnet Mask

Type the appropriate IP address into the **Subnet** Mask field. This is the subnet mask clients will use.

## Domain

Type the **Domain** name (if any) that will be allocated to clients into this text box.

## Time Parameters

For each of the following fields, type the appropriate value into the box.

### Lease

The **Lease** field contains the number of seconds an allocated IP is valid. After expiration the client has to renegotiate for getting a new IP (which is usually the same). The expiration time that the client adopts depends on the operating system running on the client and the DHCP client configuration.

### Decline

The **Decline** field contains the number of seconds that an IP will be reserved (leased) for if a DHCP decline message is received.

### Min Lease

The **Min Lease** field contains the minimum number of seconds. If a lease to be given is below this value (sec), the full lease time is used instead.

### Conflict

The **Conflict** field contains the amount of time (sec) that an IP address will be reserved (leased) if an ARP conflict (two clients with the same IP address) occurs.

### Max Lease

The **Max Lease** field contains the maximum number of current leases (allocated IP addresses). After this limit is reached the server stops assigning IP addresses to new clients.

### Offer

The **Offer** field contains the number of seconds an offered address is reserved (leased). This field specifies the number of seconds the DHCP server should cache the offers it has extended to discovering DHCP clients. The default value is 60 seconds. On fast network media this value can be decreased.

## DNS Servers

In the three **DNS Servers** fields (DNS 1, DNS 2 and DNS 3), type the IP addresses of the DNS servers that DHCP clients will use for DNS requests.

## WINS Servers

If there are WINS servers that client should use, type the addresses in the **WINS Servers** fields (WINS 1 and WINS 2).

## Routers

In the **Routers** fields (Router 1 and Router 2), type the IP addresses of the routers (default gateways) the client can use.

## Leases Info

Click the **Leases Info** button to access the **DHCP Leases** dialog box that displays all the allocated leases.

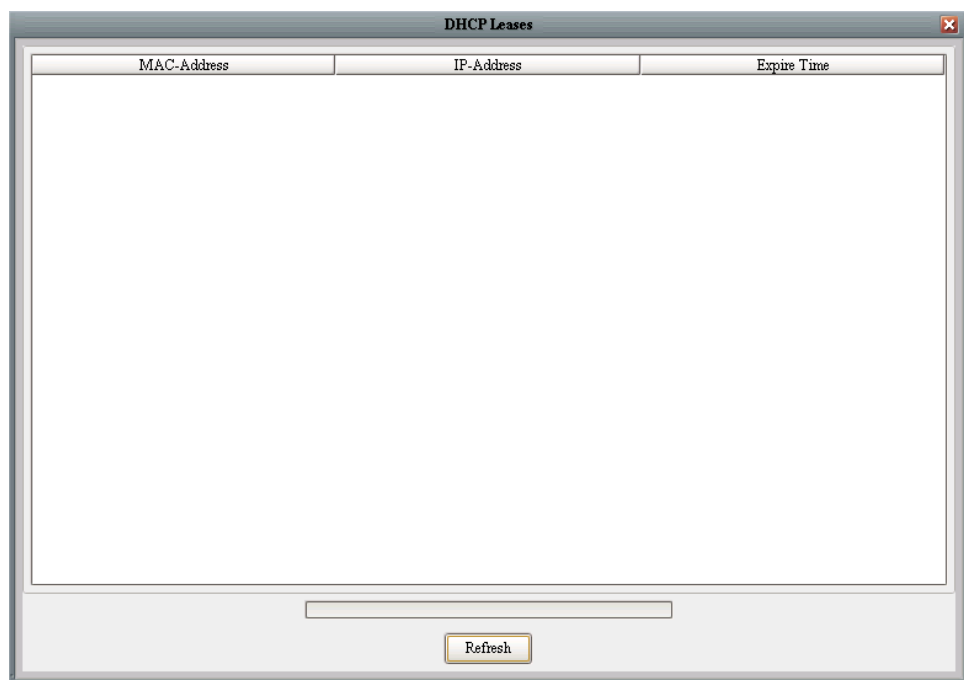


Figure 57. DHCP Leases Dialog Box

In the current version DHCP server configuration does not support dynamic changing of the DHCP leases file. After an IP allocation you are able to see the new record in the DHCP Leases dialog after approximately a 60 second delay.

## 7.1.2 Lease Time Strategies

One of the most common DHCP administration questions is, "What setting should I give my lease times?" As with many networking questions, the answer is, "It depends." The primary decision criterion is the desired frequency at which your clients update their configuration data.

If you are using DHCP only for randomized address assignments, having longer lease times will result in greater levels of stability. For example, if you use lease duration times of one month or longer, a temporary server outage is not likely to affect your normal operations much. However, if you are using DHCP for a variety of system-configuration options (such as default DNS servers and static routes), you will want to have shorter lease times so that changes to the network are recognized quickly by the DHCP clients. In this case, having lease times that are longer than a day or two can be problematic because clients that obtain a new lease just before a critical infrastructure change is made will not recognize this change until the lease expires or gets renewed.

For dynamic environments, there are two common lease-duration strategies. The first calls for leases to be renewed halfway through a working day (such as having them expire every eight hours, which will cause them to be renewed after four hours). Another strategy is to set the lease duration to a multiple of two and a half times the working day (that is, 20 hours for an eight-hour working day), causing the leases to completely expire overnight and thus be renegotiated every morning. The former strategy works well on networks that keep their machines running all of the time, while the latter strategy works well on networks where systems are powered down or otherwise removed from the network at night.

Be forewarned, however, that both strategies expose the network to problems if the DHCP server goes down or is on a remote network that is subject to outages. If the DHCP clients are getting their lease data from a remote DHCP server that is on the other side of a WAN link that is even minimally prone to failure, chances are good that short lease times will result in at least a few failed lease renewals.

## 7.2 Configuring a DHCP CLIENT

Configuration of the **DHCP Client** application is simple. The only requirement is selection of the interface where the DHCP client will search for DHCP servers.

Similar to DHCP server configuration, multiple instances of DHCP client on different interfaces are allowed.

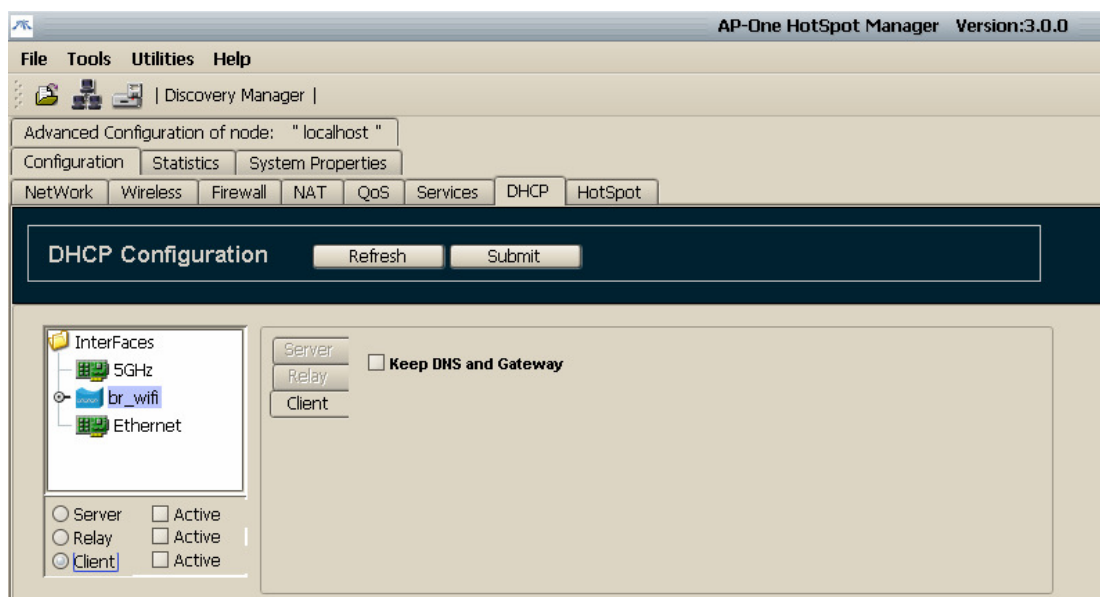


Figure 58. DHCP Client

To configure a **DHCP Client**, select the interface from the interface tree. Its background turns blue.

To configure DHCP client settings, select the **Client** option button and select the **Active** check box. The **Client** tab becomes available.

To prevent the changing of a client's default system gateway and DNS addresses when the client receives an IP address from the server, select the **Keep DNS and Gateway** check box. This is useful when you already have set a static default gateway and DNS and want them to remain unchanged, or if they are to be configured from another application (e.g. PPPoE client). In most other cases this field should remain unselected.

To complete the configuration, click the **Submit** button.

## 7.3 Configuring a DHCP Relay

DHCP does not require a server on each subnet. To allow for scale and economy, a [relay agent](#) can be installed listening to [DHCP](#) messages and forwarding them on (and onto other network segments). This eliminates the necessity of having a [DHCP](#) server on each physical network.

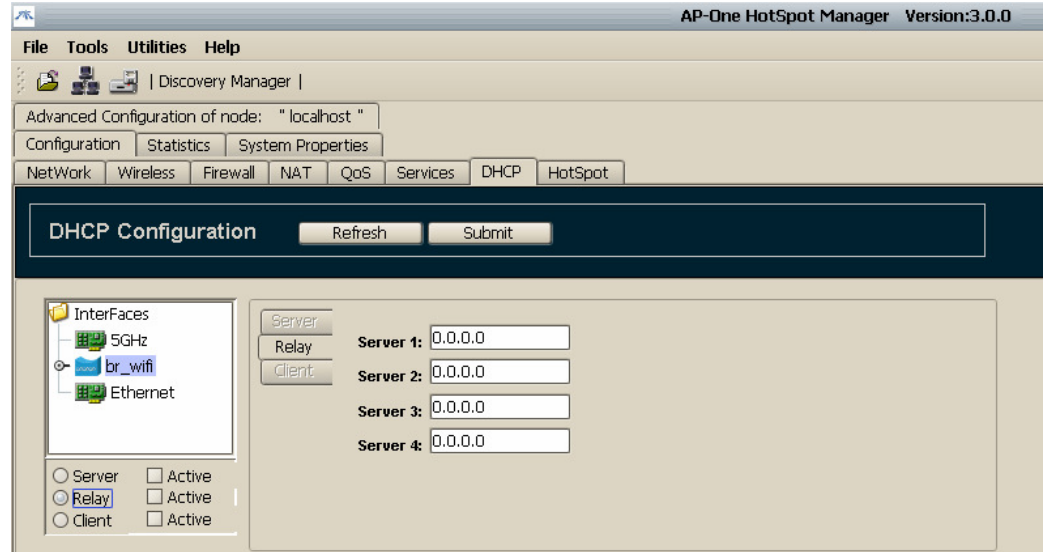


Figure 59. DHCP Relay

To configure a **DHCP Relay**, select the interface from the interface tree. Its background turns blue.

To view the full **DHCP Relay** pane, select the **Relay** option button, then select the **Active** check box. The **Relay Configuration** pane appears.

The **Relay Configuration** pane represents the subnet (LAN) where a relay listens for client DHCP requests in order to forward them to DHCP servers **Server 1**, **Server 2**, **Server 3** or **Server 4**. Type the appropriate IP addresses in these fields.

Interface where application relays on should has a valid ip and subnet mask and like the other DHCP APIs, DHCP relay can have multiple instances on different interfaces.

To complete the configuration, click **Submit**.

## 8. Quality of Service

---

Quality of service (also known as Traffic Shaping) refers to the general concept of prioritizing network traffic, according to some of its properties. By default, each packet is treated equally and in a first-come, first-served basis. However, by utilizing QoS, certain traffic patterns, can be given higher priority or can be guaranteed specific network resources. From now on, we will refer to a traffic pattern as class.

Some of the policies that can be enforced with QoS are:

- Restrict or eliminate the bandwidth consumed by P2P applications.
- Distribute the available bandwidth equally among a group of HOTSPOT users.
- Make sure that certain services (e.g. the web portal of a hotspot) will always be accessible, no matter how overloaded the network is.
- Reserve a portion of the available bandwidth for latency-sensitive applications, like VoIP.
- Mitigate DoS attacks by restricting the network usage available for specific kinds of traffic (e.g. ICMP traffic).

### 8.1 The QoS window tab

Let's have a look first, at the overall GUI interface (figure 60).

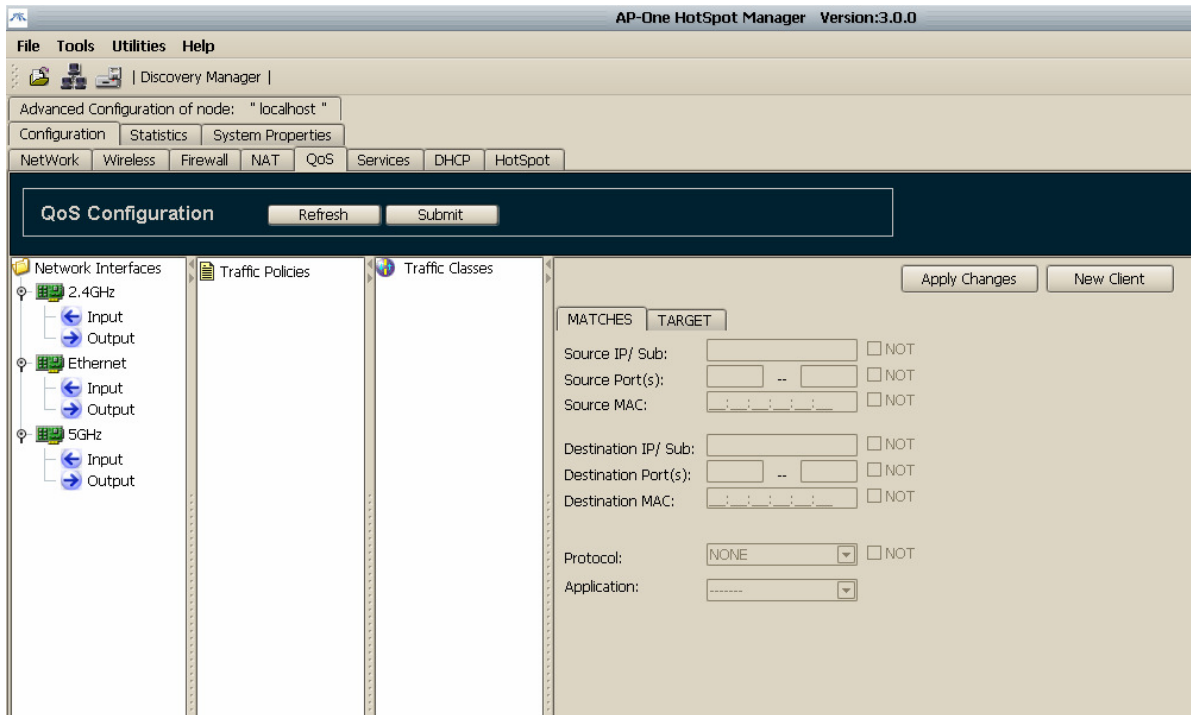


Figure 60. The QoS window

There are three main columns:

### 8.1.1 Traffic Classes

Traffic classes are entities to which we associate specific traffic patterns, and specific network resources. The traffic patterns constitute the *Matches* associated to a Traffic Class, and the network resources reserved, comprises the *Target* of the Traffic Class. These properties can be configured via the rightmost panel of the QoS window.

To add a new Traffic Class, you have to right-click on the “Traffic Classes” label in the respective Panel. You can define as many Traffic Classes as you wish. A Traffic Class can also form a tree-like hierarchy of Subclasses. The tree may have at most two layers of subclasses (Picture 67).



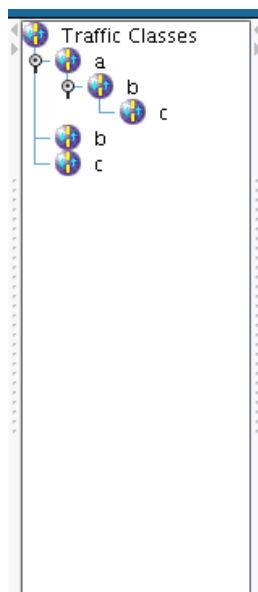


Figure 61. Three layer class hierarchy

## 8.1.2 Traffic Policies

A Traffic policy is an object to which we associate one or more classes and one or more interfaces. The set of classes assigned to a Traffic Policy, defines the policy for the associated interfaces. The way you assign classes to policies is unlimited. Traffic policies can be shared by many interfaces, in which case the interfaces are unified from the QoS standpoint. Shared policies will be discussed in more depth later in this chapter.

## 8.1.3 Network Interfaces

This panel lists all physical interfaces of the system. For each interface, we distinguish two flows: An incoming one, which corresponds to traffic coming to the interface, from the underlying physical layer, and an outgoing one, which corresponds to traffic going out of the interface, to the physical layer.

**Note:** Bridges and virtual interfaces will not be present here. If you want to set a policy to a bridge, set the same traffic policy to every physical interface that makes up the bridge. Virtual interfaces can only be distinguished, in the basis of their ip address.

Bear in mind, that you can't assign **more than one policy per interface flow**; as well as, **the same policy to both flows of the same interface**.

The way that Classes, Policies and Interfaces are interrelated is depicted in figure 62.

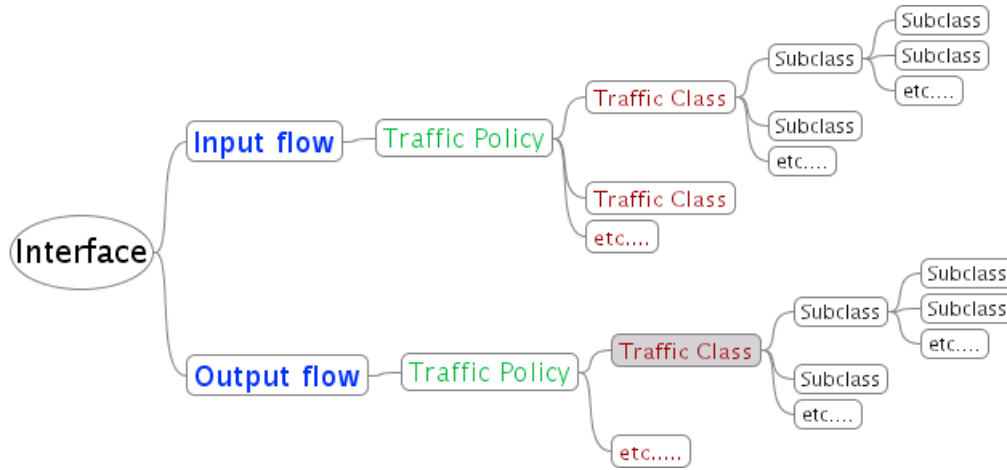


Figure 62. Classes, Policies and Interfaces

Associations are carried out by drag&dropping one item to the other.

## 8.2 Differentiating network traffic

The network traffic can be categorized by almost any combination of the following properties

Inbound/Outbound Interface	eg. Ethernet0 in, 2.4GHz out
Source/Destination IP/subnet	eg. 192.168.2.0/24, 172.16.1.1/32
Source/Destination IP port range	eg. 0-1024, 520
Source/Destination Mac	eg. 01:02:03:04:05:06
Protocol	eg. IP, TCP, UDP, ICMP, ...
Application	eg. P2P traffic, etc
Negations of most of the aforementioned	eg. ! 192.168.1.1/32

These parameters constitute the MATCH part of a class. The GUI panel responsible for these options is depicted at picture 69.

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub:   NOT

Source Port(s):  --   NOT

Source MAC:   NOT

Destination IP/ Sub:   NOT

Destination Port(s):  --   NOT

Destination MAC:   NOT

Protocol:   NOT

Application:

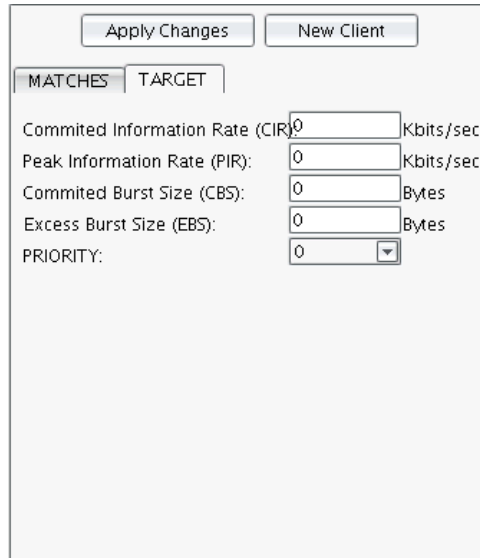
Figure 63. Network Traffic Matches

## 8.3 Guarantees and Limitations

On the other hand, the network resources that can be guaranteed or limited are:

- Committed Information Rate
- Peak Information Rate
- Committed Burst Size
- Excess Burst Size
- Priority

These parameters constitute the TARGET part of a class. The GUI interface responsible for these options are depicted in Picture 70.



The screenshot shows a configuration window with two buttons at the top: "Apply Changes" and "New Client". Below these are two tabs: "MATCHES" and "TARGET". The "MATCHES" tab is selected. The form contains the following fields:

Committed Information Rate (CIR):	<input type="text" value="0"/>	Kbits/sec
Peak Information Rate (PIR):	<input type="text" value="0"/>	Kbits/sec
Committed Burst Size (CBS):	<input type="text" value="0"/>	Bytes
Excess Burst Size (EBS):	<input type="text" value="0"/>	Bytes
PRIORITY:	<input type="text" value="0"/>	<input type="button" value="v"/>

Figure 64. Policy parameters

### 8.3.1 Committed Information Rate (CIR)

This is the rate (expressed in kbits/s) which is guaranteed that will always be available to the respective traffic class. Apparently, the CIR dedicated for a specific class, can not exceed the network bandwidth available. When multiple competing classes exist for the same interface and for the same direction (output/input), the sum of all of them should also not overrun the available bandwidth.

Note that, regardless of the CIR the traffic is always transmitted at the maximum speed supported by the physical interface. Literally, the CIR expresses the average rate in which the traffic is sent, in due time.

### 8.3.2 Peak Information Rate (PIR)

This is the maximum rate (in kbits/s) in which, the traffic of a class, can be sent or received (in average). Even if no other traffic competes for the bandwidth, this barrier can not be exceeded. This value can be as large as the capacity of the link and as small as the CIR.

The bandwidth between CIR and PIR is not guaranteed for a class. The possibility for a class to exploit this range depends on its priority as we will see later.

### 8.3.3 Excess Burst Size (EBS)

Some applications are characterized by short periods of intensive network usage and long periods with no network usage at all. For instance, when we browse the Internet, our web browser requests a web page and then remains idle for a long period of time, until another page is requested.

Such applications are not served well by the CIR/PIR mechanism alone. The EBS mechanism remedies this problem by allowing an application to send a number of bytes continuously, for some time, without being interrupted. As soon as EBC bytes have been sent, the application is forced back to normal behavior (average rate ranging between CIR and PIR).

### 8.3.4 Committed Burst Size (CBS)

The CBS corresponds to the minimum number of bytes that have to be available in order for a transmission to start. By the time that the transmission starts, it is not possible to be interrupted, until there are no other data to send. By default this value is the smallest possible (a single packet size ideally) and scarcely will you have to set a different value.

In order to better understand the concept of rate and burst, consider the analogy: Each class (or subclass as we will see later) is like a bucket with size EBS. The bucket is filled up at a rate which ranges between CIR and PIR. In accordance with this analogy, transmission starts when we throw water out of the bucket. The minimum quantity of water (traffic) that we can be thrown out is CBS. Therefore, when a class is idle for a while, it's possible for an application later on, to send a large burst of data, until the "bucket" is empty. Similarly, for a class that sends traffic at a steady rate, lower than CIR, its "bucket" will always be filled up.

