

Outdoor Router P-380

Users Guide

Revision 1.0

November, 2002



Copyright © 2002 Gemtek Systems Holding BV
www.gemtek-systems.com

1 Before You Start

1.1 Notice

Gemtek Systems Holding BV reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Gemtek Systems Holding BV shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Gemtek Systems Holding BV

1.2 Trademarks

The product described in this book is a licensed product of Gemtek Systems Holding BV.

Microsoft, Windows 95, Windows 98, Windows Millennium Edition, Windows NT, Windows 2000, Windows XP, and MS-DOS are registered trademarks of the Microsoft Corporation.

Novell is a registered trademark of Novell, Inc.

Mac OS is a registered trademark of Apple Computer, Inc.

Java is a trademark of Sun Microsystems, Inc.

Wi-Fi is a registered trademark of the Wi-Fi Alliance.

All other brand and product names are trademarks or registered trademarks of their respective holders.

1.3 National Radio Regulations



Please note:

The usage of wireless network components is subject to national and or regional regulations and laws.

Administrator must ensure that they select the correct radio settings according to their regulatory domain. Refer to the regulatory domains chapter in the appendix to get more information on regulatory domains. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values!

Channel and output power settings may be modified by experienced service personnel only!

2 Table of Contents

1	BEFORE YOU START	3
1.1	Notice.....	3
1.2	Trademarks.....	3
1.3	National Radio Regulations	3
2	TABLE OF CONTENTS	5
3	ABOUT THIS GUIDE.....	7
3.1	Purpose	7
3.2	Prerequisite Skills and Knowledge	7
3.3	Conventions Used in this Document	7
3.4	Help Us to Improve this Document!.....	7
3.5	Gemtek Systems Technical Support	8
4	INTRODUCTION	9
4.1	Overview.....	9
4.2	Operating Modes	11
4.3	System Requirements	15
5	HARDWARE AND SOFTWARE INSTALLATION	16
5.1	Overview.....	16
5.2	Scope of Delivery.....	16
5.3	Hardware Introduction	16
5.4	Hardware Installation.....	17
5.5	Software Installation	18
5.6	Find Your New P-380!	19
5.7	Modifying the Network's IP Address Space	20
5.8	Reset to Factory Defaults	21
6	SYSTEM CONFIGURATION USING HTML INTERFACE	22
6.1	Overview.....	22
6.2	Log In.....	22
6.3	Device Status.....	24
6.4	Setup Wizard	25
6.5	Advanced Settings.....	31
6.6	System Tools.....	36
7	SYSTEM CONFIGURATION USING COMMAND LINE INTERFACE.....	43
7.1	Overview.....	43
7.2	Login	43
7.3	Show	44
7.4	Configure	44
7.5	The Defaults Command.....	45
7.6	The Exit Command	45
7.7	The Reboot Command	45
8	APPENDIX.....	46
8.1	Regulatory Domains	46
8.2	CLI Configuration Commands and Parameters	47
8.3	Menu Items by Operating Mode	54
8.4	Device Configuration Default Values.....	56
8.5	P-380 Specification.....	58
9	GLOSSARY.....	62

10 INDEX 66

3 About this Guide

3.1 Purpose

This document provides information and procedures on hardware installation, setup, configuration, and management of the Gemtek Systems Operator Access Point P-380.

3.2 Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium Edition, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

3.3 Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:



Very important information. Failure to observe this may result in damage!



Important information that should be observed.



Additional information that may be helpful but which is not required.

bold	Menu commands, buttons and input fields are displayed in bold
<code>code</code>	File names, directory names, form names, and system-generated output such as error messages are displayed in constant-width type
<value>	Placeholder for certain values, e.g. user inputs
<i>note</i>	Comments or hints

3.4 Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to: manuals@gemtek-systems.com

3.5 Gemtek Systems Technical Support

If you encounter problems when installing or using this product, please consult the Gemtek Systems website at

<http://www.gemtek-systems.com>

for

- The latest software, user documentation and product updates.
- Frequently Asked Questions (FAQ).
- Direct contact to the Gemtek Systems support centers.

4 Introduction

Thank you for choosing the Gemtek Systems P-380 Operator Access Point.

This manual will give you a short introduction to the device and its hardware and show you how to install and set up the P-380.

4.1 Overview

Wireless Router and Access Point with Rugged Housing for Outdoor Applications

The Gemtek Systems P-380 Outdoor Router provides quality connectivity for Wi-Fi networks. The device is ideal for rough environments and outdoor applications.

Multiple Operating Modes

It can be configured in five different operating modes. As an inter-building wireless bridge it connects two wired networks on MAC address level. In router mode it can connect different IP subnets and in access point mode it connects wireless clients to a wired network. In client bridge or client router mode it connects a client PC or a workgroup to another WLAN Access Point..

Wi-Fi Compliant to Ensure Network Compatibility

Tested for interoperability with the Wi-Fi standard, the P-380 will support all Wi-Fi certified client devices; the global industry-standard for wireless networking.

High Performance for Maximum Coverage

Designed to support large areas, this AP combines high receiver sensitivity and proven antenna technology to maximize coverage.

Long Range

The P-380 can be ordered with an integrated high-gain antenna (P-380A), or with a connector (reverse N) for an external antenna (P-380N). With the integrated 10dBi directional antenna (40° beam width) two P-380A routers can connect at a distance of up to five kilometers.

Routing

Connecting two different networks via a wireless link is the job of a wireless router. A router can connect different networks (subnets) and minimizes the data transfer over the wireless link. One P-380 can connect up to eight different networks in a point-to-multipoint configuration.

Bridging

When protocols other than TCP/IP need to be transmitted, the P-380 can be configured as a layer 2 bridge. With no license required for wireless bridges in the 2.4 GHz band, in almost every part of the world, the P-380 can be a cost effective alternative to leased-lines for line-of-sight connections.

Access Point

The P-380 can also be a Wi-Fi access point for environmentally challenged locations like industrial plants, or when an outdoor installation can better serve the application. The weatherproof housing has a NEMA classification of IP66, and incorporates a temperature control system to support operation from -20° to +65°C.

Install and forget

A bright LED display of signal strength enables simple installation optimization. A Power over Ethernet client, the P-380 is supplied data and power over one cable, allowing remote power resets, thereby eliminating the need for any on-site-maintenance.

Installation and Set Up

The P-380 is very easy to install and set up. The Power-over-Ethernet connection additionally reduces mounting and maintenance efforts.

Management

Device management is provided through a secure web-based interface (HTTPs), a CLI (Command Line Interface), and SNMP (Simple Network Management Protocol). You can use any of these management interfaces to view and adjust the parameter settings of the P-380. Device management and firmware upgrade can be done remotely.

P-380 Features

- IEEE 802.11b Wi-Fi Access Point
- WLAN router mode, access point mode, bridge mode or client mode (configurable)
- Weather proof and rugged housing
- Wall or mast mount kit included (for both applications)
- Operating temperature range from -20°C to $+65^{\circ}\text{C}$
- Integrated or external antennas
- 64/128-bit WEP security on wireless transmissions
- Layer 2 User Isolation
- 10/100 Mbps Base-T RJ-45 Ethernet port
- Power-over-Ethernet support
- 11Mbps, 5.5Mbps, 2Mbps, and 1Mbps auto-fall-back
- Management via HTTPs, Telnet, SSH, and SNMP
- Easy to use web-based management, including remote management and remote software upgrades and web configuration wizard
- Performance Monitoring
- Integrated Site Survey

4.2 Operating Modes

The P-380 can work in different operating modes:

- bridge
- access point (AP)
- AP router
- client router
- client bridge

Even if a P-380 is connected to a wired network on one side and to a wireless network on the other side in all operating modes, there are some significant differences. The operating modes differ from each other by the possibilities to connect single or multiple stations in the same or in different IP subnets:

- How many wireless connections are allowed?
- How many wired connections are allowed?
- Are connections possible between different IP subnets?
- Which IP addresses are used by the device?
- To which wireless types can the P-380 connect remotely?
- Is the wired network or the wireless network supposed to be the local area network (LAN)?

The last point is a key for understanding the IP settings including DHCP settings, IP masquerading or network address translation (NAT) and IP routing. The terms LAN and WAN depend on the devices operating mode.

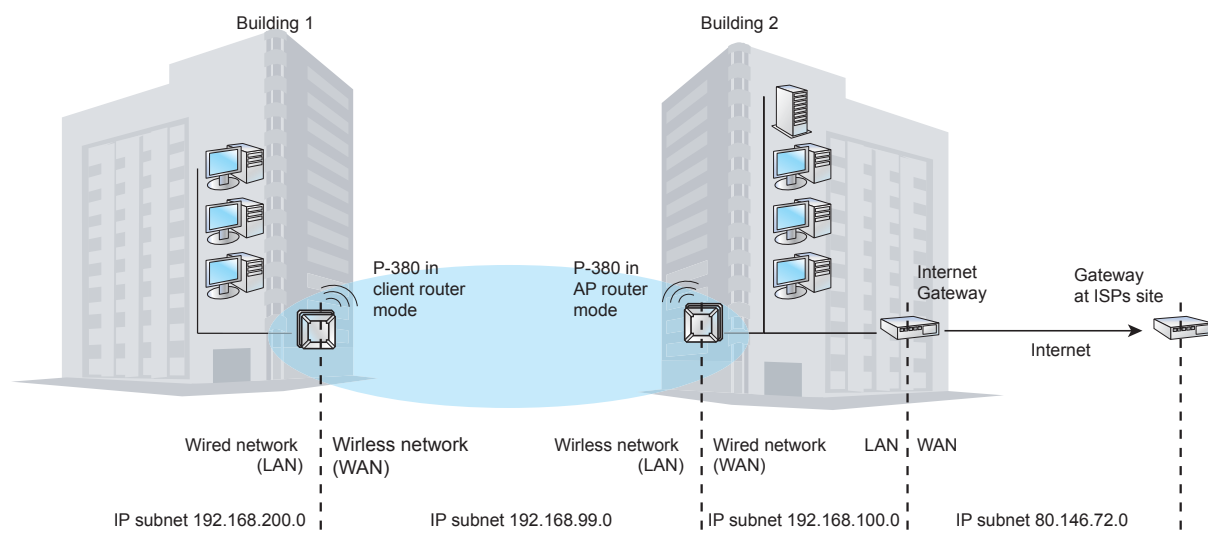


Figure 1 – Meaning of LAN and WAN in a P-380 topology

In the figure shown above we connect a subnet 192.168.200.0 in building 1 using a P-380 in client router mode and a P-380 in AP router mode to a subnet 192.168.100.0 in building 2. On the client routers side, the wired stations build his local network LAN, the wireless subnet 192.168.99.0 therefore must be the WAN. On the other hand the AP router assumes his wired network to be the WAN, where it can find an internet gateway. In this case, the wireless network builds up the AP routers LAN. Going one step further, the internet gateway in the companies building 2 will take the wired network 192.168.100.0 for LAN and the ISPs subnet for WAN.

The following sections will give a short introduction in each of the operating modes.

4.2.1 Bridge Mode

In bridge mode the P-380 connects two or more wired networks, for example networks in different buildings with no wired connections. On both sides of the connection you need a P-380 in bridge mode. In this case, the P-380 acts as a network bridge between wireless and wired networks. All data received by the P-380 on its wireless or Ethernet interface is broadcast on the wireless interface to all connected devices that are authorized in the ACL (access control list). In bridge mode the P-380 can connect up to seven remote networks.

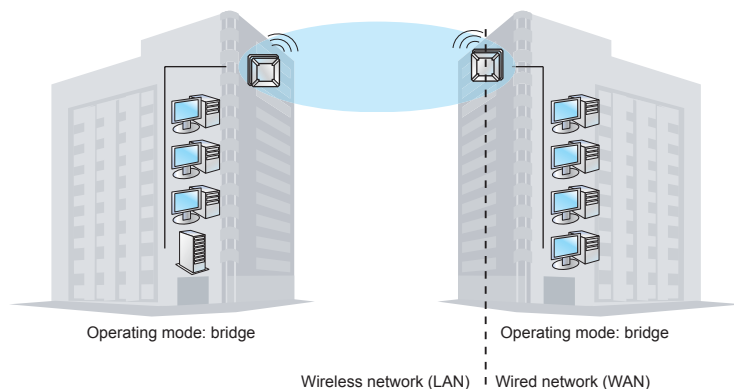


Figure 2 – Bridge mode

4.2.2 Access Point Mode (AP Mode)

In AP mode it can connect multiple wireless client stations to a wired network. In this mode P-380 can be used as an Operator Access Point for outdoor hot-spots. Wireless client stations can be mobile like notebook or fixed like a P-380 in client router mode.

Like in the bridge mode all data received by the P-380 on its wireless or Ethernet interface is broadcast on the wireless interface to all connected devices that are authorized in the ACL (access control list). It is still working as a network bridge (OSI Layer 2) between wireless and wired networks, but in difference to the bridge mode it allows access to multiple client stations.

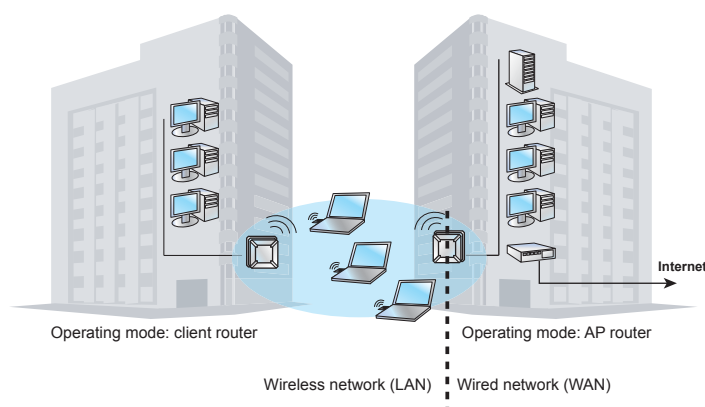


Figure 3 – AP mode

4.2.3 AP Router Mode

In AP router mode, the P-380 Outdoor Router can connect different IP subnets. Hence it does not bridge all data between Ethernet and wireless interface but only the data intended for the connected IP network.

As in AP mode, the P-380 in AP router mode allows access for multiple wireless stations like mobile stations and P-380 devices in client router or in client bridge mode. In this mode, the P-380 provides the full range of features including DHCP server, network address translation (NAT), firewall functions and port forwarding.

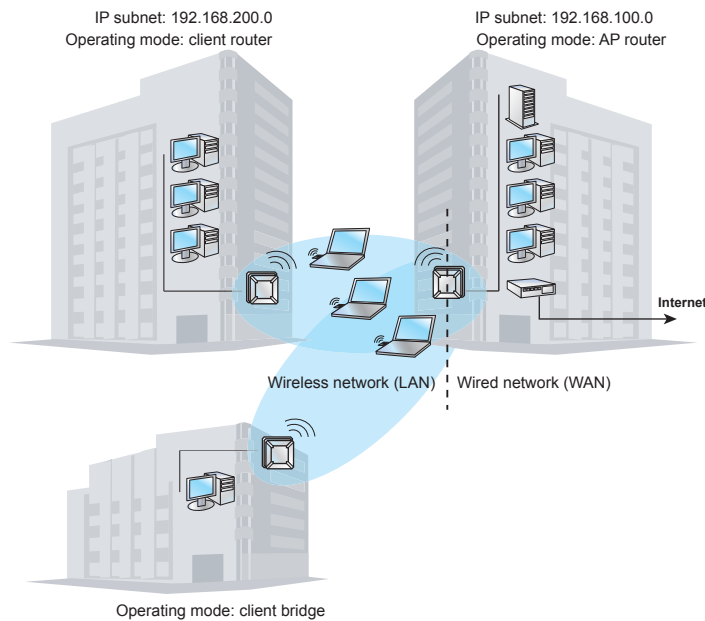


Figure 4 – AP router mode

In this mode, the P-380 is part of two networks in his router function. On the one side it is connected to a wireless network, where it provides DHCP services for example and which is called the LAN side. On the other side it is connected to the wired network, where it may find a gateway to the internet and which is called the WAN side.

