OSManager

User Guide

Version 1.24b2

Table of Contents:

1. Installation

This section provides a quick step by step guide on how to install the OSManager configuration software. Please follow the steps described below:

- Power on the computer.

- Install the application:

  Insert the given Installation CD into your CD-ROM drive.

  Locate the executable file “setup.exe” and double click it.

  Follow the installation instructions from the Installation Wizard by pressing the “Next” button.

  Provide the destination path of where the application will be installed. To set the path of your choice select Browse and then Next.

  Finish the installation.

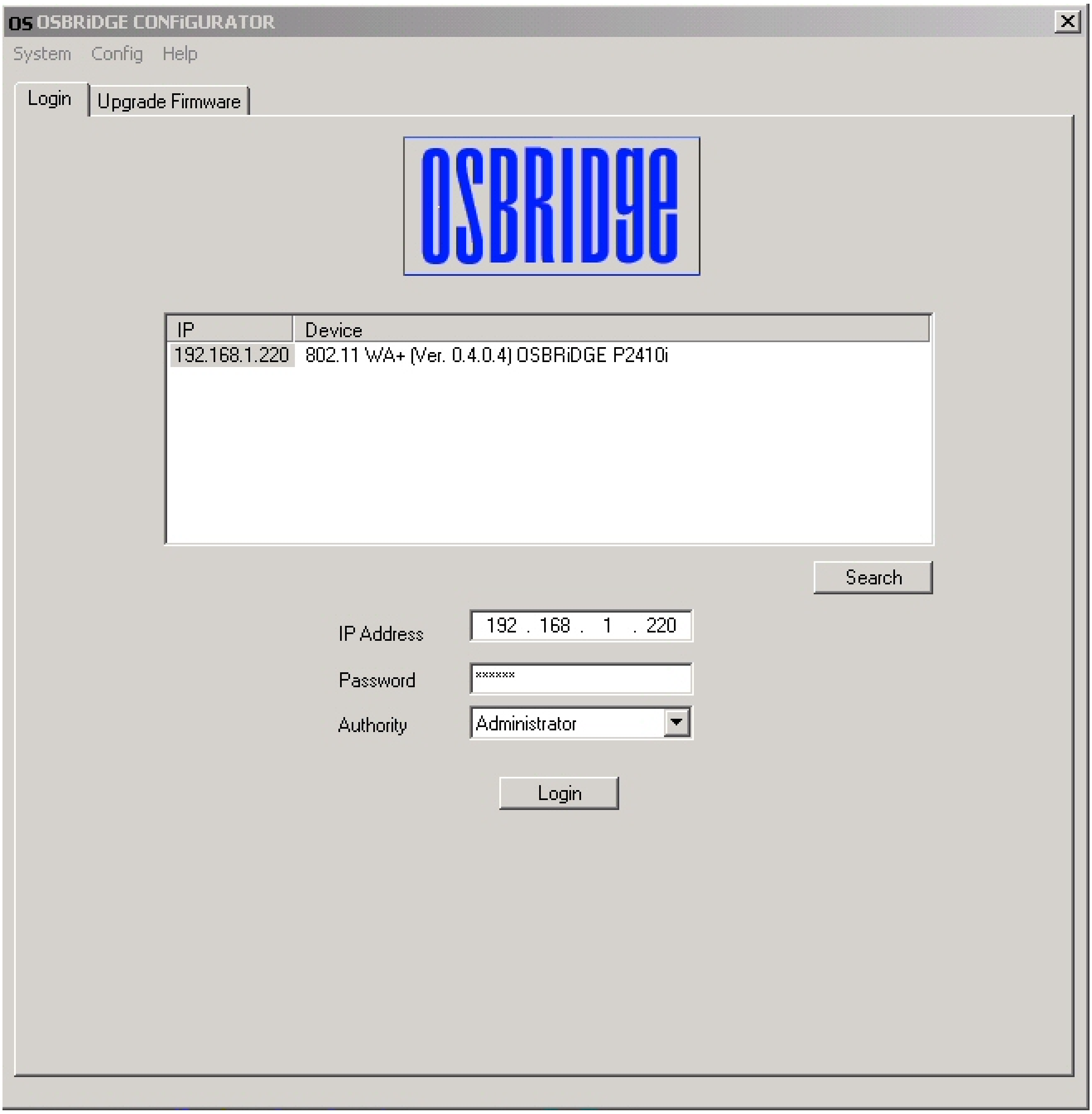
- Connect the OSBRiDGE device to the ethernet port.

- Login into the device using IP address **192.168.1.220** and password **public**. Please note that if you’re connecting to the device from a local network your computer should have IP address from 192.168.1.1 – to 192.168.1.254 range.

2. Configuration

2.1 – Starting the OSManager software.

The OSManager Configuration utility is a SNMP manager used for the configuration of an OSBRiDGE product family. Startup screen looks as follows:



IP	Device
192.168.1.220	802.11 WA+ (Ver. 0.4.0.4) OSBRiDGE P2410i

IP Address: 192 . 168 . 1 . 220

Password: ******

Authority: Administrator

Each OSBRiDGE device comes factotry pre-configured with IP address **192.168.1.220** and password **public**.

2.2 – Login Procedure.

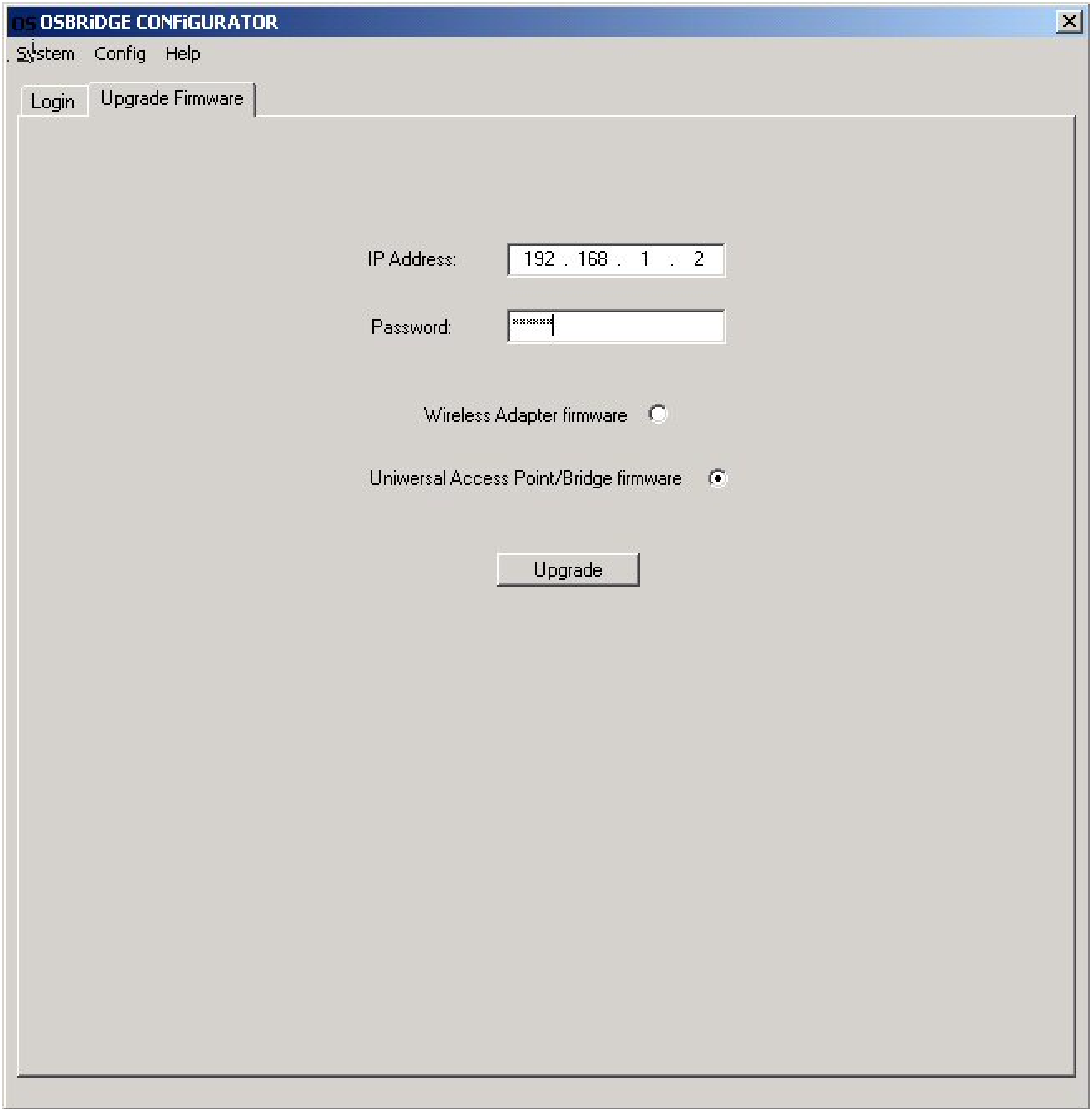
Login - Using this option you can directly connect with the Access Point or Wireless Bridge. First, type its IP Address in the appropriate field. Then, type the appropriate password in the Password field. Finally, you have to select either User or Administrator Authority in the Authority combo-box.