### 8.3.5 Priority

The Priority value dictates which class, among those at the same layer, will get the unused bandwidth. This bandwidth comes from those classes that are not fully utilizing their CIR. This extra bandwidth is delivered first to the class with the highest priority and as soon as the PIR (or EBS) of this class is reached, the distribution continues to the next class in order of priority. Priority value can vary between 0 (higher priority) and 7 (lower priority).

Consider the scenario: We have a standard 11mbps wireless link, and we want to guarantee half of it, to outgoing TCP traffic. Then we further divide it to TCP traffic destined for host x, and that destined to host y. This scenario is depicted in the following table.

Classes in the table denoted as "auto", are classes that are automatically (and transparently) created by the system to handle unclassified traffic. These automatically generated classes, get the rest of the bandwidth (as its CIR), which is not reserved for any of the user-defined ones. System generated classes are always of priority 7.

11 mbps Link Bandwidth			
USER CLASS			AUTO CLASS
CIR 5,5 mbps: Outgoing TCP			CIR 5,5 mbps: Anything but TCP
Priority 0			Priority 7
USER SUBCLASS 1	USER SUBCLASS 2	AUTO SUBCLASS	No subclasses available
1,8 mbps host x	1,8 mbps host y	Rest traffic (1,8 mbps)	
Priority 0	Priority 1	Priority 7	

Back in our scenario:

Let's assume now that 7 mbps traffic (out of the 11 mbps) qualifies for the USER CLASS. This means that we have 7 mbps TCP traffic, which has to be distributed among the three subclasses. Let's also assume that 1/3 of this traffic is destined for host x and another 1/3 for host y. Although, it might be tempting to say that, each of the subclasses will get 1/3 of the 7 mbps, in actual, SUBCLASS 2 and AUTO SUBCLASS will get exactly 1,8 mbps (the CIR) and SUBCLASS 1 will get 3,4 mbps. This is because SUBCLASS 1 has a higher priority. If there is no traffic at all for SUBCLASS 1, then SUBCLASS 2 will get 5,2 out of the 7 mbps available. By now, the role of priority should be clear.

## 8.4 Example: Bandwidth reservation for FTP Servers

Let's have a look now at one example, in order to better comprehend the QoS mechanism. Let's say that we have an AP One powered Hotspot, equipped with a standard 11mbps wireless interface. The **real available** bandwidth on such an interface is approximately 5.5mbps or 5500kbps. On the ethernet side, there are two ftp servers and a bunch of other insignificant hosts. The ftp servers are meant to serve the hotspot clients. Hence, we would like to guarantee some bandwidth for them. The network layout is illustrated in figure 65.

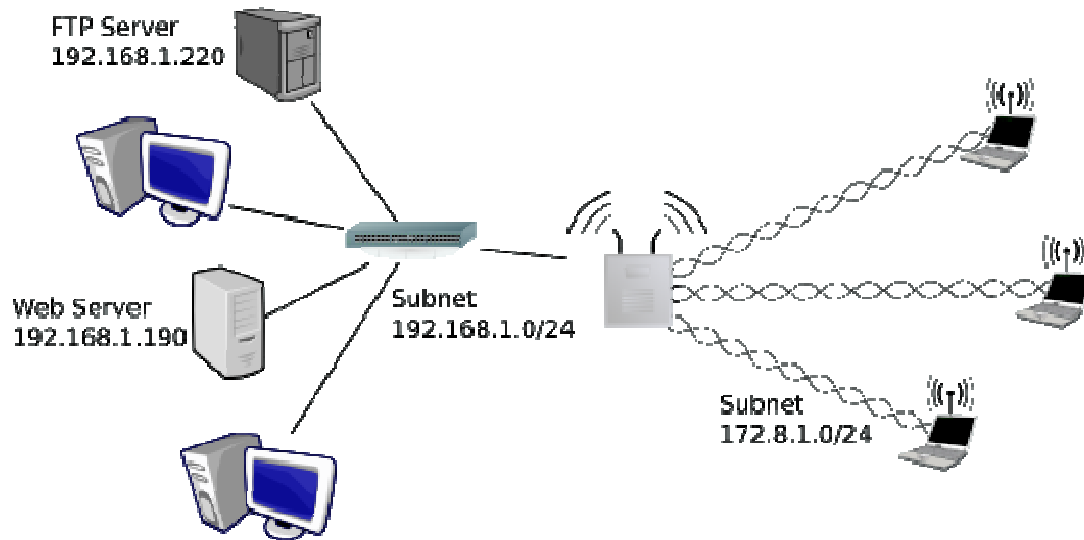


Figure 65. Hotspot with two back-end FTP servers

### 8.4.1 Single Class per Policy

We will start by defining a QoS policy to guarantee 3 mbps for FTP traffic. Since we want to guarantee both uploads and downloads from the ftp servers, we will create two different classes, one for each flow direction. On each of them, we will set a PIR limit (3.5 mbps), in order to prevent the FTP server from monopolizing the bandwidth.

Steps to follow:

1. We click on “Traffic Classes” and right-click on it.
2. We add a new class, named let's say “ftp\_traffic\_out”, to handle outgoing traffic from interface 2.4GHz.
3. We click on “ftp\_traffic\_out” class and configure the MATCHES and TARGET as depicted on picture 72.

The figure consists of two side-by-side screenshots of a network configuration interface. Both screenshots have 'Apply Changes' and 'New Client' buttons at the top.

The left screenshot shows the 'MATCHES' tab selected. It contains the following fields:
 

- Source IP/ Sub: 172.8.1.0/24 (with a 'NOT' checkbox)
- Source Port(s): -- (with a 'NOT' checkbox)
- Source MAC: 00:00:00:00:00:00 (with a 'NOT' checkbox)
- Destination IP/ Sub: 192.168.1.0/24 (with a 'NOT' checkbox)
- Destination Port(s): -- (with a 'NOT' checkbox)
- Destination MAC: 00:00:00:00:00:00 (with a 'NOT' checkbox)
- Protocol: NONE (dropdown menu, with a 'NOT' checkbox)
- Application: FTP (dropdown menu)

The right screenshot shows the 'TARGET' tab selected. It contains the following fields:
 

- Committed Information Rate (CIR): 3000 Kbits/sec
- Peak Information Rate (PIR): 3500 Kbits/sec
- Committed Burst Size (CBS): (empty) Bytes
- Excess Burst Size (EBS): (empty) Bytes
- PRIORITY: 0 (dropdown menu)

Figure 66. 'ftp\_traffic\_out' configuration

- Similarly, we set up an 'ftp\_traffic\_in' class for the incoming flow direction. (Figure 67).

The figure consists of two side-by-side screenshots of a network configuration interface, identical to Figure 66. Both screenshots have 'Apply Changes' and 'New Client' buttons at the top.

The left screenshot shows the 'MATCHES' tab selected. It contains the following fields:
 

- Source IP/ Sub: 172.8.1.0/24 (with a 'NOT' checkbox)
- Source Port(s): -- (with a 'NOT' checkbox)
- Source MAC: 00:00:00:00:00:00 (with a 'NOT' checkbox)
- Destination IP/ Sub: 192.168.1.0/24 (with a 'NOT' checkbox)
- Destination Port(s): -- (with a 'NOT' checkbox)
- Destination MAC: 00:00:00:00:00:00 (with a 'NOT' checkbox)
- Protocol: NONE (dropdown menu, with a 'NOT' checkbox)
- Application: FTP (dropdown menu)

The right screenshot shows the 'TARGET' tab selected. It contains the following fields:
 

- Committed Information Rate (CIR): 3000 Kbits/sec
- Peak Information Rate (PIR): 3500 Kbits/sec
- Committed Burst Size (CBS): (empty) Bytes
- Excess Burst Size (EBS): (empty) Bytes
- PRIORITY: 0 (dropdown menu)

Figure 67. 'ftp\_traffic\_in' configuration

- Now we will create two policies, one for each flow direction, named 'ftp\_in' and 'ftp\_out'. We accomplish this by right-clicking on 'Traffic Policies' label.



- Then we associate each class to each respective policy (Picture 74). This is done by dragging-dropping classes to policies and policies to interface flows.

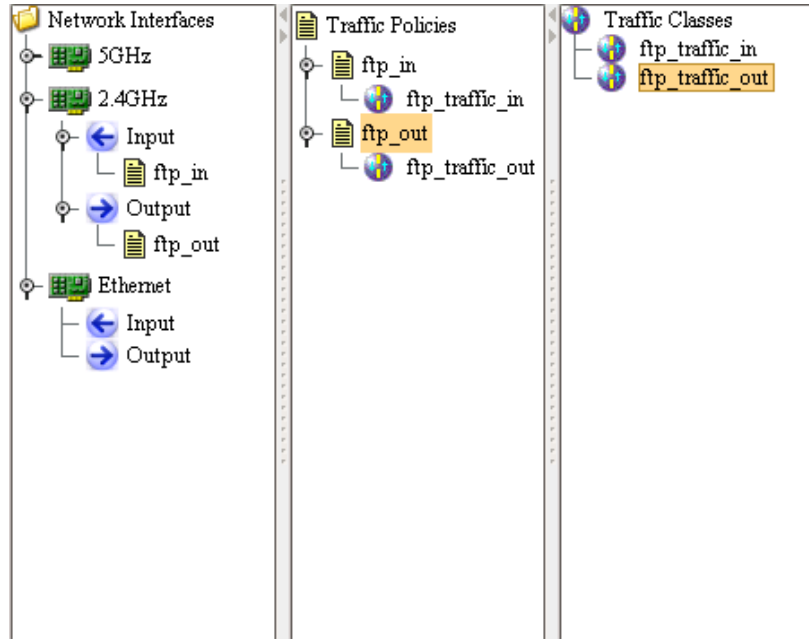


Figure 68. Single class per policy

## 8.4.2 Parallel Classes

Up to now, we guarantee 3mbps for FTP traffic coming from any of the directly connected subnets, and destined to the other one. However, we make no provisions for users (of either subnet), who might set up an FTP server on their own initiative. Such ftp servers can consume part of the 3mbps quota, which is reserved for the two original FTP servers. If we want to prevent this, we will have to be more specific when defining our classes. In particular:

- We rename 'ftp\_traffic\_out' to 'ftp\_traffic\_out\_ftp1' to handle traffic destined for FTP server 192.168.1.220. We change the destination address to 192.168.1.220/32. We leave the ftp application type to FTP.
- Similarly, we rename 'ftp\_traffic\_in' to 'ftp\_traffic\_in\_ftp1' to handle traffic originating for FTP server 192.168.1.220. Therefore, we change the source address to 192.168.1.220/32. The ftp application type of TARGET remains as it is.
- In a similar manner, we create two new classes, named 'ftp\_traffic\_out\_ftp2' and 'ftp\_traffic\_in\_ftp2' to handle traffic

destined to/originated from 192.168.1.190/32 (Picture 75). We also set the TARGET application type to FTP.

4. Since we divided the total CIR/PIR of the initial classes (one for each direction) in two classes, we have also to redefine the CIR/PIR on each subclass to 1500/1750. This way, for each direction the policy guarantees an aggregated CIR of 3000 and an aggregated PIR of 3500.

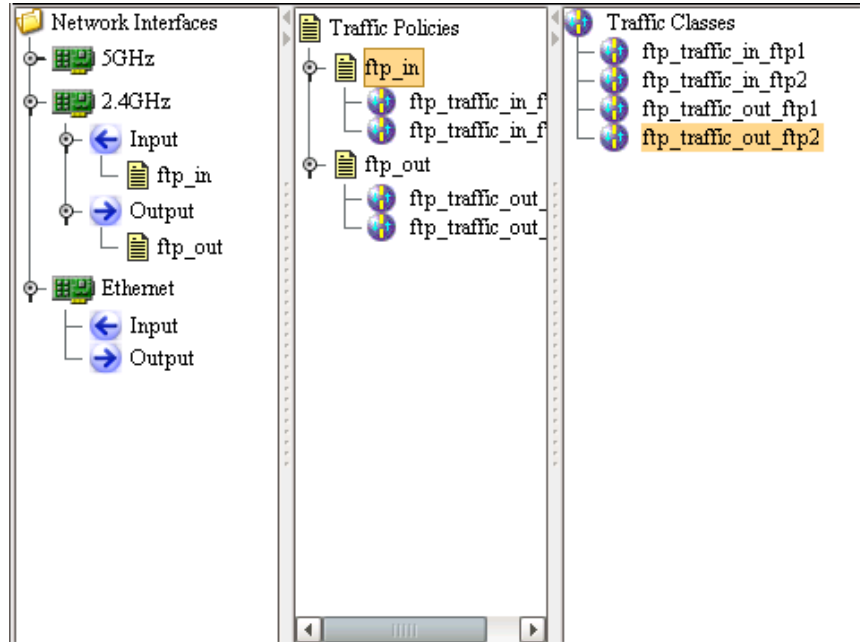


Figure 69. Parallel classes

Classes 'ftp\_traffic\_in\_ftp1' and 'ftp\_traffic\_in\_ftp2' are considered *Parallel Classes*, as far as the incoming interface flow of 2.4GHz is concerned. This is because they don't form a hierarchy and hence, for every arriving packet, both of them are evaluated against it. Classes 'ftp\_traffic\_out\_ftp1' and 'ftp\_traffic\_out\_ftp2' are also parallel classes, as far as the outgoing interface flow of 2.4GHz is concerned.

Parallel classes, although they are very convenient feature, should be used with caution. By all means, you should **avoid setting parallel classes that overlap** each other. In other words, it should be clear which class will be activated for every arriving packet. For instance, the two classes depicted at picture 76 are overlapping, cause is ambiguous which one will handle traffic originating within subnet 172.8.1.0/24 and destined to host 192.168.1.1/32 with destination port number 200.

The figure displays two side-by-side screenshots of a network configuration interface, likely for Quality of Service (QoS) settings. Each screenshot shows a form with two tabs: 'MATCHES' and 'TARGET'. The left screenshot shows a configuration for a class with the following settings: Source IP/Sub: 172.8.1.0/24, Source Port(s): (empty) -- (empty), Source MAC: 00:00:00:00:00:00, Destination IP/Sub: 192.168.1.0/24, Destination Port(s): 200 -- 300, Destination MAC: 00:00:00:00:00:00, Protocol: NONE, and Application: FTP. The right screenshot shows a similar configuration but with Destination IP/Sub: 192.168.1.0/31 and Destination Port(s): 100 -- 200. Both screenshots include 'Apply Changes' and 'New Client' buttons at the top.

Figure 70. Overlapping parallel classes

### 8.4.3 Class Hierarchy

Although the aggregated ftp traffic falls within limits (3000/3500), the maximum allowed bandwidth for each FTP server is restricted to 1750 kbps. An intuitive workaround would be to set the PIR of each class to 3500. However, in that case, if there is a lot of ftp traffic for both FTP servers, then the aggregated ftp traffic might exceed the desired restriction: 3500 (since  $3500+3500=7000$ ). In order to alleviate this problem, we will have to create a class hierarchy.

1. We set the CIR/PIR of every class created up to now to 1499/3500 and we remove the application type of FTP.
2. We create two new classes, named 'ftp\_traffic\_in' and 'ftp\_traffic\_out'. We set the CIR/PIR on each of them to 3000/3500. Source IP/Sub of 'ftp\_traffic\_in' should be set to 192.168.1.0/24 and destination IP/Sub of 'ftp\_traffic\_out' to 192.168.1.0/24. This is to allow for other ftp sessions to take place. Next, on the MATCHES part, we set the port range to 20 – 21 (ftp-data, ftp-control), and the protocol type to FTP.

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 192.168.1.220/32  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 172.8.1.0/24  NOT  
 Destination Port(s): 0 -- 0  NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: -----

*ftp\_traffic\_in\_ftp1*

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 172.8.1.0/24  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 192.168.1.220/32  NOT  
 Destination Port(s): 0 -- 0  NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: -----

*ftp\_traffic\_out\_ftp1*

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 192.168.1.190/32  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 172.8.1.0/24  NOT  
 Destination Port(s): 0 -- 0  NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: -----

*ftp\_traffic\_in\_ftp2*

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 172.8.1.0/24  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 192.168.1.190/32  NOT  
 Destination Port(s): 0 -- 0  NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: -----

*ftp\_traffic\_out\_ftp2*

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 172.8.1.0/24  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 192.168.1.0/24  NOT  
 Destination Port(s):  --   NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: FTP

*ftp\_traffic\_in*

Apply Changes    New Client

MATCHES    TARGET

Source IP/ Sub: 192.168.1.0/24  NOT  
 Source Port(s):  --   NOT  
 Source MAC: 00:00:00:00:00:00  NOT

Destination IP/ Sub: 172.8.1.0/24  NOT  
 Destination Port(s):  --   NOT  
 Destination MAC: 00:00:00:00:00:00  NOT

Protocol: NONE  NOT  
 Application: FTP

*ftp\_traffic\_out*

- We drag&drop the previous classes to these new ones to create a class hierarchy as depicted at figure 71. We also alter the structure of our policies, so that only the newly created classes are assigned to them.

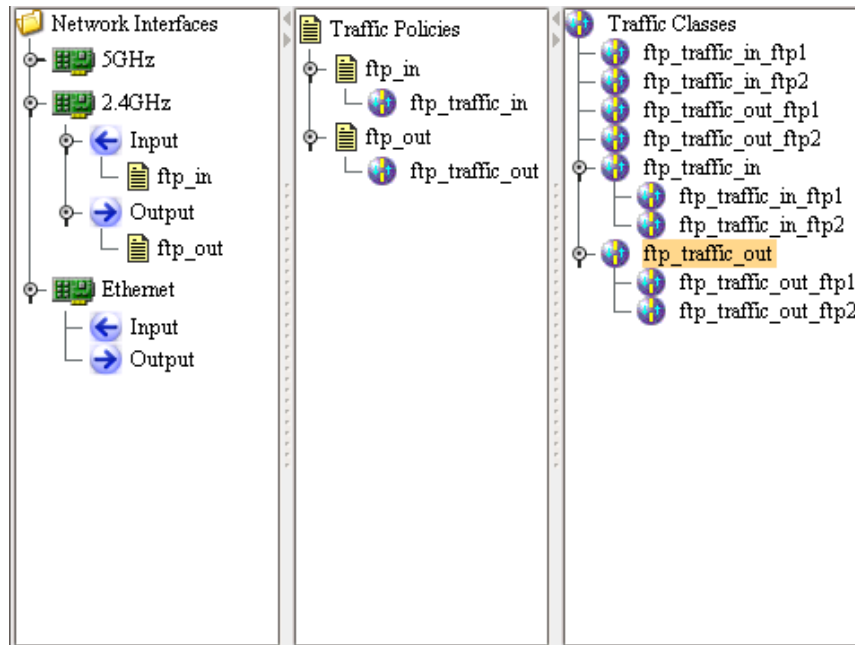


Figure 71. Class hierarchy

This way we limit the PIR at parent classes (3000/3500) and then we further distribute the bandwidth among the child classes (1499/3500 each). So, we enforce an upper limit on the amount of bandwidth used for FTP traffic, and at the same time, we enable both FTP Server to use the full potential of the reserved bandwidth.

**Note:** We couldn't have set a CIR of 1500 on each subclass, because when we subdivide a class to subclasses, there should always be some bandwidth available to accommodate for the rest of the traffic (traffic not covered by any of the subclasses).

## 8.5 Example: Elimination of P2P Traffic

Currently, AP One does not support filtering of ip traffic based on its Layer 7 properties. For example, you can't set up a firewall rule to block incoming/outgoing P2P traffic. Nonetheless, you can virtual eliminate it, by restricting the bandwidth available to it.

In this example we will set up two Traffic Policies, one for each direction, and two Traffic Classes, that will reduce the bandwidth available to P2P traffic to as low as Kbits/sec. P2P users will soon get frustrated and drop

their P2P applications altogether. The following pictures demonstrate the QoS configuration needed.

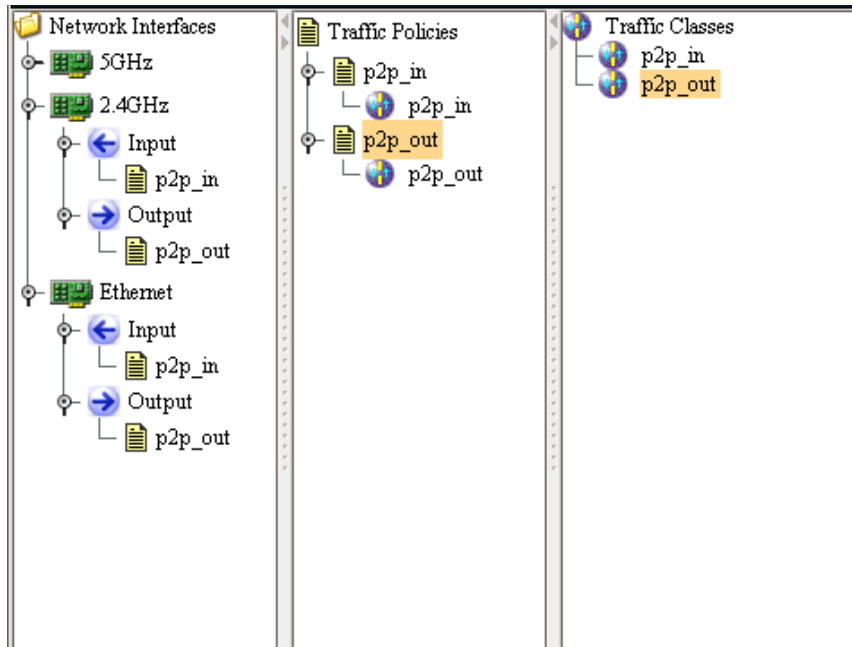


Figure 72. Class hierarchy for restricting P2P traffic on both interfaces

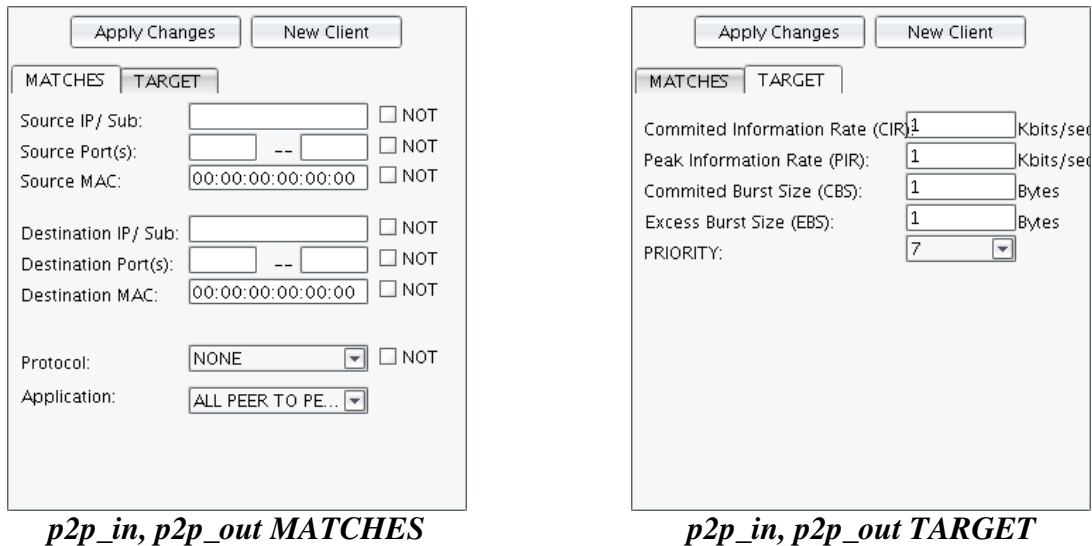


Figure 73. Overlapping parallel classes

### 8.5.1 Shared Policies

In our example, traffic policies p2p\_in and p2p\_out are shared between interfaces Ethernet0 and 2.4GHz. That makes them (both interfaces) to be regarded as a single interface, from the standpoint of QoS. In practice, this means that 1 Kbits/sec can be occupied by P2P traffic coming from either Ethernet0 or 2.4GHz, and another 1 Kbits/sec for P2P traffic leaving from either Ethernet0 or 2.4GHz (not 1 Kbits/sec each).