4.2.4 Client Bridge Mode

In client bridge mode, the P-380 acts as an wireless client (or station). It can connect a single computer to a wireless access point only. As far as user isolation is enabled in the access point, no connection between P-380 in client bridge mode an other wireless stations connected to the same access point is possible.

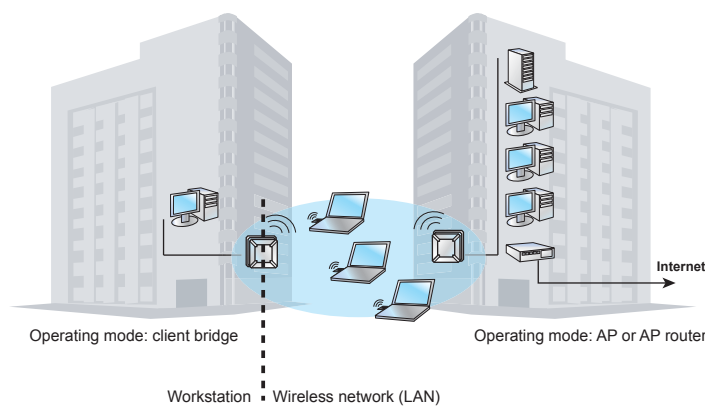


Figure 5 – Client bridge mode

Since the P-380 acts as a wireless network card in this mode, it assumes that the local network (LAN) can be found on its wireless side. So LAN in this operating mode doesn't mean the connection between P-380 and workstations, but rather the wireless network in which the P-380 is one client beside others.



Note: For selecting the client bridge mode upload the client firmware from the P-380 product CD first.

4.2.5 Client Router Mode

In client router mode, the P-380 acts as an wireless client (or station). But in difference to the client bridge mode it can connect a whole IP subnet to a wireless access point. The P-380 in client router mode can connect to a single remote access point only.

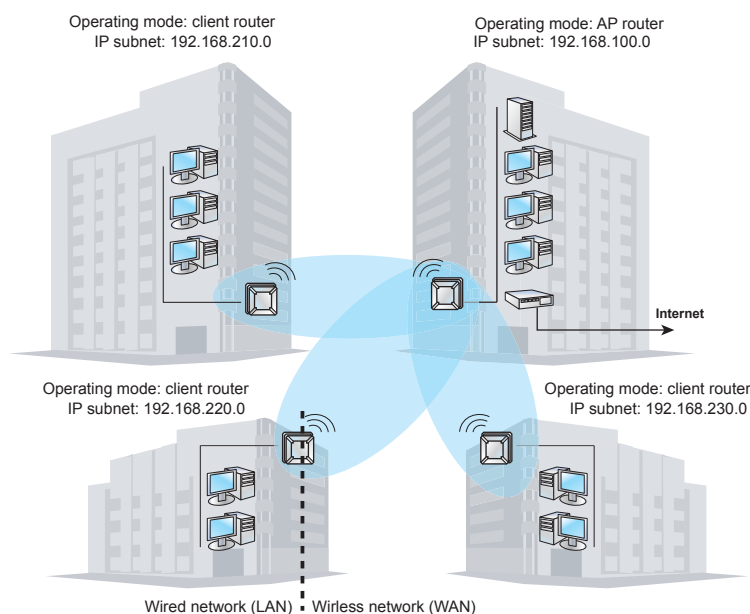


Figure 6 – Client router mode

In this mode, the P-380 is part of two networks in his router function. On the one side it is connected (wired) to his own network, the LAN. Anything outside the LAN must be the WAN, and can be found on its wireless side. So the LAN IP of a P-380 in client router mode is the IP on its wired interface, the WAN IP is the one on the wireless interface.



Note: For selecting the client bridge mode upload the client firmware from the P-380 product CD first.

4.2.6 Comparison of the Operating Modes

The following table provide a short overview about the features of the different operating modes:

	AP	Bridge	AP Router	Client Bridge	Client Router
Wireless connections	Multiple	Multiple	Multiple	Single	Single
Wired connections	Multiple	Multiple	Multiple	Single	Multiple
Wireless Remote Types	WL Clients, AP Router, Client Router, Client Bridge	Bridge	WL Clients, Access Point, AP Router, Bridge, Client Router, Client Bridge	Access Point, AP Router	Access Point, AP Router
IP addresses	WAN (wired)	WAN (wired)	WAN (wired), LAN (wireless)	WAN (wireless)	WAN (wireless), LAN (wired)
DHCP server	not available	not available	Assigns IP to wireless network	not available	Assigns IP to wired network
DHCP client	Receives IP from wired network	Receives IP from wired network	Receives IP from wired network	Receives IP from wireless network	Receives IP from wireless network
NAT	not available	not available	Hides wireless stations to wired network	not available	Hides wired stations to wireless network
Routing between different IP subnets	no	no	yes	no	yes

Figure 7 – Operating modes table

4.3 System Requirements

The management of the P-380 is independent from your operating system. Windows operating systems are required only for using the AP search and AP upgrade tools. For HTTPS management you will need a Java and JavaScript enabled HTML browser with SSL support (e.g. Internet Explorer, Netscape, Opera).

5 Hardware and Software Installation

5.1 Overview

This chapter includes the following sections:

- Package content
- Hardware introduction
- Hardware installation
- Software installation and first access to the device

5.2 Scope of Delivery

Please ensure that the package is complete before beginning with the installation. The package should include the following components:

- Outdoor Access Point P-380
- Mounting kit for wall or mast mount
- Twisted Pair LAN cable adapter
- CD-ROM containing software and documentation
- This manual



Note: There is no Power supply included in the standard package. P-380 can be used with E-110 Single Port PoE Adapter or E-810 8-Port PoE Switch.

5.3 Hardware Introduction

On the right side of the P-380 Operator Access Point you will find the LEDs.

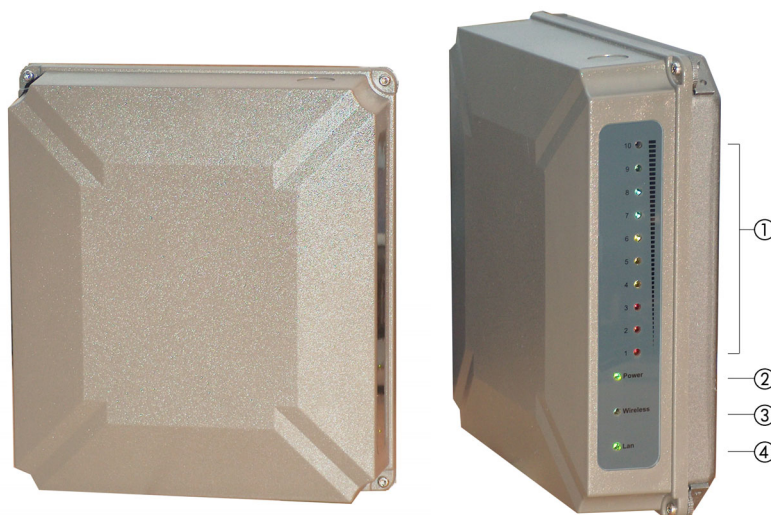


Figure 8 – P-380 LEDs

1. Signal strength LEDs (1 to 10)
These LEDs show the strength of the wireless signal received by the antenna (in client modes only). No 1 to 3 show a very poor signal in red, no 4 to 6 show a average signal in yellow and no 7 to 10 will show an excellent signal in green.

2. Power LED
Off: Power supply connection not available or broken
On: Power supply connection OK
3. Wireless activity LED
Off: no activity
Blinking: sending and receiving data
4. LAN link LED
Off: No LAN connection available
On: LAN connection OK

5.4 Hardware Installation

5.4.1 Installing the Access Point

1. Assemble part ① of the mount kit at the back of the case as shown in the following figure.

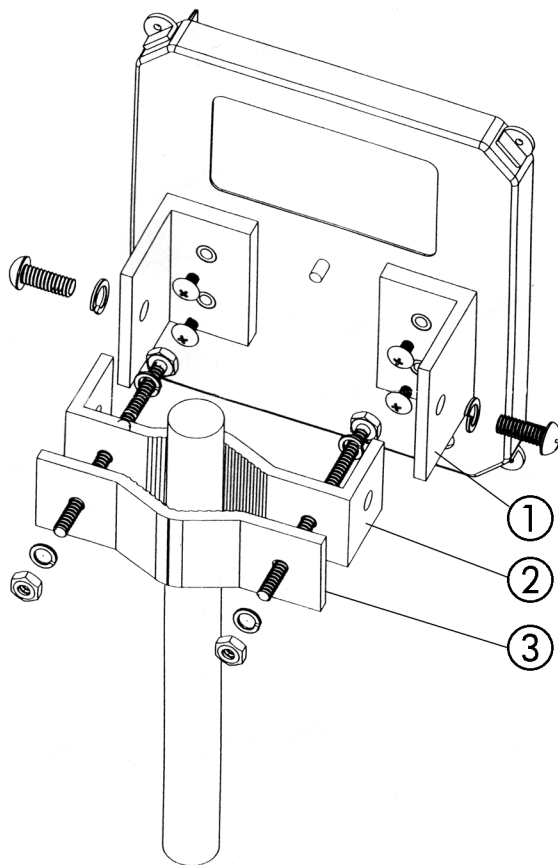


Figure 9 – Assembling the P-380 mount kit to the back of the case

2. If you are mounting the Access Point on a wall, first install the bracket ② of the mounting kit to a suitable position. Assemble the back of the P-380 case to the bracket subsequently.
3. If you are mounting the Access Point to a pole, first install the bracket ② and the clip ③ of the mounting kit to a stout pole. Assemble the back of the P-380 case to the bracket subsequently.
4. Insert the twisted pair LAN cable to a Power-over-Ethernet socket. At least the power LED and the LAN link LED should light up.

5.4.2 Connect to the Power Source and the Local Network

1. Connect the Ethernet cable from the P-380 outdoor router to a IEEE 802.3af compliant PoE hub (48V DC) (Power-over-Ethernet, E-110 PoE Single Port Adapter or E-810 8-Port Switch) labeled P-LAN OUT.
2. Connect a twisted pair Ethernet cable from the LAN-IN port of the PoE Adapter to a free port on the hub or switch within the local network.

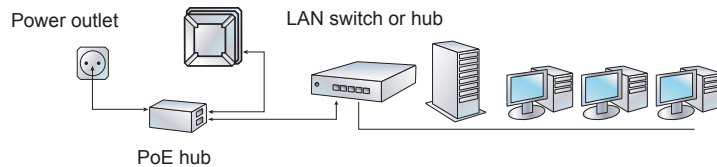


Figure 10 –Connecting P380 to the power source and to the network

5.4.3 Adjusting the P-380 for Best Reception

1. Adjust the orientation of the antenna to get the maximum range. The signal strength LEDs of the P-380 will show you the best position of the P-380 in client bridge or client router mode.
2. Secure the unit in the position.



You will need to adjust the antennas for inter-building bridge configurations only. Exact orientation of the antennas is particularly important for long-distance inter-building links. For more information please refer to the P-380 Specification section.

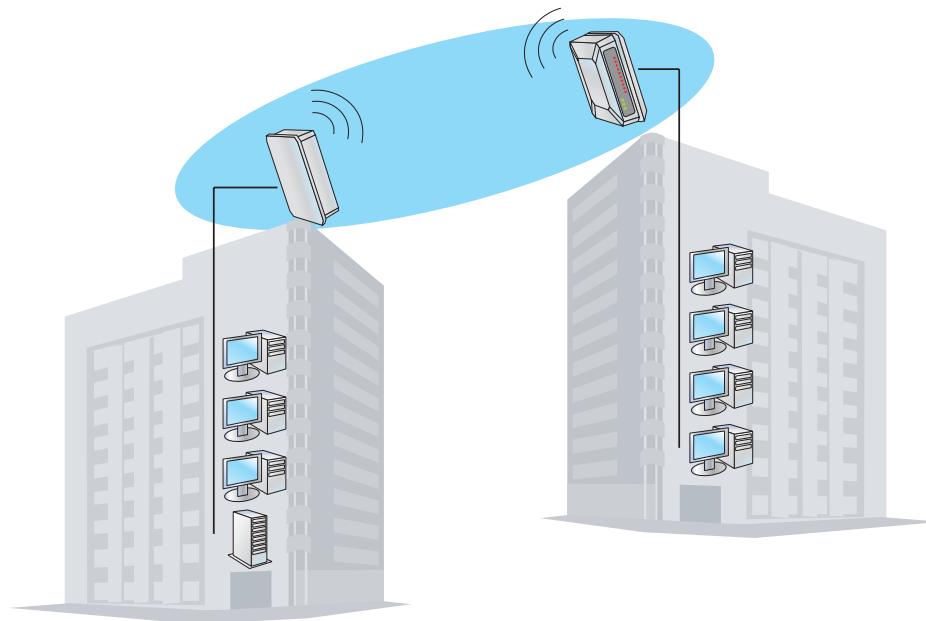


Figure 11 – Adjusting P-380 for best reception

5.5 Software Installation

Software is needed for setup and management of the P-380 Operator Access Point.

In general, there are four different ways to access the device for configuration:

- Windows applications: AP search and AP upgrade
- Standard HTML browser (Java and JavaScript enabled)
- CLI (command line interface) via telnet or SSH client

- SNMPv1 or SNMPv2

Insert the installation CD delivered with the P-380 into your CD-ROM drive

The installation wizard starts automatically and will guide you through the rest of the installation process. If the installation wizard does not start automatically, please run "autorun.exe" from the root directory of the installation CD.

5.6 Find Your New P-380!

To find your new P-380 Operator Access Point you will need to connect the AP to the same logical IP network as your PC. The standard IP address of the P-380 in factory default status is **192.168.2.2**. To access the P-380 in its default configuration you will need to use one of the following IP settings in your network:

- IP address space 192.168.x.x
- Subnet mask 255.255.0.0

If are not using one of these IP address spaces you will either need to switch your network settings to these values or set the P-380's IP address to a free IP address in your current network.

5.6.1 Test: Calling P-380 with Ping

To test the accessibility of your P-380 from your PC, just type the following from a command prompt:

```
ping 192.168.2.2
```

If you get an answer like:

```
Reply from 192.168.2.2: Bytes=32 Time=7ms TTL=255
```

you can access the P-380 from this PC.

If the answer is more like:

```
Request time limit exceeded.
```

there is a problem accessing the P-380 in default status from this PC. You should either change the IP address of your PC or of the P-380.

5.6.2 Setting the P-380 IP Address

You can change the P-380's IP address using the Gemtek Systems AP Search tool.

1. Click Start > Programs > Gemtek Systems > AP Search to launch the application.
2. Enter the MAC (Media Access Control) address of your P-380 into the specified field on the bottom left corner of the window. You will find the MAC address label on the rear of the housing.
3. Enter a free IP address (e.g. 10.0.0.3) in your network into the "IP to set" field.