- User Authority allows you to view but not to set or save changes to the OSManager.
- Administrator Authority allows you to either view or set changes to the OSManager.

Search - This option allows you to find and connect with an Access Point or Wireless Bridge without the necessity of knowing its IP Address. Choose this option in order to find the devices available for connection and select one of them. The IP of the selected devices is passed to the IP Address field and prompting you to select Authority and to write the appropriate password at the Authority field.

Logout – Terminates the connection with OSBRiDGE device.

2.3 Upgrading Firmware



IP Address: 192 . 168 . 1 . 2

Password: ******

Wireless Adapter firmware ○

Uniwersal Access Point/Bridge firmware ●

2.4 Different Firmware Versions.

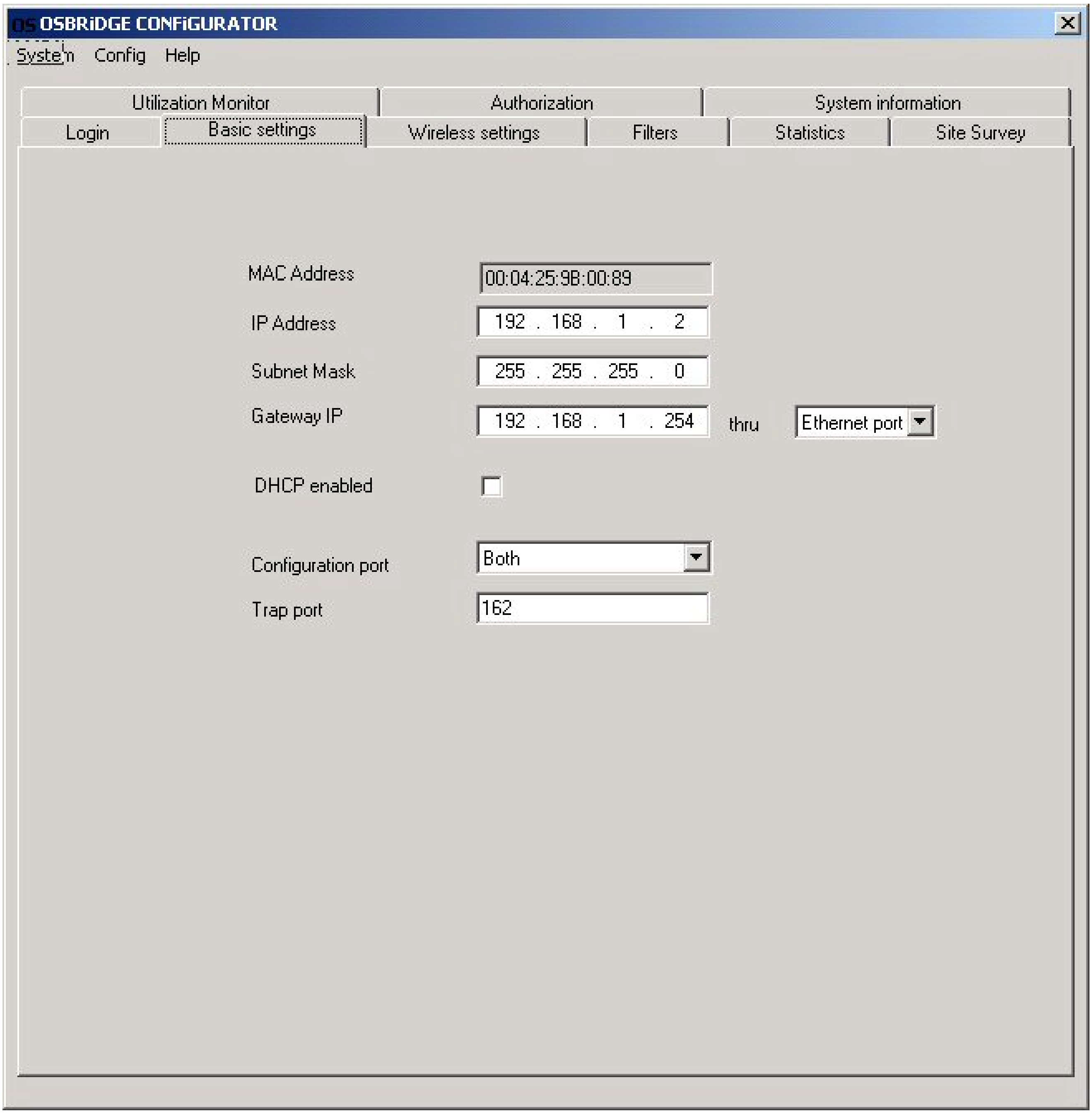
The OSManager software allows you to upload two firmware versions to the OSBRiDGE P24xx type devices – Universal Access Point Firmware (the default one that’s preconfigured at the factory) and Wireless Adapter (WA) Firmware. WA firmware should be flashed to the OSBRiDGE P24xx device **ONLY** when operating as AP Client to devices that don’t support "Address 4" field in IEEE 802.11b Specifications. Known devices not supporting this field are:

- Proxim ORiNOCO Access Points,
- Some Cisco System Access Points,
- Planet WAP-1950 and it’s clones.

All OSBRiDGE devices and most other manufacturers (ie. Smartbridges, Planet, D-Link, Linksys, HostAP based devices) support "Address 4" field in IEEE 802.11b Specifications therefore using WA firmware is not recommended.

Please note that this does not apply to OSBRiDGE M2410 which is supposed to act as an Access Point and doesn’t support uploading alternate client firmware.

2.5 Basic Settings



MAC Address 00:04:25:9B:00:89

IP Address 192 . 168 . 1 . 2

Subnet Mask 255 . 255 . 255 . 0

Gateway IP 192 . 168 . 1 . 254 thru Ethernet port

DHCP enabled □

Configuration port Both

Trap port 162

MAC Address – Device MAC address is displayed here.

IP Address – You can view/change device IP Address here.

Subnet Mask – You can view/change device Subnet Mask here.