## 8.6 QoS Statistics

By right-clicking on the traffic policy below the associated interface flow, you can get statistics regarding packets handled by this policy.

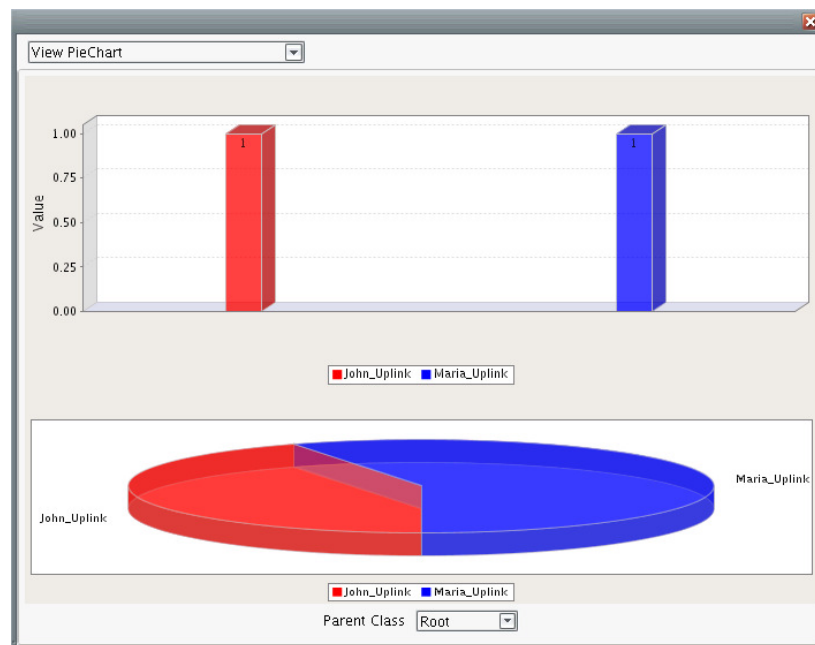
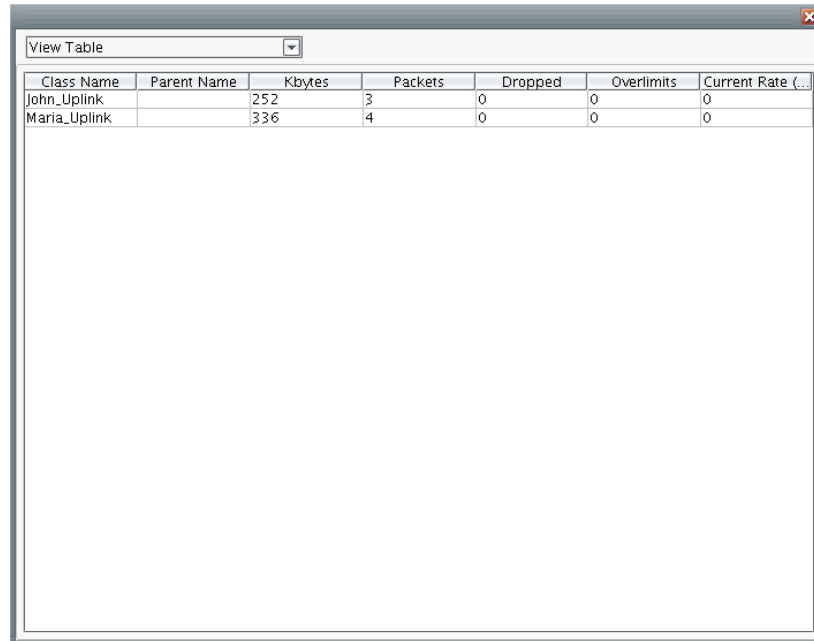


Figure 74. Current rate and packet analogy

The bar chart on the top illustrates the current average rate for each class. The pie chart corresponds to the number of packets services by the class up to now. By choosing the table view you get some more detailed statistics, including dropped packets due to rate/burst limitations.



The screenshot shows a window titled 'View Table' with a table containing network statistics. The table has seven columns: Class Name, Parent Name, Kbytes, Packets, Dropped, Overlimits, and Current Rate (...). There are two rows of data: 'John\_Uplink' and 'Maria\_Uplink'.

Class Name	Parent Name	Kbytes	Packets	Dropped	Overlimits	Current Rate (...)
John_Uplink		252	3	0	0	0
Maria_Uplink		336	4	0	0	0

Figure 75. More detailed statistics

## 8.7 Design Guidelines and Limitations

### 8.7.1 Destination/Source MAC match type

To use the destination MAC match type, you have to create a bridge interface and assign to it the desired physical interface (a single interface is ok). Then, you can use the destination MAC match type of the interface assigned to the bridge.

Also bear in mind that, on a regular ip network, all receiving packets on the gateway, have as destination mac the gateway's mac address. Similarly, all packets forwarded by the gateway, have as source mac the gateway's mac address. Hence, it's pointless to use these fields on an AP One powered AP, which acts as a gateway.



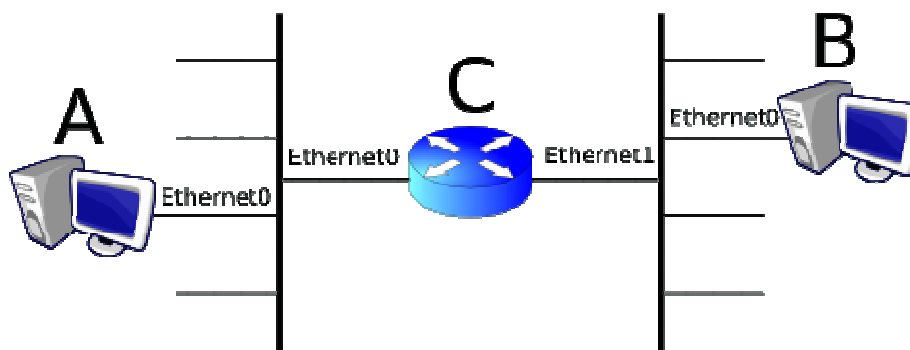


Figure 76. A Packet sent by A for B has C.Ethernet0's mac address as destination mac, and when it is resent by C, it has a source mac of C.Ethernet1.

When A sends a packet for B, the packet initially has destination mac: C.Ethernet0. Thereafter, when gateway C forwards it to its destination (host B) it has source mac: C.Ethernet1.

## 8.7.2 Application match type

You may set the application match type only on leaf subclasses, on a class hierarchy. The reason behind this is that application type is very specific and should only exist on subclasses that reside on the last level (leaf) of a class hierarchy.

Moreover, when application type is used on a leaf class, it's not possible to set the protocol match type on any of its parent classes. This is because, when you set an application type match, you implicitly define the protocol type which corresponds to the application type.

## 8.7.3 Child to Parent class relation

In a class hierarchy, a child's MATCH and TARGET part should be subset of that of each parent class. Therefore, you can't have a parent class to match a destination port range of 1-1024, when one of its child classes matches destination port range 500-2000. Port range 1025-2000 is not a subset of the parent class.

## 8.7.4 PIR on parallel classes

Currently, the QoS subsystem requires that all parallel classes (or subclasses) will either have a PIR defined or not. Therefore, it's not possible to set the PIR on a subclass and not set it on one of its sibling classes. All of them should either have or not have a PIR defined.

### 8.7.5 Efficiency considerations

Whenever possible, prefer the port or protocol match type instead of the application one. Application match type is slower and more CPU intensive.

## 8.8 Frequently Asked Questions

### 8.8.1 Submit, Apply Changes: I'm confused!

'Apply Changes' button is to save changes made to the rightmost panel of the QoS interface. This is the panel responsible for setting MATCHES and TARGET properties of a class. On the other hand 'Submit' is used to save the overall QoS configuration. Finally, don't forget to save configuration on the device via the 'Save Configuration' option on the 'View Topology' window.

## 9. System Services

AP-ONE can be configured to run the following services:

- **SNMP** (Simple Network Management Protocol) Service
- **HTTP** (Hyper-Text Transfer Protocol) Service
- **SSH** (Secure Shell Protocol) Service
- **NTP** (Network Time Protocol) Service

To configure **System Services** settings, select the **Services** tab, located under the **Advanced Configuration of Node, Configuration** tabs.

*See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.*

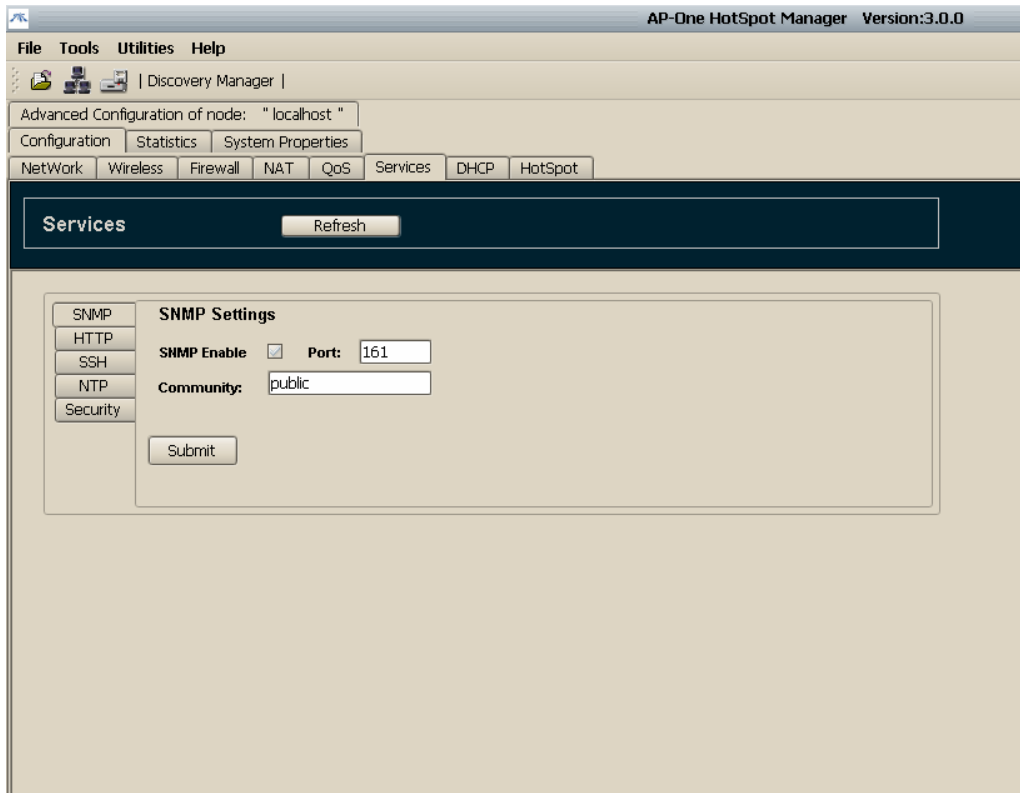


Figure 77. Services Tab

## 9.1 Configuring SNMP Settings

**SNMP** (Simple Network Management Protocol) is the most widely used protocol for managing TCP/IP Internets. A network management station (NMS) uses SNMP query (poll) SNMP processes (agents) on network devices such as routers and end stations. These agents maintain a list of variables and their values that describe the state of the network device. The variables can describe routing table entries, interface addresses, and byte counts transmitted on various interfaces. The collection of variables is described by a Management Information Base (MIB).

When SNMP is enabled, AP-ONE will respond to SNMP requests (SNMP get, getnext, getbulk, walk).

A community name can be configured, as a read-only community. SNMP set requests are not supported.

To configure **SNMP**, select the **SNMP** tab under the **Services** tab. Configure the SNMP tab fields as follows:

### SNMP Enable

Select the **SNMP Enable** checkbox to enable SNMP

### Port

The **Port** field contains the router port that the SNMP module listens to for SNMP requests (default 161). Typically you will not have to change this value.

### Community

The **Community** field contains the read-only community name of SNMP service (default: public). SNMP service will respond to requests if and only if the community name is set appropriately.

### Submit

Click **Submit** to apply the configuration.

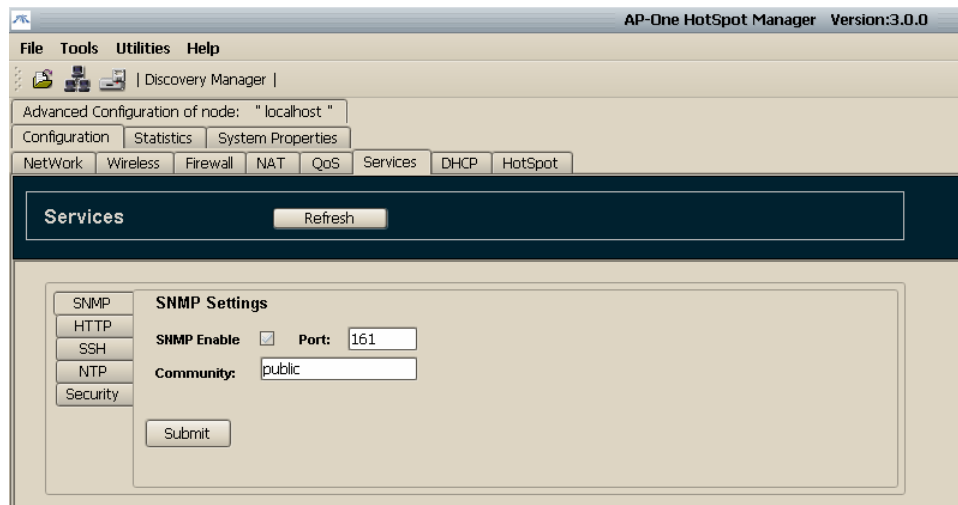


Figure 78. SNMP Service Configuration

## 9.2 Configuring HTTP Settings

Web servers are the computers that run Web sites, accepting [HTTP](#) (Hyper-Text Transfer Protocol) connections from [web browsers](#) and delivering Web pages and other files to them, as well as processing form submissions. When HTTP is enabled, AP-ONE will respond to HTTP/HTTPS requests.

To configure **HTTP**, select the **HTTP** tab under the **Services** tab. Configure the HTTP tab fields as follows:

### HTTP Enable

Select the **HTTP Enable** checkbox to enable HTTP

### Port

The **Port** field contains the router port that the HTTP module listens to for HTTP requests (default 80). Typically you will not have to change this value.

### Upload SSL Certificate

Click **Upload SSL Certificate** to open a **Select** dialog box and upload your own SSL certificate for Secure HTTP requests (HTTPS). A default certificate is included in every newly installed AP-ONE.

### Upload Key File

Click **Upload Key File** to open a **Select** dialog box and upload your own keys file for Secure HTTP requests (HTTPS). A default file is included in every newly installed AP-ONE.

## Submit

Click **Submit** to apply the configuration.

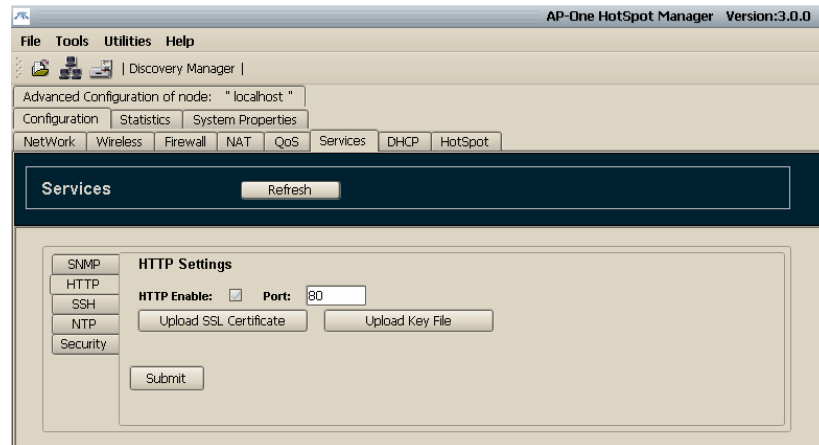


Figure 79. HTTP Service Configuration

## 9.3 Configuring SSH Settings

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force SSH to disconnect. He or she cannot play back the traffic or hijack the connection when [encryption](#) is enabled.

When using SSH's slogin (instead of rlogin) the entire login session, including transmission of [password](#), is encrypted; therefore it is almost impossible for an outsider to collect passwords. When SSH is enabled, AP-ONE will respond to SSH connection requests.

To configure **SSH**, select the **SSH** tab the **Services** tab. Configure the SSH tab fields as follows:

### SSH Enable

Select the **SSH Enable** checkbox to enable SSH

## Port

The **Port** field contains the router port that the SSH module listens to for SSH connection requests (default 22). Typically you will not have to change this value.

## Submit

Click **Submit** to apply the configuration.

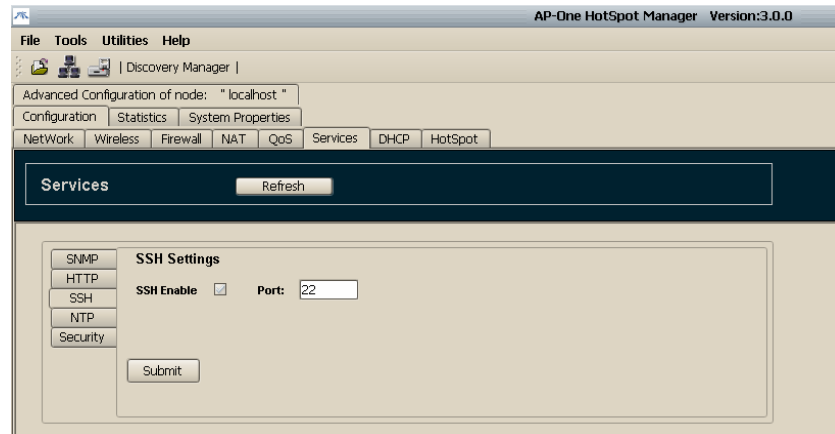


Figure 80. SSH Service Configuration

## 9.4 Configuring NTP Settings

The **Network Time Protocol (NTP)** is a time synchronization system for computer clocks through the Internet. The main characteristics of NTP are the following.

- Fully automatic, continuous synchronization
- Suitable for synchronizing one computer, or a whole computer network
- Fault tolerant and dynamically auto configuring
- Based on UTC time, independent of time zones and day-light saving time.
- Synchronization accuracy can reach 1 millisecond.

When NTP is enabled, AP-ONE will periodically send a request to a configured NTP server (based Interval time) and adjust AP-ONE's local system time.

To configure **NTP**, select the **NTP** tab under the **Services** tab. Configure the NTP tab fields as follows:

## NTP Enable

Select the **NTP Enable** checkbox to enable NTP

## Port

The **Port** field contains the router port that the NTP module listens to for NTP server responses (default 123). Typically you will not have to change this value.

## Domain

The **Domain** field contains the domain name or IP address of the NTP server.

## Interval

The **Interval** field contains the interval, in minutes, between two consecutive requests (default 60 minutes).

## Submit

Click **Submit** to apply the configuration.

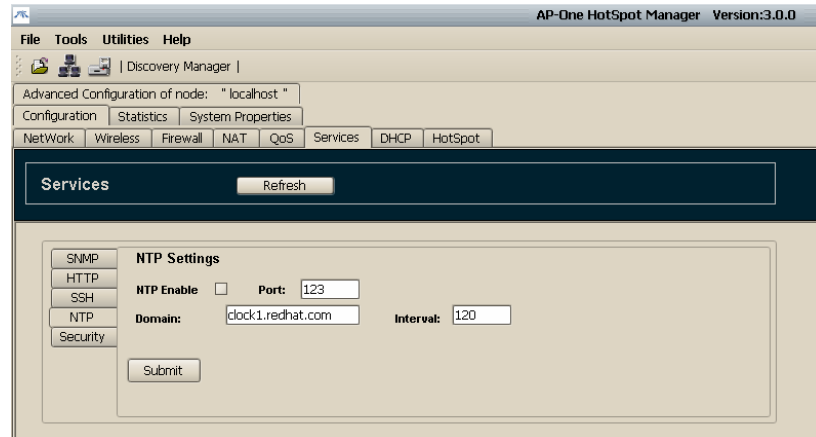


Figure 81. NTP Service Configuration

## 9.5 Setting the Administrator Password

To configure the administrator password, select the **Security** tab under the **Services** tab. Configure the Security tab fields as follows:

### Old Password

Type the current password in the **Old Password** text box. The default password is: *admin*



## New Password

Type the new password in the **New Password** text box. The new password must be at least 8 characters and no more than 63 characters

## Re-type

Re-type the new password in the **Retype** text box

## Submit

Click **Submit** to apply the configuration.

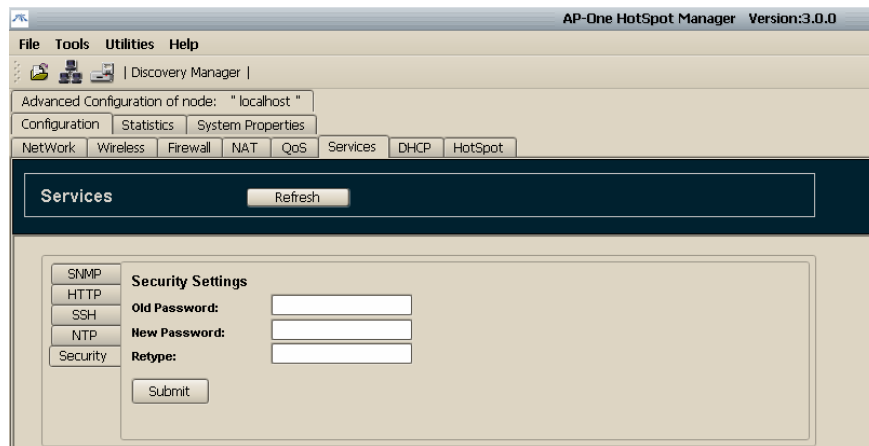


Figure 82. Change Administrator's Password



# 10. Monitoring and Statistics

The advanced statistics engine of AP-ONE, in combination with the graphing facilities of AP-ONE HotSpot Manager, lets the administrator delve into the results real-time, identifying high bandwidth nodes and possible bottlenecks.

Some **Monitoring and Statistics** features are available from the **Node Shortcut Menu**. Others are located under the **Advanced Configuration of Node, Configuration** tabs.

See Page 27 for a diagram showing Advanced Configuration tabs and sub-tabs.

## 10.1 Using the Status Info Dialog Box

The **Status Info** dialog box provides all the information displayed in the bottom pane of the **Network Topology** tab, with the addition of an extra editable field which is used to set the **Host Name** of the node. The displayed information is useful in cases where the administration unit is “hidden” behind NAT and connectionless communication (such as AP-ONE's proprietary Polling Protocol and SNMP) can not be initiated.

To view the Status Info dialog box, click **System Status Window** in the **Node Shortcut Menu**.

