LOHU 2527L

Outdoor Wireless Access Point / Bridge

User Manual
Version 2.3

LohuisNetworks

Voltlaan 408 – 2681 TV Monster – Netherlands
Tel : +31208080743
Email : Info@lohuisnetworks.com
Website : www.lohuisnetworks.com

International Numbers:

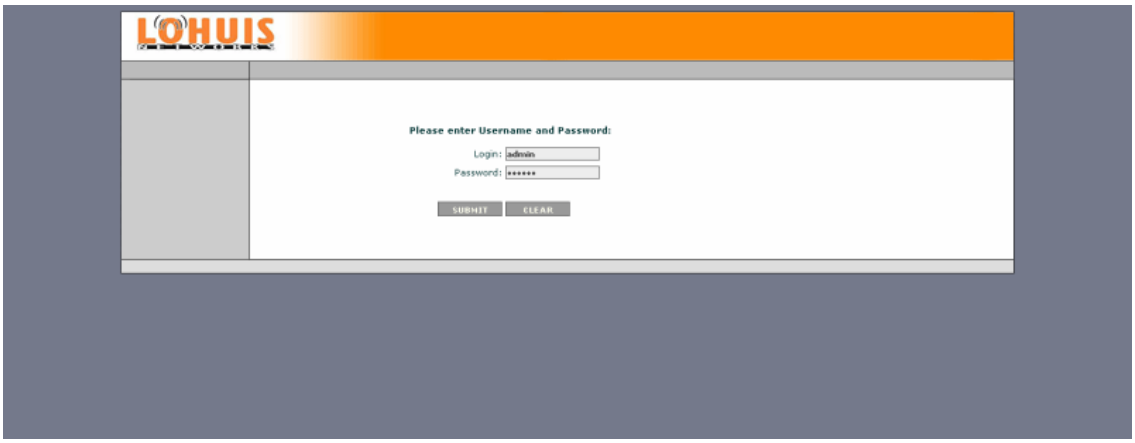
Dubai :	+97142280111
United States:	+12123812983
United Kingdom:	+442033557669
France :	+33170612716
Italy:	+390662207084
Japan:	+81345506867
Argentina:	+541152391407
Brazil :	+552135219853
Pakistan:	+92217019804

Setup and configuration

Lohuis 2527L devices are configurable via WWW interface. Each device uses following default settings:

IP Address: 192.168.1.251
Subnet Mask: 255.255.255.0
Login: admin
Password: public

The initial login screen looks as follows:

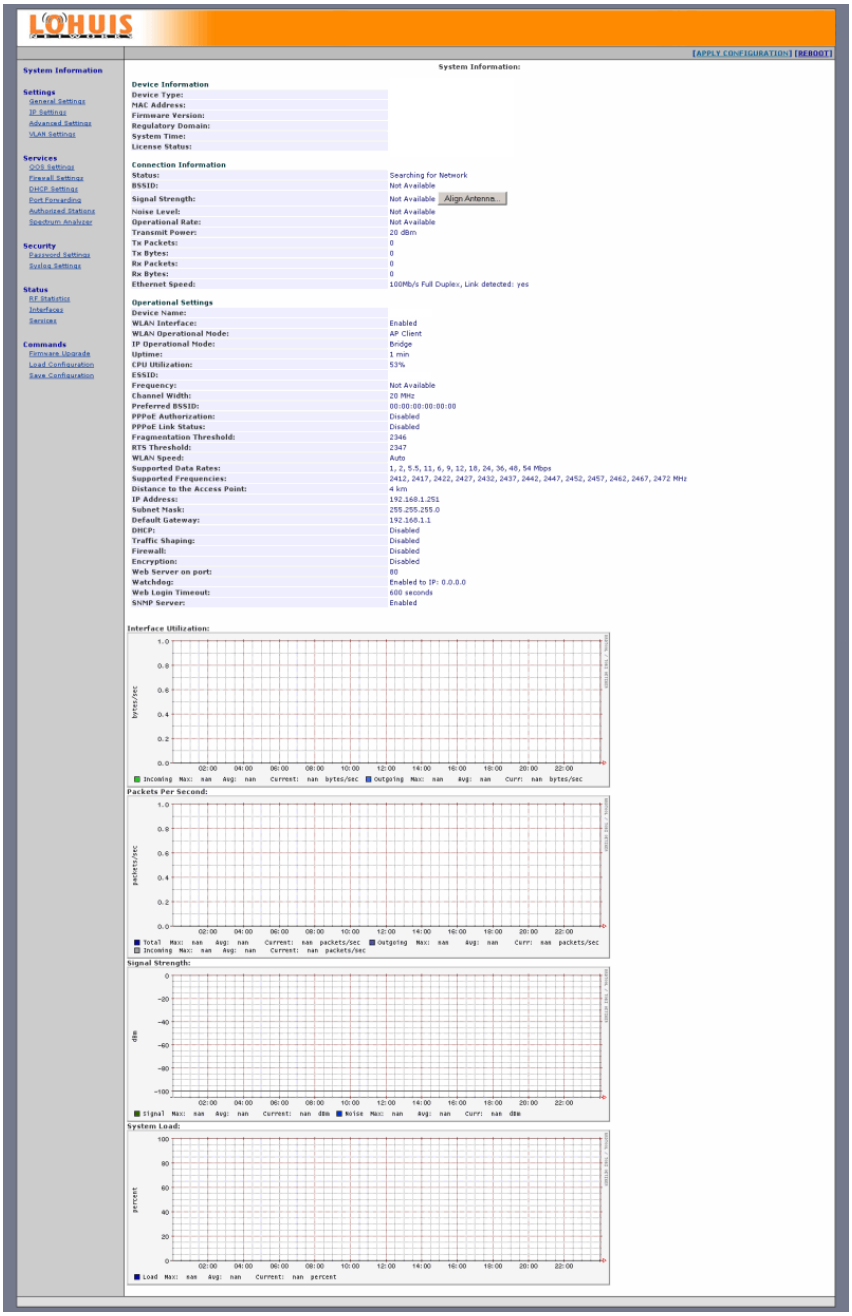


Please enter username and passwords, then press submit to log into the device.

Please note that after changing device parameters and pressing submit button, new settings will only be saved when you press "Apply Changes" button at the right bottom of the configuration page. You also need to reboot the device for the device to start with new settings.

System Information

System information tab shows information about system hardware and operational parameters:



Device Information:

Device Type – Device type you are logged into.
MAC Address – Device MAC address.
Firmware Version – Current firmware version.
Hardware Revision – Device Hardware version.
Regulatory Domain – Currently configured regulatory domain.
System Time - Time synchronized by NTP (Network Time Protocol).

Connection Information: Status:

Connected – device is currently connected to an Access Point (802.11b/g Mode) or Polling Base Station (Polling Mode).
Not Connected – the connection has not yet been established.

BSSID – MAC address of the Access Point or Base Station the device is currently connected to.
Signal Strength – Access Point signal strength.
Remote Signal Strength - Device signal strength.
Noise Level – Level of the Noise the device is sensing on the channel.
Operational Rate – Bit data rate at which device sends packets to the Access Point.
Remote Data Rate - Bit data rate at which Access Point sends packets to the device.
Transmit Power - EIRP Transmit Power at which the device is sending data over wireless link.
TX Packets – Number of data packets that have been sent to the Access Point.
TX Bytes – Number of bytes sent to the Access Point.
RX Packets – Number of data packets that have been received from the Access Point.
RX Bytes – Number of bytes received from the Access Point.
Ethernet Speed - Current Ethernet port connection speed (or No Connection if there is no connection).

Operational Settings:

Device Name - System Name for easy identification of the device.
WLAN Interface - Enabled or disabled, if enabled traffic goes through the interface.
WLAN Operational Mode – Wireless LAN Operational mode the device has been configured to.

Available modes are:
- Access Point - Plain 802.11b/g Access Point mode.
- Infrastructure Client - Client for 3rd party 802.11b/g Access Points. To achieve compatibility with all 802.11b/g Access Points the so-called MAC address NAT is being performed for all traffic going from devices connected to the Ethernet interface.
- Polling Client - Client mode for another device using proprietary TDMA polling protocol.
- Polling Base - Base Station mode using proprietary TDMA polling protocol.
- AP Client - Client for another Lohuis device operating in Access Point mode. In this mode full MAC address pass-through is achieved between bridged Ethernet segments.
- PtP Bridge Master - Master device when configured to operate as point to point wireless bridge.
- PtP Bridge Slave - Client device when configured to operate as point to point wireless bridge.
- WDS (Wireless Distribution System) – This mode allows device to operate as an Access Point for other Stations while maintaining connection with other compatible Access Points operating in WDS mode at the same time. WDS mode requires all connecting Access Points to operate on the same channel and peer Access Points MAC addresses need to be configured under Wireless Settings tab. Please note that WDS works in Bridge mode only.
- Mikrotik WDS Client - This mode allows connection to Mikrotik RouterOS based Access Point, running in Dynamic WDS mode.

IP Operational Mode – Network mode the device has been configured to work with. Available modes are Bridge, Router and NAT Router.

Uptime – How long the device has been up and running since last reboot.

System Load – Shows device processor utilization.

ESSID - An ESSID is the name of a wireless network. All wireless devices on a common wireless network must employ the same ESSID in order to communicate with each other.

Frequency – The frequency the device is currently operating on.