If you are not sure whether the selected IP address is free or not, first check it from a command prompt with "ping 10.0.0.3". If you get a positive answer, the IP address is already in use! If you need more information about the address space used in your network, get your IP configuration with "ipconfig" (Win 2000, Win NT and Win XP) or "winipcfg" (Win 9x and Win Me) from the command prompt.

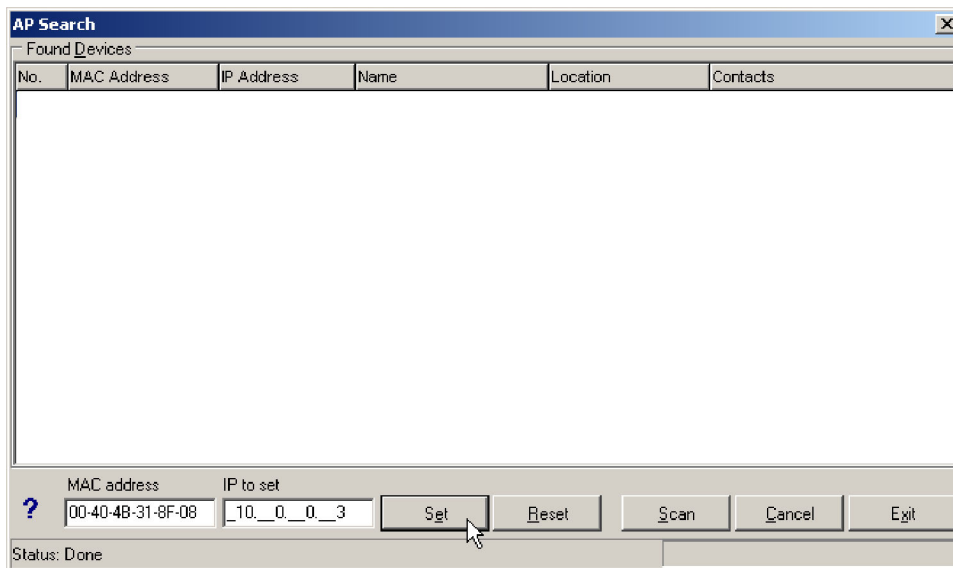


Figure 12 – Setting IP address with AP search (1)

4. After confirming the change the IP address will be set to the new value and the AP will appear in the list after a new search:

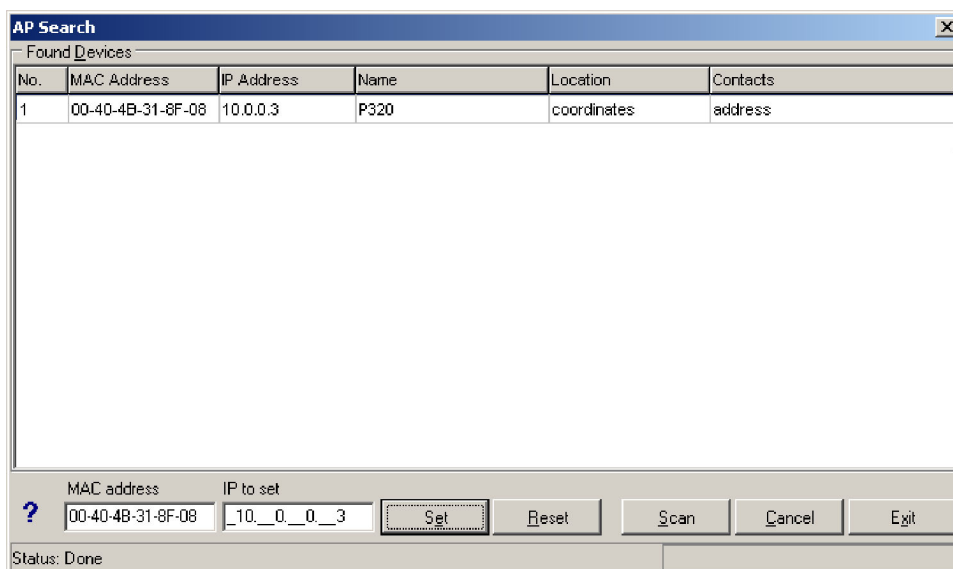


Figure 13 – Setting IP address with AP search (2)



Note: Double-clicking an item in the list will launch the web browser for configuration via HTTPs.

5.7 Modifying the Network’s IP Address Space

If you don’t want to change the P-380 IP address, you can change the IP settings of your network to the required values. If you are using a DHCP server, set the available IP address pool to:

- 192.168.2.x with a subnet mask of 255.255.255.0 or
- 192.168.x.x with a subnet mask of 255.255.0.0

After rebooting the PCs, you should find PCs as well as the P-380 within one logical network.

5.8 Reset to Factory Defaults

If you have configured your device in a way, that you cannot get access via browser or CLI to modify parameters, you can set the device back to factory defaults using the AP Search tool.

1. Enter the MAC (Media Access Control) address of your P-380 into the specified field on the bottom left corner of the window. You will find the MAC address label on the rear of the housing.
2. Enter the IP address into the "IP to set" field.
3. Click the **Reset** button. The AP Search tool will now find the device and set it back to factory defaults.



Note: Keep in mind that resetting the device is an irreversible process.

*During the **first five minutes** after reboot there is no admin password required for reset-to-factory-default or IP set.*

6 System Configuration Using HTML Interface

6.1 Overview

This chapter describes the configuration of the P-380 Outdoor Router using a standard web browser (Java and JavaScript enabled). The chapter is divided into the following sections:

- System status
- System setup
- Advanced settings
- System tools

6.2 Log In

To log in to the P-380 configuration interface, launch your browser and connect to <https://192.168.2.2>, where 192.168.2.2 is the default IP address of your P-380. The network identification dialogue appears:

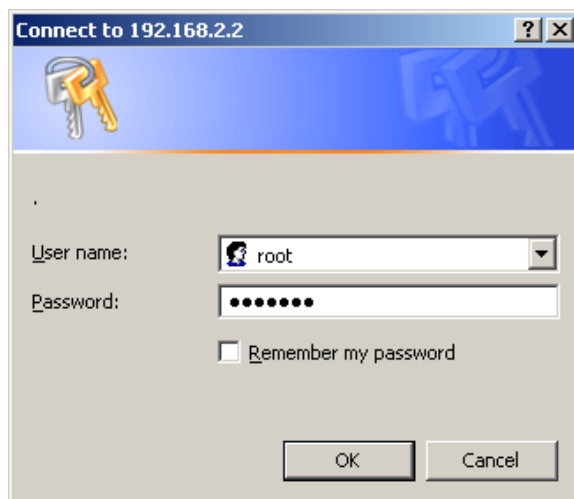


Figure 14 – Log in to HTML configuration

Use **root** as the user name and **pass** as the password. The username is fixed and cannot be changed, the password can be changed later on in the advanced settings menu.

After successful log-on, the following user interface is displayed.

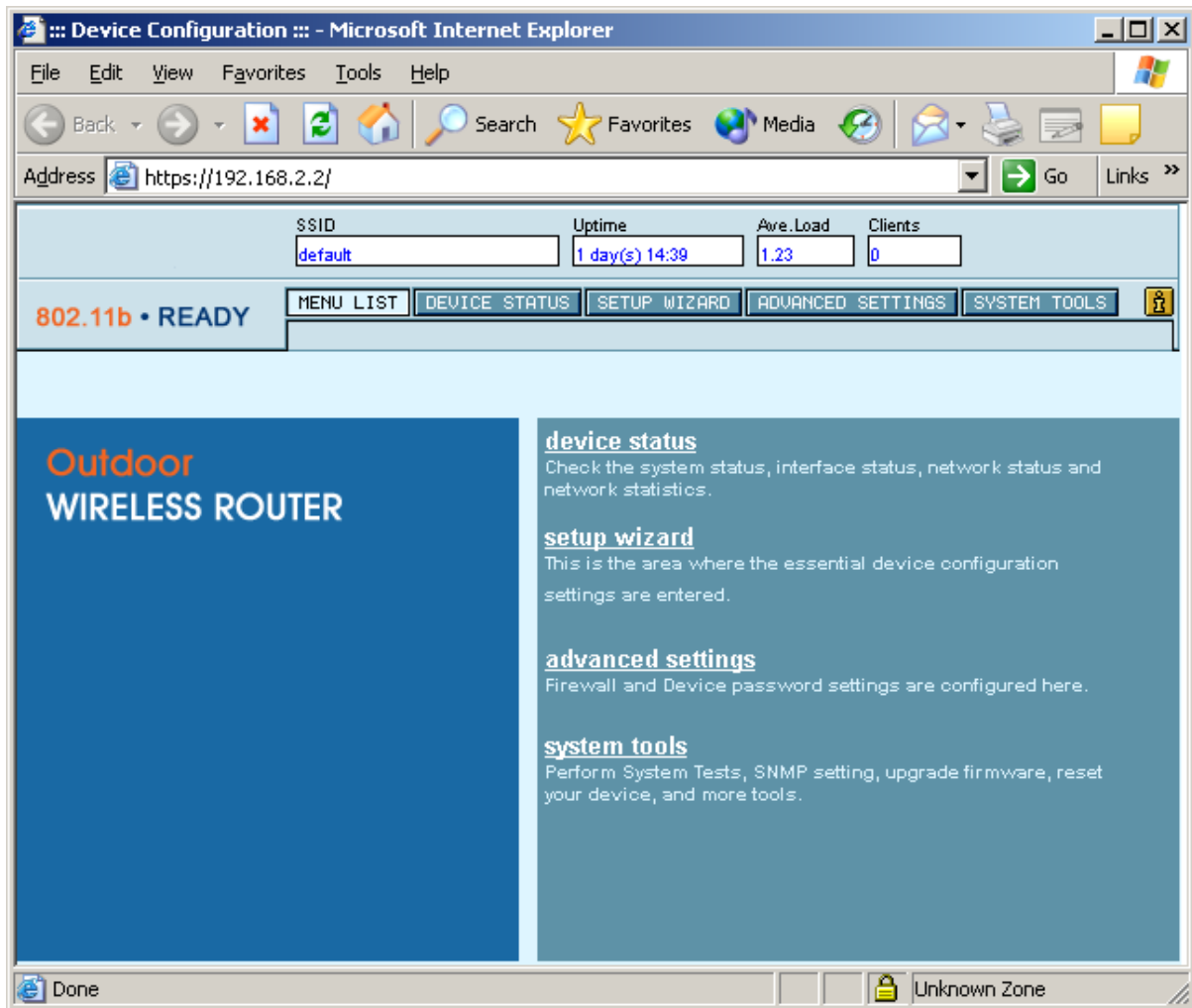


Figure 15 – Main Management Tool Page



Note: The following figures will show the content of the browser without the navigation and address bars.

In the upper part of the screen you find some general important information: The SSID of this device, the uptime since last reboot, the average processor load and the number of clients currently connected to this device.

SSID	Uptime	Ave. Load	Clients
default	1 day(s) 14:39	1.23	0

Figure 16 – Status headline

In the center of the screen you find a menu list with links to the four different setup areas:

- device status
- setup wizard
- advanced settings
- system tools

6.3 Device Status

The device status page shows some information about the P-380 itself, its position in your network and the data traffic on the wireless interface.

DEVICE STATUS						
System Status						
Version	2.4.14 #12 Mon Sep 23 13:41:09 EET 2002					
Uptime	2 day(s) 18:51					
Average Load	1.63					
System Memory Total	14.85 MB					
System Memory Free	6.11 MB					
Service/Interface Status						
IP Firewall	Disabled					
Network Status						
Device Mode	AP					
Hostname	default					
Wireless Interface IP	192.168.2.135					
Network Statistics						
Interface	Network Type	Tx Data	Tx Errors	Rx Data	Rx Errors	Collisions
Wireless	Bridge	8.07 MB	0	6.33 MB	0	0

Figure 17 – Device status

6.3.1 System Status

Version is the current version of the firmware. This is important information for support requests and for preparing firmware upload.

Uptime is the time in days since last system reboot.

Average Load shows the average load of the P-380 processor.

System Memory Total shows the total P-380 memory.

System Memory Free shows the currently available P-380 memory.

6.3.2 Network Status

Device Mode shows the P-380 operating mode (AP or Bridge).

Hostname shows the name of the P-380 in the network used for statistic routines.

Wireless Interface IP is the IP address of the wireless interface of the P-380.

6.3.3 Network Statistics

In the list of all Interfaces you can find information about the data traffic on the wireless interface:

Tx Data: data volume transmitted successfully [MB]

Tx Errors: errors while transmitting data

Rx Data: data volume received successfully [MB]

Rx Errors: errors while transmitting data

Collisions: number of data packet collisions

6.4 Setup Wizard



*Note: No settings on the setup wizard pages are stored until you press the **save settings** button on the wireless configuration setting page at the end of the wizard!*

6.4.1 Operating Mode

On the first page of the setup wizard you can select the operating mode.

Figure 18 – Operating mode settings

Select **AP Router** mode if you want to allow mobile stations to access your wired network and you need to build up a wireless connection to a different IP subnet.

Select **AP** (Access point) mode if you want to allow mobile stations to access your wired network.

Select **Bridge** mode if you want to connect two or more separate wired networks.

Select **Client Router** mode if you want to connect a whole IP subnet (workgroup) to an AP router in another IP subnet.

Select **Client Bridge** mode if you want to connect a workstation to an access point or AP router.



Please note: to run the P-380 in client bridge or client router mode you need a client firmware from the P-380 product CD!

Please refer to the Operating Modes section for more details about the different modes.

6.4.2 General Configuration Settings

On the general settings page you can specify information about the name and location of your P-380.

Figure 19 – General configuration settings

Host Name is the name under which the device will appear for example in the AP Search tool.

DNS Server Address is the IP address of a domain name server. This IP address, provided by your ISP, will be assigned to all PCs requesting address information through DHCP from the P-380. Available in AP router mode only!



If you are not sure about the IP address of the DNS server currently responsible for your local network, please get your IP configuration with “ipconfig” (Win 2000, Win NT and Win XP) or “winipcfg” (Win 9x and Win Me) from the command prompt.

System Identification is a more specific device name for better identification by service staff.

Address is the street and postal address of the location where the device is deployed.

Coordinates specifies the longitude and latitude or other coordinates of the device location.

Customer name is the customer’s name



Please note: All of the parameters above on the general configuration setting page are required!

6.4.3 Network Configuration Settings

On the network configuration settings page you can modify the IP settings for the P-380 and the default gateway.

WAN Interface Settings

Figure 20 – Network configuration settings: WAN interface

Interface: Use this option to switch the WAN interface of P-380 on (Enable) or off (Disable).

Available in AP router and client router mode only!



*Note: In AP router mode you disable the **wired** interface to the Ethernet using this radio button. When the interface is disabled, there are no connections possible between Ethernet devices and the P-380(see Comparison of the Operating Modes).*

*In client router mode you disable **wireless** interface using this radio button. When the interface is disabled, there are no connections possible between wireless devices and the P-380 (see Comparison of the Operating Modes).*

IP Address assigned by ISP is the device’s IP address on the WAN interface. If the DHCP client function is enabled, the IP address assigned by the DHCP server will be used. If no DHCP server can be found via WAN interface, the IP entered here will be used.



If you change the IP address manually, please make sure that the chosen IP address is free and belongs to the same IP subnet as the old one. Otherwise you will lose the connection to the P-380 from your current PC.

If you enable the DHCP client via web browser, the browser will lose the connection after rebooting, because the IP address assigned by the DHCP server is not predictable.

IP Subnet Mask is the corresponding network mask for the IP address on the WAN interface.

ISP Default Gateway is the gateway to other networks on WAN side (required).