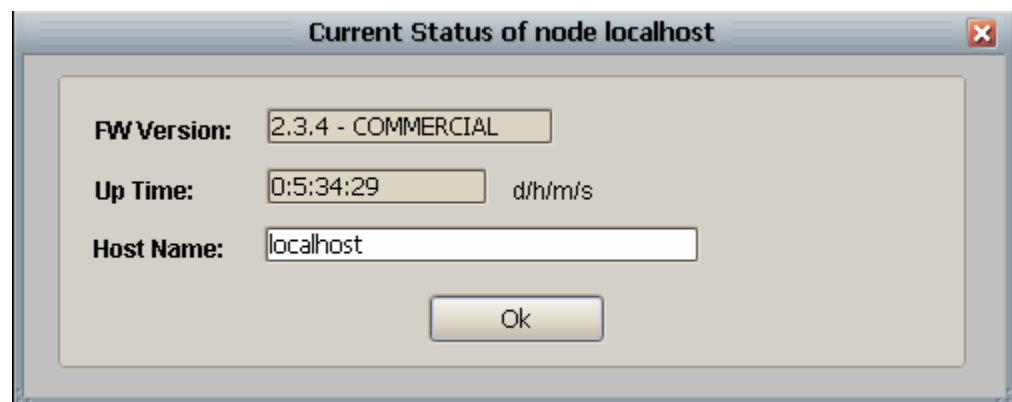


Figure 83. Current Status of Node Dialog Box

## 10.2 Using the Current Throughput Graph

The **Current Throughput** graph provides a real-time graphical display of the currently transmitting and receiving traffic of each network interface. By monitoring performance and analyzing performance data, you can

begin to see patterns in the data that will help you locate bottlenecks. After you have located a bottleneck, you can make changes to the component to improve performance. Bottlenecks can occur anywhere in your server environment at any time, so it is important to capture baseline performance information about your system and monitor performance regularly. AP-ONE NMS provides the option of real time traffic monitoring.

To view the **Current Throughput Graph**, click **Current Throughput** in the **Node Shortcut Menu**.

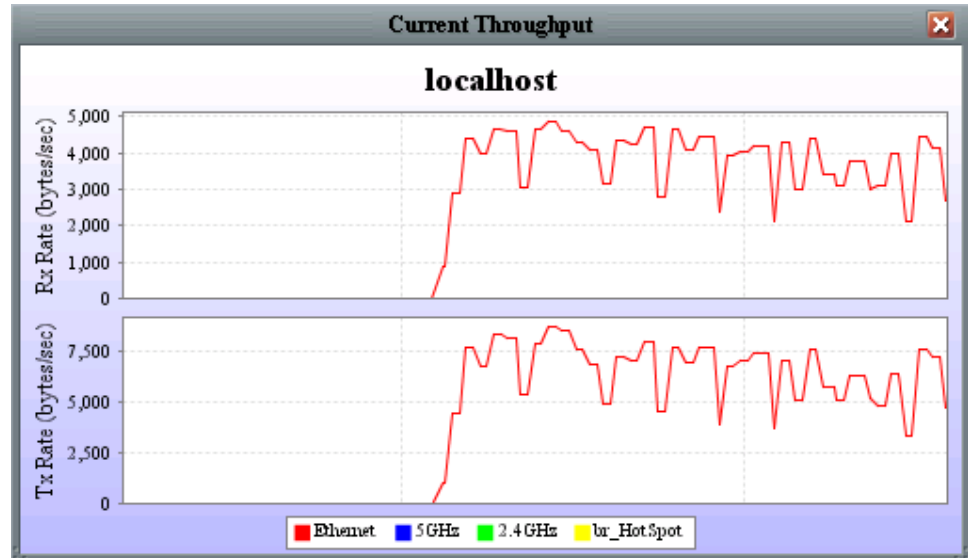


Figure 84. Current Throughput Window

## 10.3 Viewing Packet Statistics

The **Packet Stats** tab contains information concerning the total packet statistics per interface.

To view packet statistics, select the **Packet Stats** tab under the **Advanced Configuration, Statistics, Network** tabs.

### Interface

Select the interface for which you want to view statistics in the drop down list.

### Refresh

Click **Refresh** to update the graph.

## Reset

Click **Reset** to...

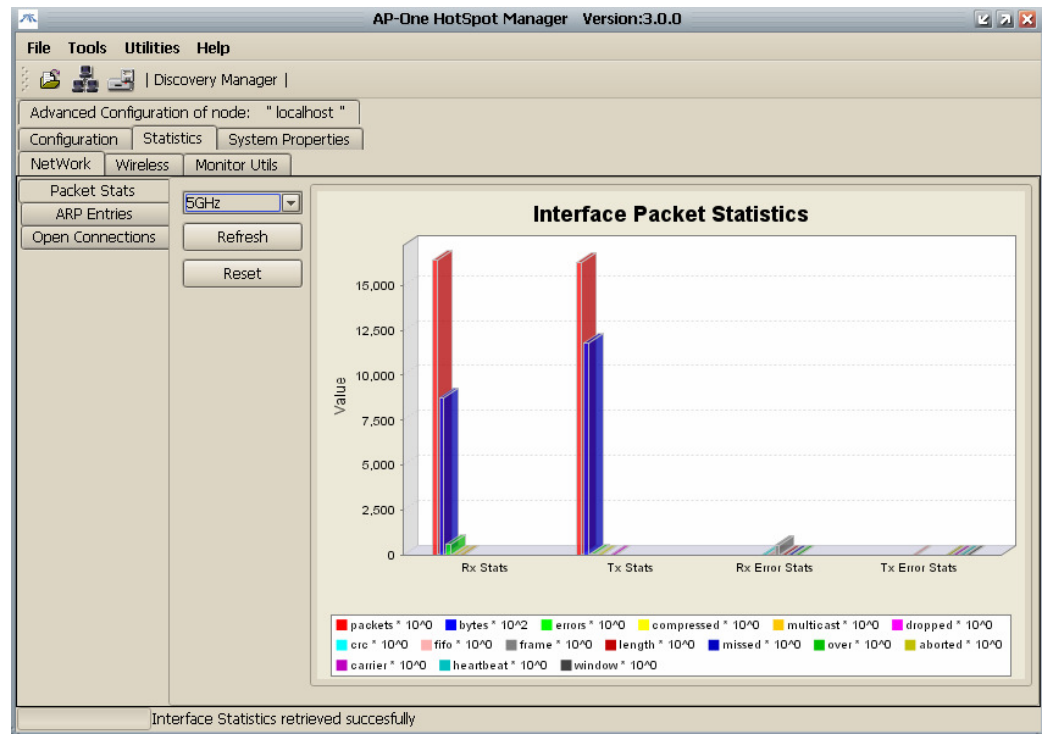


Figure 85. Interface Packet Statistics

## 10.4 Viewing the ARP Table

The **ARP Entries** tab contains the ARP (Address Resolution Protocol) table of the currently selected AP-ONE node.

On a single physical network, individual hosts are known on the network by their physical hardware address. Higher-level protocols address destination hosts in the form of a symbolic address (IP address in this case). When such a protocol wants to send a datagram to destination IP address w.x.y.z, the device driver does not understand this address.

Therefore, a module (ARP) is provided that will translate the IP address to the physical address of the destination host. It uses a lookup table (sometimes referred to as the *ARP cache*) to perform this translation.

When the address is not found in the ARP cache, a broadcast is sent out on the network, with a special format called the *ARP request*. If one of the machines on the network recognizes its own IP address in the request, it will send an *ARP reply* back to the requesting host. The reply will contain the physical hardware address of the host and source route information (if

the packet has crossed bridges on its path). Both this address and the source route information are stored in the ARP cache of the requesting host. All subsequent datagrams to this destination IP address can now be translated to a physical address, which is used by the device driver to send out the datagram on the network.

To view the ARP table, select the **ARP Entries** tab under the **Network** tab.

Advanced Configuration of node: "localhost "

Configuration | Statistics | System Properties

NetWork | Wireless | Monitor Utils

Packet Stats | Refresh

IP address	MAC address	Interface
192.168.1.100	00:02:3F:BB:DE:08	Ethernet

ARP Entries

Open Connections

Figure 86. ARP Entries Table

## 10.5 Viewing the Open Connections List

The **Open Connections** tab displays all your computer's inbound and outbound connections and lists all open ports, helping the administrator to detect host's activity. Open connections can be sorted in ascending or descending order per column by clicking on the corresponding table header.

To the Open Connections list, select the **Open Connections** tab under the **Advanced Configuration, Statistics, Network** tabs.

Advanced Configuration of node: "localhost "

Configuration | Statistics | System Properties

NetWork | Wireless | Monitor Utils

Packet Stats | Refresh

Protocol	Source IP	Dest IP	Source Port	Dest Port	State	Flags	Timeout	Open Time
UDP	192.168.1...	192.168.1.3	3517	3517	NONE	ASSURED	179	10051
TCP	192.168.1...	192.168.1.3	1028	3517	ESTABL...	ASSURED	432000	131

Open Connections

Figure 87. Open Connections Tab

### Refresh

Click **Refresh** to update the open connections information.

## 10.6 Using Monitor Utilities

The **Monitor Utilities** tab provides a user interface for implementing two useful network utilities: **Ping (ICMP)** and **Traceroute**. To access these utilities, select the **Monitor Utilities** tab under the **Advanced Configuration, Statistics** tabs. The **Monitor Util** tab has two sub-tabs: the **ICMP Util** tab and **Trace Route** tab.

### 10.6.1 Pinging (ICMP Utility)

The **ICMP Utility** tab provides a convenient tool for initiating Ping commands. Ping sends ICMP requests to the address you specify and lists the responses received and their round trip time. When the utility is terminated it summarizes the results in a graphic display, giving the average round trip time and the percent packet loss. This utility can be used to determine whether there is a problem with the network connection between two hosts.

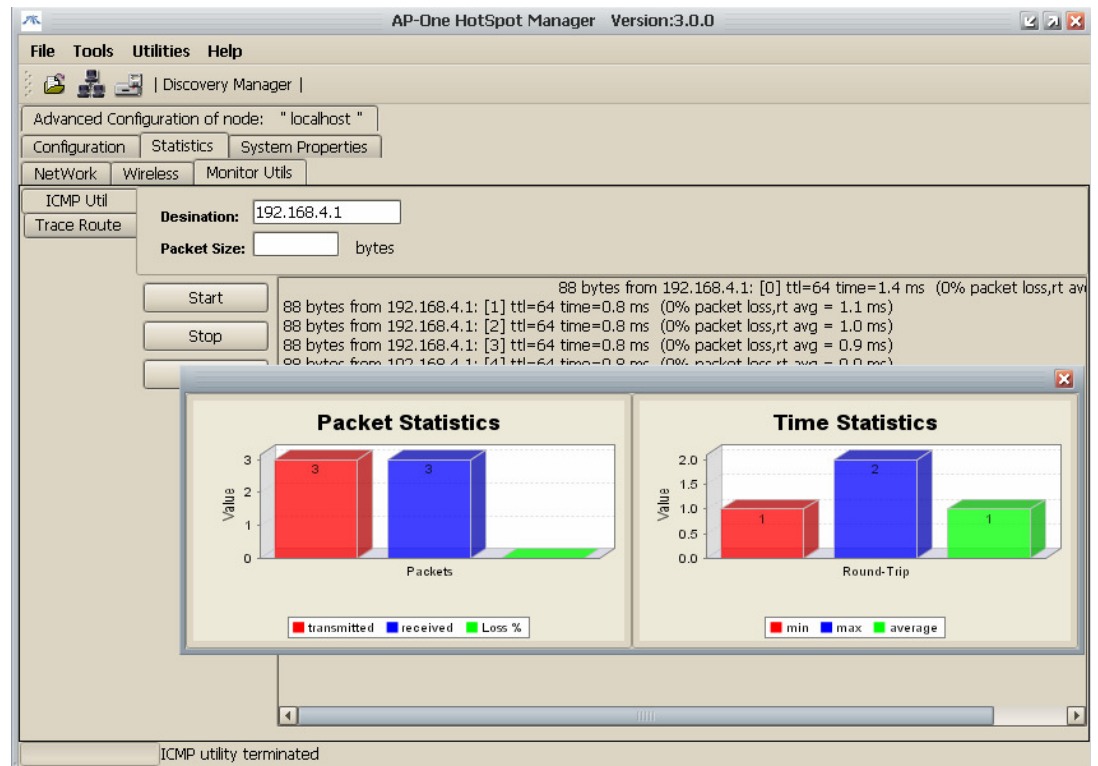


Figure 88. ICMP Utility Tab

To configure and use the ICMP Utility, select the **ICMP Util** tab, configure the **Destination** and **Packet Size** fields, then use **Start, Stop and Clear** buttons as follows:

## Destination

Type the IP address of the node you wish to ping in the **Destination** text box.

## Packet Size

Type the number of bytes to be sent in each packet in the **Packet Size** box.

## Start

Click **Start** to initiate the Ping command. The software will repeatedly ping the destination address. The window will display the number of bytes, source address, time to live (ttl), the round trip time, % packet loss, and average time.

## Stop

Click the **Stop** button to terminate the pinging process. The pinging session will end and a window will appear displaying the **Packet Statistics** (Transmitted Packets, Received Packets and Loss %) and **Time Statistics** (Min, Max and Average) in bar graph format.

## Clear

Click **Clear** to clear the data from the window. Data can be cleared while a pinging session is underway.

## 10.6.2 Using Traceroute

The **Traceroute** tab provides a convenient tool for initiating Trace Route commands.

Traceroute is a utility that records the route (the specific gateway computers at each hop) through the Internet between your AP-ONE node and a specified destination. It also calculates and displays the amount of time each hop took. Traceroute is a handy tool for understanding where problems are in the Internet network.

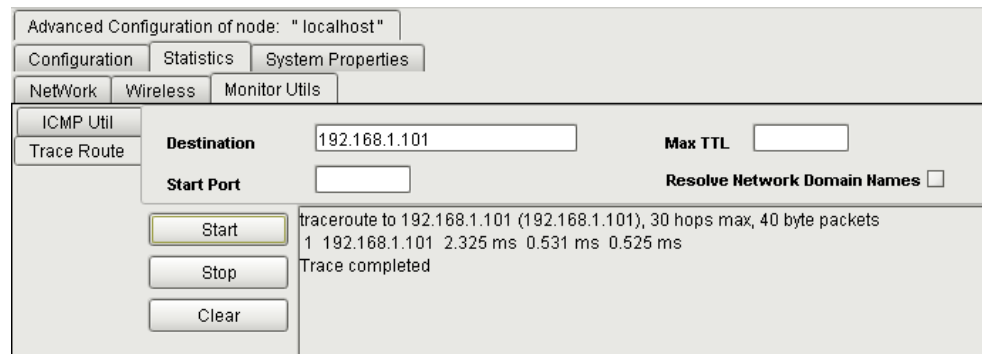


Figure 89. Traceroute Tab



To configure and use the ICMP Utility, select the **ICMP Util** tab, configure the required fields, and then use the buttons as follows:

### Destination

Type the IP address of the node to which you wish to Traceroute in the **Destination** text box.

### Start Port

Type the port number in **Start Port** box.

### Max TTL

Type the maximum time to live value in the **Max TTL** box.

### Resolve Network Domain Names

Select **Resolve Network Names** to cause the utility to include the domain names of each IP address listed.

### Start

Click **Start** to initiate the TraceRoute command. The software will trace the route to the destination address. The window will display the number of hops max, size of the packets and elapsed time.

### Stop

Click the **Stop** button to terminate the TraceRoute process. The Traceroute session will end and a dialog box will appear displaying the **Traceroute utility terminated**.

### Clear

Click **Clear** to clear the data from the window.

## 10.7 Viewing System Properties

The **System Properties** tab provides information about the currently selected nodes CPU and Memory. To access the **System Properties**, select the **System Properties** tab under the **Advanced Configuration** tab,

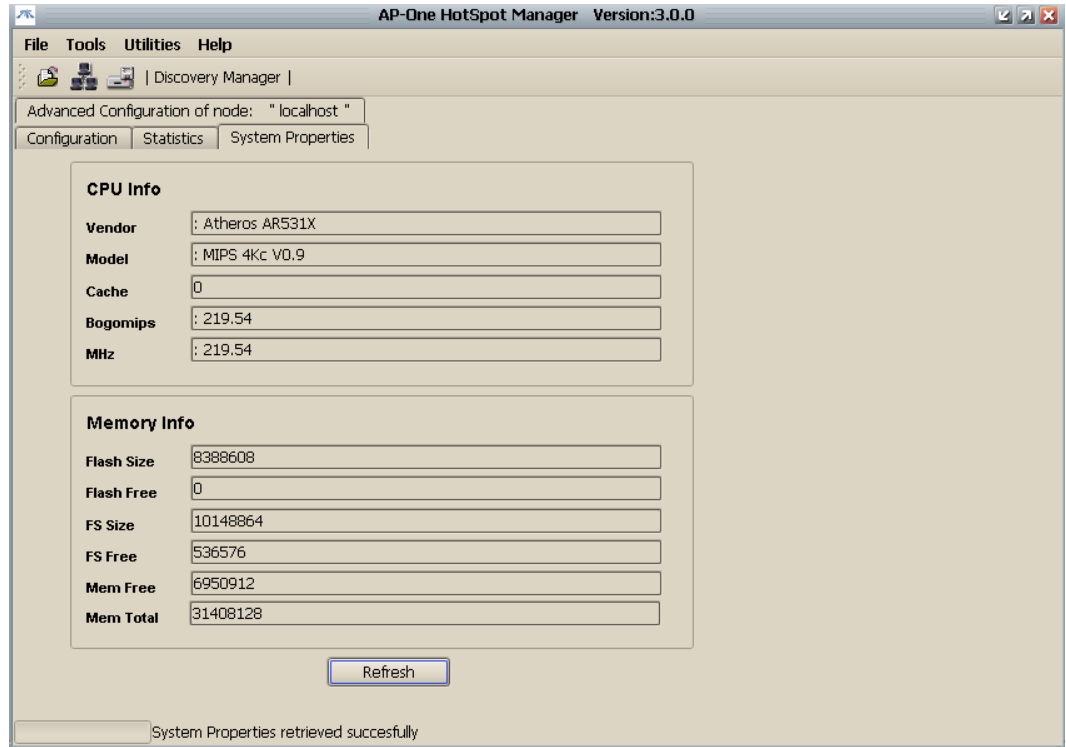


Figure 90. System Properties Dialog

To refresh the data in the **System Properties** fields, click the **Refresh** button.

# 11. MRTG Support

**Multi Router Traffic Grapher**, or **MRTG**, is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing GIF images which provide a live visual representation of this traffic.

MRTG client support of AP-ONE Hotspot Manager uses the package provided by JRobin (<http://www.jrobin.org/utilities/MRTGdemo.html>).

To use the **MRTG**, select **MRTG** under the **Utilities** menu.

## 11.1 Using MRTG

To implement MRTG, extract the required files in a network server with java support and initialize it by executing the following command: “java – jar MRTG-server-1.4.0.jar”.

Using MRTG

- After the successful MRTG server initialization, in the **Utilities** menu select **MRTG**. The built in MRTG client will be invoked and a prompt appears requesting the MRTG server IP address.
- Type the MRTG server IP address. Upon successful connection nodes can be inserted in the monitoring list.
- On each node insertion the user will be presented with a list of all available interfaces. The user may select one or more interfaces to monitor.

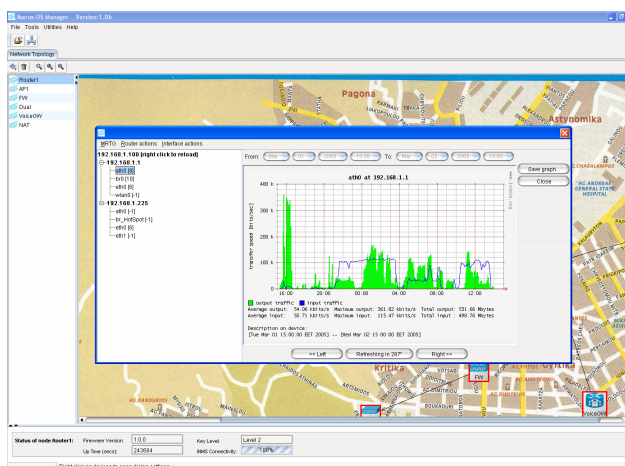


Figure 91. MRTG Display Statistics

**NOTE:** The JRobin MRTG server uses SNMP polls to retrieve information which means that the SNMP agent has to enable in the monitored node.

## 12. Appendix 1: Zero Configuration

---

*Zero Configuration of Hotspot* is an advance feature of AP-ONE, which greatly simplifies and accelerates the deployment of a wireless network over a Hotspot. Such networks are usually deployed in places like conferences and exhibitions, in which we have a single network connection that we want to share among a number of wirelessly connected clients. *Zero Configuration*, as its name implies, make this possible with **minimal administration cost** and in a **very timely manner**.

*Zero Configuration* of HotSpot is also **highly redundant**; as it makes no assumptions about the environment in which it is deployed. Therefore, *Zero Configuration* can effectively deal with situations where the physical environment undergoes spontaneous changes, or wireless nodes appear and leave in an ad-hoc manner. Provisions have been taken to guarantee that the overall configuration remains at all times the optimal (in terms of throughput), no matter how unreliable or dynamic is the underlying physical layer.

In addition to these benefits, *Zero Configuration* features **an advance reporting mechanism**, which renders the state of whole network and that of each individual AP-ONE, readily accessible to the administrator.

In order to demonstrate these benefits, consider the following scenario: Let's assume that we have four AP-ONE in our disposal, and we want to provide full coverage and Internet access for an exhibition area, depicted at figure 92. As each AP-ONE node has two wireless interfaces, one of them is devoted to the wireless clients to connect to, and the other one (backhaul) for interconnection with other AP-ONE (symbolized by  $\cdot$ ). The latter wireless interface can be said that acts as the backbone, since it forwards traffic originated by clients towards to the gateway (node A), and the other way around. Finally, the gateway node has an ethernet connection to the Internet, through which all the clients get Internet access.

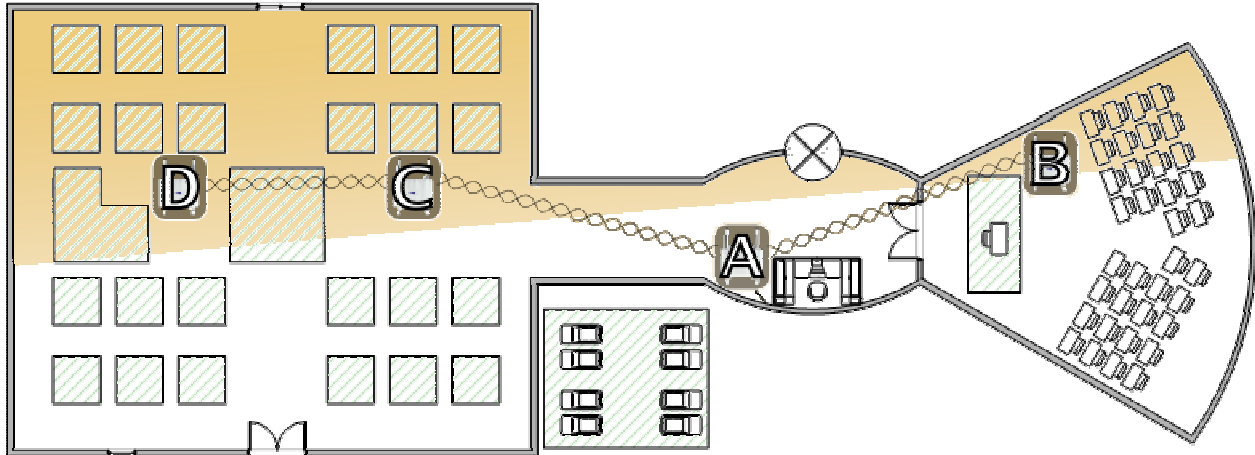


Figure 92. Example deployment of Zero Configuration in an exhibition

Traditionally, you would have to configure each node separately. Configuration entails subnetting, assignment of IP addresses, interface configuration, and configuration of SNAT on the gateway. In addition to the burden of configuration, this approach wouldn't have been able to handle system failures or inconsistencies on the physical layer (eg. movement of physical objects).