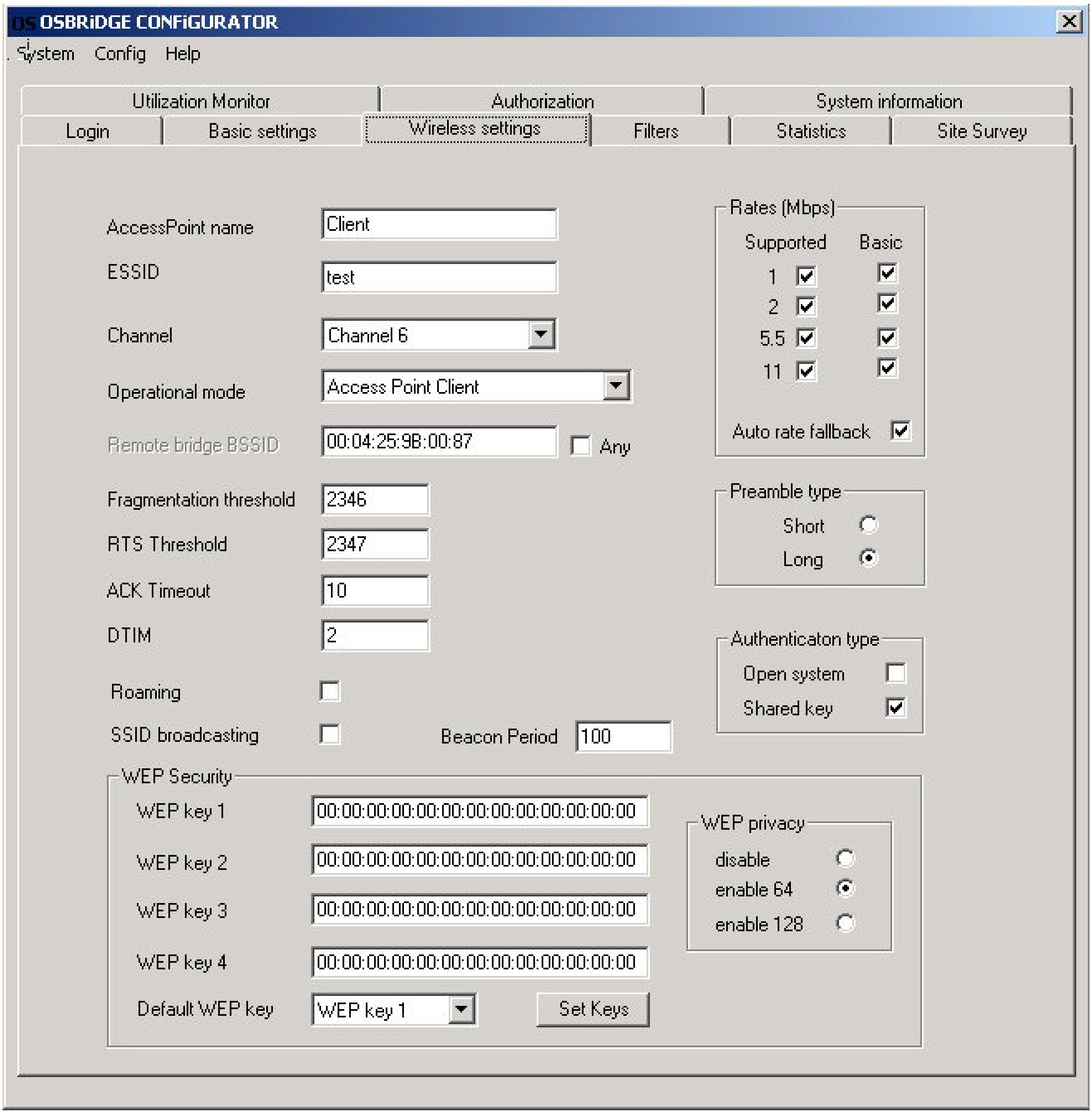
Gateway IP – You can view/change device default gateway IP here. You should also select whether the default gateway is available through wireless or ethernet port.

DHCP Enabled – The option to enable or not the DHCP client function of the Wireless Bridge. Device assumes DHCP server is available on the same port as Default Gateway selected above.

Configuration Port – Here you can select which port (Ethernet and/or Wireless) will be used for the AP configuration.

Trap Port - Trap port is UDP port that the AP will use to send the SNMP traps.

2.6 Wireless Settings



AccessPoint name: Client

ESSID: test

Channel: Channel 6

Operational mode: Access Point Client

Remote bridge BSSID: 00:04:25:9B:00:87 □ Any

Fragmentation threshold: 2346

RTS Threshold: 2347

ACK Timeout: 10

DTIM: 2

Roaming □

SSID broadcasting □

Beacon Period: 100

Rates (Mbps)

	Supported	Basic
1	☑	☑
2	☑	☑
5.5	☑	☑
11	☑	☑

Auto rate fallback ☑

Preamble type
Short ○
Long ●

Authenticaton type
Open system □
Shared key ☑

WEP Security
WEP key 1: 00:00:00:00:00:00:00:00:00:00:00:00:00
WEP key 2: 00:00:00:00:00:00:00:00:00:00:00:00:00
WEP key 3: 00:00:00:00:00:00:00:00:00:00:00:00:00
WEP key 4: 00:00:00:00:00:00:00:00:00:00:00:00:00
Default WEP key: WEP key 1

WEP privacy
disable ○
enable 64 ●
enable 128 ○

Access Point Name – The name of the OSBRiDGE device.

ESSID - It is an ASCII string up to 32 characters used to identify a WLAN that prevents the unintentional merging of two co-located WLANs. The ESSID value must be the same in all stations and AP in the extended WLAN.

Channel - Select the channel to be used. Depending on the Regulatory Domain of the device the number of available channels can be 1 - 14.

Operational Mode:

- **Access Point -** This mode provides access from Wireless Stations to Wired LANs and from Wired LANs to Wireless Stations. Furthermore, Wireless Stations within the range of the AP device may communicate with each other via the AP (unless inter client traffic is disabled).

- **Access Point Client -** This mode allows the connection of one or more remote LANs with a central LAN, creating thus an extended single virtual LAN. In this way, any station of the Remote LAN can successfully communicate with any station of the central LAN, as if all of them belonged to the same physical LAN.

- **Wireless Bridge -** This mode enables a wireless connection between two or more Wired LANs. Two types of connections are possible:

  Point to Point - The Wireless Bridge can communicate with a Wireless Bridge having the MAC address specified in the remote BSSID address field.

  Point to Multipoint - The Wireless Bridge can communicate with any Wireless Bridge available in the same channel. When the MAC Authorization Algorithm is enabled, the Wireless Bridge can communicate with any Wireless Bridge whose MAC Address exists in the Authorization Table.

- **Wireless Repeater -** This mode is used to increase the coverage area of an Wireless Network. The Wireless Repeater starts acting as an Access Point after it has associated itself with another Access Point (Parent Access Point).

Prefered bridge BSSID - It is enabled if you select the AP Client option. BSS corresponds to the MAC Address of the AP you want to connect to. You can also select **ANY** to connect to an Access Point whose ESSID matches the string selected above.

Fragmentation Threshold – The size at which the packets will be fragmented – you can choose from 256 to 2346 bytes.

RTS Threshold – Minimum packet size to require an RTS (Request To Send) handshaking limiting on-the air collisions. For packets smaller than this threshold, an RTS is not sent and the packet is transmitted directly to the WLAN. For packets larger than this threshold the RTS/CTS handshaking is established.

ACK Timeout – Value that represents the time after which wireless bridge, if ACK packet is not received, retries sending data packet. This is especialy useful for long range links and links where devices report lot of duplicate packets – increasing this value helps improving performance.

DTIM – Delivery Traffic Indication Message. A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

Roaming – (IEEE 802.11d): The OSBRiDGE device can support the International Roaming function if this option is enabled.

SSID Broadcasting - When checked the device broadcasts the ESSID to the stations, if not checked then the stations must know the ESSID in advance.

Beacon Period – Rate - By default the unit adaptively selects the highest possible rate for transmission. Select the basic & supported rates to be used among the following options 1 - 2 - 5.5 - 11 Mbps.

Auto Rate Fall Back - When this is enabled the transmission rate is the optimum rate. In case of obstacles or interference, the system will automatically fall back. Using auto rate fallback is not advised while operating in Access Point mode, as it may cause the overall wireless network performance to drop drasticaly.

Preamble Type (Short/Long) - Preamble is the first subfield of PPDU, which is the appropriate frame format for transmission to PHY (Physical layer). There are two options, Short Preamble and Long Preamble. The Short Preamble option improves throughput performance.