If you are not sure about the IP address of the gateway currently responsible for your local network, please get your IP configuration with “ipconfig” (Win 2000, Win NT and Win XP) or “winipcfg” (Win 9x and Win Me) from the command prompt.

DHCP Client: enable this option, when a DHCP server is running in the network on WAN side and you want the DHCP server to assign a free IP address the WAN interface of P-380.



If you are not sure about the IP address of the gateway currently responsible for your local network, please get your IP configuration with “ipconfig” (Win 2000, Win NT and Win XP) or “winipcfg” (Win 9x and Win Me) from the command prompt.

LAN Interface Settings (AP router and client router mode only)

Figure 21 – Network configuration settings: LAN interface

IP Address is the device’s IP address on the LAN interface. In AP router mode this is the IP address on the wireless interface, in client router mode it is the IP address on the wired (Ethernet) interface.



If you enable the DHCP server on the wireless interface in AP router mode, please make sure that the LAN IP address specified for the wireless interface here is in the same IP subnet as the IP address pool range of the DHCP server.

IP Subnet Mask is the corresponding network mask for the IP address on the LAN interface.



Please make sure that you use different IP subnets for the WAN and LAN interfaces. If both address spaces are in the same IP subnet, all routing functions will be disabled!

NAT: When you enable this function, the router will use his network address translation (NAT) function. In this case all LAN IP addresses are hidden to the WAN network behind the routers WAN IP address. A P-380 in client router mode will forward all data packets from his wired LAN using his own WAN IP address to the wireless network it is connected to. The P-380 in AP router mode on the other side of the wireless network will forward the data packets using his own WAN IP address to the wired (Ethernet) network it is connected to.

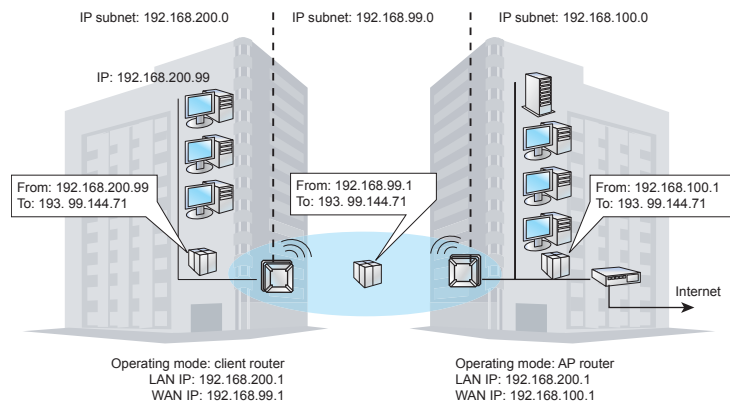


Figure 22 – NAT

6.4.4 Wireless Configuration Settings

On the wireless configuration settings page you can modify all parameters necessary for establishing wireless connections between mobile clients and the access point.



Note: Depending on the operation mode selected on the general configuration setting page, the parameters available on this page will vary.

WIRELESS CONFIGURATION SETTINGS

Warning

Before changing radio settings manually verify that these settings comply with government regulations. At all time, it will be the responsibility of the end-user to ensure that the installation complies with local radio regulations. Please refer to the user manual for more details

Enter Access Point SSID.

Access Point SSID

Bridge ID

Select channel.

Domain

Channel

Client separation settings. Select this setting if you want clients not to be able to communicate between themselves

User Isolation Enable Disable

Select the security settings. These settings help prevent unauthorized users from accessing data.

Encryption Algorithm

Key 0

Key 1

Key 2

Key 3

Select the output power of wireless LAN card.

Antenna Output Power, dBm

Total Output Power, dBm

Figure 23 – Wireless configuration settings

Access Point SSID: The SSID is the key name of the wireless network area you are establishing using the P-380. The SSID can be string of up to 32 characters of your choice.



Note: The SSID is case sensitive! The SSID may not contain special characters like [] { } / \ or spaces. Only dots and underscores are allowed.

- When you are operating the P-380 in bridge mode, the SSID must different for all devices forming the wireless bridge network.
- In access point mode, the SSID must be made known to all mobile clients, or they have to use the “auto connect to any wireless network” function in their WLAN card.
- If you are running more than one P-380 and want to enable the roaming function, please use the same SSID in all access points.
- If you want to run separate wireless networks on a site, please use different SSIDs for each wireless network.

Bridge ID (in bridge mode or client bridge mode only): This ID must be different at the two devices forming the wireless bridge.

Regulatory Domain: The full frequency range of the 2.4 GHz ISM band is not permitted to be used in all countries. Depending on the selection of the regulatory domain here the available frequency channels will vary!

Channel: Frequency channels are used to avoid interference between nearby access points. If you wish to operate more than one access points in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. For example, for three Access Points in close proximity choose channels 1, 5 and 11.



Refer to the regulatory domains chapter in the appendix to get more information concerning the regulations valid for your country and set the parameters for frequency channel to the permitted values!

Layer 2 User Isolation: Use this parameter to enable or disable the direct communication between the mobile clients (in AP or AP router mode only). Layer 2 User Isolation is meant not only to reduce traffic but also to isolate (or separate) WLAN subscribers from each other. With Layer 2 User Isolation switched on, user A cannot see user B on the wireless network. This separation is done on network layer 2.



*Note: Use the site survey tool in the **System Tools** to check the used channels in your surrounding and their signal strength.*

Encryption Algorithm: Select No, 64-Bit or 128-Bit Encryption.

Key 0 to 3: The WEP keys are entered as a series of colon-separated HEX pairs: 5 pairs for 64-Bit (e.g. 01:23:45:67:89), 13 pairs for 128-Bit (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC). If the key entered does not match the required length, the configuration wizard will return an error message.

The encryption key must also be entered into the WLAN card configuration of the mobile clients.

Output power

The Output Power, dBm, is the strength of the radio signal transmitted by the integrated antenna. The higher the number, the stronger the signal.



Refer to the regulatory domains chapter in the appendix to get more information concerning the regulations valid for your country and set the power output to the permitted values!

6.5 Advanced Settings



Setting up advanced P-380 settings requires advanced knowledge of the TCP/IP network structure and functionalities. It is recommended that only skilled network administrators should use these settings.

6.5.1 Firewall

The firewall settings allows to specify IP packet filters to enhance the data security. The firewall takes effect between LAN and WAN and is supposed to avoid forbidden intrusion to your local network. The firewall rules are divided into Input and Output rules to assign special procedures to a certain data transmission direction (AP router and Client router mode only). In AP mode, bridge mode and client bridge mode the corresponding table is called Prerouting table.



Please remember that LAN and WAN have different meanings depending on operating mode. For a P-380 in AP router mode, the incoming data packets are received on the Ethernet interface, for a P-380 in client router mode, incoming packets are received on the wireless interface!

FIREWALL SETTINGS

Enable Firewall Functions. Firewall settings are saved at once after enabling the firewall functions.

INPUT rules							
Rule No	Target	Source IP Address/Mask	Source Port (s)/ICMP Type	Destination IP Address/Mask	Destination Port(s)	Protocol	Action
ADD NEW RULE							

OUTPUT rules							
Rule No	Target	Source IP Address/Mask	Source Port (s)/ICMP Type	Destination IP Address/Mask	Destination Port(s)	Protocol	Action
ADD NEW RULE							

Figure 24 – Firewall settings

On the main firewall settings page you will find one table for input and output rules and a switch to enable or disable the firewall. Within the tables you can insert new rules, modify existing ones, delete rules and change their position by moving up or down.

The position of a rule within the list is very important, because the list is worked through from top to down. If a packet is dropped in the first lines by a very general rule, it does not help to accept it further down with a more specific rule. So please check the rules right position after defining or modifying them.

To specify a new rule please click **Add New Rule** and insert the related interface, destination, gateway and metric values.

The screenshot shows the 'FIREWALL SETTINGS' page with an 'Add new rule' button at the top. Below it, the configuration for a new rule is displayed:

- Rule No.: 1
- Chain: INPUT
- Target: ACCEPT DROP
- Source IP Address: 193.210.12.0
- Source Netmask: (empty field)
- Source Port(s): All Port range (empty fields)
- Destination IP Address: 192.168.2.0
- Destination Netmask: (empty field)
- Destination Port(s): All Port range (empty fields)
- ICMP Type: (dropdown menu)
- Protocol: TCP

At the bottom of the form, there are two buttons: 'RESET' and 'SAVE RULE'. A mouse cursor is pointing at the 'SAVE RULE' button.

Figure 25 – Specifying a new rule

Target – this implementation of firewall control supports two types of rules – ACCEPT and DROP. The appropriate policy defines what to do if the data packet received matches the rule.

Source IP Address – source IP address, leave field empty to specify as “any”.

Source Netmask – source subnet.

Source port(s) – can be specified in two ways: “All” or a given port range.

Destination IP Address – specified the same as Source IP.

Destination Netmask – specified the same as source net mask.

Destination port(s) – specified the same as Source port.

Network protocol – network protocol which the rule affects. Can be specified as one of TCP/UDP/ICMP or “any”.



Note: When defining rules, avoid DENY type rules using “any” as the address space, which can cause inadvertently loss of web management connection (e.g., deny traffic from any to any IP address).



When using the masquerading function of the P-380, IP addresses used in the LAN are not visible to the external world or WAN. Please check if packet filters needs to be specified with destination in masked subnets.

6.5.2 ACL (Access Control List)

In the ACL Settings page you can restrict access to the P-380. Access control is based on the networks devices’ MAC address and is individually controlled for the wireless and Ethernet networks.

Network devices whose MAC addresses are listed in the ACL control table has specific rules for accessing the AP which will override the default policy.

The screenshot shows the 'ACL SETTINGS' page. At the top, there is a section for 'Default ACL policies'. Below this, there are two rows of settings: 'Default ACL policy for wireless network:' and 'Default ACL policy for ethernet:'. Each row has two radio buttons, 'Accept' and 'Deny', with 'Accept' selected. Below the policies is a section for the 'Access control table'. It features a table with four columns: 'Rule No', 'MAC Address', 'Target', and 'Action'. The table is currently empty. To the right of the table header, there are icons for editing and deleting. Below the table, there is a yellow button labeled 'ADD NEW RULE'.

Figure 26 – ACL settings

Default ACL policy for wireless network: Select **Accept** to allow all mobile clients to access this access point or **Deny** to prevent all mobile clients from accessing this access point. Clients may also be subject to rules in the Access control table.

Default ACL policy for Ethernet: Select **Accept** to allow all LAN clients to access this access point or **Deny** to prevent all LAN clients from accessing this access point. Clients may also be subject to rules in the Access control table.

If you need to define special rules for specific network devices, you can add new rules to the Access control table.

The screenshot shows the 'ACL SETTINGS' page with the 'Edit rule' form. At the top, there is a blue button labeled 'Edit rule'. Below this, there is a text box with the instruction: 'Specify the MAC address of the device you want to add to the ACL. The format is a list of colon separated hexadecimal numbers (example: 00:00:78:0A:CD:FF)'. Below the instruction, there are three input fields: 'Rule No.' with the value '1', 'MAC Address' with the value '00:30:84:79:07:1E', and 'Target' with radio buttons for 'ACCEPT' (selected) and 'DENY'. At the bottom, there are two yellow buttons: 'RESET' and 'SAVE RULE'.

Figure 27 – Specifying a new rule

1. Click the **Add New Rule** button to open the Access Control Table.
2. Specify the MAC address of the device you want to add to the ACL. The format is a list of colon separated hexadecimal numbers (for example: 00:00:78:0A:CD:FF).
3. Select the state of the rule, whether the specified network device should be allowed or denied as an Access Points client.



Note: The improper use of the ACL rules (e.g. Deny all from all interfaces) without special rules for some clients may lock you out of accessing the device.

Use the reset function in this cases as described in the Reset to Factory Defaults section.

6.5.3 IP Routing Table

In the Static Routing Settings you can add or delete static routes, and modify static routes settings.

STATIC ROUTING SETTINGS					
Routing table					
Interface	Destination	Gateway	Netmask	Metric	Action
wireless	255.255.255.255	default	host route	0	
wireless	192.168.100.0	default	255.255.255.0	0	
ethernet	192.168.2.0	default	255.255.255.0	0	
ethernet	default	192.168.2.254	0.0.0.0	0	

ADD NEW ROUTE

Figure 28 – Static routing table

Opening the page you will find a list of all present routes, each consisting of the related interface, the destination IP address, the gateway and the subnet mask. The default values in this list are generated from your current IP settings in the Network Configuration Settings menu.

The routing list shows, how the router will handle data packets received on an interface at destination to a specific IP address. In this example, all data received on the Ethernet interface with an destination IP address in the 192.168.2.0 network will be forwarded to the default gateway. All other data packets received on the Ethernet interface will be forwarded to the gateway 192.168.2.254.

If there is more than one route specified for one destination, the metric value shows the priority, how the router will try the routes. The metric value indexes the number of gateways between sender and destination.

To specify a new static route please click **Add New Route** and insert the related interface, destination, netmask, gateway and metric values.

Please specify the following parameters to add new route in the routing table.

Interface: ethernet

Destination: 192.168.200.0

Netmask: 255.255.255.0

Gateway:

Metric: 0

RESET **SAVE ROUTE**

Warning: If route is specified incorrectly, no warning is provided, and no route is added to the system.

Figure 29 – Specifying a new route

6.5.4 DHCP

The DHCP server settings specify, which IP addresses are assigned to the DHCP clients in the LAN. For a P-380 in AP router mode, these are the mobile wireless stations or P-380 devices in client router mode with DHCP client function enabled.

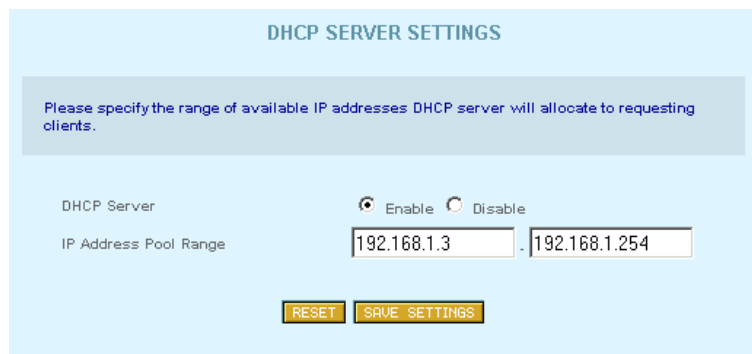


Figure 30 – DHCP server settings

On the DHCP server settings page you can switch the DHCP server on or off and specify the IP address pool range, which is intended to be assigned to the clients.

Click the Save Settings button to confirm. The changes will take immediately without rebooting the device.



Note:

Clients probably needs to refresh their IP configuration to get a new IP address from the P-380.

To avoid IP address conflicts we advise to run one DHCP server in an IP subnet only.

If you enable the DHCP server on the wireless interface in AP router mode, please make sure that the static LAN IP address of the wireless interface is in the same IP subnet as the IP address pool range of the DHCP server.