Last but not least, the manual approach has the significant limitation that, internal nodes cannot be easily configured remotely, due to the SNAT at the gateway. This also rules out the possibility of getting information about the state of each node.

*HotSpot Zero Configuration's* ingenuity lies on the fact that this whole aforementioned process is simplified to the extent of just plugging the gateway node to the Internet and distributing the rest of the nodes. All the nodes will automatically form associations between them, and configure themselves accordingly. No user intervention is required. The end result will be the sharing of the Internet connection in the most efficient manner, and the on-the-fly adaptation to unanticipated events (system failures etc). In addition to these benefits, configuration is also possible through the Internet for all nodes.

To summarize, *ZC (Zero Configuration)* is about automatic configuration of a set of AP-ONE as HotSpots, in order to share a single outgoing connection and provide access to wireless clients throughout an area.

This task is carried out

1. Instantly
2. Easily
3. With optimal performance in mind
4. With redundancy
5. And transparency

## 12.1 Operation

All AP-ONE nodes in a ZC network have exactly the same software; however they have different responsibilities depending on their role. Each AP-ONE can play one of the following roles in the context of ZC:

- It can be a *Primary Master (Master in short)*
- a *Secondary Master*
- or a *Slave on a Master*

Each ZC network can only have one Primary Master and as many Secondary Masters and Slaves as necessary. The node that is elected Primary Master is the one connected directly (or through a switch/hub) to a router and gets a global ip address (via DHCP or statically). Other nodes are connected as slaves on the Primary Master and can also act as Masters themselves (Secondary Masters) for other slaves. Whether a node will be a Slave or a Secondary Master depends on its physical location in relation to the other nodes. The role of each AP-ONE may change to reflect rearrangements at the physical topology.

The overall network layout resembles a tree (figure 93). Associations are formed in the basis of optimal network performance and can change in time to accommodate for events at the physical environment. Therefore, when a slave has multiple masters in sight to connect to, it chooses the one from which it gets the maximum throughput and reconsiders this choice periodically.

The 802.11a interface of each AP-ONE is devoted for these negotiations to take place, and for forwarding traffic originated from (or destined to) the wireless clients. The clients (users) get network access via AP-ONE's 802.11b/g interface, and their ip is assigned via DHCP from the subnet 192.168.4.0/24. The 802.11a interface of each AP-ONE is called the *Backhaul* interface, whereas the 802.11b/g interface is called the *Wifi Coverage* interface.

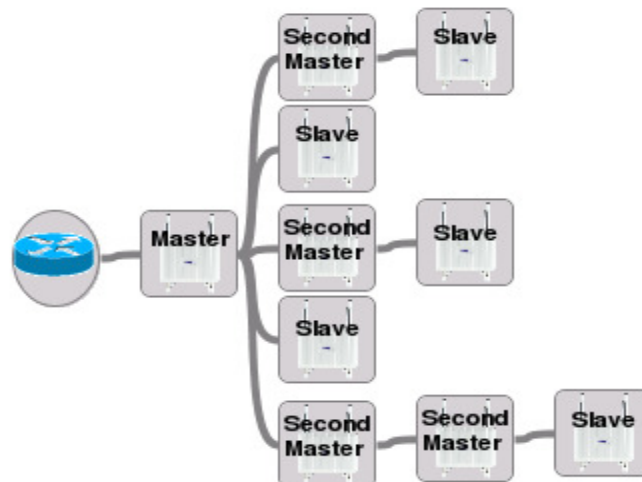


Figure 93. Logical Topology

Another way to perceive inter-node associations is through the parent/child type of relationship:

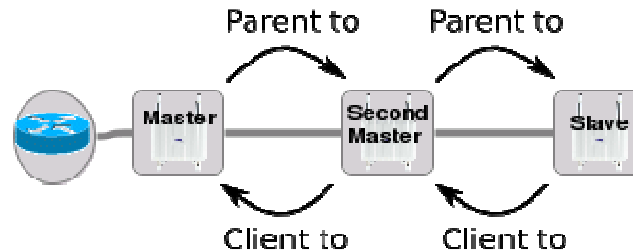
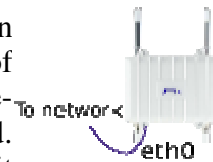


Figure 94. Logical Topology

## 12.2 Physical Distribution

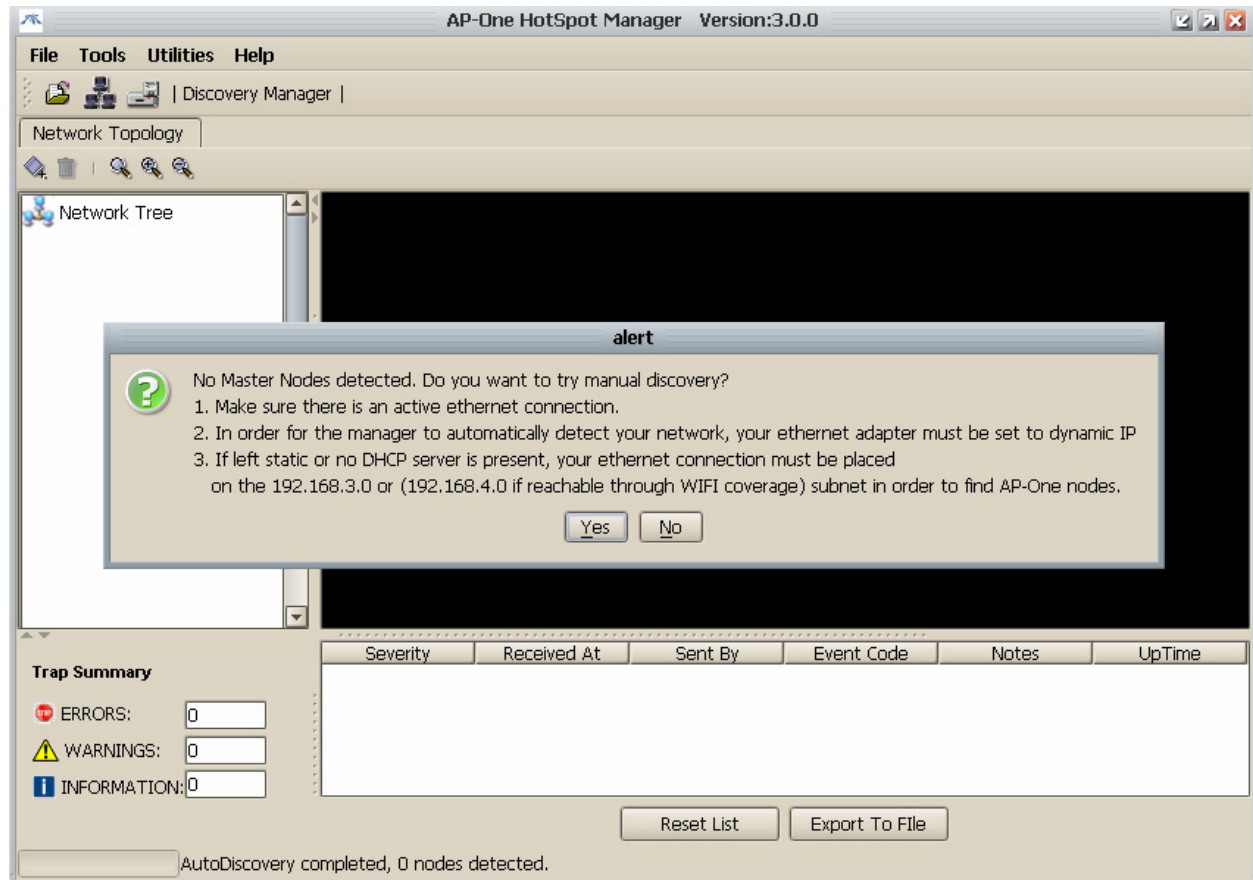
The first step to deploy a ZC HotSpot is to attach an AP-ONE on an Internet connection. The ip address of the ethernet interface can be either issued by a pre-configured DHCP server or can be statically assigned. In either case, as soon as the AP-ONE gets an ip, it will start functioning as Primary Master for the rest of the ZC Hotspot network.



**Note:** In AP-ONE with multiple ethernet interfaces, use the one on the left (picture on the right).

The rest of nodes are distributed throughout the area to be covered. This placement doesn't have to be accurate at first place, since it can change at any time without any additional administration cost.

Next step is to launch Hotspot Manager which will automatically retrieve your connection settings in order to perform an auto-discover to formulate the HotSpot Network. If no node is discovered within the subnet of user's PC interface IP settings then below pop-up will be launched. Pressing yes, discovery manager will be popped up to give you the opportunity to perform a manual discovery.



A second possible state is the one that NMS can not perform an auto discover due to mismatch in user's PC IP settings. In that case a pop up will be launched to warn user for any possible mismatch in IP configuration setting. User should either check the connection settings and re-launch NMS or he can use manually the *Discovery Manager* (Tools -> Discovery Manager). In second case Discovery manager can be launched by clicking to the shortcut that is placed in the item bar above network topology. Fill in the fields in order to search the whole subnet served by the DHCP server. Thereafter, the Master node should appear on the list. Finally, set the password field of this node to "admin".

**Note:** If your connection settings are configured correctly concerning the MASTER you wish to discover (IP of your computer is compliant with the subnet with the dhcp server's pool which provide IP to master)



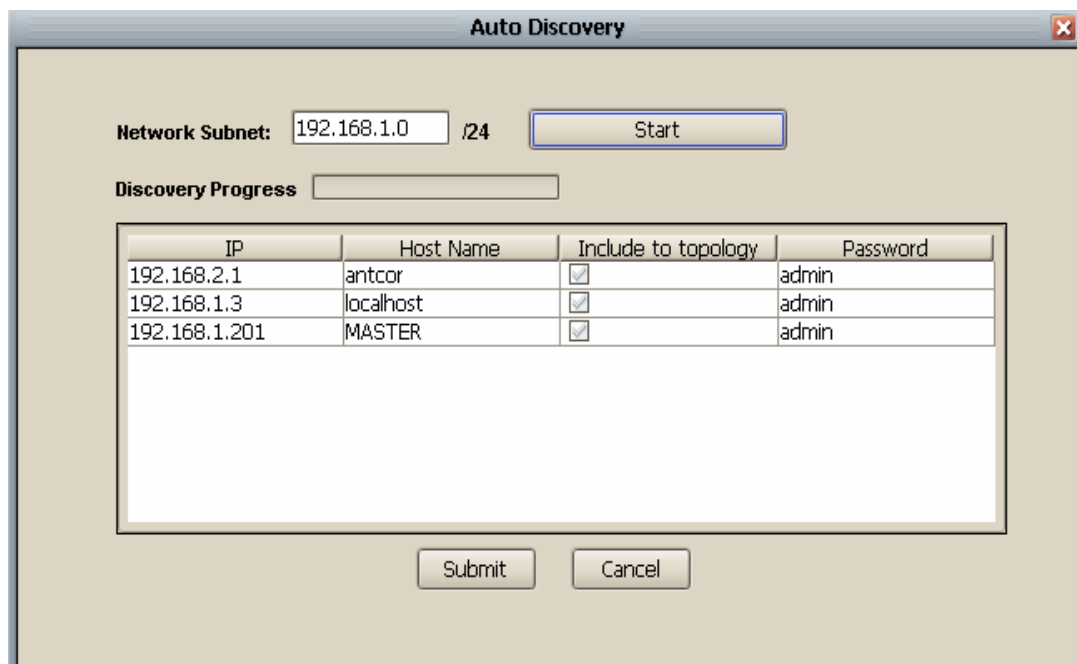


Figure 95. Discovery Manager

**Note:** Depending on network congestion, sometimes you may have to initiate the search more than once, in order to find the desired Access Point.

In case the Master's IP address is assigned statically (as discussed later on this chapter), just add the node via with the “Add New Node” window panel (Tools -> Add New Node).

As soon as the Master node is either determined or automatically discovered, it starts searching for slave nodes on the backhaul interface, and wireless clients (users) on the Wifi Coverage interface. The initial network layout is shown in figure 96 after loading the appropriate background image.

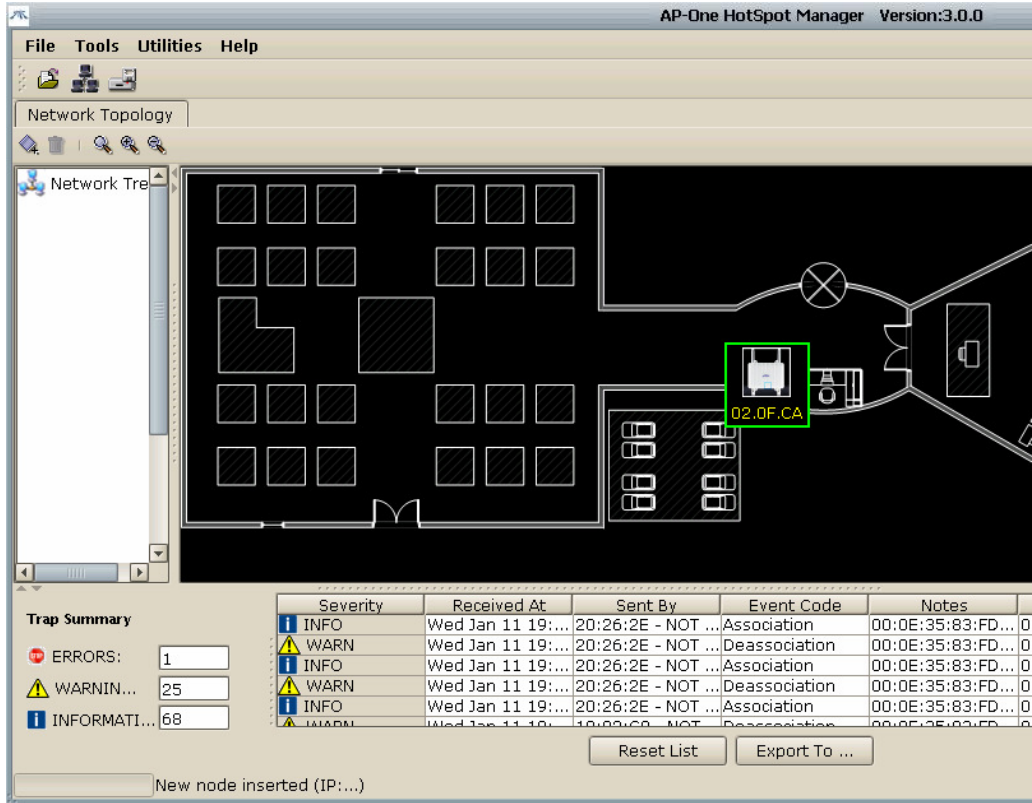


Figure 96. Initial network layout

Messages will start to flow by, as new AP-ONE slaves and wireless clients are discovered. Each message is categorized, based on its significance, on ERROR, WARNING or INFORMATIONAL. Several types of events are reported, among them the most notable are described in following table.

<i>Event</i>	<i>Severity</i>	<i>Description</i>
System Started	INFORMATIONAL	Signifies the start of the discovery process on the Master node.
New HotSpot Node Detected	ERROR (OF HIGH SIGNIFICANCE)	Signifies the discovery of a new node. This message is reported once per node. This message succeeds the 'System Started' message type.
HotSpot Child Arrived/Left HotSpot Parent Found/Left	INFO/WARNING INFO/WARNING	Signifies transitions on the role of a node. This message succeeds the 'New HotSpot Node Detected' message type.
Associations/Disassociations	INFO/WARNING	This message type reflects events at the Wifi Coverage cell. Connections and disconnections of wireless clients.

<i>Event</i>	<i>Severity</i>	<i>Description</i>
State of various system services	INFO/WARNING	This message type reports initiations/ terminations of various system services.

After a while (and after arranging the nodes on the map properly) we get the network layout at picture 104.

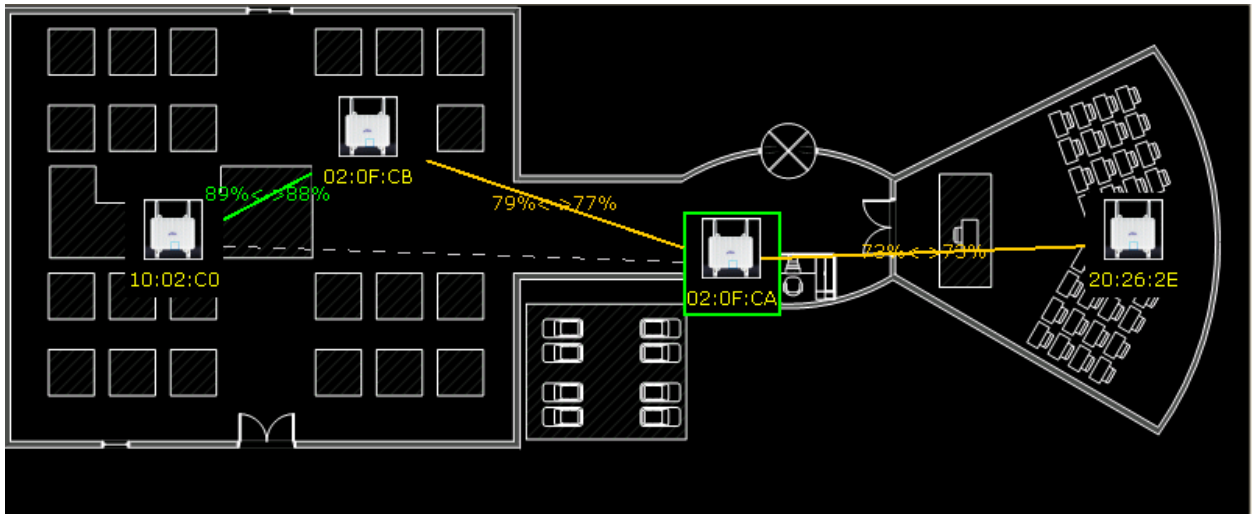


Figure 97. Complete ZC network deployment

Line coloring corresponds to the quality of the respective link. It can be Green, yellow or red in order of decreasing quality. Lines are also accompanied by the RSSI values of each participating node. The left RSSI value corresponds to the parent of this particular connection, whereas the right one corresponds to the client.

## 12.3 HotSpot Configuration

HotSpot configuration is carried out via a dedicated menu, specific to every node and accessible by right-clicking on the node (Picture 105). Options “*Detect/Update Adjacent Nodes*” and “*Remove inactive connections*” are valid ONLY for the Primary Master.

### Detect/Update Adjacent Nodes:

This option causes the network map to be refreshed. This action can be used to re-draw and recreate your network from the beginning. User can activate this command if there is a possibility that some traps are not received by MASTER and there is any possible mismatch in the representation of the ZC network

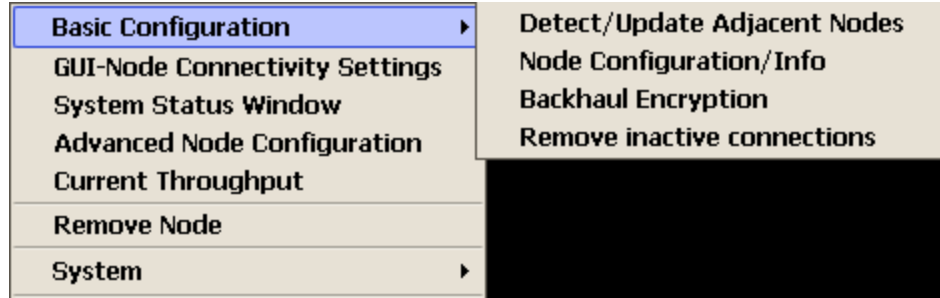


Figure 98. Node menu

### Remove inactive connections:

Inactive connections are associations between nodes, which are not any more present. They are depicted as dashed lines on the network map (figure 97). For instance, in picture 104, node 10.02.C0 was client on 02:0F:CA (Master) some time in the past, whereas now is client on 02.:0F:CB.

### Node Configuration/Info:

Opens the Backhaul Configuration window. It comprises out of three tabs:

- Backhaul Interface Settings
- Ethernet Settings
- HotSpot
- Statistics

It's one of these will be discussed on the separate section which follows.

### BackHaul Encryption:

It gives user the opportunity to enable an auto-distributed Security Scheme in order to secure all ZC HotSpot Network Backhaul Connections. A PassPhrase is filled which is used for the derivation of the Security Keys.

## 12.3.1 Backhaul Interface Settings

This tab is divided into two sub sections.

### Backhaul:

On this panel you can configure the frequency used for the backhaul connection throughout the network. This configuration parameter should always be applied on the Primary Master, and then, it will be propagated throughout the ZC network.

## Wifi Radio Coverage:

Channel and SSID for the Wifi Coverage interface used on this particular node. This configuration parameter can be applied separately on each node of the network, and can very-well differ among them. The number of associated stations is also provided, as well as the complete association list.

The screenshot displays a configuration window titled "Node status information & configuration". It features four tabs: "Backhaul interface Settings", "Ethernet Settings", "Hot Spot", and "Statistics". The "Backhaul interface Settings" tab is active. Under the "Backhaul" section, the "Frequency" is set to 5805. The "WIFI Radio Coverage" section includes a "Frequency" dropdown set to 2462, a checked "Best Frequency Auto-Selection" option with the label "Enable", an "SSID" field containing "AP ONE HOTSPOT", and a "Number of Associated Stations" field containing the number 3. A "View Association List" button is located below the station count. At the bottom of the window, there are three buttons: "Submit", "Refresh", and "Exit".

Figure 99. Backhaul Interface Settings configuration tab

### 12.3.2 Ethernet Settings

The ethernet settings tab allows you to set a static IP address on the ethernet interface of a node. This way you also force the node to switch to Primary Master mode.

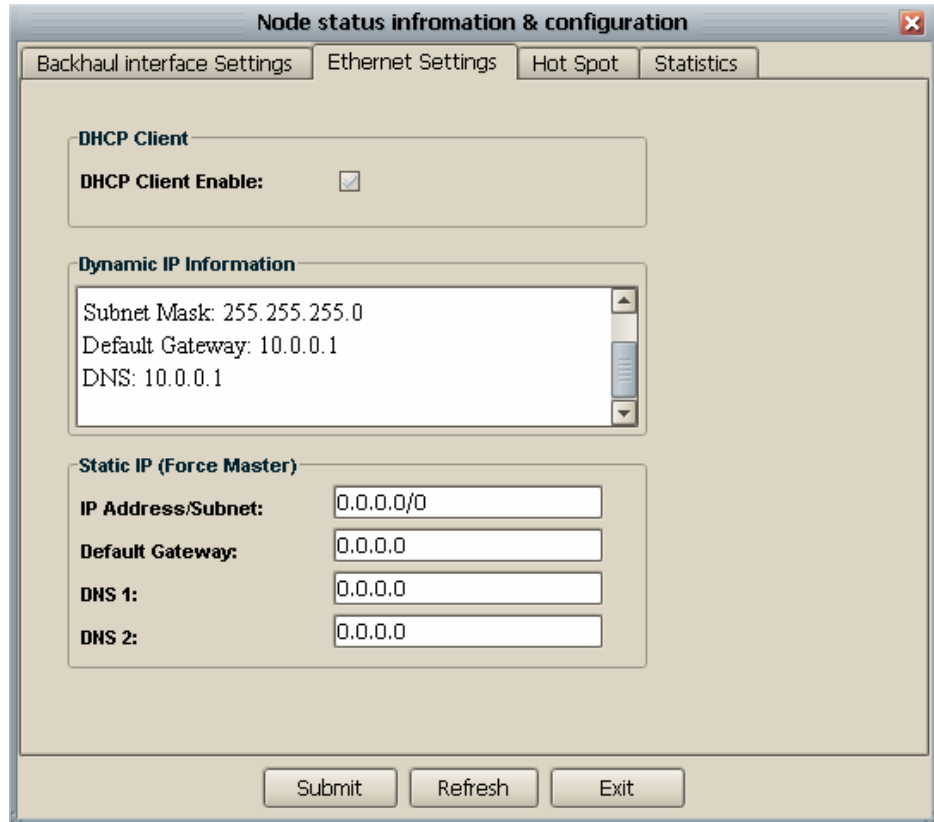


Figure 100. Ethernet Settings configuration tab

### 12.3.3 Hot Spot

With the third tab of the Node Configuration/Info window, we are able to enable Hot Spot Service and enable radius server authentication by defining a secret password and the authentication type we prefer (figure 101)

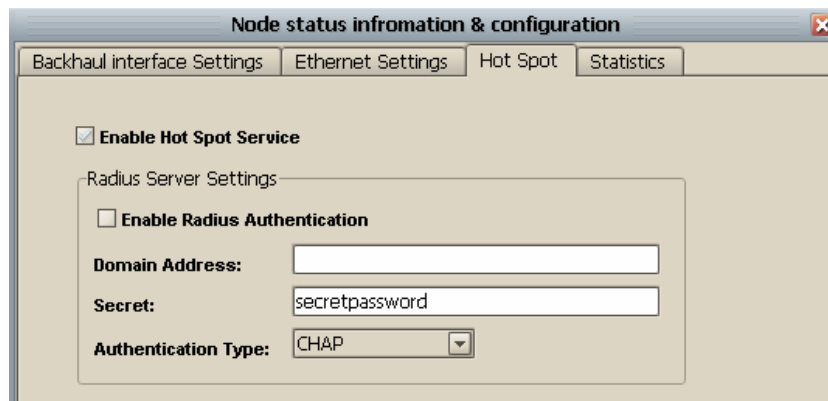


Figure 101. Hot Spot tab

## 12.3.4 Statistics

The fourth tab of the Node Configuration/Info window provides a graphical representation of the traffic associated to a node's interfaces. The interfaces listed are those related to the backhaul networking.