Authentication Type -

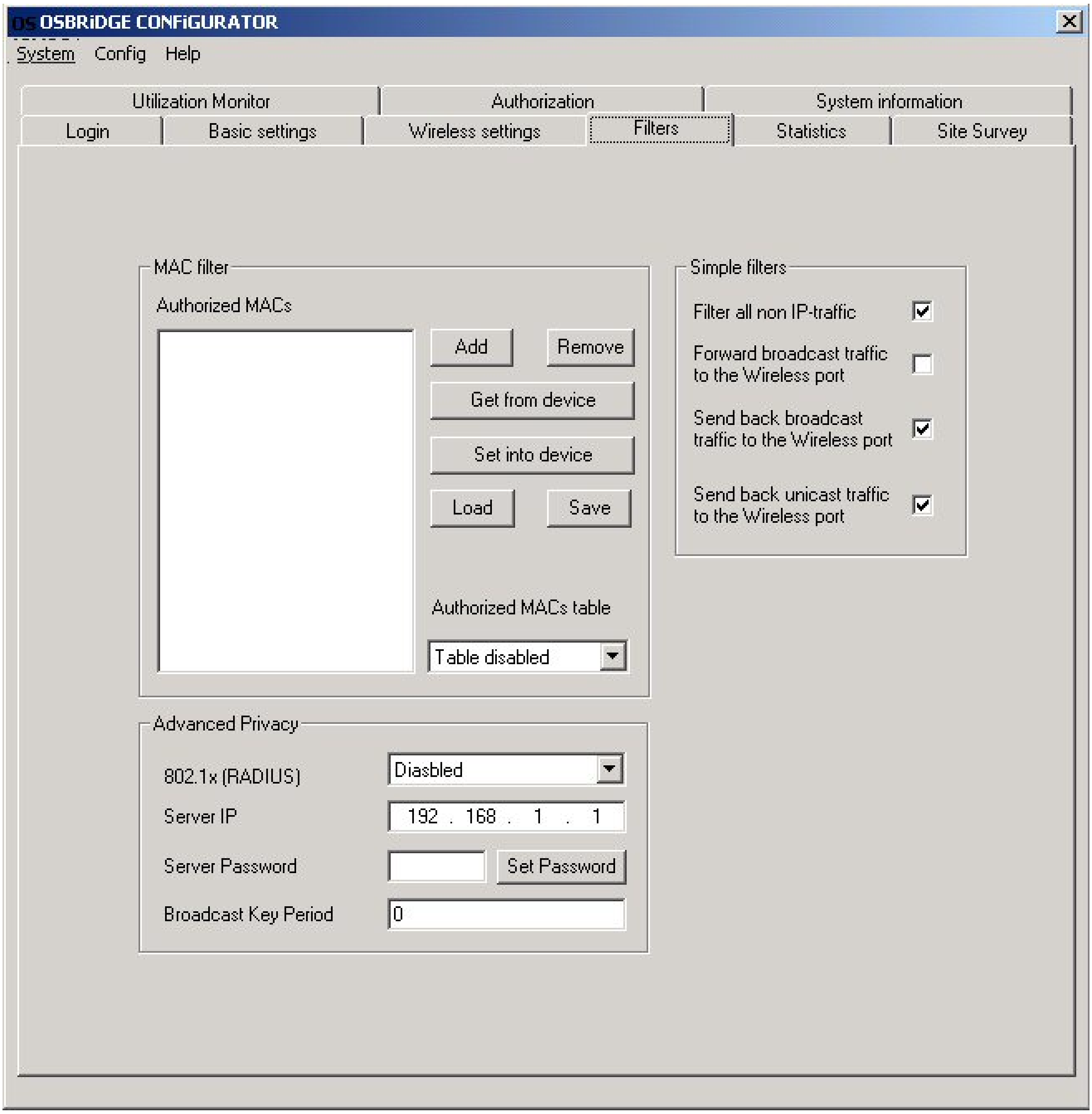
Open System: With this setting any station in the WLAN can associate with an AP and receive and transmit data (null authentication).

Shared Key: With this setting only stations using a shared key encryption identified by the AP are allowed to associate with it.

Both: With this setting stations communicate with the Access Point either with or without data encryption.

WEP Security - Here you can enter the encryption key values using the Wireless Equivalent Privacy (WEP) option. Write the values and press "Set" to download (WEP key is write-only, so it is not possible to retrieve the key values). There are four 5 Hex digit encryption keys available if you select 64bit WEP and there are four 13 Hex digit encryption keys available if you select 128bit WEP. Enable the WEP (Wired Equivalent Privacy) option in order to activate WEP encryption for transmissions between the stations and the AP. WEP is an authentication algorithm which protects authorized Wireless LAN users against eavesdropping.

2.7 Filters



Filter all non IP-traffic ☑

Forward broadcast traffic to the Wireless port ☐

Send back broadcast traffic to the Wireless port ☑

Send back unicast traffic to the Wireless port ☑

Authorized MACs table: Table disabled

802.1x (RADIUS): Diasbled

Server IP: 192 . 168 . 1 . 1

Server Password:

Broadcast Key Period: 0

MAC Filter - For security reasons the AP can use the Authorization Table option. The AP allows only authorized stations to get associated to it. Under the Authorized MAC Address option you may press the following buttons:

Add – With this button you can add MAC address to the Authorized MAC address list.

Remove - With this button you can remove MAC address from the Authorized MAC address list.

Get from device – this button allows you to read Authorized MAC address list from the device.

Set into device – this button allows you to write Authorized MAC address list to the device.

Load - Use this button in order to load a text file with the MAC Addresses that can be associated with the AP (Authorized MAC Addresses).

Save - Use this button in order to save a text file with the MAC Addresses that can be associated with the AP (Authorized MAC Addresses).

Authorized MAC Table – Here you can select the way MAC filtering option operates:

Table disabled - the device will not use MAC authorization.

Acccept table type – the device will allow only the MAC addresses from the table to pass through.

Deny table type – the device will deny the MAC addresses from the table and not let them pass through.

Please note that MAC authorization applies to wireless interface while operating in Access Point mode and to the ethernet interface while operating in the Access Point Client mode. The MAC authorization is not currently supported with Wireless Adapter firmware (figure 2.4).

Advanced Privacy – Here you can enable the 802.1x authorization. Please provide Server IP address, server password and Beacon Key period values.

Simple Filters:

Filter all non-IP traffic – Only the IP protocol packets will pass through the WLAN and any other protocol will be filtered out.

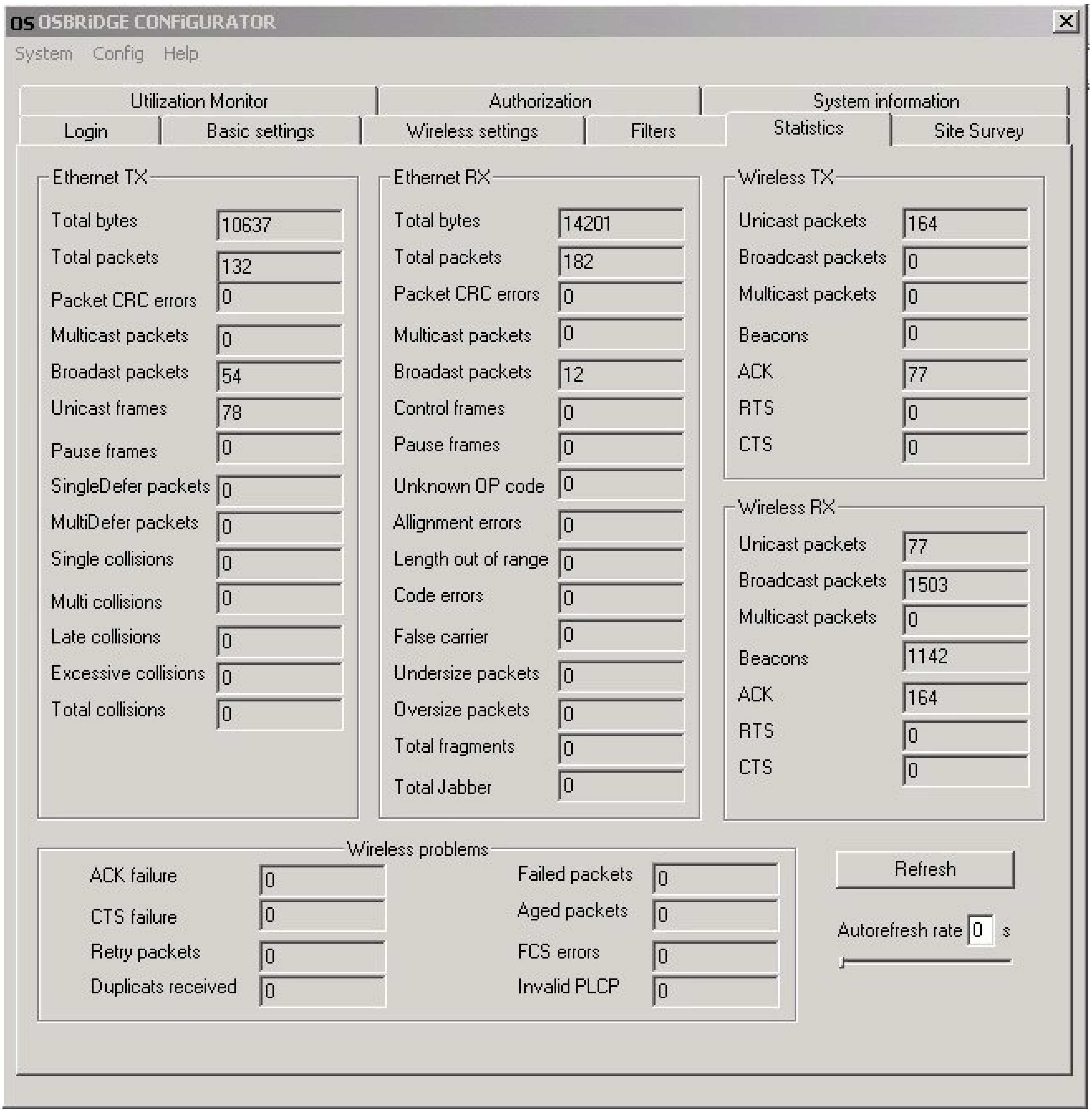
Forward Broadcast Traffic to the Wireless Port – The device should not forward broadcast traffic to the air.