6.5.5 Port Forwarding

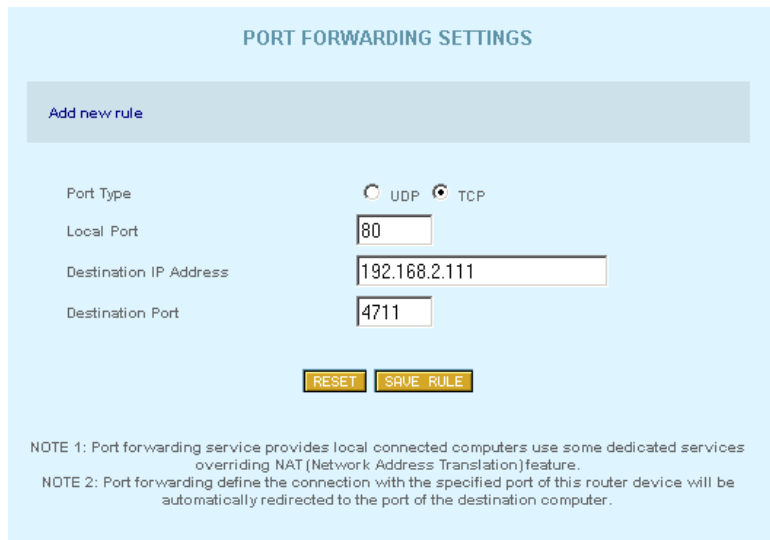
Port forwarding service provides access to computers in the LAN with dedicated services by overriding the NAT (Network Address Translation) feature. Example of such services could be a web server on a computer in the LAN, which should be open to public access for testing purposes. The administrator can define the port of the application, which should be open to public access, the LAN IP address of the computer running the service and a destination port, which is used in the router to override the network address translation.

In the Port Forwarding Settings main page you can add, modify or delete forwarding rules.



Figure 31 – Port Forwarding Settings

To specify a new port forwarding rule please click **Add New Rule** and insert the port type, the local port, the destination IP address and the destination port.



PORT FORWARDING SETTINGS

[Add new rule](#)

Port Type UDP TCP

Local Port

Destination IP Address

Destination Port

NOTE 1: Port forwarding service provides local connected computers use some dedicated services overriding NAT (Network Address Translation) feature.

NOTE 2: Port forwarding define the connection with the specified port of this router device will be automatically redirected to the port of the destination computer.

Figure 32 – Specifying a new forwarding rule

In this example, all requests to the P-380 on port 80 will be redirected to the IP address 192.168.2.111 on port 4711.

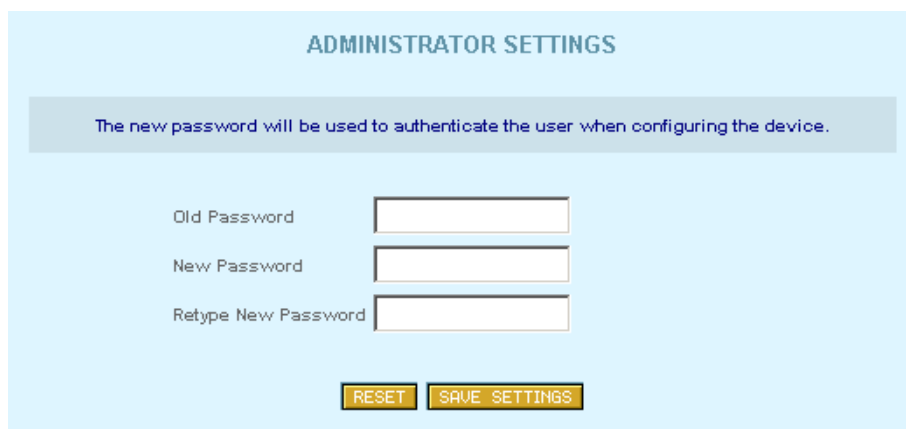


Note: Port forwarding is a kind of reverse function to IP masquerading. Hence this function can take effect only when NAT is enabled!

Please refer to your firewall settings to check if the port forwarding settings are suitable.

6.5.6 Administrator Settings

On the administrator settings page you can change the administrator's password (default: pass). Type the old password, enter the new password of your choice and retype it. Click the **Save Settings** button to store the new password to the P-380.



ADMINISTRATOR SETTINGS

The new password will be used to authenticate the user when configuring the device.

Old Password

New Password

Retype New Password

Figure 33 – Administrator settings

6.6 System Tools

6.6.1 Clients

All clients connected to the AP are listed by MAC address in the **Connected Clients** table:

CONNECTED CLIENTS

Connected clients table				
No.	Client MAC Address	Signal	Noise	Rate Mb/s
1	00:90:8C:CD:00:00	100%	0	11.0

REFRESH

Figure 34 – Connected clients statistic table

Refresh – click the button to refresh connected clients statistic information.

6.6.2 Loopback Test

The loopback test is used for wireless link diagnostics. The loopback test graphically shows the data transfer rate in Mb/s between the P-380 and a specified wireless network device. The transfer rate is measured by sending an ICMP stream to the specific device. Data is refreshed every 10 seconds.

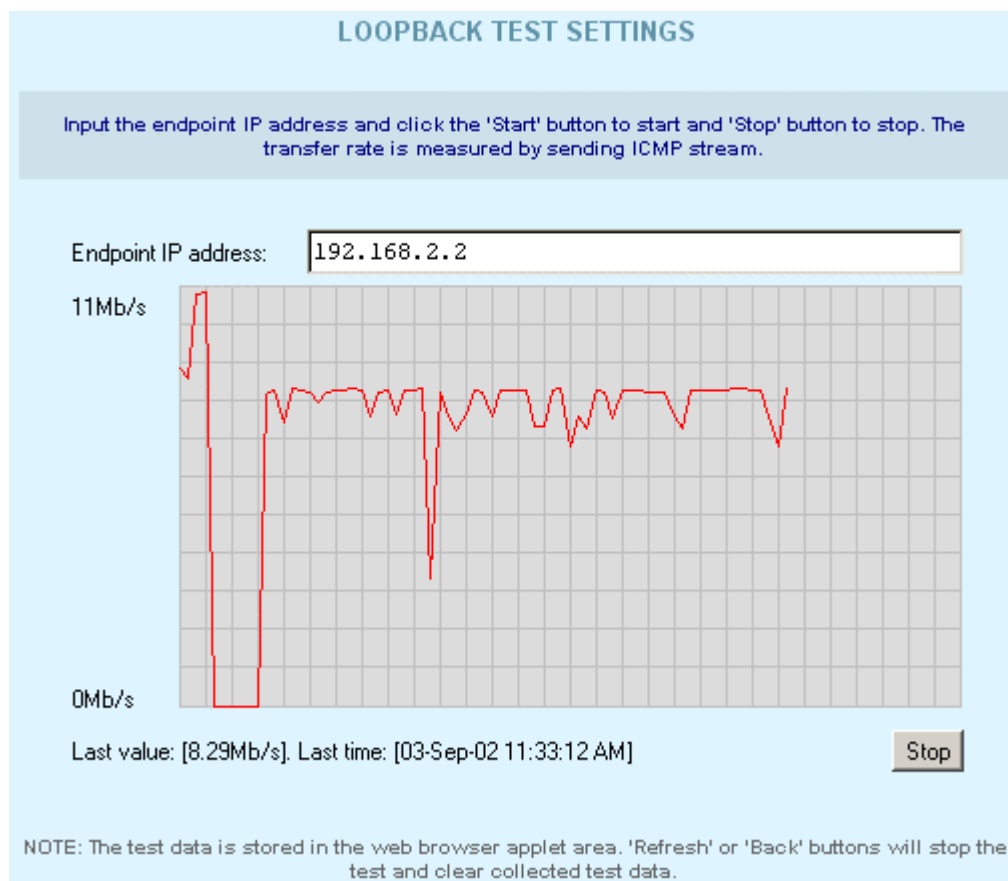


Figure 35 – Loopback test results

To start the loopback test, do the following:

Endpoint IP – specify the device’s IP address, whose transfer rate needs to be measured.

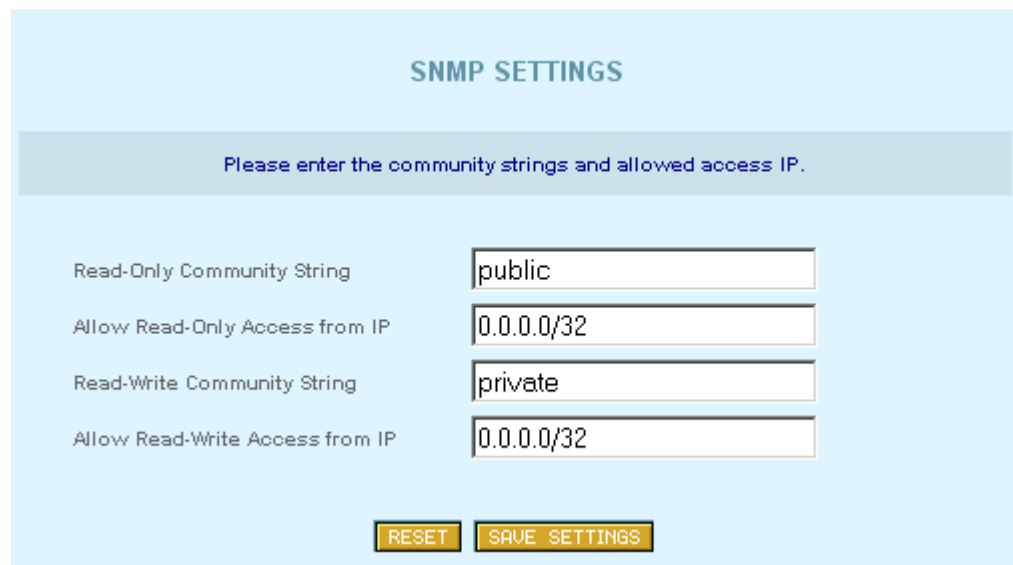
Start – click to start measuring the specified wireless link.

The status line will show the last measured data transfer rate and the time when this data was received from the wireless network device.

To stop loopback testing simply click the **Stop** button.

6.6.3 SNMP

SNMP (Simple Network Management Protocol) can be configured using the **SNMP Settings**. Read-only and read-write communities can be specified here. The Community strings are used for SNMP authentication purposes. It is possible to allow or deny IP address groups from accessing the P-380 using SNMP. An IP address and netmask combination of 0.0.0.0/32 means “ANY” IP address can connect. Access can be controlled for one specified IP (for example 192.168.2.100/32) or by a range (for example 192.168.2.0/24 for IP numbers 192.168.2.1 to 192.168.2.254).



SNMP SETTINGS

Please enter the community strings and allowed access IP.

Read-Only Community String	<input type="text" value="public"/>
Allow Read-Only Access from IP	<input type="text" value="0.0.0.0/32"/>
Read-Write Community String	<input type="text" value="private"/>
Allow Read-Write Access from IP	<input type="text" value="0.0.0.0/32"/>

Figure 36 – SNMP settings

Read-Only Community String – community name for read-only access.

Allow Read-Only Community Access from IP – IP address/netmask for read-only community.

Read-Write Community String – community name for read-write access.

Allow Read-Write Access from IP – IP address/netmask for read-write community.



Note: For security purposes, use only local IP addresses for Read/Write access.

Click the **Reset** button to reset all page fields to their default values or click the **Save Settings** button to save the SNMP settings.

6.6.4 Site Survey

The site survey test shows overview information for wireless networks in a local geography. Using this test, users can scan for working access points, check their operating channels and see signal/noise levels. To start the scan simply select the **Site Survey** menu. The following confirmation message appears:

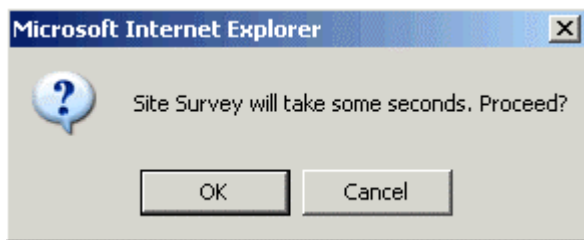


Figure 37 – Site survey confirmation message

Confirm the Site Survey process and get the results in the following table:

AVAILABLE ACCESS POINTS

Access Points table				
Channel	AP MAC Address	SSID	Signal	Noise
6	00:90:8C:CD:04:00	Gemini	100%	22
6	00:90:4B:03:81:95	GEMTEK	100%	34
10	00:02:6F:01:63:76	test_ax	80%	42

RESCAN

Figure 38 – Site survey results table

Available access points are listed in the table by MAC address and SSID.

To refresh the access points availability list simple click the **Rescan** button.

6.6.5 Monitoring

The **monitoring** function shows Received/Transmitted bytes statistics per device.

These statistics show a five-minute average traffic rate over the last 24 hours period. RX (blue) indicates incoming (Received) traffic and TX (red) indicates outgoing (Transmitted) traffic.

TX/RX monitoring is restarted on every reboot of the device. The reason is that the device has no real time clock, so the time used is relative to the restart time. The first statistics appear as two points, five minutes after the device has been restarted. A normal view is acquired 10 minutes after the P-380 reboots. First click the Show button to view the initial TX/RX statistics in the browser window. Click the **Refresh** button instead of the Show button to get updated TX/RX statistics.

You can also change the TX/RX graph time interval. There are two drop-down menus used for this purpose. The first one is used to choose the start hour of the interval. It is possible to choose any hour from the last 24 hours, but the choice may be limited depending on the devices reboot time. The second drop-down is used to choose the time interval duration in hours. The possible choices are from 1 to a maximum of 25 hours.

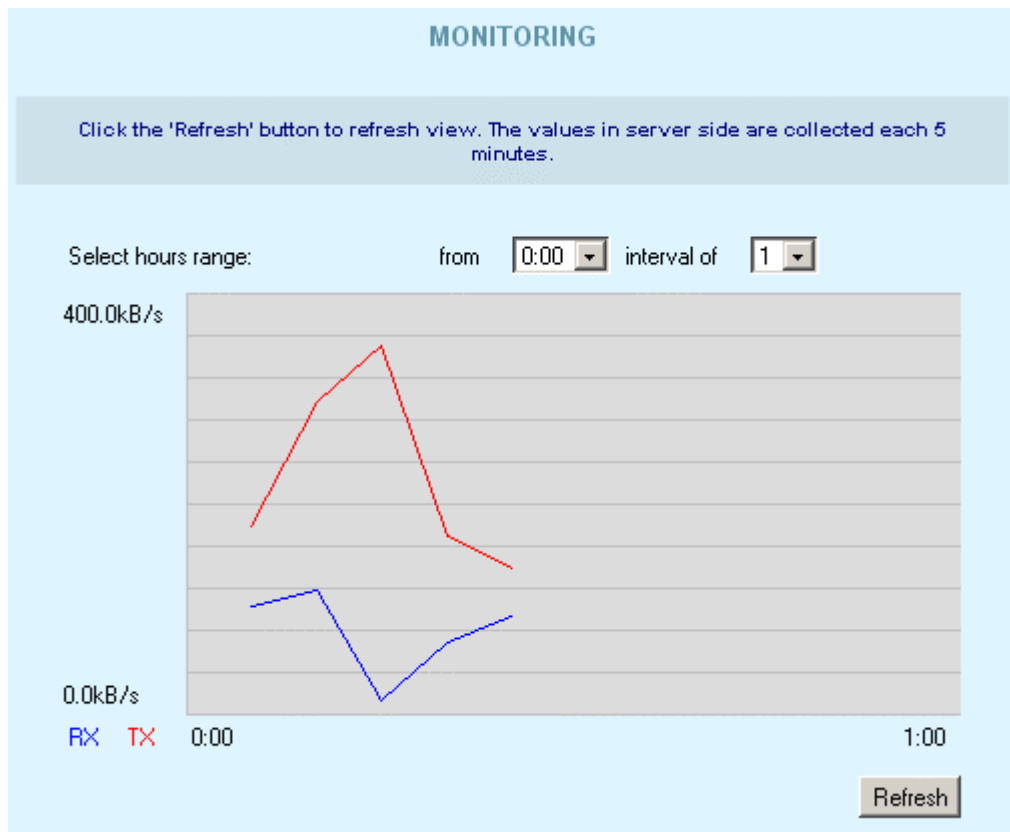


Figure 39 – Monitoring test

RX – Received Kbytes per selected interval.