Channel Width – Channel width the device is configured to operate. Available values are 40, 20, 10 and 5 MHz. Smaller size channels general offer lower throughput, but are much more resilient to interference from other 802.11b/g networks using 20MHz channels.

Preferred BSSID – MAC Address of the Access Point the device should connect to. If set to 00:00:00:00:00:00 then only ESSID is taken into account when connecting to the Access Point. Please note that when operating in PtP Bridge Mode (Master or Slave) it is mandatory to configure other peer MAC address for the devices to communicate.

PPPoE Authorization – Disabled or Enabled.

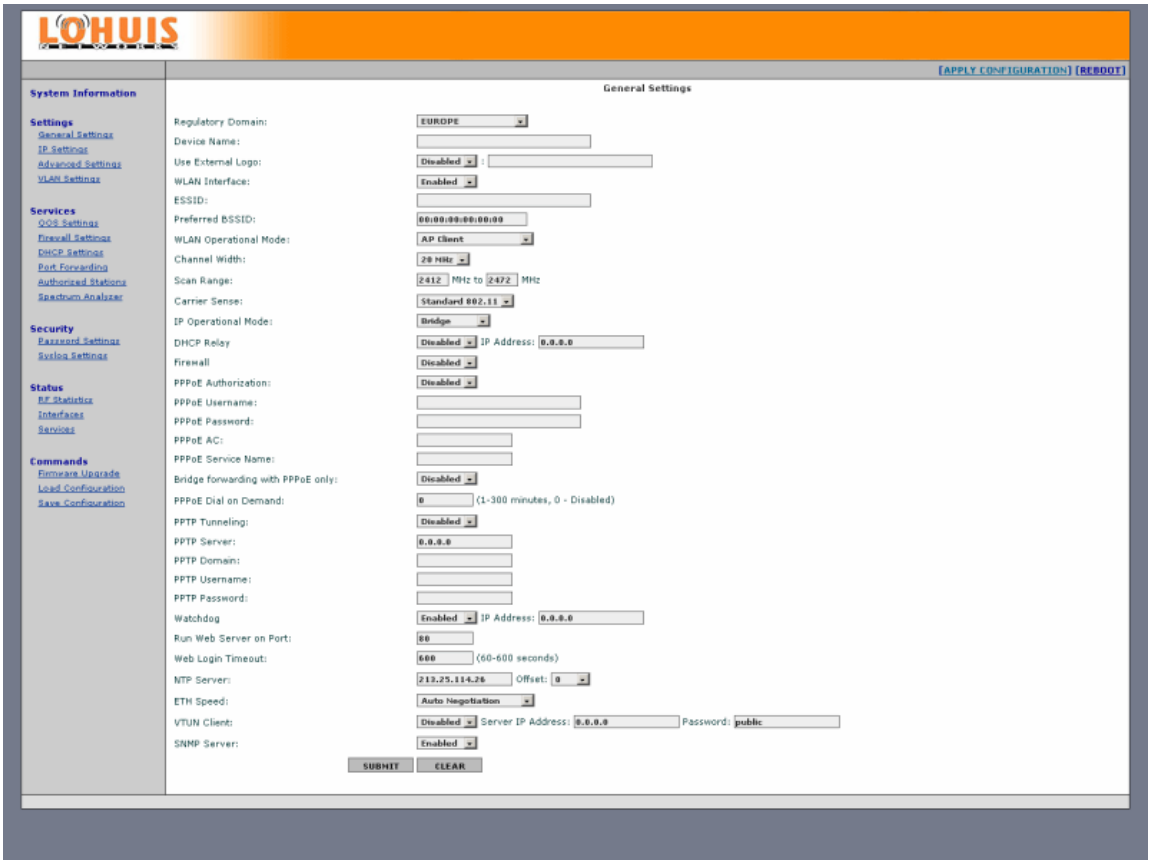
PPPoE Link Status – If the Lohuis device successfully established PPPoE connection

to the PPPoE concentrator the status will show Connected. Otherwise it will show Not Connected.
Fragmentation Threshold - The size at which WLAN packets are fragmented.
RTS Threshold - Minimum packet size to require RTS (Request To Send) handshaking limiting on-the air collisions. For packets smaller than this threshold, 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.
WLAN Speed – Configured wireless interface Data Rate.
Supported Data Rates – Wireless Data rates the device supports.

Available Data Rates are:
12, 18, 24, 36, 48, 72, 96, 108 Mbps for 40 Mhz channel width,
6, 9, 12, 18, 24, 36, 48 and 54 Mbps for 20 MHz channel width mode,
3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps for 10 MHz channel width,
1.5, 2.25, 3, 4.5, 6, 9, 12 and 13.5 Mbps for 5 MHz channel width.

Supported Frequencies – Supported Frequencies for currently configured Regulatory Domain.
Distance to the Access Point – Configured distance between this device and the Access Point (or other Wireless Bridge) it is connecting to. This setting is not required when operating in Access Point mode.
IP Address – Device IP address.
Subnet Mask – Currently defined subnet mask.
Default Gateway – Currently defined default gateway.
DHCP – Whether built in DHCP (Dynamic Host Configuration Protocol) server or client is disabled or enabled.
Traffic Shaping – If enabled then device will use traffic shaping to limit data according to defined rules. If disabled then there will be no data traffic limiting.
Firewall – If enabled then device will use build in firewall to pass/block traffic according to the defined rules. If disabled then there will be no packet filtering.
Encryption - Enable or Disable over the air Lohuis proprietary data Encryption.
Web Server on Port - Port number the build-in web server currently runs on.
Watchdog – Disabled or enabled, depending on current Watchdog configuration.
Web Login Timeout – Currently configured Web Login Timeout variable.
SNMP Server - System Network Management Protocol (SNMP) Server if enabled there is a possibility to manage by remote.

General Settings



Regulatory Domain – Please select regulatory domain that is most appropriate to your location.

Supported Regulatory Domains and allowed frequency ranges are defined as follows:
Europe – 2412 – 2483 MHz, 20, 10 and 5 MHz selectable channel width
USA – 2412 - 2473 MHz, 20, 10 and 5 MHz selectable channel width
Far East & Africa – 2.5 ~ 2.7 GHz, 40, 20, 10 and 5 MHz selectable channel width.

Device Name - This is the system name for easy identification of the Lohuis device.
WLAN Interface - Enabled or disabled, if enabled traffic goes through the interface.
ESSID - An ESSID is the unique name shared among all peers in your wireless network. The name must be identical for all devices and points attempting to connect to the same network. It shall be up to 32 characters length.

Preferred BSSID - BSSID corresponds to the MAC Address of the Access Point or Wireless Bridge you want to connect to. Using 00:00:00:00:00:00 as BSSID will make the device connect to any Access Point based on correct ESSID only.

WLAN Operational Mode - Wireless LAN Operational mode for the device. Available modes are:

- **Access Point** - 802.11b/g Access Point mode.
- **Infrastructure Client** - This mode allows connection to any 802.11b/g based Access Point.
- **Polling Client** - Client mode for another device using proprietary TDMA polling protocol. This mode allows connection to another device, utilizing proprietary Polling Wireless MAC Protocol, which has been specifically optimized for high performance outdoor networks.
- **Polling Base** - Base Station mode using proprietary TDMA polling protocol. Base Station mode is available only when operating in 2.4 GHz (802.11b/g) mode.
- **AP Client** – This mode allows connection to another Lohuis device or 3rd party compatible Access Point and full MAC address pass-through in Bridge mode.
- **PtP Bridge Master** – This mode allows creation of a point to point connection with another Lohuis device operating in Slave (or Client) mode.
- **PtP Bridge Slave** – This mode allows creation of a point to point connection with another Lohuis device operating in Master mode.
- **WDS** (Wireless Distribution System) – This mode allows device to operate as an Access Point for other Stations while maintaining connection with other compatible Access Points operating in WDS mode at the same time. WDS mode requires all connecting Access Points to operate on the same channel and peer Access Points MAC addresses need to be configured under Wireless Settings tab. Please note that WDS works in Bridge mode only.
- **Mikrotik WDS Client** - This mode allows connection to Mikrotik RouterOS based Access Point, running in Dynamic WDS mode.

Channel Width – The channel width device uses - depending on configured Regulatory Domain available values are 40 MHz, 20 MHz (default), 10 MHz or 5 MHz.
Carrier Sense - This option allows to disable standard 802.11 CSMA/CA backoff mechanism. Disabling 802.11 CSMA greatly improves performance when operating in area with noise generated by other (especially non 802.11 compliant) devices.

IP Operational Mode
Bridge - Bridge works at OSI model Layer 2. This means it does not know anything

about protocols, but just forwards data depending on the destination address in the data packet. This address is not the IP address, but the MAC (Media Access Control) address that is unique to each network adapter card. With a Bridge, all your computers are in the same network subnet, so you don't have to worry about not being able to communicate between computers or share an Internet connection. The only data that is allowed to cross the bridge is data that is being sent to a valid address on the other side of the bridge.

Router - Router is an OSI model Layer 3 device, and forwards data depending on the network address, not the hardware (MAC) address. For TCP/IP networks this means the IP address of the network interface. Routers isolate each LAN into a separate subnet. Routers provide bandwidth control by keeping data out of subnets where it doesn't belong, however routes need to be set up before they can get going.