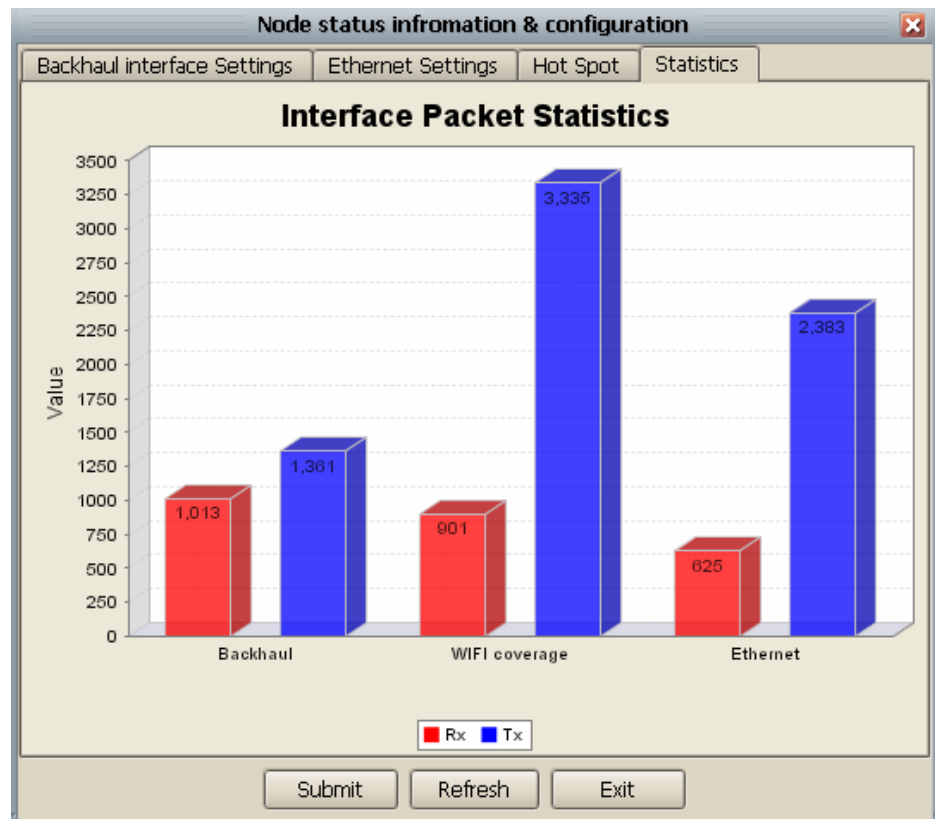


Figure 102. Statistics tab

## 12.4 Design Guidelines

### 12.4.1 Stability Considerations

Sometimes, you may witness a node flipping between a number of Secondary Master nodes. In other words, the node isn't able to settle on which secondary master to connect to. This instability parameter may cause degradation of network performance. The cause of this, is usually the existence of multiple connections to Master nodes, with similar quality characteristics. By all means, you should try to avoid such conditions, by changing the position of the dubious node towards to one of the Master nodes.

However, bear in mind, that this phenomenon is expected and desirable to some extent. This is an expression, after all, of ZC Hotspot's capability of dealing with diversities in the physical environment.

## 12.4.2 Performance Considerations

### Overhead of Zero Configuration of HotSpot

Some overhead is introduced by Zero Configuration of Hotspot. This overhead is closely related to the magnitude of the ZC network. In other words, the more the nodes that comprise the ZC network, the higher the impact on performance. However, this factor rarely is of significance, since, in most cases, the bottleneck is introduced at the outgoing connection (Figure 103).

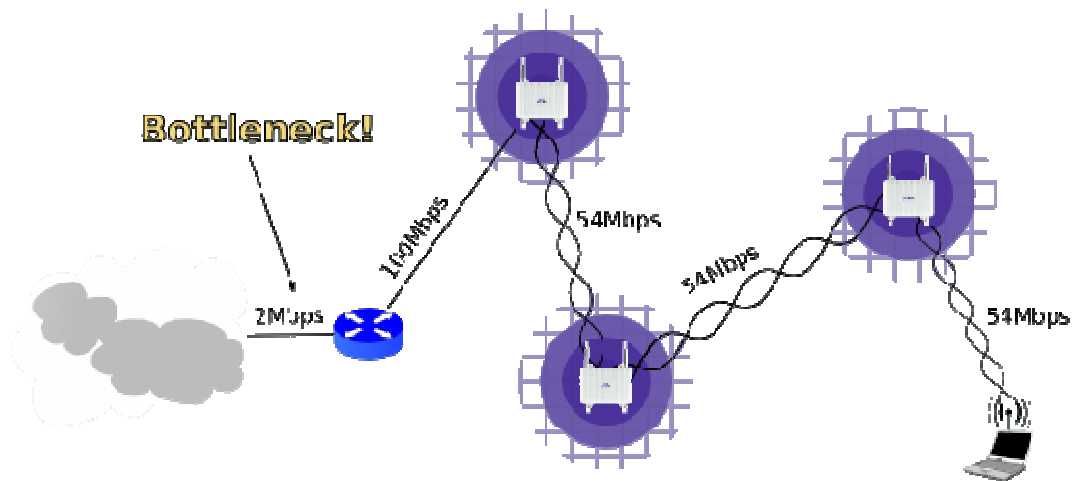


Figure 103. Bottleneck on the Internet connection

### Overlapping Wifi Coverage Cells

Another parameter that affects network performance, is the noise caused by overlapping Wifi Coverage cells (Picture 104). By default Wifi Coverage interfaces propagate at one of the 3 channels that do not interfere. These are 1 (2412Mhz) 6 (2437Mhz) 11 (2462MHz). By default the Best Channel selection algorithm is enabled during auto configuration phase of a node. This means that a passive scan is implemented to check what is the optimal of the three channels that a new configured wifi coverage interface should transmit to. This is calculated according to the APs that are transmitting on these frequencies. However, user has the option to configure every single node individually, and setting the channel of its Wifi Coverage interface to custom values.



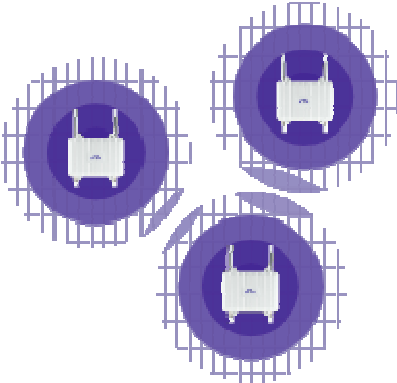


Figure 104. Overlapping Wifi Coverages

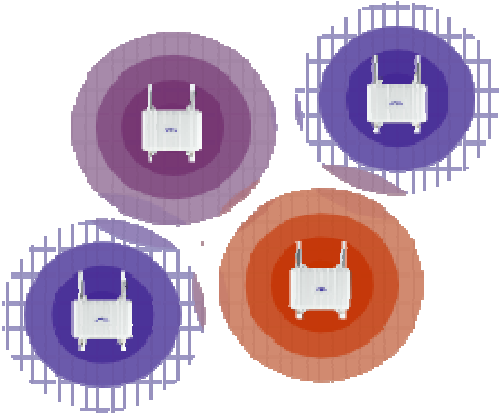


Figure 105. Non-overlapping Wifi Coverages

## Multiple Zero Configuration Trees

Consider the network layout at picture 106. There are multiple Internet connections on different physical locations. To take advantage of all of them, we have to attach a separate AP-ONE node on each outgoing connection. This way, two concurrent ZC networks will be formed, each of them distributing their respective network connection among its clients.

This design technique is also helpful for minimizing the overhead caused by the ZC protocol on very large networks. On such network is often preferable to segment them into multiple smaller ones, each one representing an autonomous ZC HotSpot tree.

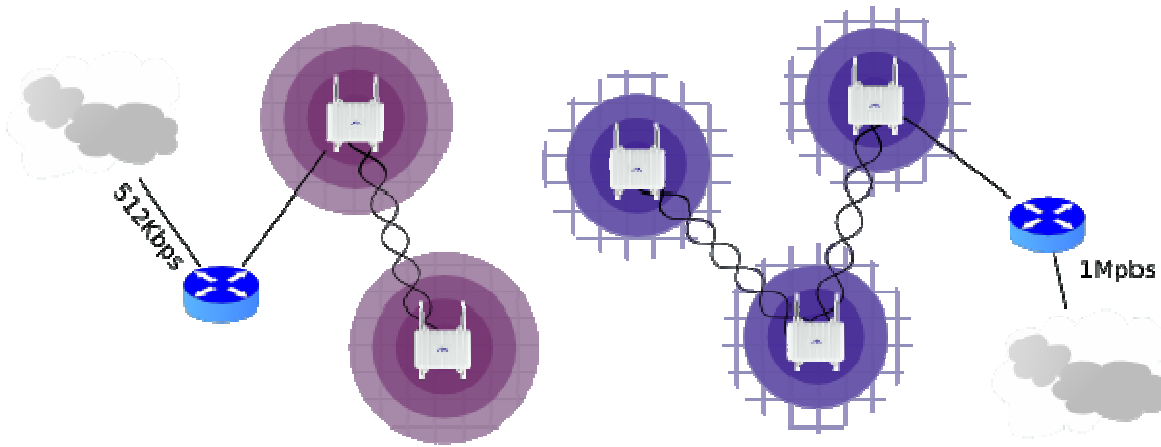


Figure 106. Multiple concurrent ZC networks. The total bandwidth shared among wireless clients is 1.5 Mbps

### 12.4.3 Security Considerations

#### Security on Wifi Coverage

The full potential of 802.11i can be utilized at every Wifi Coverage cell. It's also possible to use a different authentication/encryption scheme per cell. Hence, multiple authentication/encryption schemes can be used (Figure 107) on a single Hotspot network. In any case, the configuration of each cell has to be done by the administrator manually. If you are to configure 802.1X, make sure that the RADIUS server is placed outside of the ZC Hotspot network, otherwise it won't be accessible by all AP-ONE nodes.

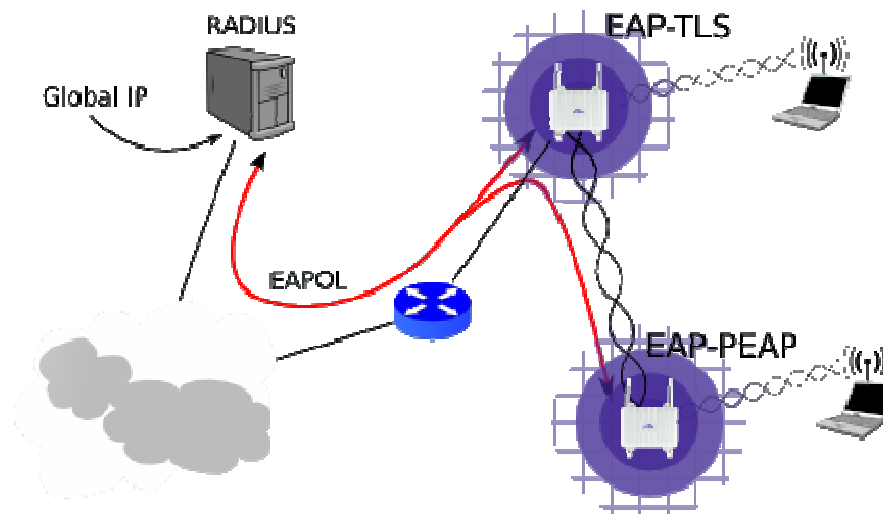


Figure 107. Authentication Server should be placed outside of the hotspot network

## Security on Backhaul

Contrary to Wifi Coverage, Backhaul connections can only use WEP encryption. Next versions of ZC protocol will feature more advance security protocols (EAP-PSK). For the time being, users are advised to enforce their own security measures (SSL tunnels, VPNs etc) for end-to-end security sensitive applications.

There are two ways to secure your backhaul.

### Auto-Configured Security Scheme

You can take advantage of ZC auto Security distribution scheme to secure your backhaul .This can be done by selecting right Click on MASTER NODE > Backhaul Encryption. The following pop up (picture 108) will be launched in which you can enable/disable Security Scheme and fill the

passphrase which will be used to create the distributed Keys. Master Node takes this passphrase as input and through a highly complicated algorithm creates 128bit keys which are distributed to the nodes of the ZC HotSpot network automatically. Every new node that comes to join the Network is informed by its Parent of the security manifesto of the Network.

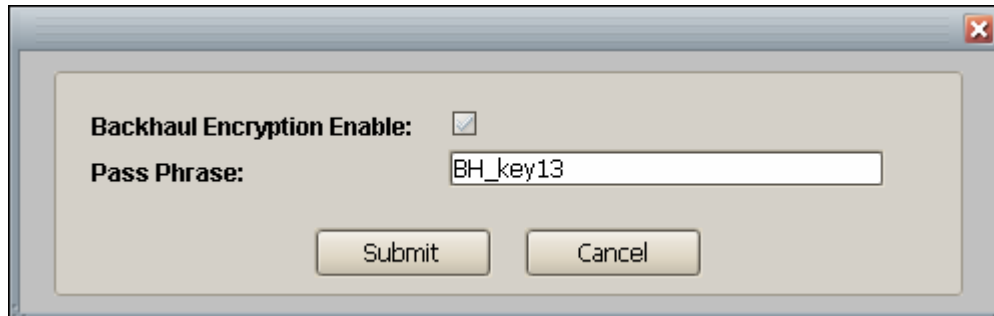


Figure 108. Backhaul Encryption Configuration

### Manual Configuration

The configuration of WEP keys for every node should be carried out in a progressive manner, starting from the far most nodes (leafs) and gradually approaching the Primary Master (root). Picture 109 illustrates this. Nodes of the same number signify that order of configuration is not significant among them.

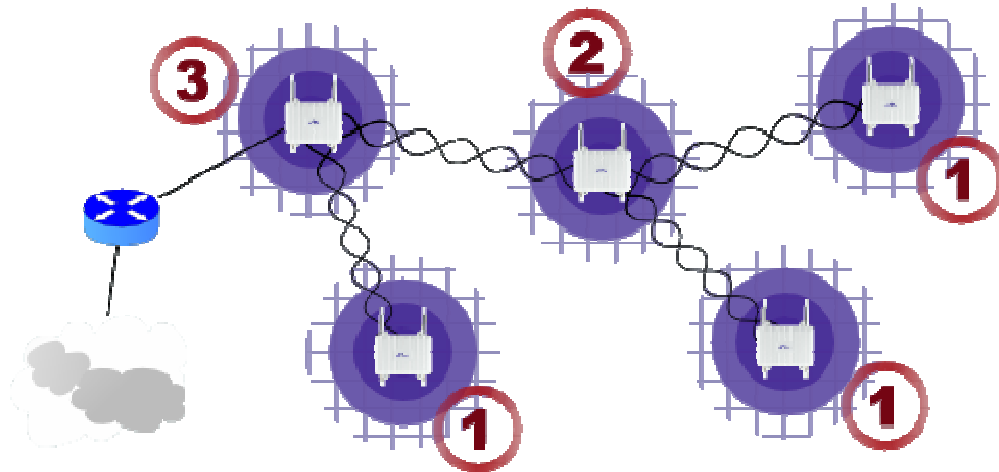
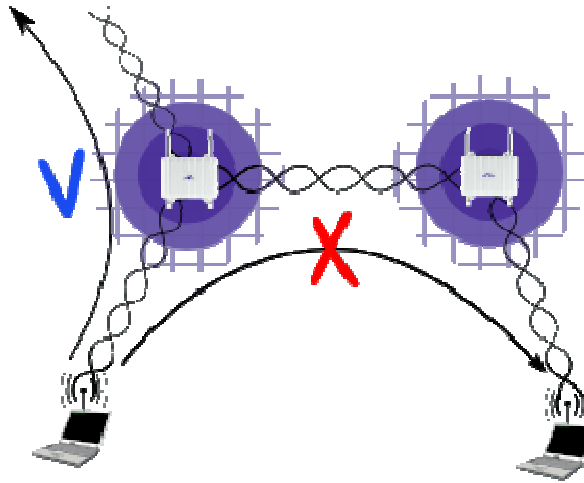


Figure 109. Authentication Server should be placed outside of the Hotspot network

### Wifi Coverage Isolation

*Wifi Coverage Isolation* is a build-in security feature of Zero Configuration. It prevents wireless clients of one Wifi Coverage from contacting clients of another. This way we isolate potentially malicious

clients on their own Wifi Coverage, and hence, protect unsuspected clients of other Wifi Coverages. This restriction is not expected to cause any inconvenience to the end-user, since end-users normally want to access the



Internet and not establish direct connections between them.

*Figure 110. Communication is not permitted between Wifi Coverage*

## 12.4.4 Deployment Considerations

### Server Placement

The whole ZC HotSpot network is behind a NAT and shares a private address space. The only host on the network with real IP address is the Primary Master; for which reason is also the only accessible from outside of the ZC HotSpot network. Therefore, you should never place a server inside the ZC HotSpot network. Another reason not to place a server on a ZC network is that by design ZC is dynamic in nature, and cannot guarantee availability of resources.

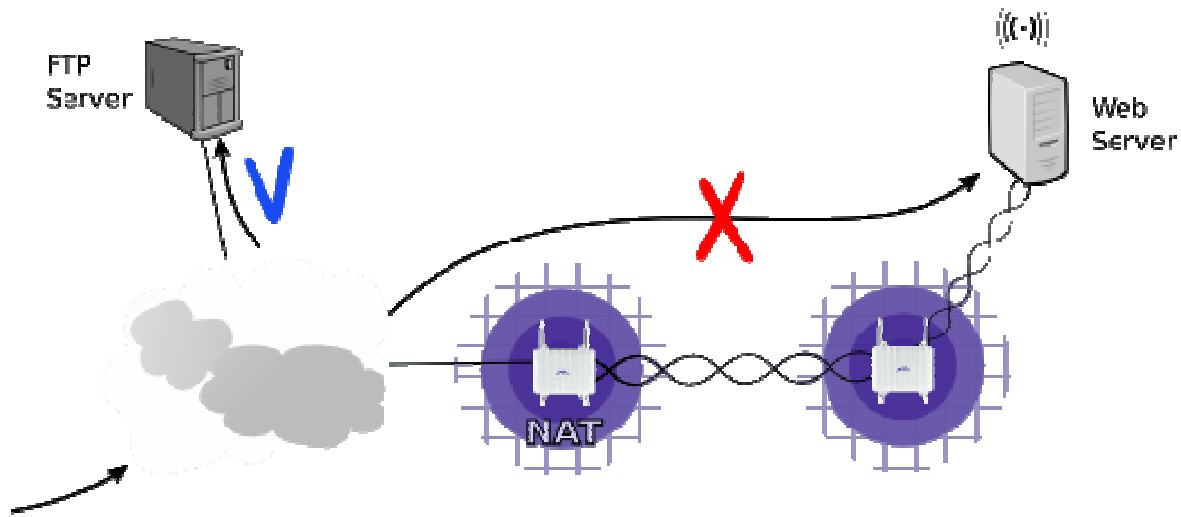


Figure 111. Internal servers are not recommended.

## Attachment on an intranet

As aforementioned, the Primary Master usually gets its IP via DHCP on its Ethernet0 interface. Most preferably, this IP should be a global one, not a private one. This is because ZC HotSpot has been designed to be attached directly on an Internet connection. However, it's still possible to attach a ZC network to an intranet, but this poses some restrictions on the address space used on the rest of the intranet. In particular, hosts that reside on the ZC network will not be able to access hosts on the intranet (and contrariwise) with IPs from the subnets:

- 10.0.0.0/8
- 192.168.1.0/24
- 192.168.4.0/24

## 12.4.5 Security Considerations

### Non-Permanent Modifications

Zero Configuration assumes that specific IP and bridging configuration is present on every AP-ONE HotSpot. This configuration is automatically generated at boot time. Therefore, you should not make any modifications on the IP setting (addresses, bridging, etc) on any AP-ONE. After all, these changes will be lost at the next reboot.

## 12.5 Limitations

### 12.5.1 Roaming

Currently, Zero Configuration does not provide for roaming users. Hence, a user who switches from one AP-ONE cell to another, will be forced to re-associate/re-authenticate to the new one, and a new IP address will be issued to him.

## 12.6 HotSpot Wizard

The AP-One HotSpot Access Gateway enables telcos, operators, wireless ISPs, enterprises, government institutions, or school campuses to deploy WLANs with secured user authentication support. Based on both RADIUS (Remote Authentication User Dial-In Service) and Web Redirection technology, when an unauthenticated wireless user is trying to access a Web page, a logon page is shown instead of the requested page, so that the user can type his/her user name and password for authentication. Then, the user credential information is sent to a back-end RADIUS server to see if the user is allowed to access the Internet. This web-redirection also supports Web page customization, allowing operators or HotSpots to easily designate a Web page / Advertisement URL before / after user login, not to mention Web-redirection bypass for paid users and/or those frequently using HotSpot services, where authentication can be performed using their MAC address.

To configure the **HotSpot Wizard** settings, select the **HotSpot** tab, located under the **Advanced Configuration of Node, Configuration** tabs.