TX – Transmitted Kbytes per selected interval.

6.6.6 Firmware Update

This function is used to update the current firmware version to a new one. If there is need to change the firmware, a valid firmware file must be selected first by clicking the **Browse** button.

The figure shows an upgrade settings interface. It includes a text box with the instruction: "Please input the valid firmware file to upgrade." Below this, there are two rows of information: "Current Version" with the value "P380a.GSI.1.00.rc3 2002.11.12" and "Firmware" with a text input field containing "fimage_P380a.GSI.1.0" and a "Browse..." button. At the bottom, there are two buttons: "RESET" and "UPGRADE". A note at the bottom states: "NOTE: Writing flash image may take several minutes. Do not switch off the device and do not plug out network cable. If no activity is shown in the bottom of the page, wait at least 5 minutes, then reconnect to the device using web browser. If message about successfully write appears in the bottom of the page - you can reconnect to the device without waiting. See users manual for more information."

Figure 40 – Upgrade settings

After selecting a valid firmware version file, click the **Upgrade** button to proceed. The upgrade process page with the upgrade status messages is displayed:

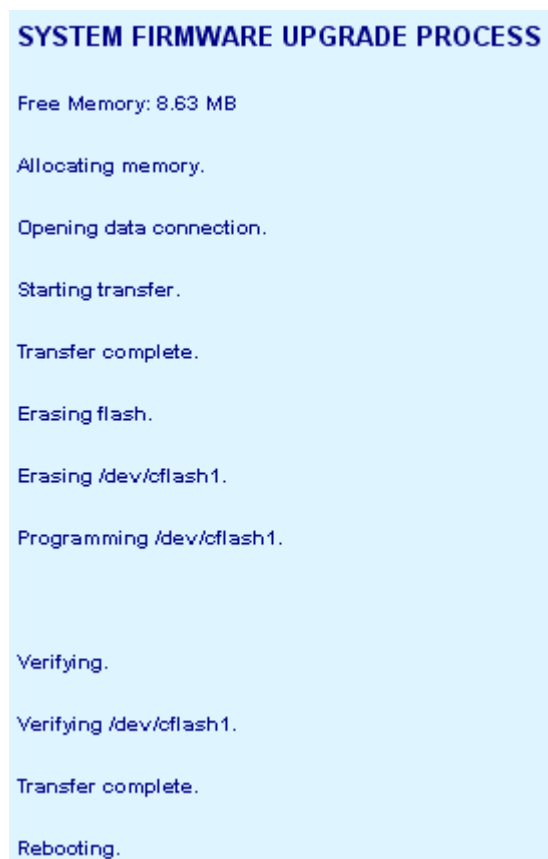


Figure 41 – Upgrade process status page



Do not switch off and do not disconnect P-380 from power supply during firmware update process because the device could be damaged. Best use Ethernet connection (not wireless) for firmware update process.

After a successful upgrade process, the device firmware is upgraded, the **Menu Management** page is displayed, and the previous device configuration set is maintained.

6.6.7 Reboot

Use the **Reboot** function to stop all working device functions and restart the device.

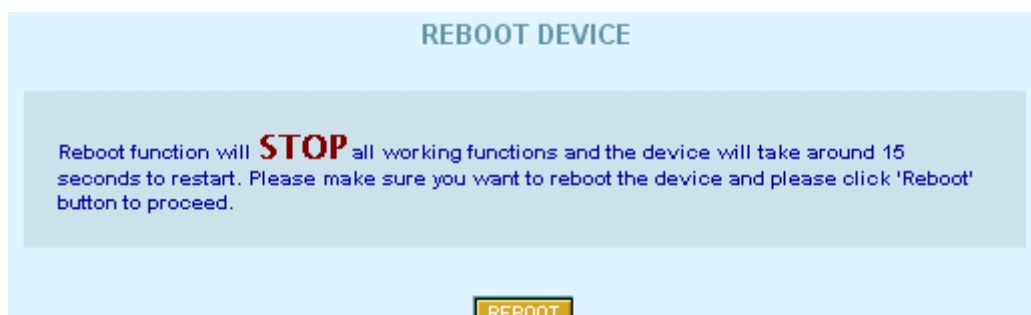


Figure 42 – Reboot device

Reboot – click the button to restart device.

Note: To complete the reboot process, confirm the reboot request.

6.6.8 Reset Device

To reset the device settings to factory defaults use the **Reset Device** menu:



Figure 43 – Reset device

Reset – click the button to reset the device to its default settings.



Note: Keep in mind that resetting the device is an irreversible process. The confirmation message appears before starting the reset process. Read it carefully and confirm as described.

You must enter the administrator password to perform the reset function. Please note that even the password will be set back to the factory default!

The device is restarted. All previous device configuration settings will be erased and the factory default values applied.

7 System Configuration Using Command Line Interface

7.1 Overview

The CLI (Command Line Interface) software is a configuration shell for the Operator Access Point (P-380). Using the CLI, the operator can:

- Configure all essential Access Point configuration settings;
- View system, interface, network status, and network statistics;
- Use the system tools, such as Site Survey.

In general, there are two ways to connect to the CLI:

- Telnet
- SSH client (encrypted)

These following sections describe the CLI command line interface used with telnet and the command set available.



The commands and parameters shown in the CLI configuration will vary depending on operating mode. The screenshots in this section just show examples, which may differ from your display.

To get more information about the full range of commands and parameters please refer to the CLI Configuration Commands and Parameters section.

7.2 Login

To access the P-380 via the CLI, open a command prompt and type

```
telnet 192.168.2.2
```

where 192.168.2.2 is your device's IP address. CLI mode starts automatically. The login password is the same as the HTML system's administrator password.

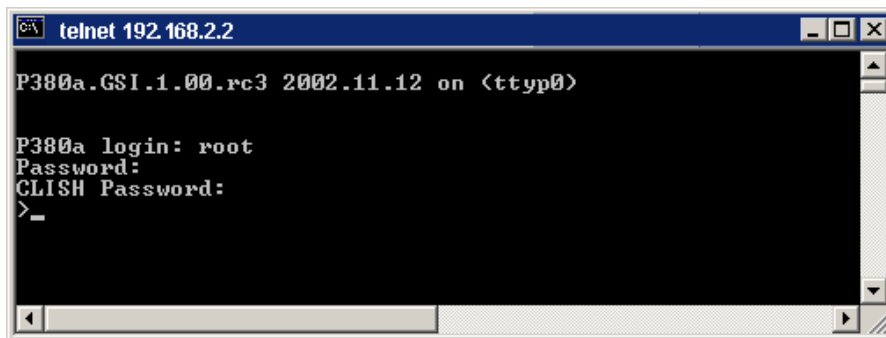
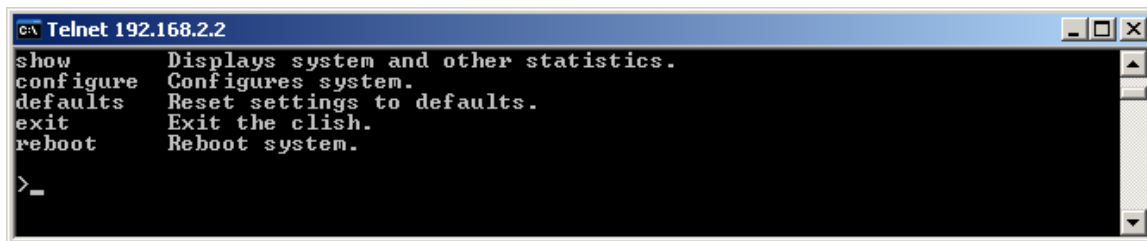


Figure 44 – CLI Login Dialog

After successful login, the command prompt is displayed and the CLI is ready for commands. Press '?' to get a list of available commands:

Note: The ? will not appear on the screen. In the same moment you are pressing this character, the display changes to the desired help page.



```

c:\ Telnet 192.168.2.2
show      Displays system and other statistics.
configure Configures system.
defaults  Reset settings to defaults.
exit      Exit the clish.
reboot    Reboot system.

>_

```

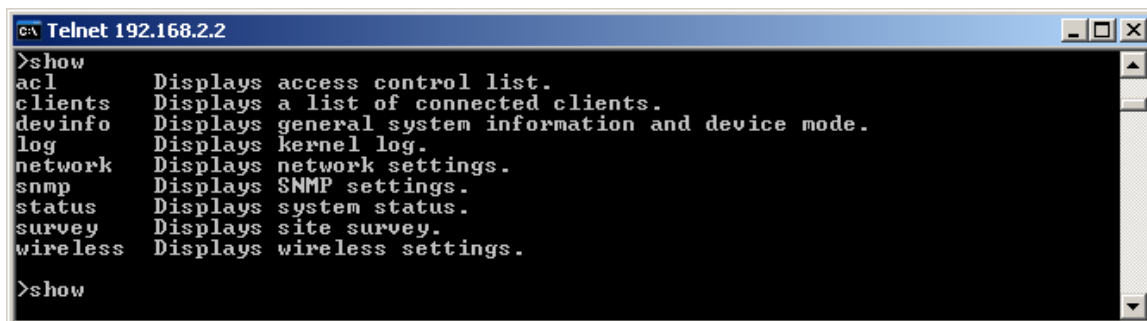
Figure 45 – CLI Main Menu Commands

7.3 Show

Show is a category of commands that display system statistics and settings. The show commands list depends on the device mode. In general its usage is

```
show <command>
```

where <command> is one of the following:



```

c:\ Telnet 192.168.2.2
>show
acl      Displays access control list.
clients  Displays a list of connected clients.
devinfo  Displays general system information and device mode.
log      Displays kernel log.
network  Displays network settings.
snmp     Displays SNMP settings.
status   Displays system status.
survey   Displays site survey.
wireless Displays wireless settings.

>show

```

Figure 46 – Show Commands List

Use one of these commands to get the desired information.

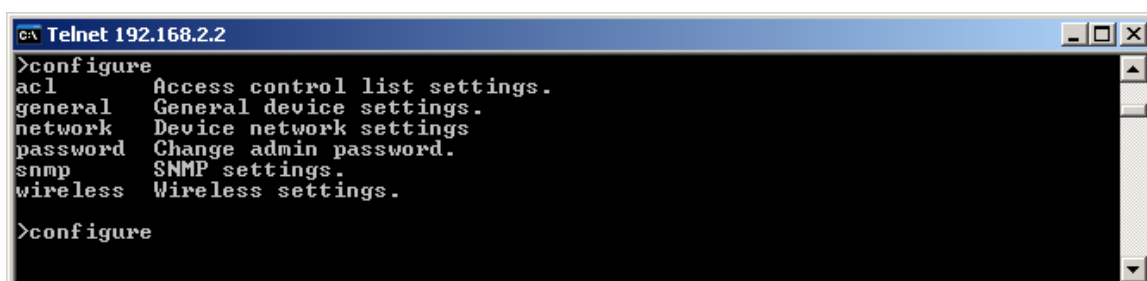
7.4 Configure

Configure is a category of commands that configures all essential system settings. The configure commands themselves contain several subcommands and the subcommands again contain several parameters. In general, configure usage is as follows:

```
configure <command> <subcommand> [parameter]
```

To get a list of all available commands in the configure category please type:

```
configure?
```



```

c:\ Telnet 192.168.2.2
>configure
acl      Access control list settings.
general  General device settings.
network  Device network settings.
password Change admin password.
snmp     SNMP settings.
wireless Wireless settings.

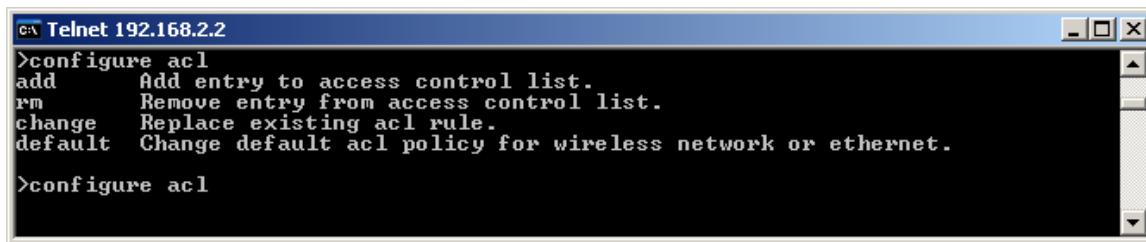
>configure

```

Figure 47 – Configure Commands List

To get a list of all available subcommands for a specific command please type:

```
configure <command>? (e.g. configure acl?)
```

A screenshot of a Telnet window titled 'Telnet 192.168.2.2'. The window shows a command-line interface with the following text:

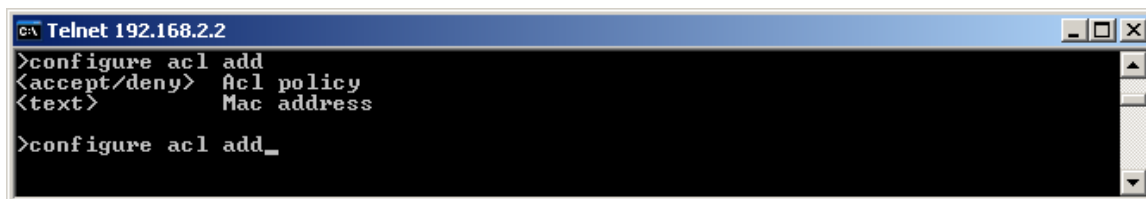
```
>configure acl
add      Add entry to access control list.
rm       Remove entry from access control list.
change   Replace existing acl rule.
default  Change default acl policy for wireless network or ethernet.

>configure acl
```

Figure 48 – Configure ACL Commands List

To get a list of all the available parameters for a specific subcommand please type:

configure <command> <subcommand>?, (e.g. configure acl add?)

A screenshot of a Telnet window titled 'Telnet 192.168.2.2'. The window shows a command-line interface with the following text:

```
>configure acl add
<accept/deny>  acl policy
<text>         Mac address

>configure acl add_
```

Figure 49 – Configure ACL Add Parameters List

In this example, the command configure acl add has two parameters: The ACL policy can be set either to accept or to deny and the MAC address of the target network device must be defined.

If you wish to allow a specific network device to access the P-380, please type:

```
configure acl add accept 00:40:4B:31:8F:08
```

where 00:40:4B:31:8F:08 is the MAC address of the specific device.

Note: A full list of all available commands, subcommands and parameters can be found in the reference section.

7.5 The Defaults Command

To set Access Point device settings values back to their default values, type the Default command in the command line.

7.6 The Exit Command

Type the Exit command to exit the CLI mode.

7.7 The Reboot Command

To reboot the Access Point and stop all processes type the Reboot command in the command line.