NAT Router – This mode is similar to the Router mode only that all traffic coming on wired interface and going out on wireless interface is masqueraded. Masquerade allows a set of machines to invisibly access the Internet via the gateway (Lohuis in this case). To other machines on the Internet, all this outgoing traffic will appear to be from the Lohuis device itself. In addition to the added functionality, IP Masquerade provides the foundation to create a fairly secure networking environment.

DHCP – Enable or disable built in DHCP client/server.

DHCP Relay – In IP Router/NAT Router mode enable DHCP Relay so DHCP requests coming from the LAN subnetwork will be relayed to the WLAN subnetwork and DHCP Server replies will be relayed back to the LAN interface. If no specific DHCP server IP address is configured (default value 0.0.0.0) then DHCP requests will be relayed to any DHCP server on the WLAN address. If the DHCP server IP address is configured then all DHCP requests will be relayed to that particular DHCP server.

Firewall – Enable or disable built in packet filtering firewall.

PPPoE Authorization – Enable or disable built in PPPoE client:

- In IP Bridge mode, if PPPoE is enabled, the device will authorize itself to the PPPoE concentrator and establish a PPP link to it. Ethernet traffic will be bridged as usual.
- In IP Router/NAT Router mode, if PPPoE is enabled, the Lohuis device will authorize itself to the PPPoE concentrator and establish a PPP link to it – over the wireless interface in the Access Point Client mode or over the wired interface in the Access Point mode, PPPoE link will be then used as a default gateway by the device. While operating in Router/Access Point Client all traffic originating from the wired LAN subnetwork will be transported over PPPoE link to the PPPoE concentrator.

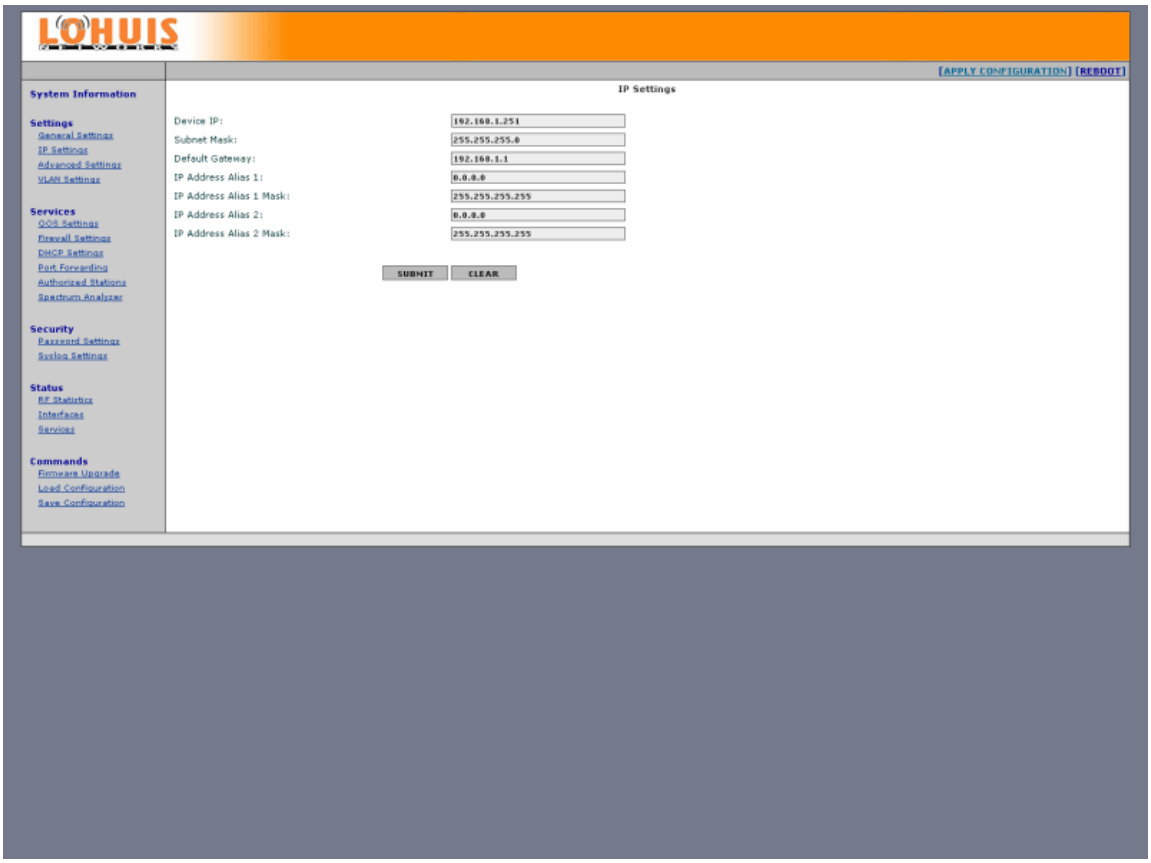
PPPoE Username/Password – A PPPoE Username and Password that are required to create PPP link to the PPPoE concentrator.

Currently supported PPPoE authorization types are CHAP, PAP, MSCHAP and MPPE.

Watchdog – If enabled then device will send 3 ICMP Echo Requests to the configured IP address, each in 1 minute interval. If there is no single ICMP Echo Reply to any of these requests, then the device will reboot itself.
The system also has an independent hardware watchdog built in, that checks for critical operational parameters and reboots the device, should the system hang or become unstable. That watchdog works all the time, regardless of the ping watchdog configuration.
Run Web Server on Port – Enter the port the build-in Web server should be configured to run on.
Web Login Timeout – Enter the value the management Web session should be kept alive without any action from the user.
Reset to Default Password – Password that is used to reset device to factory default settings using Reset software.
NTP Server – Configure IP address of the external NTP (Network Time Protocol) server Lohuis running device will obtain current time from at startup time.
ETH Speed - LAN Port connection speed - available values are Auto (Auto Negotiation), 100Mbps FDX, 100Mbps HDX, 10Mbps FDX, 10Mbps HDX.
VTUN Client - Please enter IP address of the VTUN server to connect and create Layer-2 bridge.
SNMP Server - System Network Management Protocol (SNMP) Server, if enabled there is a possibility to manage by remote.

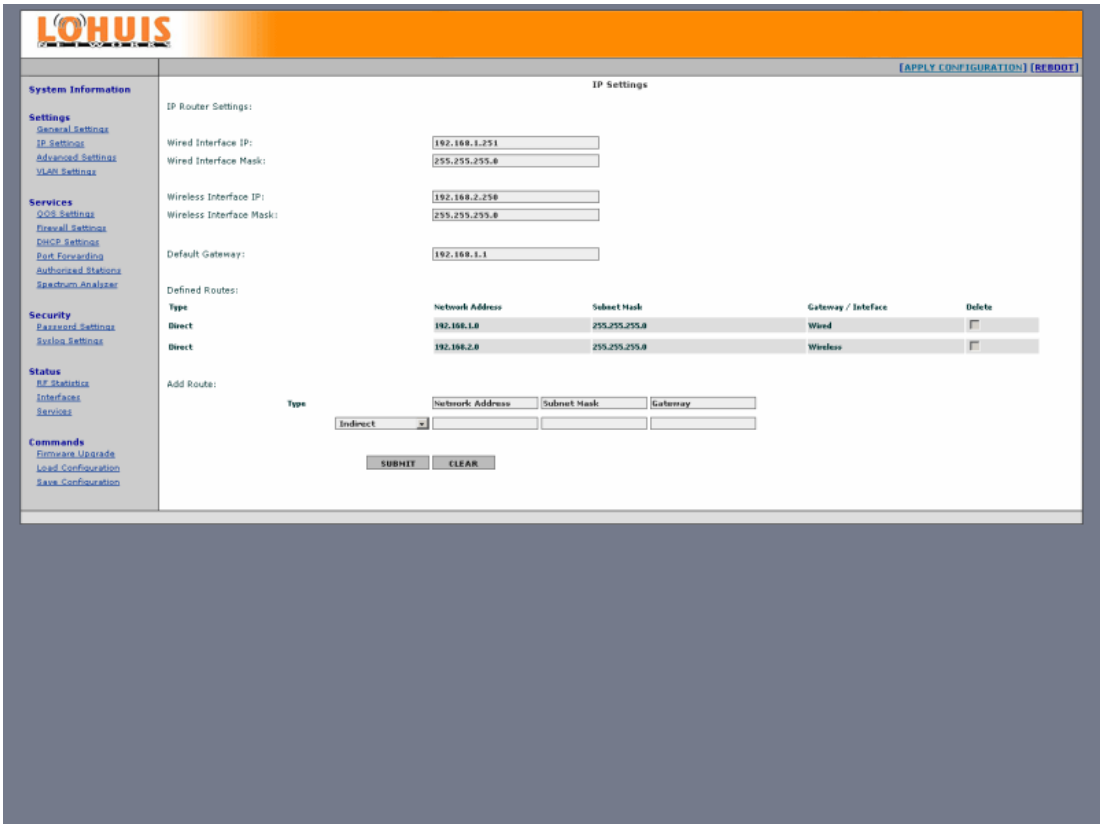
IP Settings

Bridge Mode



Device IP – Enter device IP address here.
Subnet Mask – Enter network subnet mask here.
Default Gateway – IP address of a router where traffic going outside of the local network will be forwarded.