Send back Broadcast Traffic to the Wireless Port - The AP should not send back to the air broadcast traffic received from the air.

Send back Unicast Traffic to the Wireless Port - The AP should not send back to the air unicast traffic received from the air.

Please note that enabling both "Send back unicast/broadcast traffic to the wireless port" filters, while operating in the Access Point mode, will disable inter-client traffic between wireless stations connected to this Access Point.

2.8 Statistics



Ethernet TX

Total bytes	10637
Total packets	132
Packet CRC errors	0
Multicast packets	0
Broadast packets	54
Unicast frames	78
Pause frames	0
SingleDefer packets	0
MultiDefer packets	0
Single collisions	0
Multi collisions	0
Late collisions	0
Excessive collisions	0
Total collisions	0

Ethernet RX

Total bytes	14201
Total packets	182
Packet CRC errors	0
Multicast packets	0
Broadast packets	12
Control frames	0
Pause frames	0
Unknown OP code	0
Allignment errors	0
Length out of range	0
Code errors	0
False carrier	0
Undersize packets	0
Oversize packets	0
Total fragments	0
Total Jabber	0

Wireless TX

Unicast packets	164
Broadcast packets	0
Multicast packets	0
Beacons	0
ACK	77
RTS	0
CTS	0

Wireless RX

Unicast packets	77
Broadcast packets	1503
Multicast packets	0
Beacons	1142
ACK	164
RTS	0
CTS	0

Wireless problems

ACK failure	0	Failed packets	0
CTS failure	0	Aged packets	0
Retry packets	0	FCS errors	0
Duplicats received	0	Invalid PLCP	0

Autorefresh rate 0 s

Statistics:

Ethernet TX:

Total bytes - The number of bytes in the frames that were transmitted.

Total packets – The number of transmitted packets.

Packet CRC errors – The number of packets transmitted with CRC Errors.

Multicast packets – The number of multicast packets that were transmitted.

Broadcast packets – The number of broadcast packets that were transmitted.

Unicast frames – The number of unicast frames that were transmitted.

Pause frames – The number of pause control frames that were transmitted.

SingleDefer Packets - The number of packets which was deferred on its first transmission attempt and did not experience any subsequence collisions during transmission.

MultiDefer Packets - The number of packets aborted which were deferred for an excessive period of time.

Single Collisions - The number of single collision packets. The statistic counter register is incremented during transmission.

Multi Collisions - The number of Multiple Collision Packets. It is incremented for each frame transmitted which experienced 2-15 collisions (including any late collisions) during transmission.

Late Collisions - The number of late collision packets. It is incremented for each packet transmitted which experienced a late collision during a transmission attempt.

Excessive Collisions - The number of Excessive Collision packets. It is incremented for each frame that experienced 16 collisions during transmission and was aborted.

Total Collisions - The number of collisions experienced during the transmission of a frame as defined as the simultaneous presence of signals on the DO and RD circuits.

Ethernet RX:

Total bytes - The number of bytes in the frames that were received.

Total packets – Total number of received packets.

Packet CRC errors - The number of packets with CRC Errors.

Multicast packets - The number of multicast packets that were successfully received.

Broadcast packets - The number of broadcast packets that were successfully received.

Control frames - The number of control frames that were received.

Pause frames - The number of pause frames that were successfully received.

Unknown OP code - The number of frames that were received which contains an opcode other than a pause.

Alignment Error - The number of alignment errors.

Length Out Of Range - The number of frames received in which the 802.3 length field did not match the number of data bytes actually received.

Code Error - The number of received code error.

False Carrier - The number of false carriers.

Undersize Packets - The number of packets that were received which are less than 64 bytes in length and contains a valid FCS and were well formed.

Oversize Packets - The number of packets that were received with exceeded 1518 bytes and contains a valid FCS and were otherwise well formed.

Total Fragments - The number of packets received which are less than 64 bytes in length and contain an invalid FCS, include integral and non-integral lengths.

Total Jabber – This value corresponds to the number of packets received which exceed the 1518 byte length and contain an invalid FCS, include alignment errors.

Wireless TX:

Unicast Packets - The number of unicast packets successfully transmitted.

Broadcast Packets - The number of broadcast packets transmitted.

Multicast Packets - The number of multicast packets transmitted.

Beacon - The number of Beacon packets transmitted.

ACK - The number of ACK packets transmitted in response to successfully received packets.

RTS - The number of Request To Send packets that were successfully transmitted.

CTS - The number of Clear To Send packets that were successfully transmitted.

Wireless RX:

Unicast Packets - The number of unicast packets successfully received.

Broadcast Packets - The number of broadcast packets received.

Multicast Packets - The number of multicast packets received.

Beacon - The number of Beacon packets received.

ACK - The number of packets transmitted that had their corresponding ACK packet successfully received.

RTS - The number of Request To Send packets that were successfully received.

CTS - The number of Clear To Send packets received in response to a RTS.

Wireless Problems:

ACK Failure - The number of packets transmitted that did not have their corresponding ACK packet successfully received.

CTS Failure - The number of packets for which no CTS packet was received in response to a RTS packet being sent.

Retry Packets - The number of packets that were retransmitted.

Duplicates Received - Number of duplicate frames received.

Failed Packets - The packets not transmitted successfully.

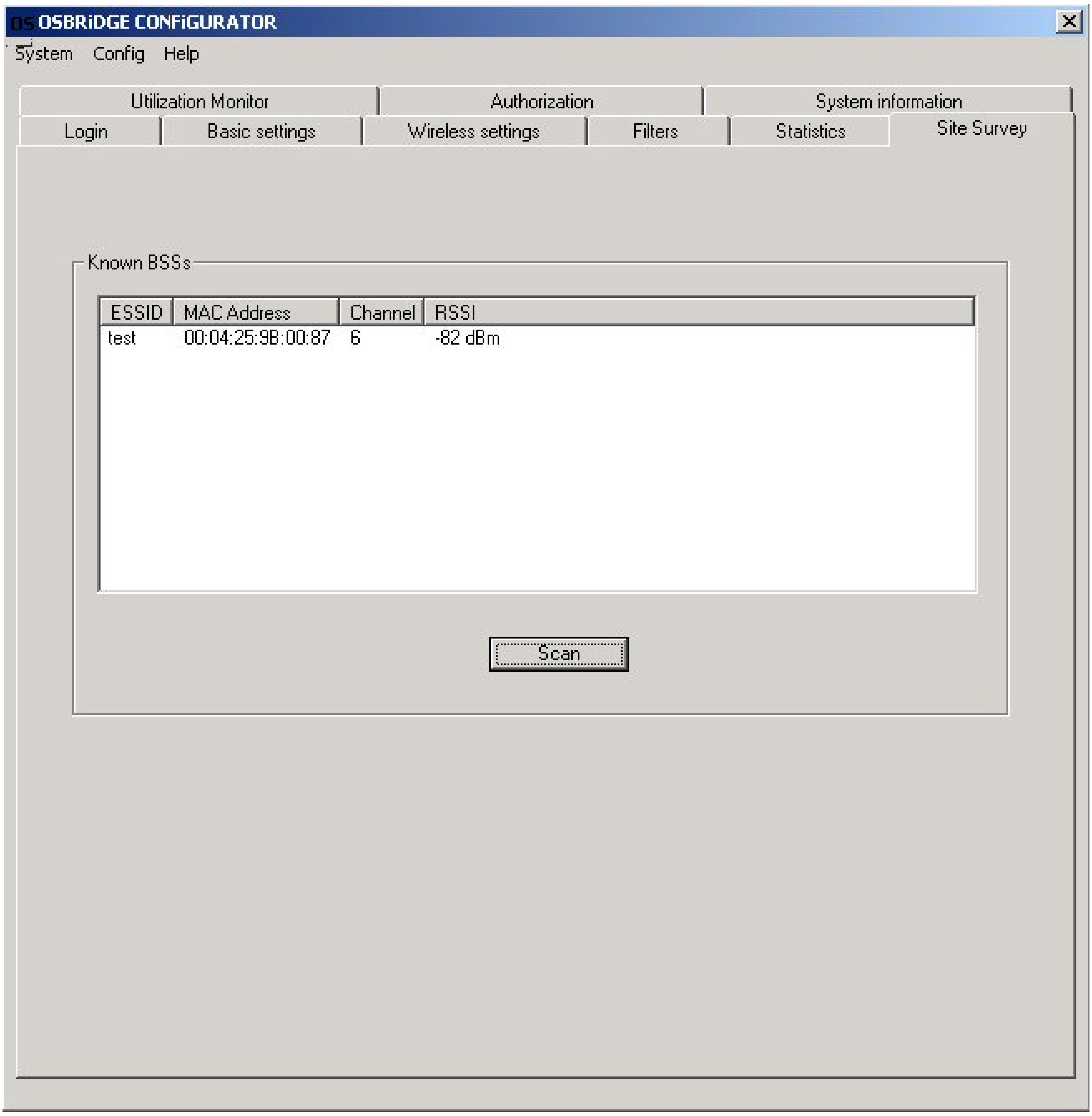
Aged Packets – Number of buffered frames that were aged out from buffer per station.