8 Appendix

8.1 Regulatory Domains

Channel	Frequency in MHz	USA, Canada (FCC)	ETSI	WORLD	France	China	Japan	Manual
1	2412	•	•	•	—	•	•	•
2	2417	•	•	•	—	•	•	•
3	2422	•	•	•	—	•	•	•
4	2427	•	•	•	—	•	•	•
5	2432	•	•	•	—	•	•	•
6	2437	•	•	•	—	•	•	•
7	2442	•	•	•	—	•	•	•
8	2447	•	•	•	—	•	•	•
9	2452	•	•	•	—	•	•	•
10	2457	•	•	•	•	•	•	•
11	2462	•	•	•	•	•	•	•
12	2467	—	•	—	•	•	•	•
13	2472	—	•	—	•	•	•	•
14	2484	—	—	—	—	—	•	•
Maximum power levels		30 dBm	20 dBm	20 dBm	20 dBm	10 dBm	20 dBm	20 dBm



Mexico is included in the Americas regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

8.2 CLI Configuration Commands and Parameters

8.2.1 Configuration Overview

acl	Access control list settings.
dhcpserver	DHCP server settings
firewall	Firewall settings
forwarding	Port forwarding settings
general	General device settings.
network	Device network settings
password	Change administrator password.
routes	Routes management
snmp	SNMP settings.
wireless	Wireless settings.

8.2.2 ACL Configuration

configure acl	
add	Add entry to the access control list.
rm	Remove entry from the access control list.
change	Replace existing acl rule.
default	Change default acl policy for wireless network or Ethernet network

configure acl add	
<accept/deny>	Acl policy
<text>	MAC address

configure acl rm	
<text>	Either rule number or MAC address of the rule to be removed

configure acl change	
<text>	Either rule number or MAC address of the rule to be changed
<text>	New acl policy: accept/deny
<text>	New MAC address

configure acl default

<1/2>	1 for wireless network, 2 for Ethernet default policy
<accept/deny>	New default acl policy

8.2.3 DHCP Server Configuration**configure dhcpserver**

service	Enable/Disable firewall
iprange	IP address range

configure dhcpserver service

<enable/disable>	Enable/Disable DHCP service
------------------	-----------------------------

configure dhcpserver iprange

<ipaddress>	Starting IP address
<ipaddress>	Ending IP address

8.2.4 Firewall Configuration**configure firewall**

service	Enable/Disable firewall
rules	add new rule

configure firewall service

<enable/disable>	Enable/Disable firewall service
------------------	---------------------------------

configure firewall rules

<-A/-D/-R/-I>	action: -A:add/-D:delete/-R:replace/-I:insert
<chain>	Chain name. Can be INPUT or OUTPUT in station and ap router modes, otherwise has to be PREROUTING
<number>	Number of rule in the chain (has to be used with actions D, R and I only)
<-p tcp/udp/icmp/any>	Protocol
<-s [ip[/netmask]]>	Source IP and netmask
<-d [ip[/netmask]]>	Destination IP and netmask
<-j ACCEPT/DROP/REJECT/LOG>	Firewall rule target

<--source-port [port[:port]]>	Source port(s). Can be used only with '-p tcp' and '-p udp'
<--destination-port> [port[:port]]	Destination port(s). Can be used only with '-p tcp' and '-p udp'
<--icmp-type number>	ICMP type. Can be used with '-p icmp' only

8.2.5 Forwarding Configuration

configure forwarding	
service	Enable/Disable port forwarding
add	Add new rule
rm	Remove existing rule
change	Replace existing rule with new one

configure forwarding service	
<enable/disable>	Enable/Disable port forwarding service

configure forwarding add	
<udp/tcp>	Port type
<port>	Local port
<ipaddress>	Destination
<port>	Destination port

configure forwarding rm	
<value>	Rule number

configure forwarding change	
<value>	Rule number
<udp/tcp>	Port type
<port>	Local port
<ipaddress>	Destination
<port>	Destination port

8.2.6 General Configuration

configure general	
devicemode	Device mode.

hostname	Hostname.
systemid	System identification.
address	Device address(country, state etc.)
coordinates	Device coordinates (longitude and latitude).
customer	Customer name.

configure general devicemode

<text> Device mode: sta_router, ap_router, ap, bridge, sta_bridge

configure general hostname

<text> Hostname

configure general systemid

<text> System ID

configure general address

<text> Address(country, state, city, street address)

configure general coordinates

<x,y> Geodesic coordinates (i.e. longitude and latitude)

configure general customer

<text> Customer name

8.2.7 Network Configuration

configure network

lan	LAN interface settings.
wan	WAN interface settings.



The assignment of LAN and WAN to wired and wireless interfaces is dependent on operating mode. Please refer to the operating modes section to find more information about the meaning of LAN and WAN in different modes.

configure network lan

interface	Set LAN interface
masquerade	Enable/Disable masquerading

configure network lan interface

<ipaddress>	LAN IP address
<netmask>	LAN subnet mask

configure network lan masquerade

<enable/disable>	Enable/disable LAN masquerade.
------------------	--------------------------------

configure network wan

dhcp	Enable/disable DHCP client service
interface	Set WAN interface

configure network wan interface

<enable/disable>	Enable or disable WAN interface. MUST be the only parameter.
<ipaddress>	WAN IP address
<netmask>	WAN subnet mask
<ipaddress>	WAN default gateway

configure network wan dhcp

<enable/disable>	Enable/disable DHCP client on WAN interface
------------------	---

8.2.8 Routes Configuration

configure routes

add	Add new rule
rm	Remove existing rule

configure routes add

<text>	Interface: eth0/prism0 (Ethernet/Wireless)
<destination>	Destination
<netmask>	Netmask
<ipaddress>	Gateway

<value>	Metric
---------	--------

configure routes rm

<value>	Route number
---------	--------------

8.2.9 SNMP Configuration

configure snmp

<text>	Read only community string.
<ipaddress>	Allow read only access from IP.
<number>	Netmask bits for RO access IP.
<text>	Read write community string.
<ipaddress>	Allow read write access from IP.
<number>	Netmask bits for RW access IP.

8.2.10 Wireless Configuration

configure wireless

ssid	Access point SSID.
separate	Blocks traffic between clients
channel	Default channel for BSS.
encryption	Encryption settings.
power	Output power, dBm.

configure wireless ssid

<ssid>	Access port SSID.
--------	-------------------

configure wireless separate

<enable/disable>	Enable/disable Layer 2 User Isolation
------------------	---------------------------------------

configure wireless channel

<domain>	The domain to which your country belongs
----------	--

<channel>	Default channel for BSS: channel number
-----------	---

Note:	<p>Only the following domains are available:</p> <p>FCC: USA, Canada, frequency 2412-2462 MHz</p> <p>ETSI: European countries, frequency 2412-2472 MHz</p> <p>WORLD: frequency 2412-2472 MHz</p> <p>FRANCE: frequency 2457-2472 MHz</p> <p>Japan: frequency 2484 MHz</p> <p>China: frequency 2412-2472 MHz</p> <p>MANUAL: frequency 2412-2484</p>
-------	---

configure wireless encryption

wep	Enable/disable WEP.
-----	---------------------

key	Edit encryption keys.
-----	-----------------------

activekey	Set the active key.
-----------	---------------------

configure wireless encryption wep

<no/64/128>	Choose either no encryption, 64-bit, or 128-bit encryption
-------------	--

configure wireless encryption key

<number>	Encryption key number
----------	-----------------------

<text>	Encryption key value, hex pairs separated by :
--------	--

8.3 Menu Items by Operating Mode

	AP Router	AP	Bridge	Client Bridge	Client Router
Advanced settings					
Firewall	•	•	•	•	•
Enable/Disable	•	•	•	•	•
Input rules	•	—	—	—	•
Output rules	•	—	—	—	•
Prerouting rules	—	•	•	•	—
ACL	•	•	—	—	—
AC policy	•	•	—	—	—
AC Table	•	•	—	—	—
Routes	•	—	—	—	•
DHCP	•	—	—	—	•
Enable/Disable	•	—	—	—	•
IP Addr. pool	•	—	—	—	•
Port FW	•	—	—	—	•
Enable/Disable	•	—	—	—	•
Port FW table	•	—	—	—	•
Admin. password	•	•	•	•	•
System tools					
Clients	•	•	•	—	—
Loopback test	•	•	•	—	•
SNMP settings	•	•	•	•	•
Site Survey	•	•	•	•	•
Monitoring	•	•	•	•	•
Upgrades	•	•	•	•	•
Reboot	•	•	•	•	•
Reset	•	•	•	•	•
Set Up Wizard					
Operating Mode	•	•	•	•	•

AP Router	•	•	•	—	—
AP	•	•	•	—	—
Bridge	•	•	•	—	—
Client Bridge	—	—	—	•	•
Client Router	—	—	—	•	•
General	•	•	•	•	•
Host name	•	•	•	•	•
DNS Server	•	•	•	•	•
System ID	•	•	•	•	•
Serial No	•	•	•	•	•
Address	•	•	•	•	•
Coordinates	•	•	•	•	•
Cust. Name	•	•	•	•	•
Network	•	•	•	•	•
Interface Enable	•	—	—	—	•
IP Address	•	•	•	•	•
IP Mask	•	•	•	•	•
Default Gateway	•	•	•	•	•
DHCP Client	•	•	•	•	•
LAN IP Address	•	—	—	—	•
LAN IP Mask	•	—	—	—	•
LAN Default Gateway	•	—	—	—	•
Masquerade	•	—	—	—	•
Wireless	•	•	•	•	•
SSID	•	•	•	•	•
Bridge ID	—	—	•	—	—
Channel	•	•	•	—	—
Encryption	•	•	•	•	•
WEP Keys	•	•	•	•	•

8.4 Device Configuration Default Values

Parameter	Default value			
ACL Configuration Settings				
Default ACL policy for wireless network	Accept			
Default ACL policy for ethernet	Accept			
Rules	no rules defined			
Firewall Configuration Settings				
Firewall function	disabled			
Input rules	no rules defined			
Output rules	no rules defined			
Routes Configuration Settings				
interface	Destination	Gateway	Netmask	Metric
wireless	255.255.255.255	default	host route	0
wireless	LAN IP	default	255.255.255.0	0
ethernet	default	192.168.2.1	0.0.0.0	0
ethernet	WAN IP	default	255.255.255.0	0
DHCP Server Configuration Settings				
DHCP server	disabled			
Starting IP	xxx.xxx.xxx.3, where xxx.xxx.xxx is the WAN IP			
Ending IP	xxx.xxx.xxx.254, where xxx.xxx.xxx is the WAN IP			
Forwarding Configuration Settings				
Forwarding function	disabled			
Rules	no rules defined			
General Configuration Settings				
Device mode	AP (AP firmware), sta_router (client firmware)			
Hostname	P380a (AP firmware), P380s (client firmware)			
System identification	identification			
Serial number	devices MAC address			
Address	address			
Coordinates	coordinates			
Customer name	customer_name			
Network Configuration Settings				

Interface	enabled
WAN IP address	192.168.2.2
WAN Subnet mask	255.255.255.0
Default gateway	192.168.2.1
DHCP client	disabled
WAN IP address	192.168.2.2
WAN Subnet mask	255.255.255.0
Masquerade	disabled
Wireless Configuration Settings	
SSID	P380a (AP firmware), P380s (client firmware)
Bridge-ID	1
Domain	World
Channel	11
User Isolation	disabled
Encryption	disabled
Key 0	not set, default key
Key 1	not set
Key 2	not set
Key 3	not set
Output power	20 dBm
SNMP Configuration Settings	
Read-Only Community String	public
Allow Read-Only Access from IP	0.0.0.0
Allow Read-Only Access from netmask	255.255.255.255
Read-Write Community String	private
Allow Read-Write Access from IP	0.0.0.0
Allow Read-Write Access from netmask	255.255.255.255

8.5 P-380 Specification

8.5.1 Technical Data

Features
IEEE 802.11b Access Point, Router, Bridge
Wi-Fi compliant
40/128-bit WEP security
Layer 2 isolation for security
802.1x/EAPoLAN/with MD-5/TLS/TTLS/SIM support (in preparation)
IAPP roaming (in preparation)
RADIUS AAA client with EAP support (in preparation)
Remote management via HTTPs, Telnet, SNMP (MIB II, Ethernet MIB, Bridge MIB, private MIB)
IP routing with NAT, port forwarding and firewall filters Remote software upgrade via HTTP
Integrated Site Survey, Loop-back test
DHCP server, DHCP client
Access Control List (MAC address filter)
Programmable output power

Interface
Ethernet Interface, 10/100 Base-T, RJ-45 Power-over-Ethernet port for connection to Power-Switch

Wireless			
Standard	IEEE 802.11b DSSS (2.4GHz ISM band)		
Data Rate	11Mbps, 5.5Mbps, 1Mbps (Auto scaling)		
Transmit Power	P-380A: 29 ±1dBm, P-380N: 19 ±1dBm		
Sensitivity	Data Rate	Sensitivity	Modulation
	11Mbps	-82dBm	CCK
	5.5Mbps	-84dBm	CCK
	1Mbps	-90dBm	DBPSK
Antenna connector (P-380N only!)	Reverse N-type connector (FCC compliant)		
Integrated Antenna (P-380Aonly!)	integrated 10dBi directional antenna, 45° beam width vertical and horizontal, vertical polarization		

Physical Specification

Dimension	180 x 160 x 58mm (7.1 x 6.3 x 2.3in)
Weight	1100g (includes mounting kit)

Environment Specification

Temperature	-20°□ to +65°C
Humidity	up to 95%

Power Supply

Type	external AC/DC converter 100/230V to 5V DC/1.5A, 3W max.
Power-over-Ethernet	IEEE 802.3af compliant

Mechanical Specification

Ruggedized and flame-resistant plastic housing, wall or mast mount

LEDs

3 + 10 LEDs	RF activity, LAN activity, Power, 10 LED link quality display
-------------	---

Management

Interfaces	HTTPs, Telnet, SSH, SNMP (MIB II, Ethernet MIB, Bridge MIB, private MIB), Terminal
Software Update	Remote Software Update via HTTPs
Test	Integrated site survey, Loop-back test
Reset	Remote reset / Manufacturing reset

Warranty

2 years

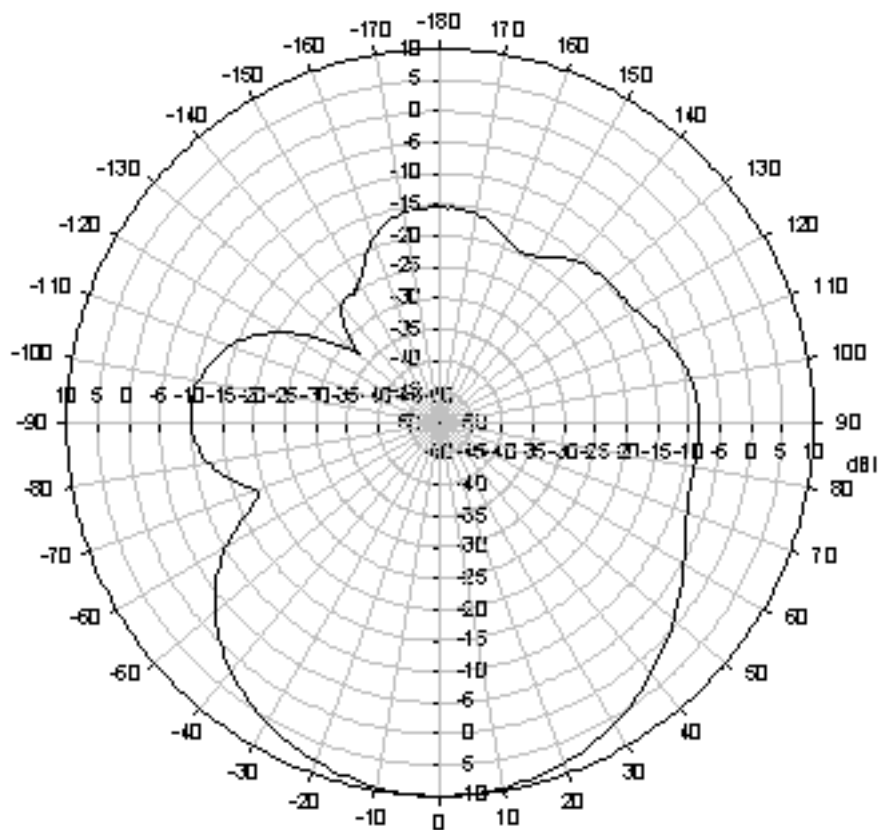
Package Contents

P-380 Outdoor Access Point & Router
CD-ROM with software and documentation
Mounting kit