Router Mode / NAT Router Mode



Wired Interface IP – Enter IP address of the wired interface here.
Wired Interface Mask – Enter wired network subnet mask here.
Wireless Interface IP – Enter IP address of the wireless interface here.
Wireless Interface Mask – Enter wireless network subnet mask here.
Default Gateway – IP address of a router where traffic not destined for defined routes / local routes will be forwarded.
Defined Routes – This table displays currently defined static routes. To delete a route select "Delete" checkbox and press Submit on the bottom of the page. Please note that it is not possible to delete first two entries – direct routes to local interfaces.

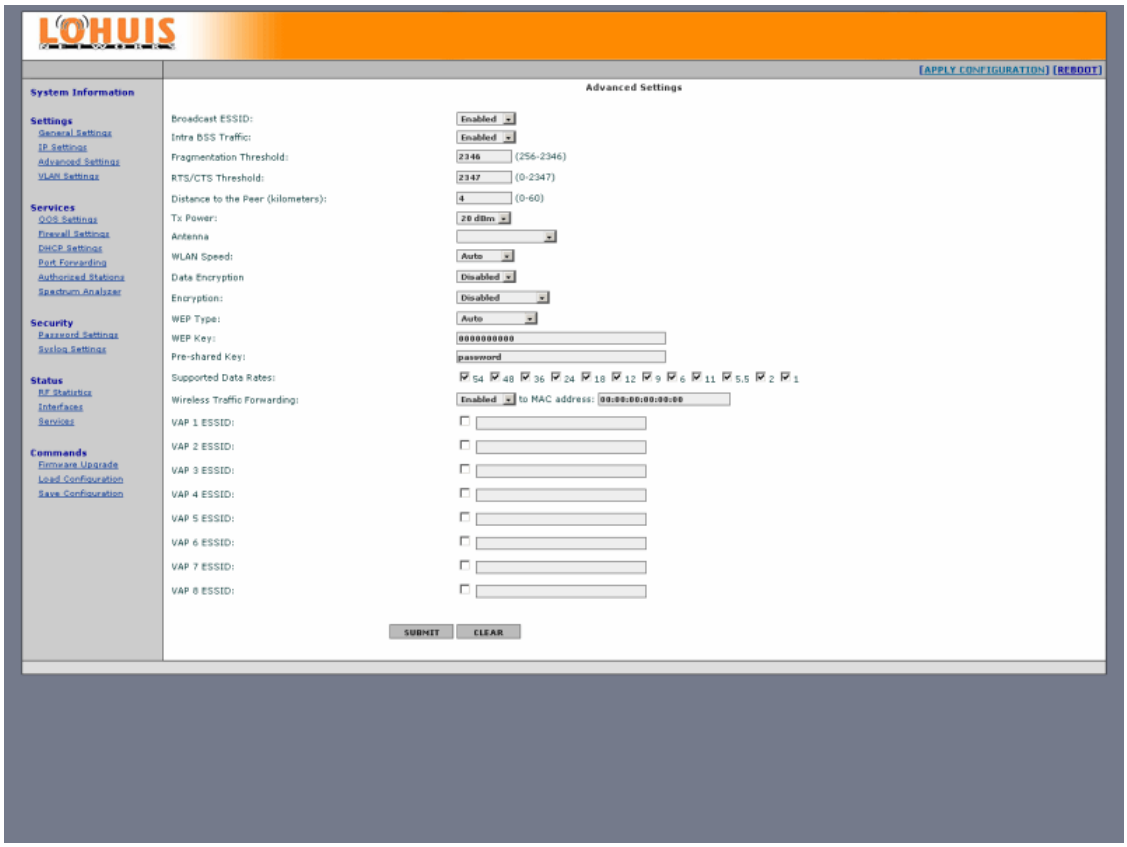
Add Route:

Direct – Wired/Wireless - When router has two or more IP subnets directly attached to its different interfaces, it can route IP packets between those subnets using a direct route. A direct route consists of an IP Address which specifies the basic IP address to route, a Subnet Mask which defines the class of IP addresses that will be routed, and an

interface which specifies where the IP subnet is attached. When an IP packet addressed to a system on the directly routed subnet arrives at the router, the router will send it directly to the target machine on the interface specified. When entering direct route use 0.0.0.0 as Gateway.

Indirect - When router needs to send IP packets between IP subnets which are not directly connected to one of its interfaces, it must have an indirect route for sending those packets. An indirect route consists of an IP Address which specifies the basic IP address to route, a Subnet Mask which defines the class of IP addresses that will be routed and a Gateway that will relay the IP packet. When an IP packet addressed to a system on the indirectly routed subnet arrives at the router, the router will route it over to the specified Gateway to be routed further.

Advanced Settings



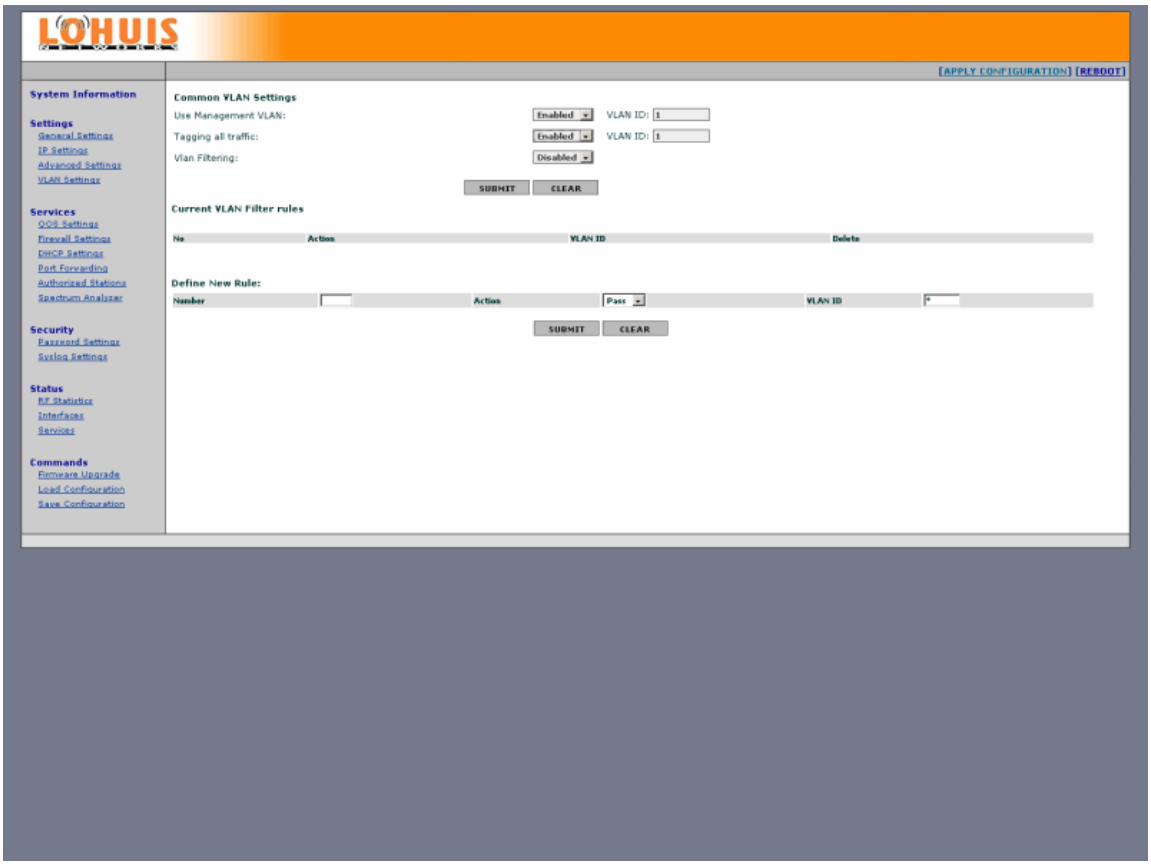
Fragmentation Threshold – Enter the size at which the packets will be fragmented.
RTS/CTS Threshold – Enter the minimum packet size to require RTS (Request To Send) handshaking limiting on-the air collisions. For packets smaller than this threshold, a RTS is not sent and the packet is transmitted directly to the WLAN. For packets larger than this threshold the RTS/CTS handshaking is established. This value should only be changed when operating as an Access Point Client.
Distance to the Access Point – Configure distance between Lohuis running device and the Access Point (or other bridge when operating as PtP Bridge) it is connecting to.
TX Power - By default, the Lohuis running device transmits data at the maximum output power for the regulatory domain selected and frequency used. With Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference from neighboring devices.
Antenna – Select which device antenna is used to transmit and receive packets - first one, second one or both of them.

Antenna Diversity – Select if antenna diversity should be used or disabled.
WLAN Speed – Choose Data Rate the device will support while connecting to the Access Point.

Available Data Rates are:
12, 18, 24, 36, 48, 72, 96, 108 Mbps for 40 MHz channel width,
6, 9, 12, 18, 24, 36, 48 and 54 Mbps for 20 MHz channel width mode,
3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps for 10 MHz channel width,
1.5, 2.25, 3, 4.5, 6, 9, 12 and 13.5 Mbps for 5 MHz channel width.