Invalid PLCP - The number of packets received with Invalid Physical Layer Convergence Procedure.

Refresh – Manualy read current device statistics.

Auto Refresh Rate – Here you can select the interval (1 to 9 seconds) the OSManager will automaticaly refresh statistics data from device.

2.9 Site Survey



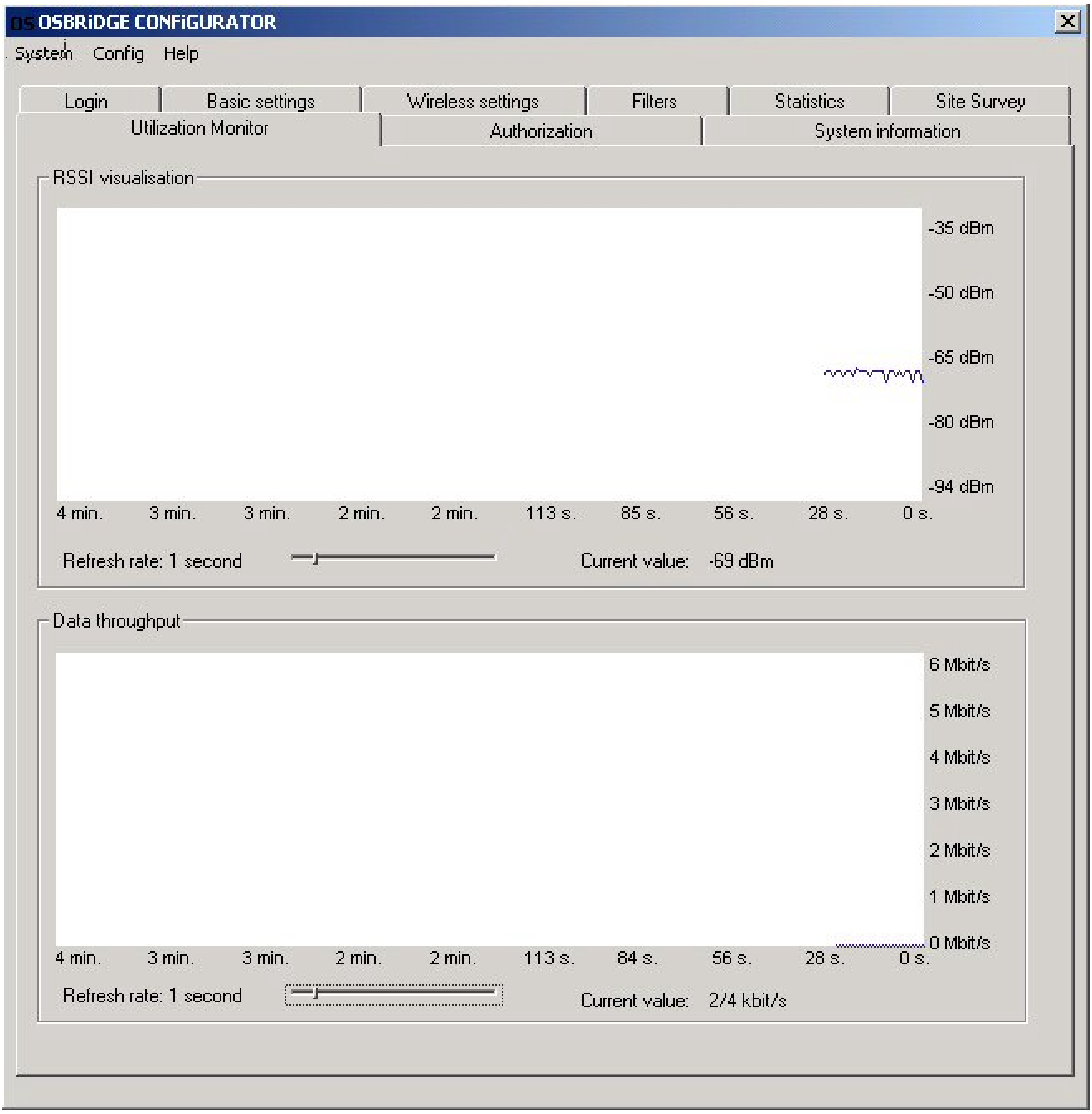
Known BSSs

ESSID	MAC Address	Channel	RSSI
test	00:04:25:9B:00:87	6	-82 dBm

Site Survey window allows you to scan for other WLAN devices operating nearby your OSBRiDGE and allow to see which of them are in range and what channel they operate in.

Please note that pressing Scan button puts device into scan mode, which will last for a couple of seconds, where normal wireless communication is interrupted. Using Scan option is not advised while you're connected to the OSBRiDGE device through the radio interface – it will cause connection loss with the managed device.