### 12.6.1 HotSpot Main Tab

When the HotSpot tab is selected a simple user interface is displayed as a starting point for the HotSpot configuration process. From the HotSpot Main tab you can:

- enable the HotSpot
- view the status of the Hotspot
- view the administrator's MAC address
- start the HotSpot Wizard
- open a window to view a file containing configuration information
- open a window to view user information
- open a window to view Radius statistics

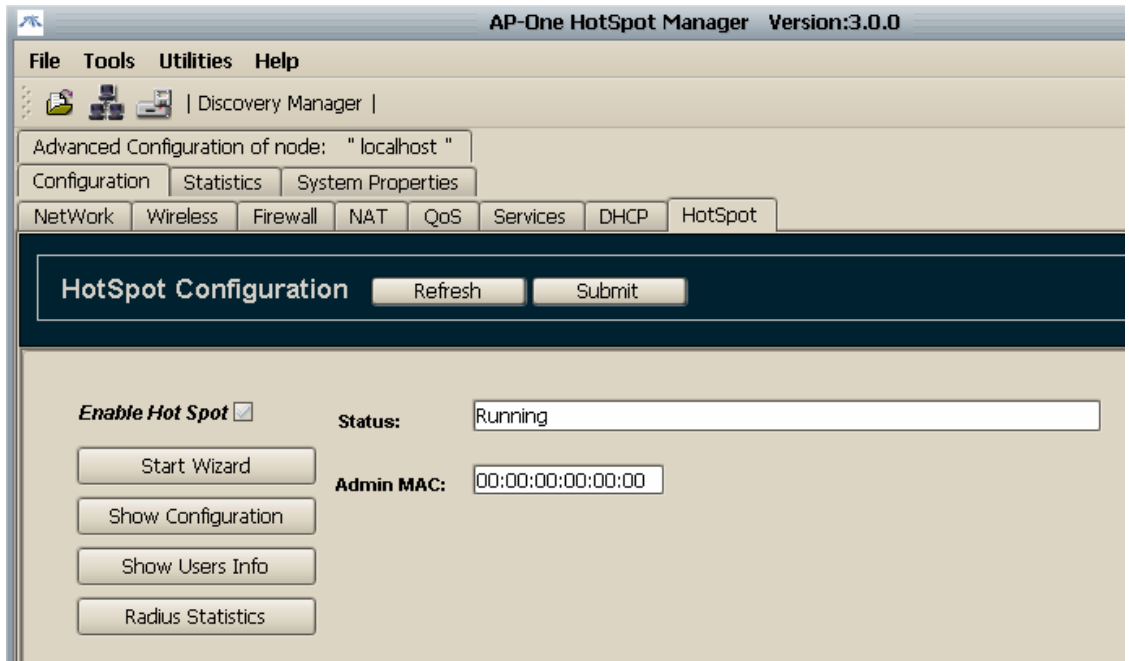


Figure 112. Main HotSpot Tab

## Enable HotSpot

Click the **Enable HotSpot** button to stop or start Hotspot functionality.

## Status

**Status** displays current HotSpot status (**Stopped**, **Running** or **Initializing**). In case there is a problem with HotSpot initialization procedure, an error message is displayed.

*Example: DNS error*

*The HotSpot needs to connect to a DNS server, but cannot find one. This may be a possible incorrect configuration of the HotSpot's WAN interface settings, or a possible temporary unreachable state of the DNS server (WAN is not initialized yet, PPP connection is not established yet). The HotSpot will keep retrying to initialize at certain intervals.*

## Admin MAC

**Admin MAC** is the administrators MAC Address. This MAC address (if not zeros), is always considered authenticated and assigned the first HotSpot Dynamic IP address (x.x.x.2). Setting it is recommended, to avoid losing connectivity with the HotSpot, if connected to one of its HotSpot interfaces.

## Users Info



**Users Info** is a list of users that have obtained an IP address, their authentication status (TRUE or FALSE), and users' statistics. To access this list, click the **Users Info** button. The **HotSpot Users** dialog box appears. The **Users Info** button is available when the HotSpot configuration is complete and the HotSpot is running.

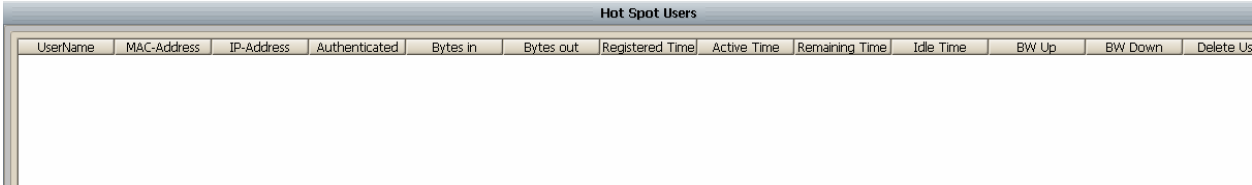


Figure 113. Users Info Window

### Radius Statistics

The **Radius Statistics** window allows you to view information about the operation of the Radius server. To access the **Radius Statistics** window, click the **Radius Statistics** button. The **Radius Statistics** button is available when the HotSpot configuration is complete and the HotSpot is running.

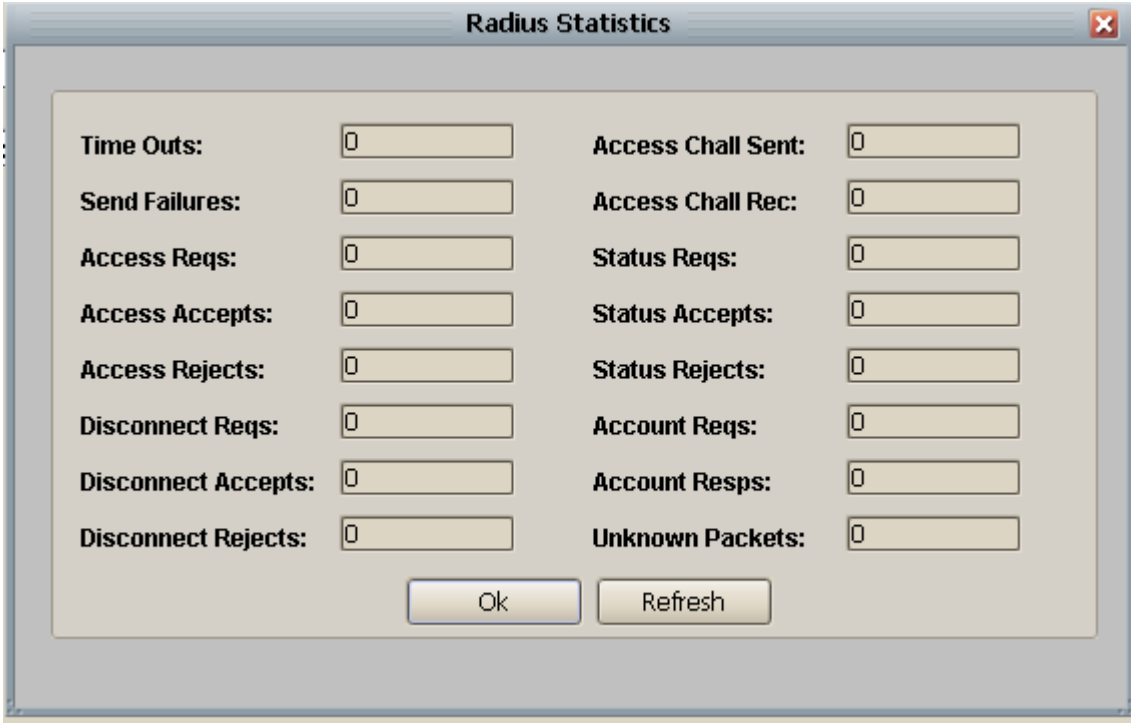


Figure 114. Radio Statistics Window.

## 12.6.2 Using the HotSpot Wizard

To begin the wizard configuration, click the **Start Wizard** button in the configuration panel. A multi-tabbed pane opens with the **WAN** tab on top. To navigate between tabs, click the **Next** or **Previous** buttons at the bottom of the pane. The following sections describe the configuration settings for each tab.

### DHCP

Hotspot will assign HotSpot users with an IP address in the range of the configured dynamic IP addresses. Configure the HotSpot DHCP tab as follows:

The screenshot shows the 'AP-One HotSpot Manager Version:3.0.0' window. The 'HotSpot' tab is selected, and the 'DHCP' sub-tab is active. The 'HotSpot Configuration' section has 'Refresh' and 'Submit' buttons. On the left, a sidebar lists configuration options: DHCP, Radius, Auth Type, Walled Garden, Advertisement, Web Customization, and Summary. The main configuration area includes:

- Dynamic IPs:** 192 168 4 0 / 24
- Static IPs:** 0 0 0 0 / 0
- DNS 1:** 0 0 0 0
- DNS 2:** 0 0 0 0
- Domain:** AP-one
- Lease:** 600 secs

Figure 115. Hotspot Wizard DHCP tab

*Warning: Hotspot uses its build-in DHCP server, which is not displayed in the DHCP panel of the router.*

### Dynamic IPs

Type the base IP address and subnet into the **Dynamic IPs** field. **Example:** If the dynamic IP addresses are 192.168.4.0/24, the Hotspot will assign IP addresses in the range of 192.168.4.2 to 192.168.4.254. IP address 192.168.4.0 is the Network IP, which cannot be assigned. IP address 192.168.4.1 will be assigned to the HotSpot itself (br\_HotSpot interface). IP address 192.168.4.255 is the Broadcast IP, which cannot be assigned.

### DNS 1 and DNS 2

If DNS values are set to 0.0.0.0, the Hotspot will assign the router's DNS IP addresses.

## Domain

**Domain** is the domain name assigned to HotSpot users.

## Lease

Is the number in seconds users' DHCP client services will have to renew their assigned IP.

## Static IP

**Static IP** is an advanced option left to the administrator. Using it, Hotspot will never assign this range of IP addresses, unless MAC authentication is used and the Radius server's response forces an IP address of this range to be assigned (Framed-IP-Address).

**Example:** If dynamic IP addresses are configured as above and static IP addresses are 192.168.4.0/30, the Hotspot will assign IP addresses in the range 192.168.4.4 to 192.168.4.254, leaving IP addresses 192.168.4.2 to 192.168.4.3 to be assigned from the Radius server.

**Warning:** The Static IPs subnet should be a sub-subnet of the Dynamic IPs subnet.

## Radius

The radius server used to authenticate HotSpot users.

The screenshot shows the 'Radius Server (1)' configuration tab in the HotSpot Wizard. On the left is a sidebar with navigation buttons: DHCP, Radius (selected), Auth Type, Walled Garden, Advertisement, Web Customization, and Summary. The main configuration area contains the following fields:

- IP Address 1:** Four input boxes, each containing '0'.
- IP Address 2:** Four input boxes, each containing '0'.
- Domain 1:** An empty text input field.
- Domain 2:** An empty text input field.
- Authentication Method:** A dropdown menu with 'CHAP' selected.
- Secret Key:** A text input field containing 'secretpassword'.
- Nas ID:** A text input field containing 'wisp2\_1'.
- Authentication Port:** A text input field containing '1812'.
- Accounting Port:** A text input field containing '1813'.

Figure 116. HotSpot Wizard Radius Tab

IP Address 1 and 2 / Domain 1 and 2

Either the **IP address** or **Domain** name of at least one Radius Server must be configured. The second Radius server is used as a backup server (if present).

### Authentication Method

Authorization to Radius server will be performed using the **Authentication Method** (**CHAP** or **PAP**) selected in the **Authentication Method** drop down list.

### Secret Key

Type the **Secret Key** of the Radius Server in this field.

### NAS ID

Type the HotSpot's NAS identifier in the **NAS ID** box.

### Authentication Port

The **Authentication Port** is the port used to send Access Requests to Radius Server (1812 by default).

### Accounting Port

The **Accounting Port** is the port used to send Accounting Requests to the Radius Server (1813 by default).

### Authentication Type

**Authentication Type** is the method used to authenticate HotSpot users. At least one must be enabled.

The screenshot shows the 'Authentication Tab' of the HotSpot Wizard. On the left is a vertical menu with buttons for 'DHCP', 'Radius', 'Auth Type', 'Walled Garden', 'Advertisement', 'Web Customization', and 'Summary'. The main area is titled 'UAM Authentication' and contains a form with the following fields:

- Enable:** A checked checkbox.
- Domain:** A text box containing 'localhost' and a checked 'Local' checkbox.
- Secret:** An empty text box.
- Port:** A text box containing '3990'.

Below this is the 'MAC Authentication' section, which contains a form with the following fields:

- Enable:** An unchecked checkbox.
- Passwd:** A text box containing 'password'.
- Suffix:** An empty text box.

Figure 117. HotSpot Wizard Authentication Tab

## UAM Authentication

**UAM** is the common Web-redirection authentication type. Hotspot users, after they have obtained an IP address, and opened a Web browser, will be redirected to the HotSpot's Web page to provide their Username and Password.

### Enable

Select the **Enable** check box to enable **UAM Authentication**.

### Domain

Type the URL of the authentication webpage into the **Domain** text box.

### Secret

The **Secret** field is currently unused.

### Port

**Port** is the local port the HotSpot will use for redirection (default 3990).

## MAC Authentication

Hotspot users can be authenticated to the Radius Server using their MAC address (the MAC address of their media used to obtain an IP address).

Hotspot will send an access request to the Radius Server, using as Username the MAC address of the user (followed by the suffix string if present). It also sends password configured in the **Password** field. If authentication is successfully completed, the user obtains the Framed IP Address of the Radius Access Response (if present), or the next available IP address in the range of Dynamic IP addresses. If authentication fails and UAM Authentication is enabled, user obtains an IP address in the range of Dynamic IP addresses and UAM authentication is performed (WEB-redirect page).

## Enable

Select the **Enable** check box to enable **MAC Authentication**.

## Password

**Password** is the password used to authenticate HotSpot users to Radius Server.

## Suffix

**Suffix** is the string attached to the HotSpot users' MAC address used as Radius Username.

*Warning: If MAC authentication is enabled, HotSpot users will obtain an IP address ONLY if the Radius Server is reachable.*

## Walled Garden

**Walled Garden** is a set of at most five domains or IP addresses or subnets that a user can access without having performed authentication (The user must have previously obtained an IP address from the HotSpot). Type the URLs for these domains or IP addresses into the **Walled Garden URLs** text boxes.

The screenshot shows the 'Walled Garden' configuration tab in the HotSpot Wizard. On the left is a vertical sidebar with buttons for 'DHCP', 'Radius', 'Auth Type', 'Walled Garden' (which is highlighted), 'Advertisement', 'Web Customization', and 'Summary'. The main content area is titled 'Walled Garden URLs:' and contains five numbered text input fields (1) through (5) for entering domain names or IP addresses.

Figure 118. HotSpot Wizard Walled Garden Tab

## Advertisement

**Advertisement** is a set of at most five URLs that a HotSpot user will be redirected to, after having authenticated successfully using UAM authentication.

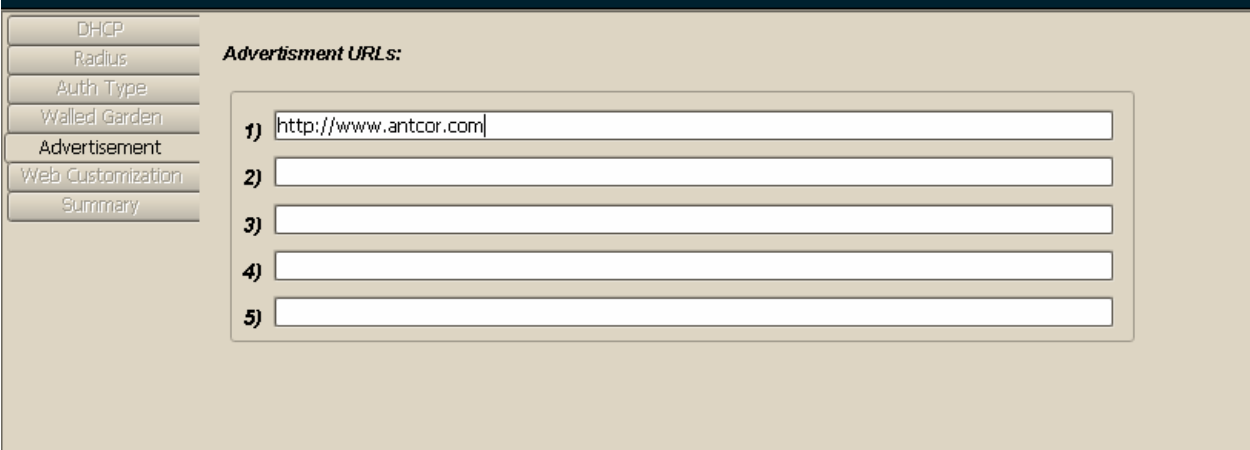


Figure 119. HotSpot Wizard Advertisement Tab

## Web Customization

From the **Web Customization** tab, the login Web page to which a HotSpot user is redirected can be customized according to administrator's needs.



Figure 120. HotSpot Wizard Web Customization Tab

The following text fields that the administrator can fill with info describing his needs.

## Brand Name

Type the Brand name of the company providing the HotSpot. E.g. *Downtown Bistro's Hotspot*

## Extra Text

Type additional text for promotional purposes. E.g. *Featured by Tony's HotSpot Operators.*

## Select Color

Click **Select Color** to access the **Select Background Color** dialog box. Select the background color of the redirection Web page.

## Select Image

Click **Select Image** to access the **Select** dialog box and import a .jpg, .bmp or .jpeg graphics file that is superimposed on the Web redirection page.

## Summary

All configuration data is stored in the **Summary** field. When the **Summary** tab is on top the configuration data is shown in this tab.



The screenshot shows a web-based configuration interface for a HotSpot Wizard. On the left, there is a vertical navigation menu with tabs for DHCP, Radius, Auth Type, Walled Garden, Advertisement, Web Customization, and Summary. The 'Summary' tab is currently selected. The main content area displays the configuration details for 'Ikarus HotSpot Configuration'. The configuration is organized into several sections, each preceded by a separator line of asterisks. The sections include: DHCP Configuration (Dynamic IPs: 192.168.4.0 / 24, Static IPs: 0.0.0.0 / 0, DNS 1: 0.0.0.0, DNS 2: 0.0.0.0, Domain: AP-one, Lease Time: 600), NAT & SECURITY Configuration (Protection Level: DISABLED), Radius Configuration (RADIUS 1 IP: 0.0.0.0, RADIUS 1 DOMAIN, RADIUS 2 IP: 0.0.0.0, RADIUS 2 DOMAIN, AUTH PROTOCOL: CHAP, Secret: secretpassword, NAS\_ID: wisp2\_1, Authentication port: 1812, Accounting port: 1813), Authentication Configuration (UAM Authentication: Enabled, UAM Domain: localhost, UAM Secret, UAM Port: 3990, MAC Authentication: Disabled, MAC Password: password, MAC Suffix), Walled Garden Configuration, and Advertisement Links Configuration. At the bottom right of the configuration area, there are two buttons: 'Exit' and 'Submit'.

Figure 121. HotSpot Wizard Summary Tab

**Submit**

To apply the configuration to the router, click the **Submit** button at the bottom of the **Summary** tab.

**Exit**

Click **Exit** to return to the main HotSpot configuration tab

### 12.6.3 HotSpot Configuration Example

Assume that the user's system is equipped with two Ethernet interfaces and one wireless interface.

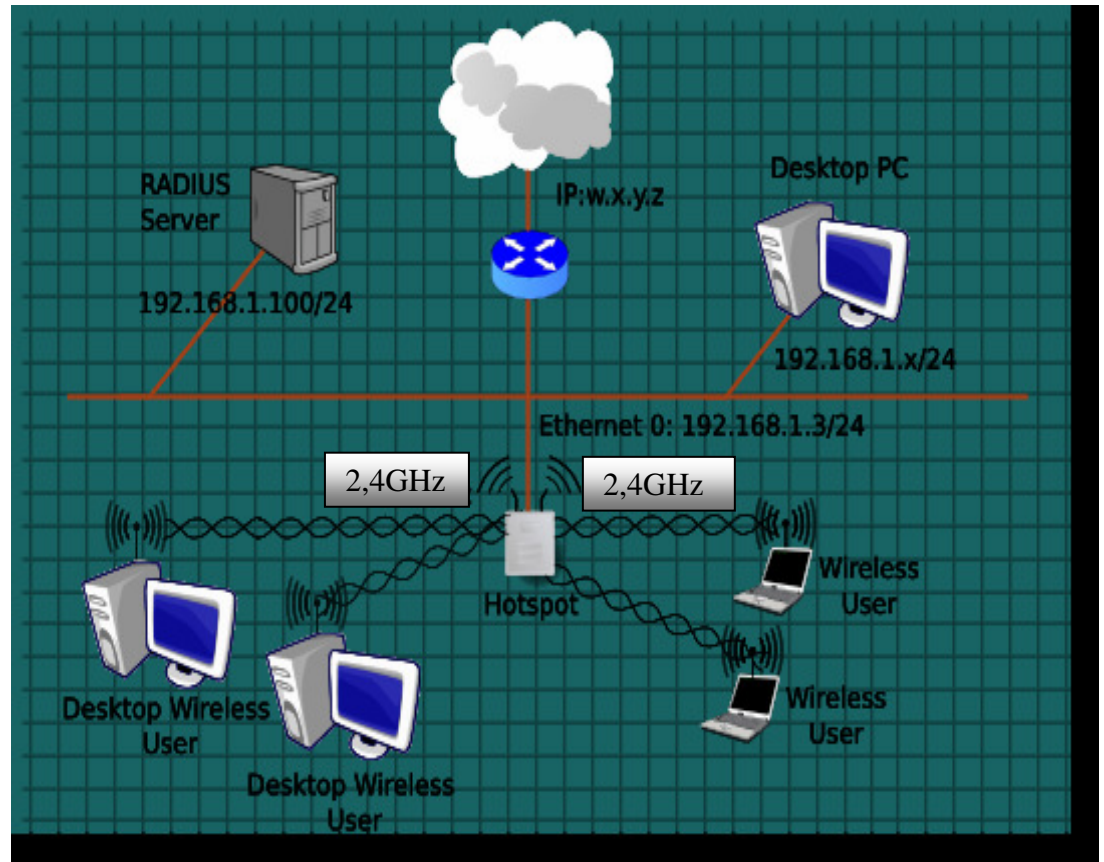


Figure 122. Network Topology-Example

The user is connected to the internet via a router with public IP  $w.x.y.z$ . His/her private IP subnet is  $192.168.1.0/24$ . The router masquerades private IPs to its public IP.

The user must authorize users connected to HotSpots' wireless interface `br_wifi`. This is accomplished by configuring AP One to act as a HotSpot DHCP Server and authenticate users connected to that interface (HotSpot Wireless Interface). The authentication is assumed to be handled by the user's local Radius Server (assume having IP  $192.168.1.100$ ).