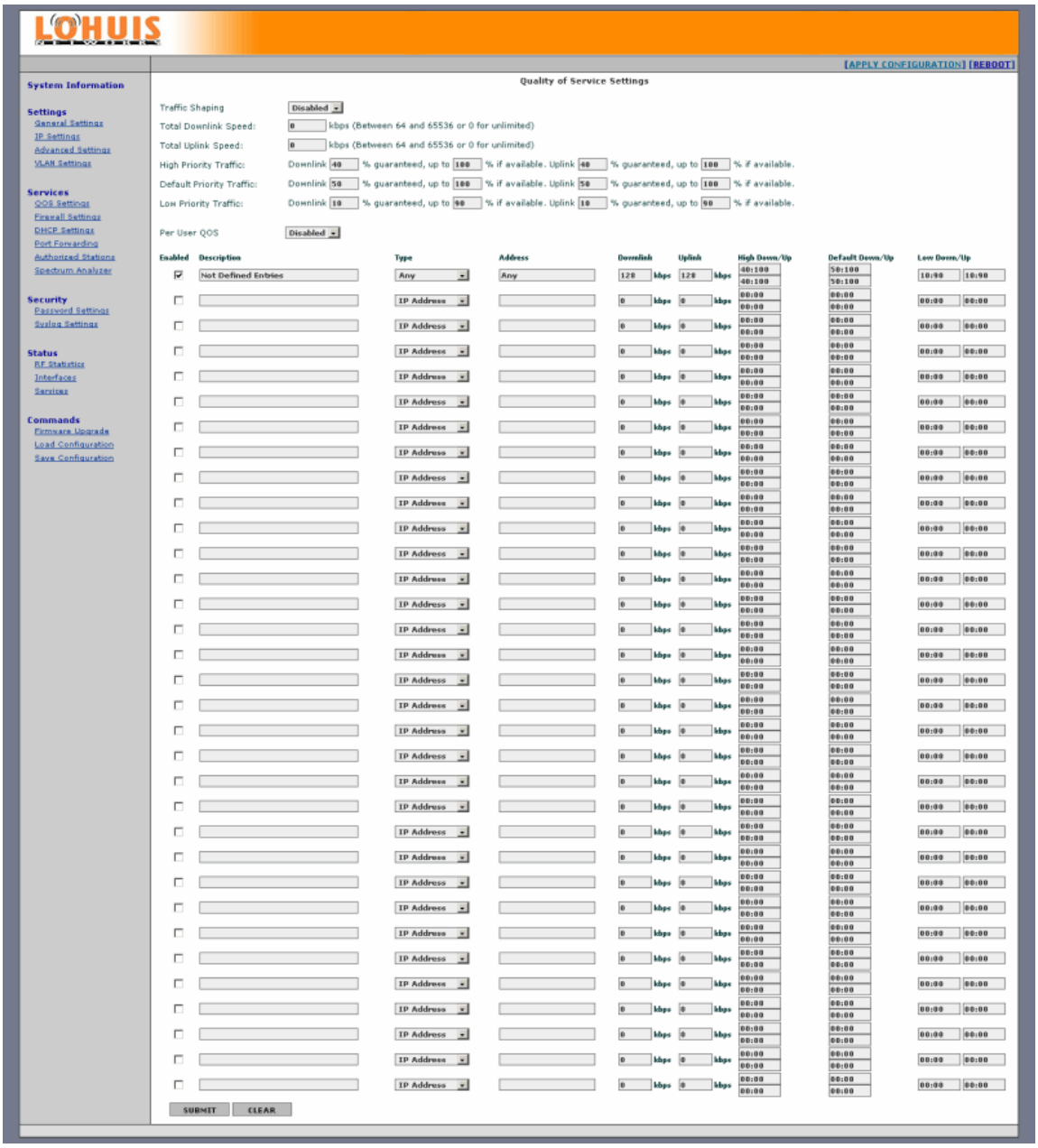
Encryption – Please select generic WLAN encryption scheme: WEP, WPA-PSK TKIP or WPA-PSK CCMP (AES).
WEP Key – Enter WEP encryption key here. Keys are entered as hexadecimal numbers in following format:
64 bit WEP: xxxx-xxxx-xx
128 bit WEP: xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xx
156 bit WEP: xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx
Pre-shared WPA Key – the key is entered as 8-63 characters long string, ie. password.
Supported Data Rates – Enable or Disable WLAN Data Rates the Lohuis running device should support when communicating with other devices.

VLAN Settings



Use Management VLAN – If enabled, only packets tagged with this configured VLAN ID will be able to reach the bridge for management.
Tagging all traffic – Tag all traffic traversing the bridge and going out of the wireless interface with this configured VLAN ID. All traffic coming on the wireless interface and leaving on the Ethernet side that are tagged with this VLAN ID will be automatically untagged.
VLAN Filtering – Here you can configure which VLAN ID's can traverse the wireless bridge and which ones should be dropped.

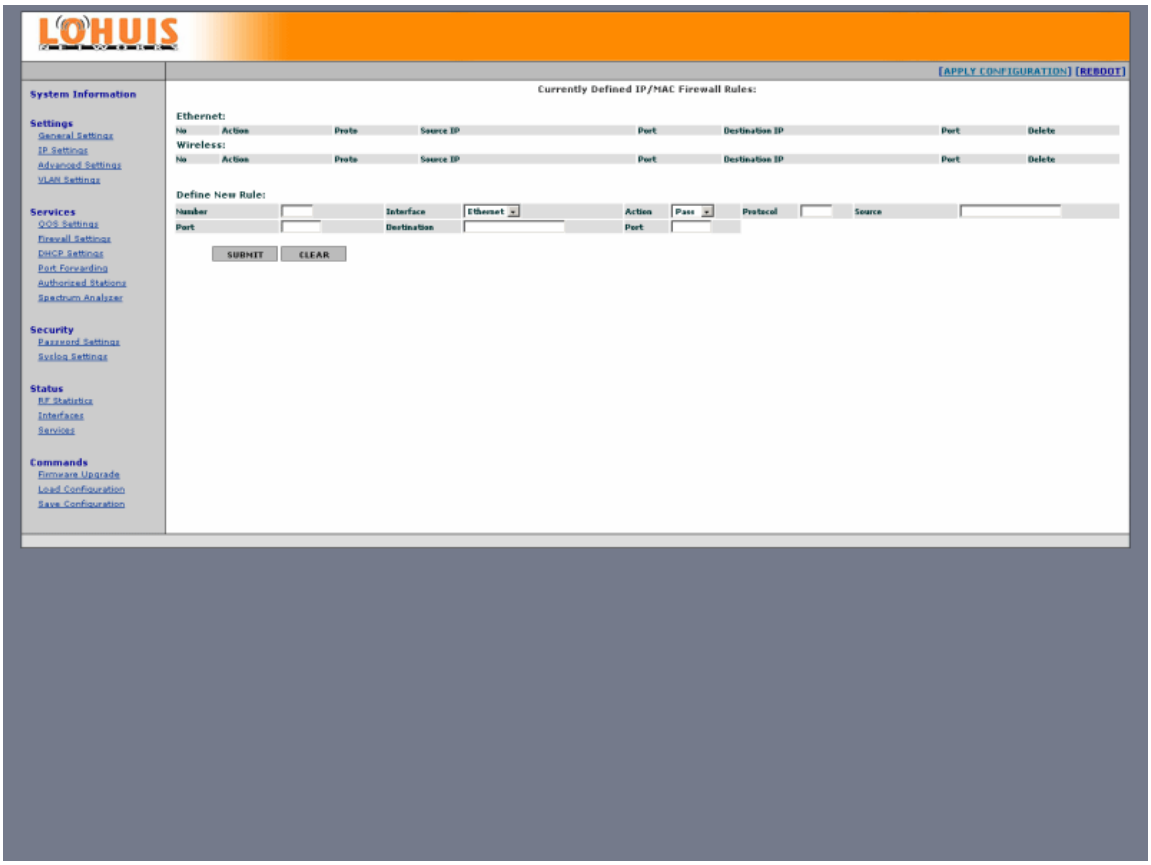
QOS Settings



The built-in traffic shaper allows you to set up different data flow speeds for devices connected to it's Ethernet interface
In IP Bridge Mode - based on MAC Address,

In IP Router Mode - based on IP Address or IP Subnetwork.
Downlink – This is speed of the data going out of the wired interface.
Uplink – This is speed of the data going out of the wireless interface.
Total Downlink Speed - Cumulative speed the data can flow through the device.
Total Uplink Speed - Cumulative speed the data can flow through the device.
High Priority Traffic - Size that will be reserved for high priority queue and sent before any other traffic. High Priority traffic is defined as traffic from VOIP applications and other types of applications requiring low latency for correct operation.
Default Priority Traffic - Size that will be reserved for default priority queue from which data is sent after the High Priority queue is empty. Default Priority traffic is defined as traffic originating from well known services (http, smp, pop3, ssh etc.) which should be prioritized but is not as latency dependent as high priority traffic.
Low Priority Traffic - Size that will be reserved for all traffic that does not fall into other queues.
Per User QOS - If enabled then individual entries from the table below will be used for further configuration of the traffic shaping.
QOS Entries Enabled – If checked then this particular entry is enabled, in not checked then that entry is disabled.
Description - Entry description.
Type - MAC Address or IP Address.
Address – For MAC Address enter it as xx:yy:xx:yy:xx:yy. For single IP Address enter it as x.x.x.x/32, or if you want to limit speed for whole subnetwork enter it as x.x.x.x/y (ie. 192.168.0.0/24 if you want to limit all IP addresses within 192.168.0.0 - 192.168.0.255 range).
Downlink Speed – Queue size for all packets matching defined IP/MAC Address.
Uplink Speed - Queue size for all packets matching defined IP/MAC Address.
High Down/Up - Queue size for high priority traffic in format xx:yy, where xx is percentage of the queue size that will be guaranteed for high priority traffic and yy is percentage of queue size that can be used if queue is not used by other kind of traffic.
Default Down/Up - Queue size for default priority traffic in format xx:yy, where xx is percentage of the queue size that will be guaranteed for default priority traffic and yy is percentage of queue size that can be used if queue is not used by other kind of traffic.
Low Down/Up - Queue size for default priority traffic in format xx:yy, where xx is percentage of the queue size that will be guaranteed for default priority traffic and yy is percentage of queue size that can be used if queue is not used by other kind of traffic.