2.10 Utilization Monitor



Refresh rate: 1 second

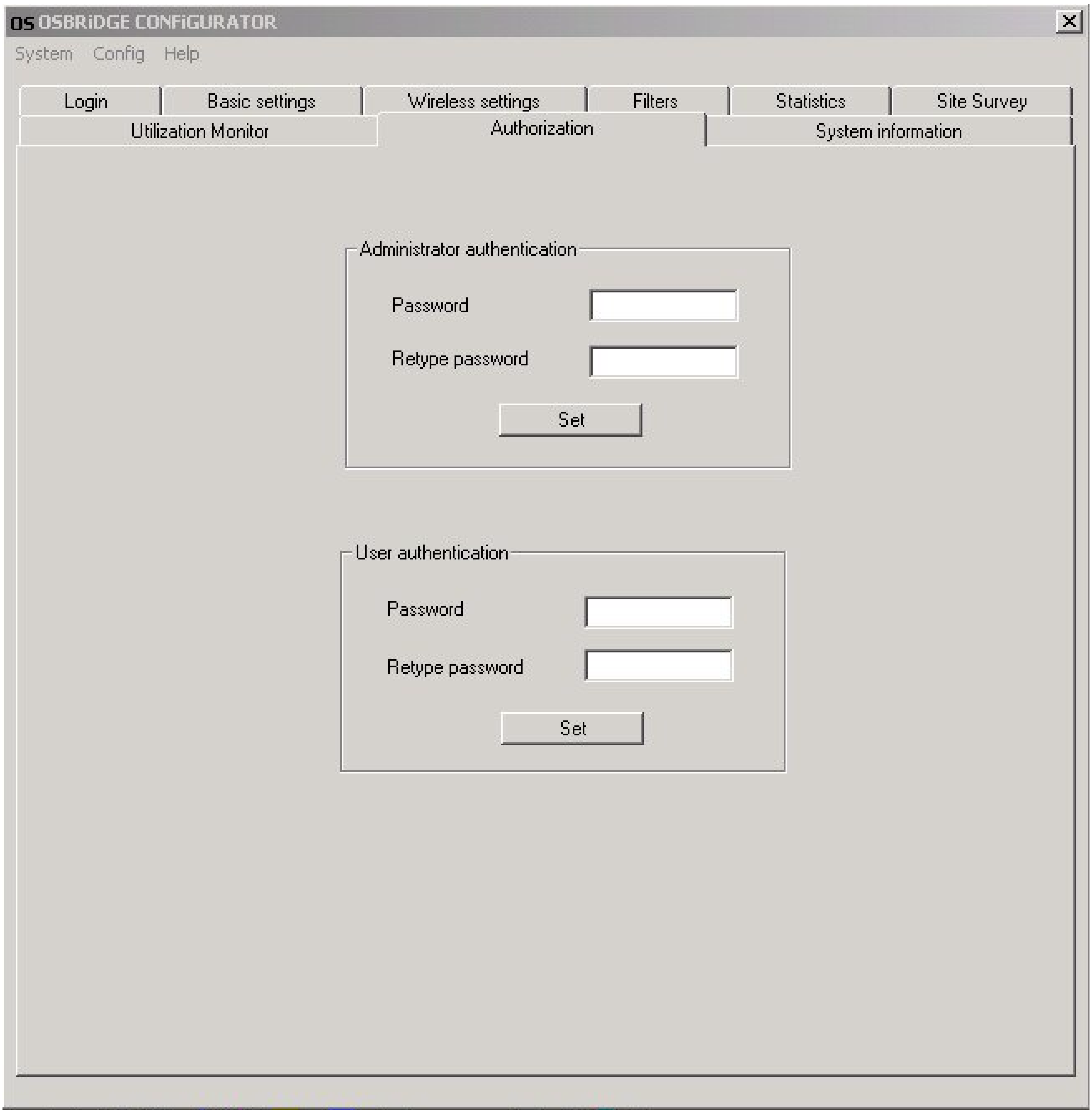
Current value: -69 dBm

Refresh rate: 1 second

Current value: 2/4 kbit/s

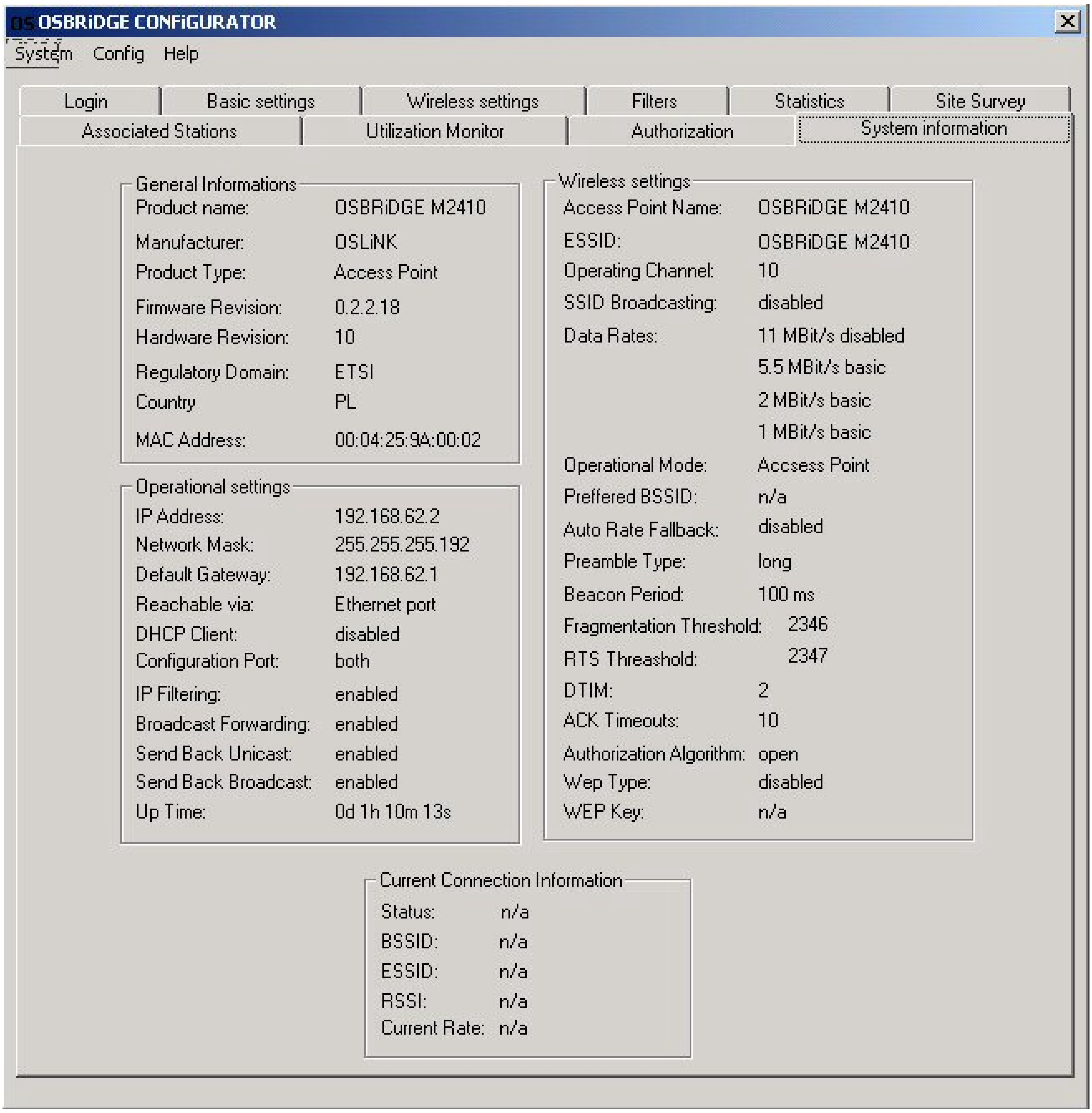
This windows of the OSManager shows RSSI graph history (devices operating as Access Point Clients and Wireless Adapters only) and Data Throughput history. You can change interval time the Manager will read current values from the monitored device.

2.11 Authorization



Authorization - Using this option the Administrator can change the passwords used in the login window of the OSManager for the User and the Administrator Authority.

2.12 System Information



General Informations

Product name:	OSBRiDGE M2410
Manufacturer:	OSLiNK
Product Type:	Access Point
Firmware Revision:	0.2.2.18
Hardware Revision:	10
Regulatory Domain:	ETSI
Country	PL
MAC Address:	00:04:25:9A:00:02

Operational settings

IP Address:	192.168.62.2
Network Mask:	255.255.255.192
Default Gateway:	192.168.62.1
Reachable via:	Ethernet port
DHCP Client:	disabled
Configuration Port:	both
IP Filtering:	enabled
Broadcast Forwarding:	enabled
Send Back Unicast:	enabled
Send Back Broadcast:	enabled
Up Time:	0d 1h 10m 13s