Ikarus HotSpot's WAN Interface in that case is `eth0`, the one connected to the router (and Internet). Hotspot users will be assigned with IPs in the subnet  $192.168.4.0/24$ . To sum up, AP One HotSpot should be configured with:

- WAN interface: `eth0`, with static IP  $192.168.1.3/24$

- LAN Interface: br\_wifi
- Gateway: 192.168.1.1 (router's private IP)
- DNS: say 65.173.1.1 (obtained from your internet connection)
- Radius Server: 192.168.1.100 (let radius secret be "secretpassword")
- Dynamic IPs assigned to users: 192.168.4.0/24

Applying this example, network topology will change to:

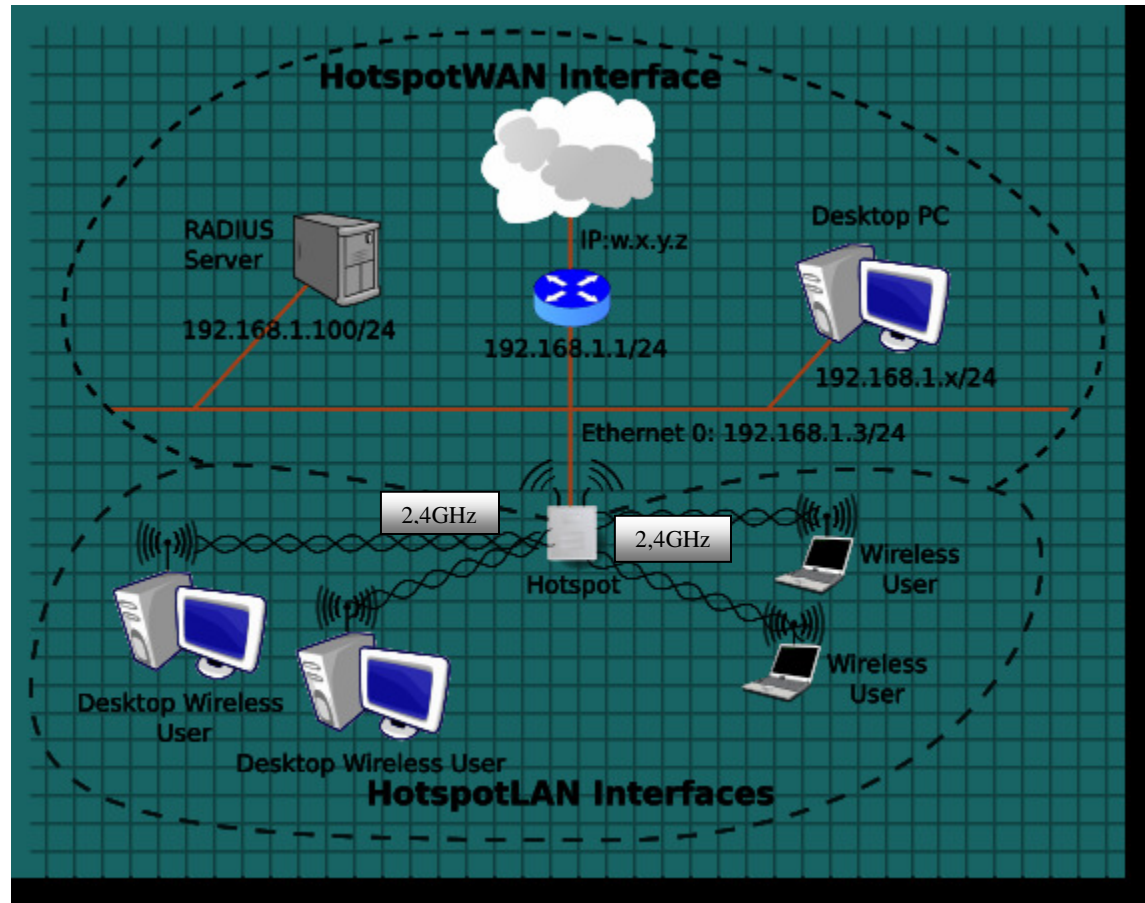


Figure 123. Network Topology-After HotSpot Example

Red lines show the user's LAN (WAN for HotSpot), where there is no authentication performed.

Black dotted lines show the user's public LAN (LAN for HotSpot), where authentication is required.

## HotSpot Configuration Procedure

Select **Advanced Node Configuration** from the **Node Shortcut Menu** in Ikarus NMS. Click the **HotSpot** tab to begin the HotSpot configuration and then click the **Start Wizard** button. The **HotSpot Configuration** pane appears containing several tabs. The **DHCP** tab is on top.

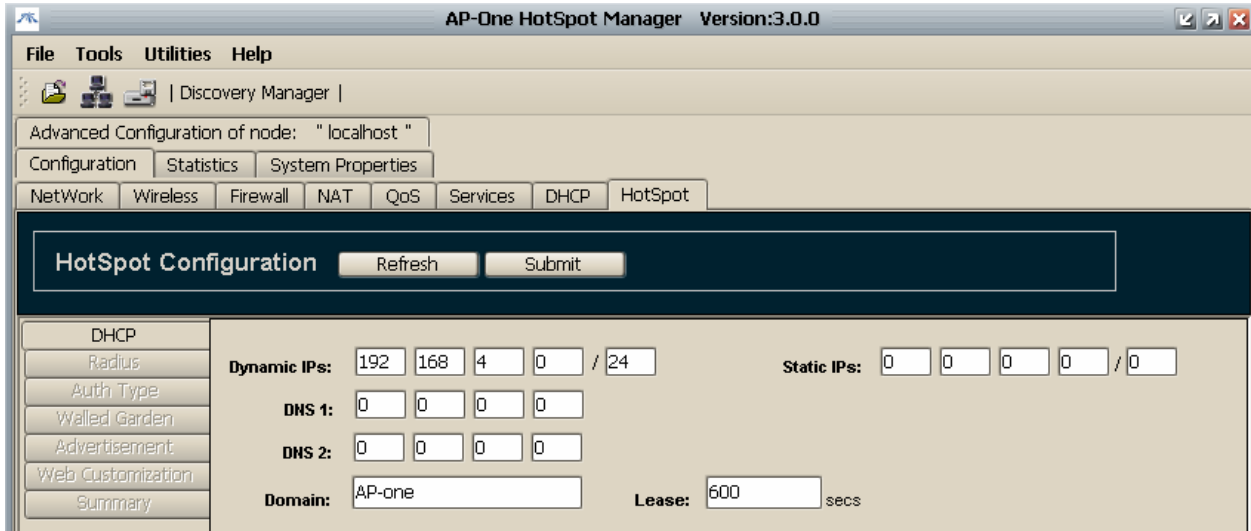


Figure 124. Hotspot DHCP Server's Configuration Example

Configure **DHCP** server settings (IP addresses to be assigned from HotSpot to Users) as follows:

1. In the **Dynamic IPs** field, type: 192.168.4.0 / 24 (24 is the Subnet Mask portion representing 255.255.255.0)
2. In the **DNS 1** field, type: 0.0.0.0 (This will tell it to get AP-One WAN DNS IP)
3. In the **Domain** field type: **domain\_of\_your\_choice**
4. In the **Lease** field, type 600, the lease time for DHCP (in seconds)

Click the **Next** button. The **Radius** tab will appear.

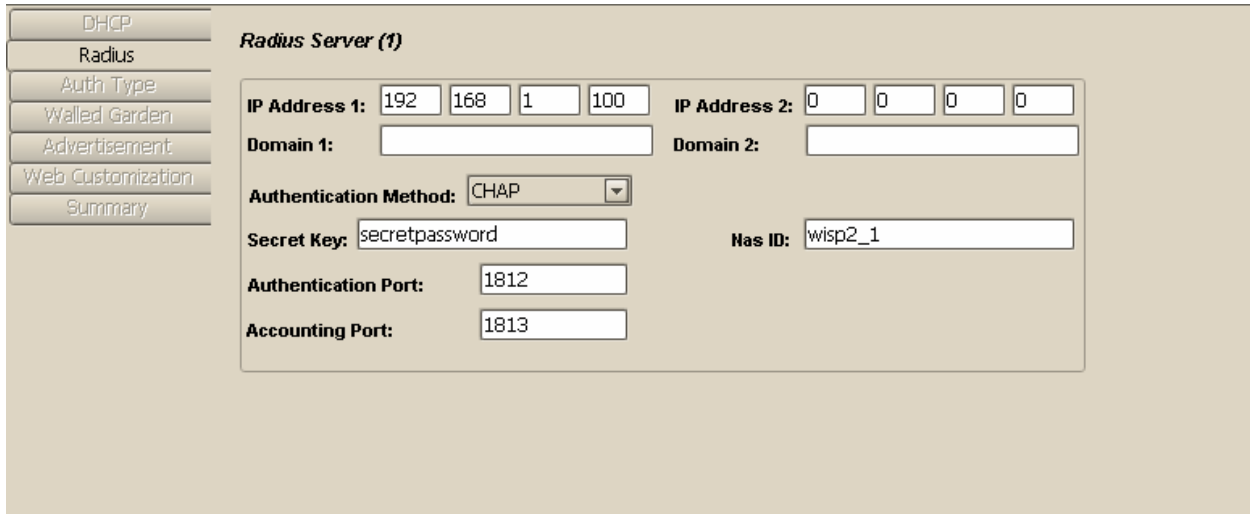


Figure 125. Hotspot Radius Configuration Example

Configure **Radius** settings as follows:

1. In the IP Address 1 field, type: 192.168.1.100
2. In the IP Address 2 field, type: 0.0.0.0 (no backup radius server)
3. In the Authentication Method drop down list, select: CHAP
4. In the Secret Key field, type: secretpassword
5. In the Authentication Port field, type: 1812
6. In the Accounting Port field, type: 1813
7. In the Nas ID field, type : wisp2\_1 (if needed by radius server)

Click the **Next** button. The Auth Type tab will appear.

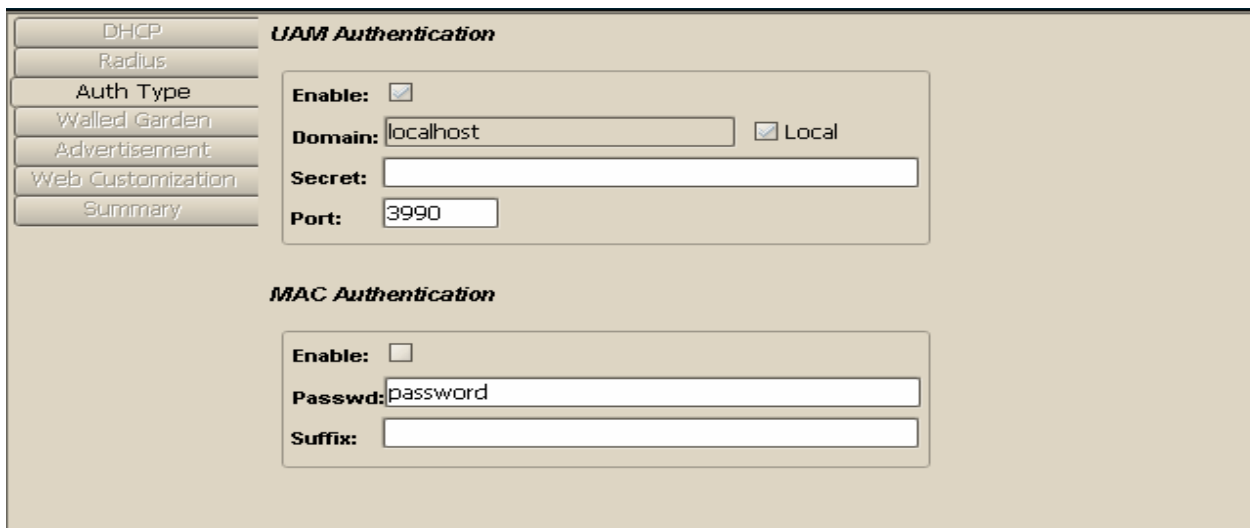


Figure 126. Hotspot Auth Type Configuration Example

Configure **Authentication Type** settings as follows:

In the **UAM Authentication** section, select the **Enable** check box to authenticate users via Web redirection.

Click the **Next** button. The **Walled Garden** tab will appear.

The screenshot shows a web interface for 'HotSpot Configuration'. At the top, there are tabs for 'NetWork', 'Wireless', 'Firewall', 'NAT', 'QoS', 'Services', 'DHCP', and 'HotSpot'. Below the tabs is a dark blue header with the text 'HotSpot Configuration' and two buttons: 'Refresh' and 'Submit'. On the left side, there is a vertical menu with buttons for 'DHCP', 'Radius', 'Auth Type', 'Walled Garden', 'Advertisement', 'Web Customization', and 'Summary'. The 'Walled Garden' button is highlighted. The main content area is titled 'Walled Garden URLs:' and contains five numbered input fields. The first field, labeled '1)', contains the IP address '192.168.1.20'. The other four fields, labeled '2)', '3)', '4)', and '5)', are empty.

*Figure 127. Hotspot Walled Garden Configuration Example*

In the **Walled Garden** tab you can configure domains that a user can access without being authenticated. Configure **Walled Garden** settings as follows:

In the **Walled Garden URLs** box, type 192.168.1.20 into field 1. (For this example, this address is assumed to operate a public web server. A user connected to a HotSpot LAN Interface can then access that address without authentication. ).

Click the **Next** button. The **Advertisement** tab will appear.

The screenshot shows a web interface for configuring Advertisement URLs. On the left, there is a vertical menu with buttons for 'DHCP', 'Radius', 'Auth Type', 'Walled Garden', 'Advertisement', 'Web Customization', and 'Summary'. The 'Advertisement' button is highlighted. The main content area is titled 'Advertisement URLs:' and contains five numbered input fields (1) through (5). Field (1) contains the text 'http://www.antcor.com'. Fields (2) through (5) are empty.

Figure 128 Redirection URL's Configuration Example

In the **Advertisement** tab you can configure domains that a user will be directed to after being authenticated. Configure **Advertisement** settings as follows:

In the **Advertisement URLs** box, type the URL of any Web site. Click the **Next** button. The **Web Customization** tab will appear.

The screenshot shows the 'Web Page Customization' configuration page. At the top, there is a navigation bar with tabs for 'Network', 'Wireless', 'Firewall', 'NAT', 'QoS', 'Services', 'DHCP', and 'HotSpot'. Below this is a 'HotSpot Configuration' section with 'Refresh' and 'Submit' buttons. On the left, there is a vertical menu with buttons for 'DHCP', 'Radius', 'Auth Type', 'Walled Garden', 'Advertisement', 'Web Customization', and 'Summary'. The 'Web Customization' button is highlighted. The main content area shows 'Brand Name: Brand A' and an 'Extra Text' field. Below these are 'Select Color' and 'SelectImage' buttons. A 'Select Background Color' dialog box is open, showing sliders for Red, Green, and Blue, and a preview area with 'Sample Text'.

Figure 129. Web Page Customization Example

In the **Web Customization** tab you can customize the redirection Web page. Configure **Web Customization** settings as follows:

1. In the **Select Background Color** box, set the Red, Green and Blue fields by dragging the controls or changing values in the corresponding spin boxes.

2. In the **Brand Name** and **Extra Text** boxes, type a text message.
  3. Click the **Select Image** button to browse for image files to insert into the Web page.
- Click the **Next** button. The **Summary** tab will appear.



Figure 130. Summarize Configuration Example

Click the **Exit** button. The main **HotSpot** pane appears. Although the configuration has been loaded, Hotspot is not running. (Status field displays: **Stopped**). To complete the procedure:

1. In the **Admin MAC** box, type the administrator’s MAC address. This is recommended to ensure connectivity is not lost with HotSpot in the event of a Radius mis-configuration.
2. Click the **Submit** button to apply the configuration to HotSpot. The original **HotSpot** tab appears.
3. To complete the process, select the **Enable HotSpot** check box. Click the **Submit** button to start HotSpot

To poll HotSpot’s status, click the **Refresh** button. If the **Status** box displays **Initializing**, retry a few minutes later. The **Status** box will display **Running** when initialization is complete. With HotSpot running all changes have been applied to the router.



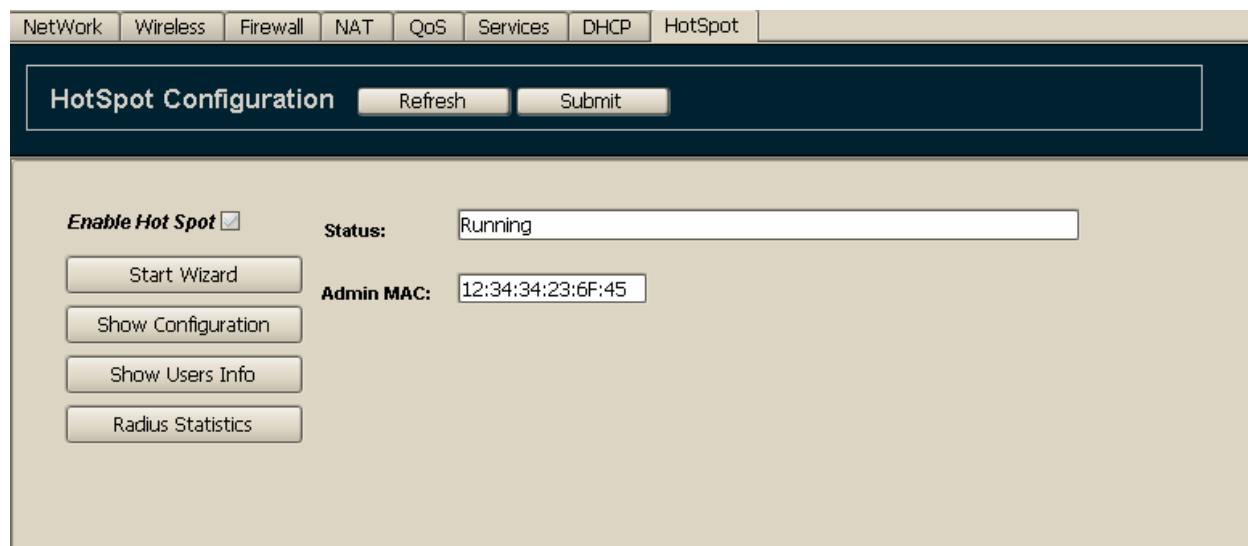


Figure 131. HotSpot is running Example

If a user connects to the HotSpot, it will assign the next free Dynamic IP address.

```
Ethernet adapter Wireless Network Connection 4:
    Connection-specific DNS Suffix . : AP-one
    Description . . . . . : Intel(R) PRO/Wireless 3945ABG Network
k Connection
    Physical Address. . . . . : 00-13-02-BF-79-A4
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.4.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.4.1
    DHCP Server . . . . . : 192.168.4.1
    DNS Servers . . . . . : 10.0.0.1
```

Figure 132. HotSpot has assigned an IP Address Example

If this user now tries to access the Internet, a Redirection Web-page is displayed.

## Troubleshooting

### Cannot set wireless interface configuration

- Check if you have selected channel and ESSID.

### Cannot obtain an IP address

- Check if the Dynamic IP addresses are all allocated by selecting **Show User Info**. If more IP addresses are required, reconsider configuring an extended IP pool for Dynamic IP addresses.

- If MAC authentication is enabled, check if your RADIUS server is operating and has connectivity with the HotSpot, or Radius Settings are right (Secret Key, Ports) .
- Check if Hotspot Status in the Main HotSpot tab is running.

### Obtained an IP address but cannot Ping HotSpot

Check if the user is authenticated.

### A user not authenticated, but can access the Internet

Check if the domain the user has accessed is in the Walled Garden domains.

# 13. Index

---

<b>Access Point</b>	<b>42</b>
<b>5.3.3ACL</b>	<b>49</b>
Allowing Access	50
Denying Access	50
Extracting lists	50
<b>Add</b>	
Firewall	65
Background Image	20
New Node	21
Rule Entries	38
Static Route	36
<b>AES(CCMP)</b>	<b>49</b>
<b>Alias</b>	<b>24</b>
<b>Antenna Options</b>	<b>46</b>
<b>AP Client</b>	<b>47</b>
<b>ARP Table</b>	<b>108</b>
<b>Association List</b>	<b>42</b>
<b>Authentication</b>	
MAC	96
<b>Backend Radius</b>	
Configuration	129
<b>Backup</b>	<b>16, 28</b>
<b>Beacon Period</b>	<b>42</b>
<b>Best Channel</b>	<b>44</b>
<b>BSSID</b>	
Preferred	47
<b>Chains</b>	
Firewall	57
NAT	57
<b>Current Throughput</b>	<b>16, 28, 106</b>
<b>Default Gateway</b>	<b>32</b>
<b>DHCP</b>	
Client	76
Configuration	76

Fields	73
Lease Time Strategies	75
Leases	73
Relay	77
Time Parameters	73
Decline	74
Lease	74
Min Lease	74
Conflict	74
Max Lease	74
Offer	74
<b>Discovery Manager</b>	
Auto Discovery	66
<b>Diversity Options</b>	<b>66</b>
<b>DNAT</b>	<b>68</b>
<b>DNS</b>	
Keep DNS and Gateway	77
Spoofing	66
<b>DNS Address</b>	
DHCP Servers	73
Global Settings	32
<b>Fade Margin</b>	<b>43</b>
<b>Firewall</b>	<b>57</b>
Chains	57
Examples	68
Matching Fields	59
<b>Global Settings</b>	<b>32</b>
<b>Hide ESSID</b>	<b>45</b>
<b>HTTP</b>	<b>101</b>
<b>ICMP</b>	<b>110</b>
<b>Idle Time</b>	<b>44</b>
<b>Inactivity Limit</b>	<b>42</b>
<b>Interface</b>	
Select/Disable	32
<b>IP Address</b>	<b>31</b>
<b>IP Address</b>	
Remote Peer	32

---

<b>IP Forwarding</b>	<b>32</b>
<b>IP Networking</b>	
Configuration	32
<b>IP settings</b>	<b>31</b>
<b>Link Distance</b>	<b>51</b>
<b>MAC</b>	<b>97</b>
Address	32, 66
Spoofing	32
<b>MRTG</b>	<b>115</b>
<b>NAT</b>	
Chains	57
Matching Fields	65
Rules	64
<b>Network Interfaces Tree</b>	
Using	31
<b>Node</b>	
Add	18
Status Window	17, 14
Advanced	15
Connectivity Settings	20
Moving/Resizing Icons	18
Save	22
Shortcut Menu	15, 22
<b>Noise Level</b>	<b>43</b>
<b>NTP</b>	<b>103</b>
<b>Open Connections List</b>	<b>109</b>
<b>Outdoor Settings</b>	
Configuration	40
Link Distance	40
<b>Packet Statistics</b>	<b>107</b>
<b>Pairwise Cipher</b>	<b>49</b>
<b>Password</b>	<b>104</b>
<b>Pinging</b>	<b>110</b>
<b>Point to Point Links</b>	<b>54</b>
<b>PPPoE Client</b>	<b>77</b>
<b>PPTP Client</b>	<b>33</b>

<b>Profiles</b>	
Saving and Loading	22
<b>PSK</b>	<b>49</b>
<b>Radio</b>	
Channels and Frequencies	46
Configuration	45
MAC Address	46
Physical Layer	45
Transmission Rates	45
<b>Reboot</b>	<b>16, 29</b>
<b>Routers</b>	<b>86</b>
<b>Routing</b>	
Modifying	37
Removing	37
Repositioning	37
Static	37
Tables	35
<b>Rules</b>	
NAT	63
<b>Security</b>	
Access Control Lists	49
Configuration	47
WEP	47
WPA	47
<b>Signal Level</b>	<b>47</b>
<b>Site Survey</b>	<b>49</b>
Align	50
Continuous Scan	49
Operation	49
<b>SNAT</b>	<b>67</b>
<b>SNMP</b>	<b>100</b>
<b>SSH</b>	<b>102</b>
<b>SSID</b>	<b>44</b>
Preferred	44, 56
<b>State and Link Quality</b>	<b>47</b>
<b>Status</b>	
Info Dialog Box	106

---

<b>Stealth Mode</b>	<b>44</b>
<b>Stop Traffic</b>	<b>45</b>
<b>Subnet</b>	<b>31</b>
Backend Radius Fields	129
DHCP Server Fields	72
Discovery Manager Fields	46
Firewall Matching Fields	59
NAT Matching Fields	65
<b>System Properties</b>	<b>25,113</b>
<b>System Services</b>	
Configuration	99
<b>Table View</b>	<b>33</b>
<b>Throughput</b>	<b>106</b>
<b>TKIP</b>	<b>49</b>
<b>Trace Route</b>	<b>110,111</b>
<b>Transmission Rate</b>	<b>45</b>
<b>Transmitted Power</b>	<b>46</b>
<b>Type</b>	
Node	19
<b>Upgrade</b>	
Firmware	16
<b>Utilities</b>	<b>110</b>
<b>WDS</b>	<b>45</b>
<b>WEP</b>	<b>47, 130</b>
<b>WINS</b>	
Servers	75
<b>Wireless</b>	<b>46</b>
Point to Point Links	45
Setting Modes	41
<b>WPA</b>	<b>48</b>