Related Products		
Gateways:	G-6000/4000 Hot-spot Gateways	P-360 Hot-spot Access Point
Client Adapters:	T-300 series (2.4 GHz)	T-800 series (Dual-band 2.4 & 5 GHz) PoE
Switches:	E-810 8-port Power-over-Ethernet Switch	E-110 Single-port PoE Feeder Network
Management:	S-6000 Network Management System	S-200 Smart Client Manager

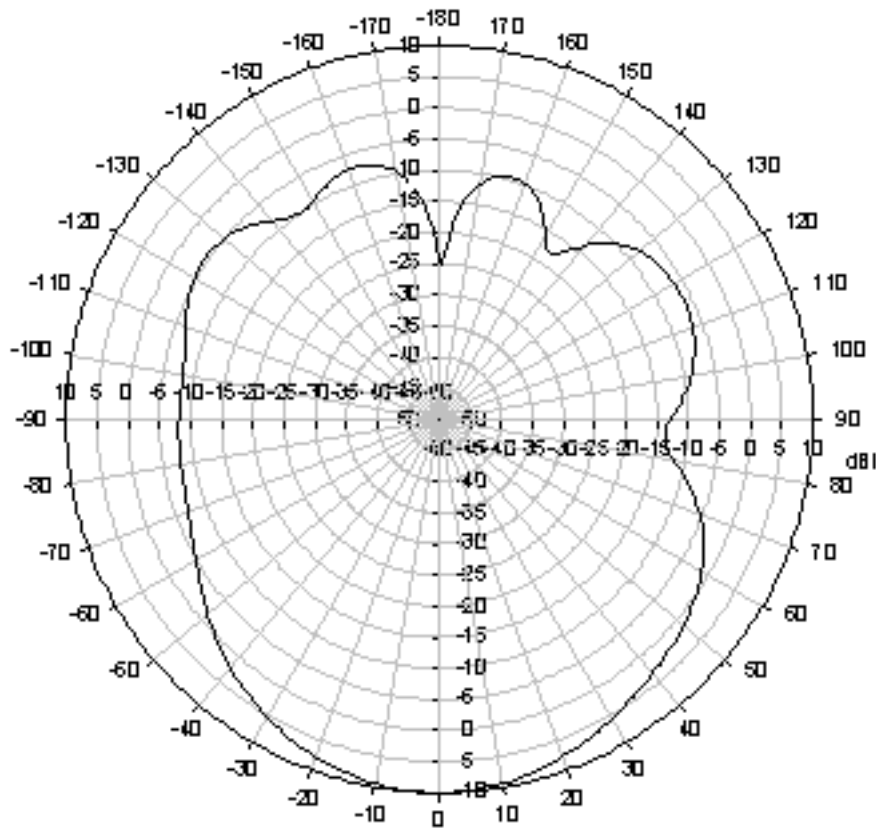
8.5.2 P-380 Antenna Pattern

H-plane antenna pattern



- Peak gain: 10dBi
- 3dB beam width: 47°

E-plane antenna pattern



- Peak gain: 10dBi
- 3dB beam width: 48°

9 Glossary

Symbols:

10BASET 10 Mbps/baseband/twisted pair. The IEEE standard for twisted pair Ethernet.

802.11b The IEEE standards for the definition of the Wireless high speed (11Mbit) protocol for wireless communication.

A

Authorization the process of determining what types of activities a user is permitted to undertake. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity.

B

backbone The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

bandwidth Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps bits per second. A measure of the data transmission rate.

D

DHCP Dynamic Host Configuration Protocol. A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DNS Domain Name System. The distributed name/address mechanism used in the Internet. It comprises distributed online databases that contain mappings between human-readable names and IP addresses, and servers, which provide translation services to client applications.

domain A part of the DNS naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), e.g., "machine.company.com". See DNS.

E

Ethernet A common, 10Mbps local area network technology invented by Xerox Corporation at the Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over thinwire coaxial cable (10BASE2), thickwire coaxial cable (10BASE5), twisted pair cable (10BASET), or fibre optic cable.

F

filter Within the router, A filter is a process used to select which packets will be processed by the router, and which will be ignored or discarded. Selection may be based on addresses or protocol type.

firewall A system or combination of systems that enforces a boundary between two or more networks.

FLASH A new memory technology, which combines the nonvolatile features of EPROMs with the easy in-system reprogramming of conventional volatile RAM. See EPROM.

G

gateway The original Internet term for what is now called router or more precisely, IP router. In modern usage, the term “gateway” and “application gateway” refers to systems, which perform translation from some native protocol, or physical data format to another. Examples include electronic mail gateways, which translate between X.400 and RFC 822 mail message formats. See router.

H

host An (end-user) computer system that connects to a network, such as a PC, minicomputer or mainframe.

I

ICMP Internet Control Message Protocol. The TCP/IP protocol used to handle errors and control messages at the IP layer. ICMP is part of the IP protocol. Gateways, routers and hosts use ICMP to send reports of problems about datagrams back to the original source that sent the datagram.

interface One of the physical ports on the router, including the Ethernet and asynchronous ports.

interface type The type (Ethernet or Point-to-Point) of one of the interfaces on the router.

Internet A collection of networks interconnected by a set of routers, which allow them to function as a single, large virtual network.

Internet (note the capital “I”) The largest internet in the world consisting of large national backbone networks (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. The Internet is a multiprotocol network, but generally carries TCP/IP.

Internet address See IP address.

Internet Protocol See IP.

ISP Internet service provider. A company that provides Internet - related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

IP Internet Protocol. The network layer protocol for the TCP/IP protocol suite. It is a connectionless, best-effort packet switching protocol.

IP address A 32-bit address assigned to hosts using TCP/IP. The address specifies a specific connection to a network, not the host itself. See dotted decimal notation.

L

LAN Local Area Network. Any physical network technology (such as Ethernet) that operates at high speed (typically 10 Mbit per second or more) over short distances (up to a few kilometers). See WAN.

LED Light Emitting Diode. A luminous indicator.

M

MAC address. The hardware address of a device connected to a shared media. For example, the MAC address of a PC on an Ethernet is its Ethernet address.

metric A concept used to describe the cost of a route across a network, the distance to the destination at the remote end of the route, or the capacity of the route.

N

name resolution The process of mapping a name into the corresponding address. See DNS.

NAT Network Address Translation, an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. NAT is used for two main tasks – to provide a type of firewall by hiding internal IP addresses and enable a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.

network A computer network is a data communications system which interconnects computer systems at various different sites. A network may be composed of any combination of LANs or WANs.

network address The network portion of an IP address. For a class A network, the network address is the first byte of the IP address. For a class B network, the network address is the first two bytes of the IP address. For a class C network, the network address is the first three bytes of the IP address. In each case, the remainder is the host address. In the Internet, assigned network addresses are globally unique. See IP address.

node An addressable device attached to a computer network. See host, router.

P

packet The unit of data sent across a network. "Packet" is a generic term used to describe units of data at all levels of the protocol stack, but it is most correctly used to describe application data units. See datagram, frame.

policy Organization-level rules governing acceptable use of computing resources, security practices, and operational procedures.

port The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. A port is a transport layer demultiplexing value. Each application has a unique port number associated with it. It is also used to refer to one of the physical network connectors on the router.

protocol A formal description of message formats and the rules two computers must follow to exchange those messages. Protocols can describe low-level details of machine-to-machine interfaces (e.g., the order in which bits and bytes are sent across a wire) or high-level exchanges between allocation programs (e.g., the way in which two programs transfer a file across the Internet).

Q

QOS Quality of Service. Transmission system qualities measure in terms of reliability and availability.

R

route The path that network traffic takes from the source to the destination. It may include many gateways, routers, hosts and physical networks.

route table A table listing information about routes to other hosts or networks, such as the remote network or host address, the interface down which the route exists, the distance to the remote address and the cost of sending data over the route.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this it uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as "routing metrics".

S

server A network device that provides services to client stations. Examples include file servers and print servers.

service A term used with the router to refer to a connection to another port on (another) router, used to access dialup modems, hosts that do not support TCP/IP and other asynchronous devices.

SNMP Simple Network Management Protocol. The Internet standard protocol developed to manage nodes on an IP network. See MIB.

subnet A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an internet.

subnet address The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address or subnet mask. See subnet mask, IP address and network address.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called address mask.

T

TCP Transmission Control Protocol. The TCP/IP standard transport layer protocol in the Internet suite of protocols, providing reliable, connection-oriented, full-duplex streams. It uses IP for delivery.

TCP/IP Protocol Suite Transmission Control Protocol over Internet Protocol. This is common shorthand, which refers to the suite of transport and application protocols that runs over IP. See IP, ICMP, TCP, UDP, FTP, Telnet, and SNMP.

Telnet The virtual terminal protocol in the TCP/IP suite of protocols, which allows users of one host to log into a remote host and interact as normal terminal users of that host.

topology A network topology shows the computers and the links between them. A network layer must know the current network topology to be able to route packets to their final destination.

U

UDP User Datagram Protocol. A transport layer protocol in the TCP/IP suite of protocols. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgements or guaranteed delivery.

URL Uniform Resource Locator. A standard format for specifying the name, type and location of documents and resources on an Internet. The syntax is type://host.domain[:port]/path/filename, where type specifies the type of document or resource (e.g. http is a file on a WWW server; file is a file on an anonymous FTP server; telnet is a connection to a Telnet-based service). See WWW.

W

WAN Wide Area Network. Any physical network technology that spans large geographic distances. WANs usually operate at slower speeds than LANs. See LAN.

WWW World Wide Web. A hypertext-based, distributed information system based on client - server architecture. Web browsers (client applications) request documents from Web servers. Documents may contain text, graphics and audiovisual data, as well as links to other documents and services. Web servers and documents are identified by URLs (Uniform Resource Locators). See URL.

10 Index

- Access Point9, 10, 11, 14, 26, 31, 32, 35, 41, 42
- ACL12, 35, 36, 49, 51, 52, 59, 61
- Address 9, 11, 13, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 34, 35, 36, 37, 38, 39, 40, 41, 42, 47, 49, 51, 52, 54, 55, 62, 63, 68, 69, 70, 71
- Antenna.....9, 18, 19, 33, 64, 66, 67
- AP search 16, 20, 21
- Application10, 20, 38, 69, 70, 71
- Average load 25
- bridge...9, 10, 11, 12, 13, 14, 15, 19, 26, 32, 33, 52, 53, 54, 56
- Browser.....16, 20, 22, 23, 24, 28, 42
- Channel..... 3, 50, 56, 57, 68
- CLI5, 10, 20, 22, 47, 48, 49, 51
- Client....9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 26, 28, 29, 30, 32, 33, 36, 37, 47, 55, 56, 61, 62, 63, 68, 70, 71
- Commands..... 7, 47, 48, 49, 51
- Community..... 41, 56
- Configuration 7, 9, 10, 20, 21, 22, 23, 26, 27, 28, 29, 31, 32, 37, 45, 47, 50, 51, 52, 53, 54, 55, 56, 61, 68
- Coordinates..... 27, 54, 62
- Data traffic..... 25
- Default 20, 22, 23, 28, 35, 36, 37, 39, 41, 45, 49, 51, 52, 55, 61, 62
- Device mode 48
- Device status..... 24, 25
- DHCP server 13, 16, 22, 28, 29, 37, 51, 61, 63
- DNS 27, 60, 68, 69
- Domain.....3, 27, 32, 50, 57, 68, 71
- Encryption 32, 56, 57, 59
- Ethernet 35, 51, 52, 61
- Examples 5, 47
- Exit 49
- Firewall..... 13, 33, 34, 39, 51, 52, 63, 68, 70
- Firmware 10, 14, 15, 25, 26, 43, 44, 45, 61, 62
- Firmware upload 25
- Frequency 3, 32, 57
- Frequency channel..... 3, 32
- General configuration..... 27, 31
- Hardware 5, 7, 17, 18
- Hardware installation..... 7
- HEX..... 32
- Hostname..... 52, 54
- Hot-Spot..... 12
- HTML browser..... 16, 20
- HTTPS 16
- ICMP34, 39, 53, 69, 71
- Installation 7, 10, 17, 18, 20
- IP address 11, 16, 20, 21, 22, 23, 25, 27, 28, 29, 30, 34, 36, 37, 38, 40, 41, 47, 52, 55, 62, 68, 69, 70, 71
- JavaScript 16, 20, 23
- Key 11, 32, 57, 62
- LAN 7, 11, 12, 13, 14, 15, 16, 17, 18, 19, 29, 30, 33, 34, 35, 37, 38, 55, 60, 61, 64, 68, 69, 70, 71
- Log in..... 23, 47, 71
- Loopback..... 39, 40
- MAC9, 21, 22, 27, 35, 36, 39, 42, 49, 51, 52, 62, 63, 69
- Management 7, 10, 16, 20, 34, 51, 63
- Mobile..... 12, 13, 26, 31, 32, 35, 37
- Monitoring.....42
- Mounting..... 10, 17, 18, 19, 64
- NAT 11, 13, 16, 30, 38, 39, 63, 70
- Network configuration..... 28
- Network statistics 47
- Network status..... 47
- Operating mode 9, 11, 12, 14, 16, 25, 26, 33, 47, 55
- Operating system 7, 16
- Output power 3, 63
- Package content..... 17
- Parameter..... 10, 28, 32, 48, 55
- Password..... 22, 23, 39, 45, 47, 51, 59
- Ping 20, 21
- Policy..... 34, 35, 49, 51, 52, 59, 61, 70
- Port Forwarding..... 13, 38, 39, 53, 63
- Processor load 24
- Reboot..... 24, 25, 42, 45, 49
- Reset..... 22, 36, 41, 45, 65
- Roaming 32, 63
- Router...9, 10, 11, 12, 13, 14, 15, 19, 26, 27, 28, 29, 30, 32, 33, 37, 38, 53, 54, 61, 68, 69, 70, 71
- Rule 33, 34, 35, 36, 37, 38, 51, 52, 53, 56
- Set up 9, 10
- Setup..... 7, 20, 23, 24, 26
- Setup wizard..... 24, 26
- SNMP 10, 20, 41, 51, 56, 59, 62, 63, 64, 71
- Software 5, 17, 20, 65
- Software installation 7
- SSID 24, 32, 42, 56, 57, 60, 62
- Status 20, 23, 24, 25, 40, 44, 47
- Subcommands 48, 49
- Subnet mask 22, 36, 55, 71
- Survey 32, 41, 42, 65
- System tools 24, 47
- Telnet 10, 47, 63, 64, 71
- Upgrade..... 10, 16, 20, 44, 45, 63
- Uptime 24
- User isolation..... 14
- Version 25, 43, 44
- WEP 57
- Wireless... 3, 7, 9, 10, 11, 12, 13, 14, 15, 16, 18, 25, 26, 28, 29, 30, 31, 32, 33, 35, 37, 39, 40, 41, 45, 51, 52, 55, 56, 57, 61, 68
- Wireless configuration 26, 31
- WLAN..... 9, 10, 32