Wireless settings

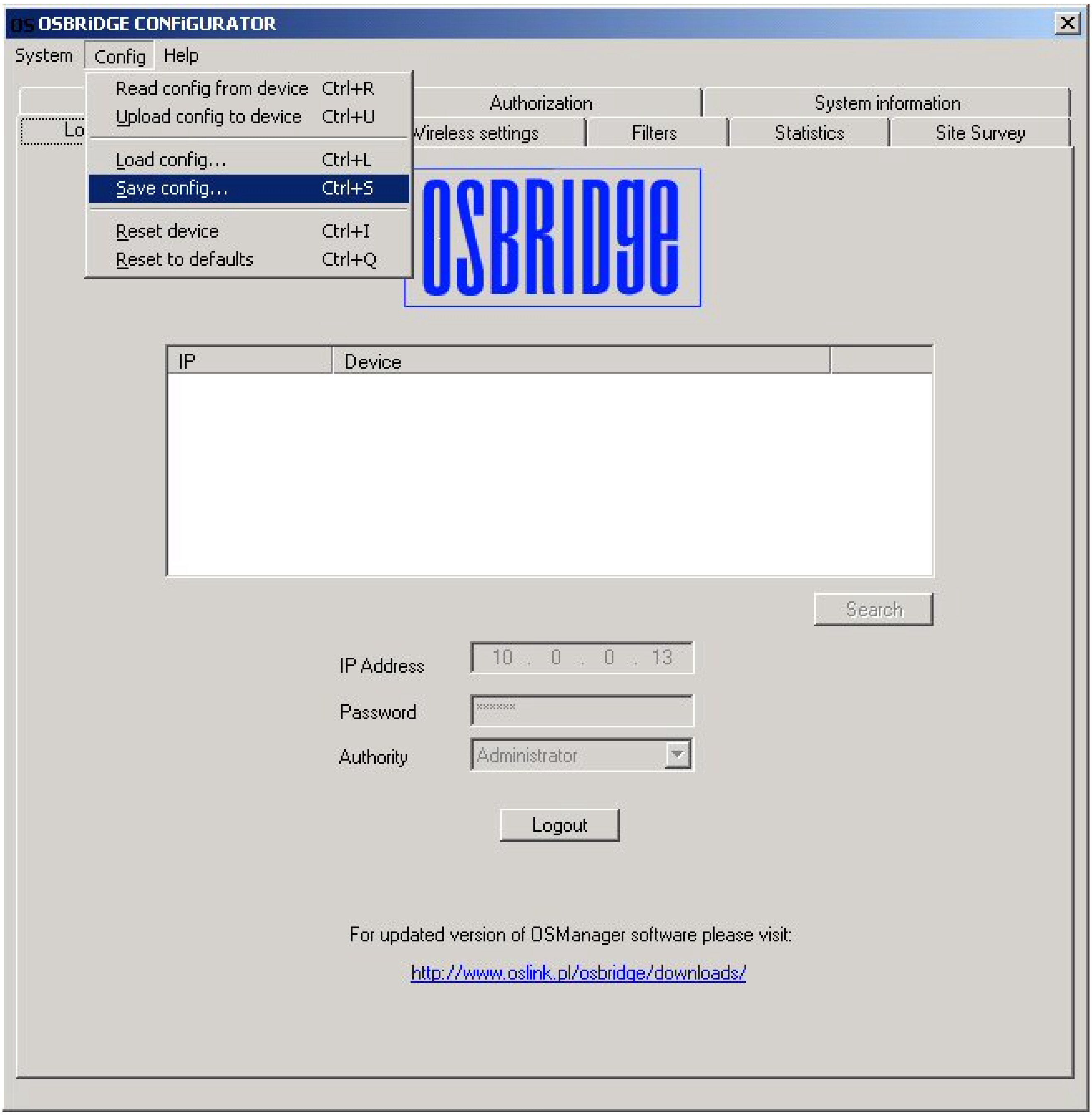
Access Point Name:	OSBRiDGE M2410
ESSID:	OSBRiDGE M2410
Operating Channel:	10
SSID Broadcasting:	disabled
Data Rates:	11 MBit/s disabled 5.5 MBit/s basic 2 MBit/s basic 1 MBit/s basic
Operational Mode:	Accsess Point
Preffered BSSID:	n/a
Auto Rate Fallback:	disabled
Preamble Type:	long
Beacon Period:	100 ms
Fragmentation Threshold:	2346
RTS Threashold:	2347
DTIM:	2
ACK Timeouts:	10
Authorization Algorithm:	open
Wep Type:	disabled
WEP Key:	n/a

Current Connection Information

Status:	n/a
BSSID:	n/a
ESSID:	n/a
RSSI:	n/a
Current Rate:	n/a

This is the default screen you will see after logging into OSBRiDGE device. It shows summary information about device operating parameters, configuration and its current state.

2.13 Configuration Menu



IP Address 10 . 0 . 0 . 13

Password ******

Authority Administrator

For updated version of OSManager software please visit:

http://www.oslink.pl/osbridge/downloads/

Read config from device (CTRL+R) – This option reloads configuration from the currently managed device.

Upload config to device (CTRL+U) – This option uploads current configuration to the device.

Load config (CTRL+L) – This option loads configuration from file to the manager.

Save config (CTRL+S) – This option saves current configuration to file.

Reset device (CTRL+I) – This option resets currently managed device.

Reset to defaults (CTRL+Q) – This option resets currently managed device to factory default settings.

3. Glossary

A

Ad-Hoc Mode - A client setting that provides independent peer to peer connectivity in a wireless LAN. An alterative setup is where PCs communicate with each other hrough an access point.

B

Bandwidth - The transmission capacity of a given facility, in terms of how much ata the facility can transmit in a fixed amount of time; expressed in bits per second bps).

Bit - A binary digit. The value - 0 or 1- used in the binary numbering system. Also, he smallest form of data.

D

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

DHCP server and client - DHCP stands for Dynamic Host Configuration Protocol. This protocol is designed to automatically load parameters for the TCP/IP network, including the IP address, host name, domain name, net mask, default gateway, and name server address. The machine that provides this service is called the DHCP server, and its client computers are called DHCP clients. If client computers support DHCP, a TCP/IP configuration is not needed on each client computer.

Driver - A workstation or server software module that provides an interface between a network interface card and the upper-layer protocol software running in the computer; it is designed for a specific NIC, and is installed during the initial installation of a network compatible client or server operating system.

DSSS (Direct-Sequencing Spread-Spectrum) - DSSS operate over the radio airwaves in the unlicensed ISM band (industrial, scientific, medical). DSSS uses a radio transmitter to spread data packets over a fixed range of frequency band.

E

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - The most widely used LAN access method which is defined by the IEEE 802.3 standards. Ethernet is normally a shared media LAN meaning all devices on the network segment share total bandwidth. Ethernet networks operate at 10Mbps using CSMA/CD to run over 10Base T cables.

F

Firmware - Program that is inserted into programmable read-only memory (programmable read-only memory), thus becoming a permanent part of a computing device.

Fragmentation Threshold Value - Indicates how much of the network resources is devoted to recovering packet errors. The value should remain at its default setting of 2432. If you experience high packet error rates, you can decrease this value.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

I

IEEE - The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers.

IEEE 802.11b Standard - The IEEE 802.11b Wireless LAN standards subcommittee formulatings standards for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate.

Infrastructure Mode - A client setting providing connectivity to an Access Point. As compared to Ad-Hoc Mode where PCs communicate directly with each other clients set in infrastructure Mode all pass data through a central Access Point. The Access Point not only mediates Wireless network traffic in the immediate neighborhood but also provides communication with the wired network.

IP Address - An IP address is a 32-bit number that identifies each sender & receiver of information that is sent across the Internet. An IP address has two parts: the identifier of a particular network on the Internet and one identifier of a particular device (which can be a server or a workstation within that network).

ISM band - The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

L

LAN - A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within anoffice building).

M

MAC Address - 12-digit hexadecimal number that identifies a networking product on the network.

Mbps (**M**ega**b**its **p**er **s**econd) - One million bits per second; unit of measurement for data transmission.

N

Network - A system that transmits any combination of voice, video and/or data between users.

Node - A network junction or connection point, typically a computer or work station.

O

Open System - Is when the sender and the recipient do not share a secret key. Each party generates its own key -pair and asks the receiver to accept the (usually randomly) generated key. Once accepted, this key is used for a short time only; then a new key is generated and agreed upon.

P

Packet - A unit of data routed between an origin and a destination in a network.

PCMCIA - Personal Computer Memory Card International Association

Plug and Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

R

Roaming - The ability to use a wireless device and be able to move from one access point's range to another without losing the connection.

S

Shared Key - Is when both the sender and recipient share a secret key. Both units use this key for an extended length of time, sometimes indefinitely. Any eavesdropper that discovers the key may decipher all packets until the key is changed.

Signal Strength - The signal level indicates the strength of the signal as received at the wireless network interface.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A standard network protocol that can be used to manage networks locally, or worldwide via the Internet.

SSID (Service **S**et **I**dentifier) - Is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the network. It is case sensitive and must not exceed 32 characters.

Static IP Address - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.

Subnet - A subnet is a logical sub-division of a Local Area Network that has been divided by means of routers or gateways. A subnet may include multiple LAN segments. Each subnet is identified by the Subnet Mask.

T

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

W

WEP (**W**ired **E**quivalent **P**rivacy) - The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired LAN medium that does not employ cryptographic techniques to enhance privacy.