Firewall Settings:



Built in Firewall allows you to pass or block traffic going through the device, based on selected criteria.
There are two tables shown on the configuration screen. "Ethernet" table shows currently defined firewall rules for the wired interface of the Lohuis running device. "Wireless" table shows currently defined rules for the wireless interface. You can delete existing firewall rule by selecting "Delete" checkbox on the right side of the rule and pressing Submit button.

Define New Rule (IP Bridge Mode):

Interface – Select the incoming interface the rule should apply to. Choose either Ethernet or Wireless interface.
Action – Select what to do with the packet matching the rule. You can either pass that packet through, or block it.
Protocol – Enter the number representing IP Protocol that should be matched. Use "*"

to match all protocols. Most common numbers are:
"*" All IP protocols
1 – ICMP protocol
6 – TCP protocol
17 – UDP protocol

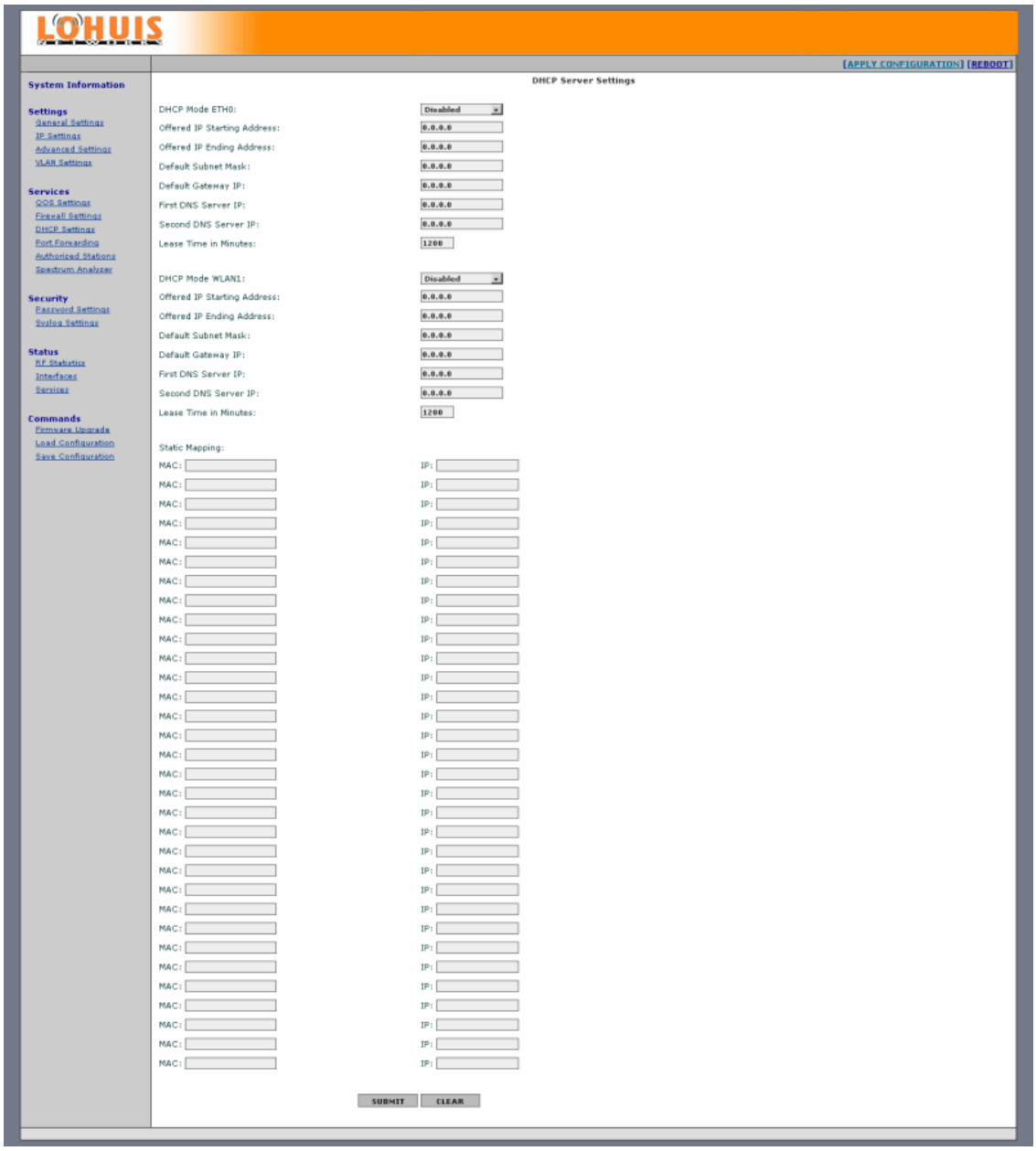
For complete list of protocols please see Appendix 1 of this document, or go to: http://www.iana.org/assignments/protocol-numbers

Source – Source MAC address of the packet to be matched. Use "*" to match any MAC address.
Source Port – Source port of the packet to be matched. Use "*" to match any source port.
Destination – Destination MAC address of the packet to be matched. Use "*" to match any MAC address.
Destination Port - Destination port of the packet to be matched. Use "*" to match any destination port.

Define New Rule (IP Router Mode):
Interface – Select the incoming interface the rule should apply to. Choose either Ethernet or Wireless interface.
Action – Select what to do with the packet matching the rule. You can either pass that packet through, or block it.
Protocol – Enter the number representing protocol that should be matched. Use "*" to match all protocols. Most common numbers are:
"*" – All IP protocols
1 – ICMP protocol
6 – TCP protocol
17 – UDP protocol

For complete list of protocols please see Appendix 1 of this document, or go to: http://www.iana.org/assignments/protocol-numbers
Source – Source IP address or IP subnet (in x.x.x.x/y format) of the packet to be matched. Use "0.0.0.0/0" to match any IP address.
Source Port – Source port of the packet to be matched. Use "*" to match any source port.
Destination – Destination IP address or IP subnet (in x.x.x.x/y format) of the packet to be matched. Use "0.0.0.0/0" to match any IP address.
Destination Port - Destination port of the packet to be matched. Use "*" to match any destination port.

DHCP Settings

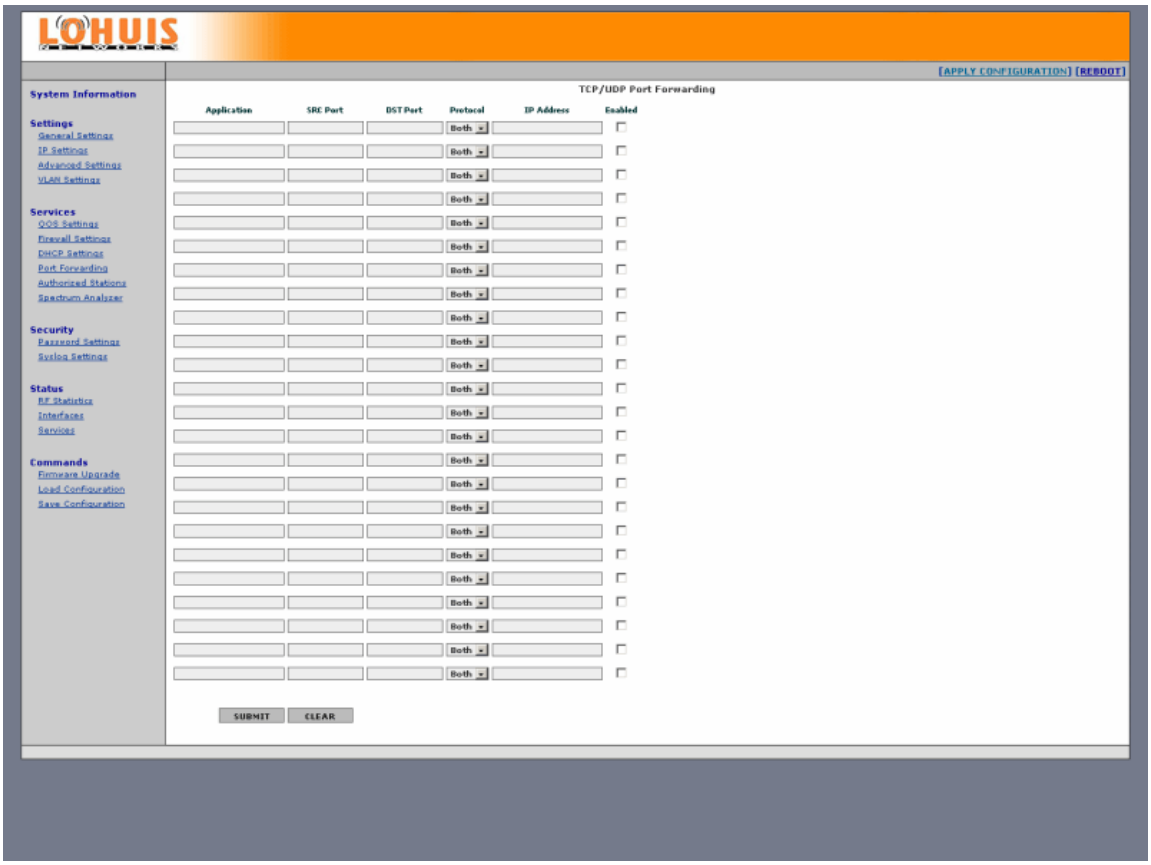


Depending on which DHCP option is enabled (or disabled) on the General Settings page, this page will show appropriate information.

If DHCP server is enabled then you can configure it's operational parameters on this page.

Server Enabled on Interface – Choose the interface the DHCP server should listen for requests on. You can choose either Wired or Wireless interface.
Offered IP Starting Address – First IP address from the range that will be provided to hosts requesting DHCP server to provide them an address.
Offered IP Ending Address – Last IP address from the range that will be provided to hosts requesting DHCP server to provide them an address.
Default Subnet Mask – Subnet Mask that will be provided to hosts requesting IP information.
Default Gateway IP – Gateway IP address that will be provided to hosts requesting IP information.
First DNS Server IP – First DNS IP address that will be provided to hosts requesting IP information.
Second DNS Server IP - Second DNS IP address that will be provided to hosts requesting IP information.
Lease Time in Minutes – Lease time the information received from DHCP service is valid. After that time computer that has requested the DHCP server to provide it IP addres information will automaticaly request that information again.
Static Mapping – This option allows static mapping of MAC addresses to specific IP addresses offered by DHCP server.

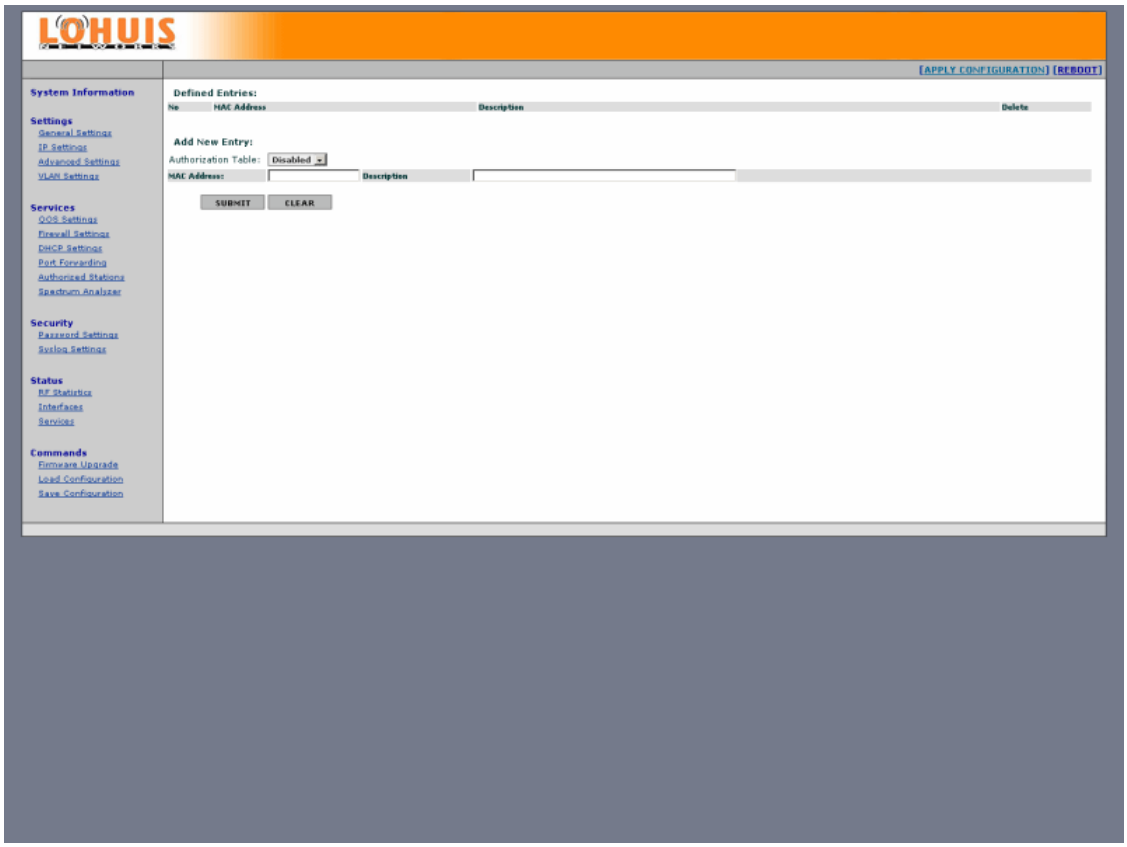
Port Forwarding



When the device is operating in Access Point Client and IP Router/NAT Router mode this menu will let you configure port forwarding from external (WLAN) interface to the host available on the internal (Ethernet) interface.

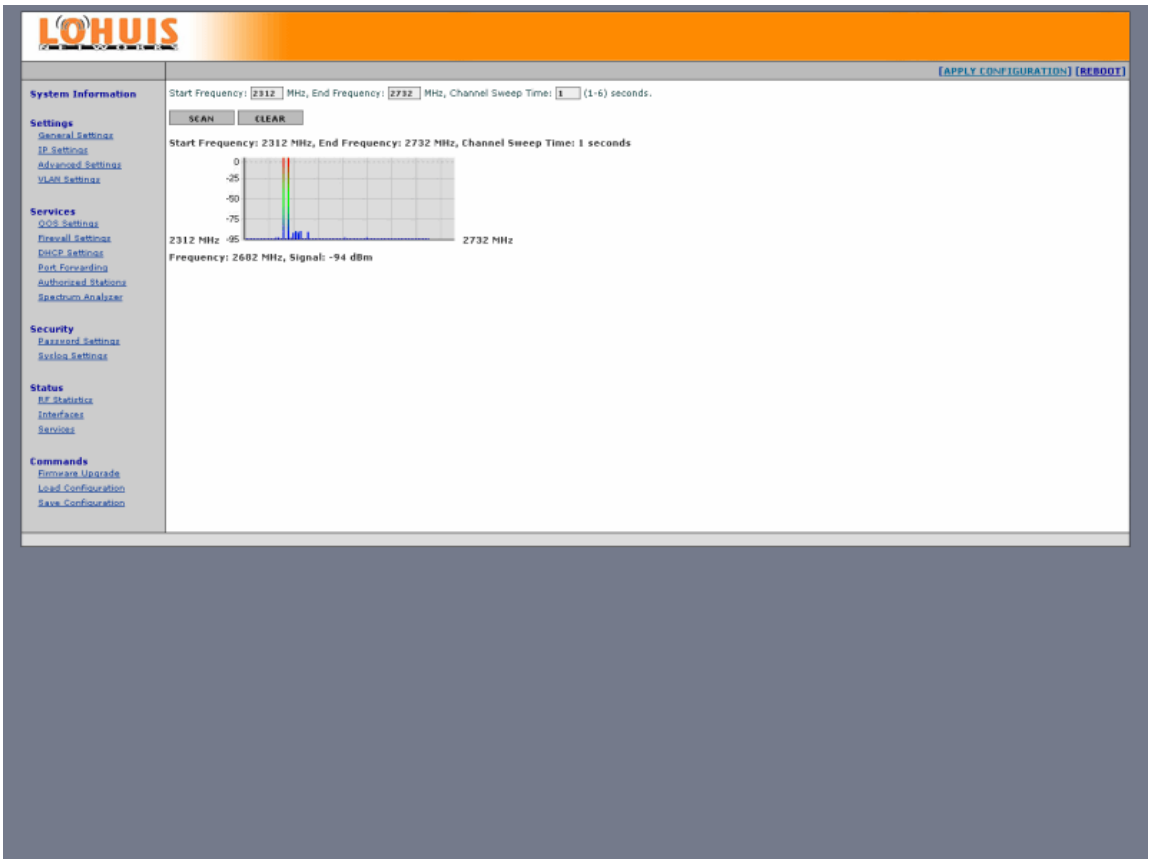
Each forwarding rule consists of:
Application - Description of the application the rule applies to.
Port - Port on the external (WLAN) interface - when connection is made to that port it will be forwarded to defined IP address.
Protocol - protocol type this rule applies to - TCP, UDP or both TCP and UDP.
IP Address - IP address on the internal (Ethernet) interface connection will be forwarded to.
Enabled - select checkbox to enable the rule or leave it not selected to disable the rule.

Authorized Stations

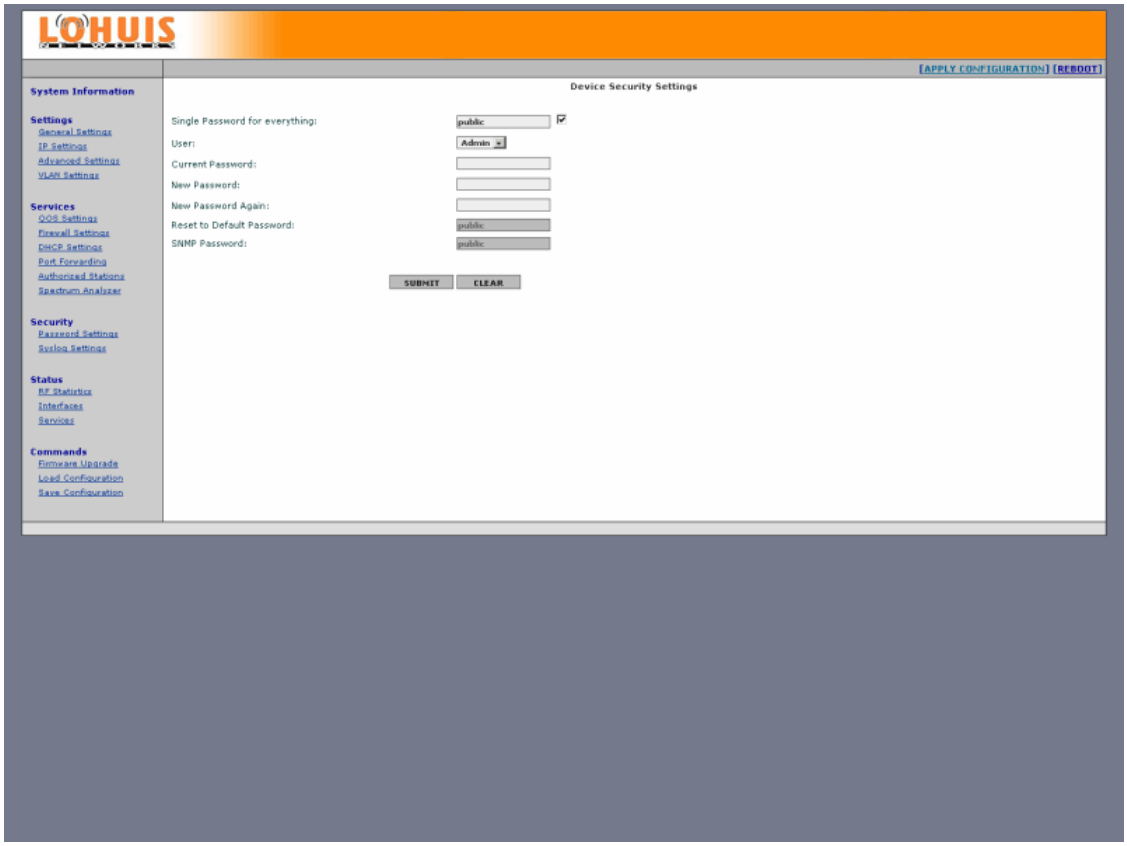


This tab allows to configure list of MAC addresses of client devices that can associate with the Access Point or Polling Base.

Spectrum Analyzer

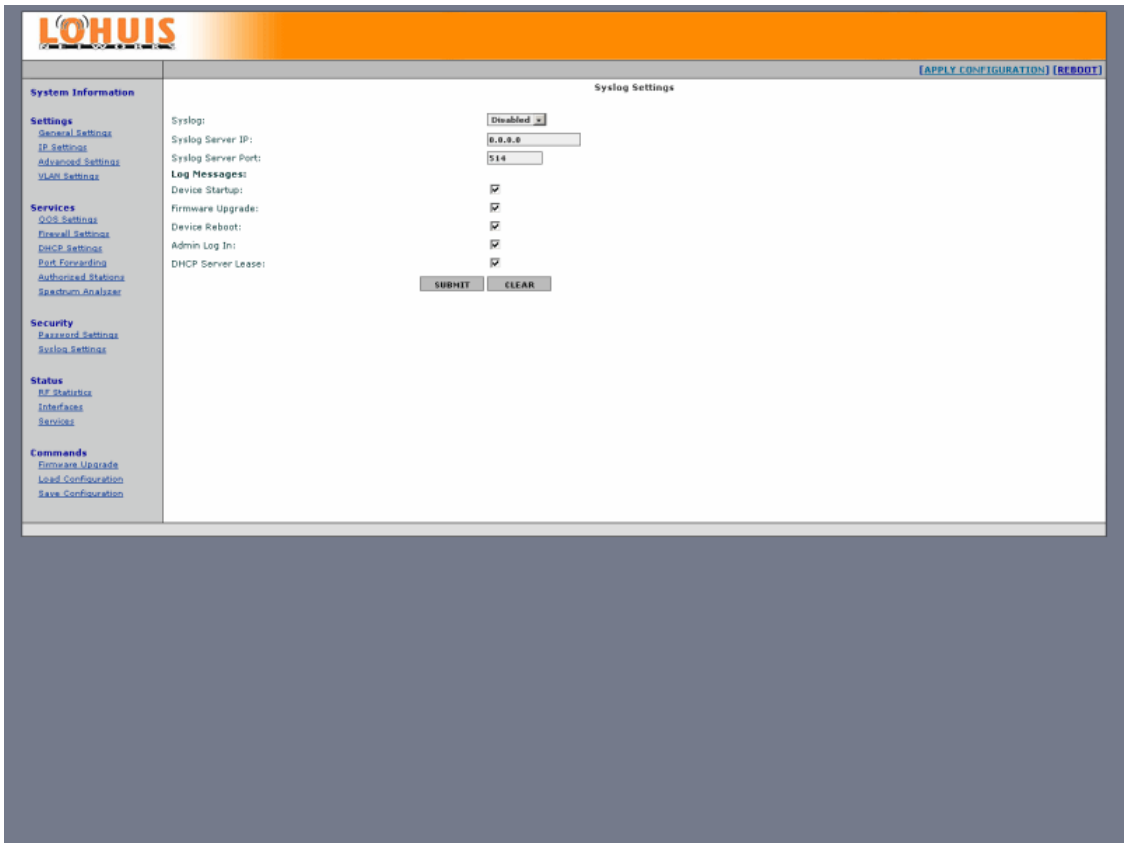


Password Settings



Use this screen to change password which is used to access and configure the device.

Syslog Settings

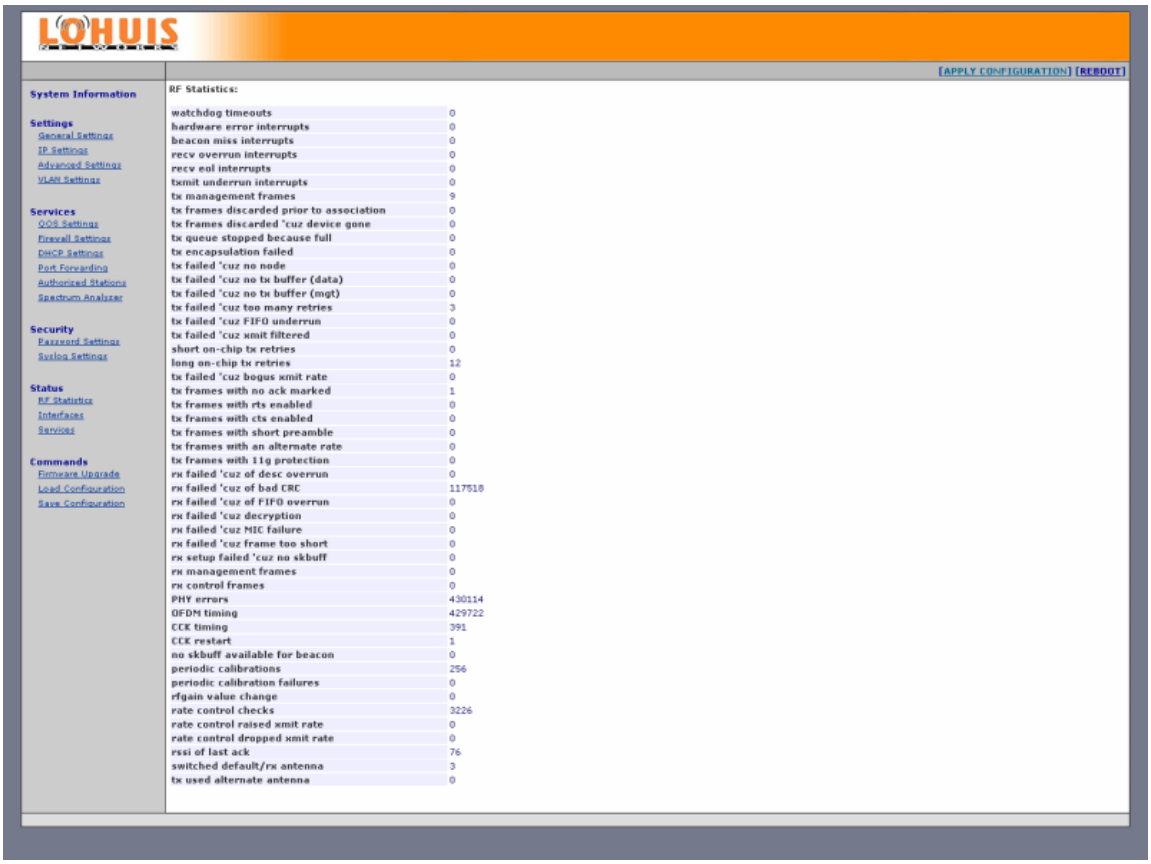


This option allows device events logging to remote Syslog server.

Syslog Server IP - IP Address of the computer where Syslog server is running.
Syslog Server Port - Port the Syslog server is listening on.
Log Messages - Enable or disable logging for specific events:

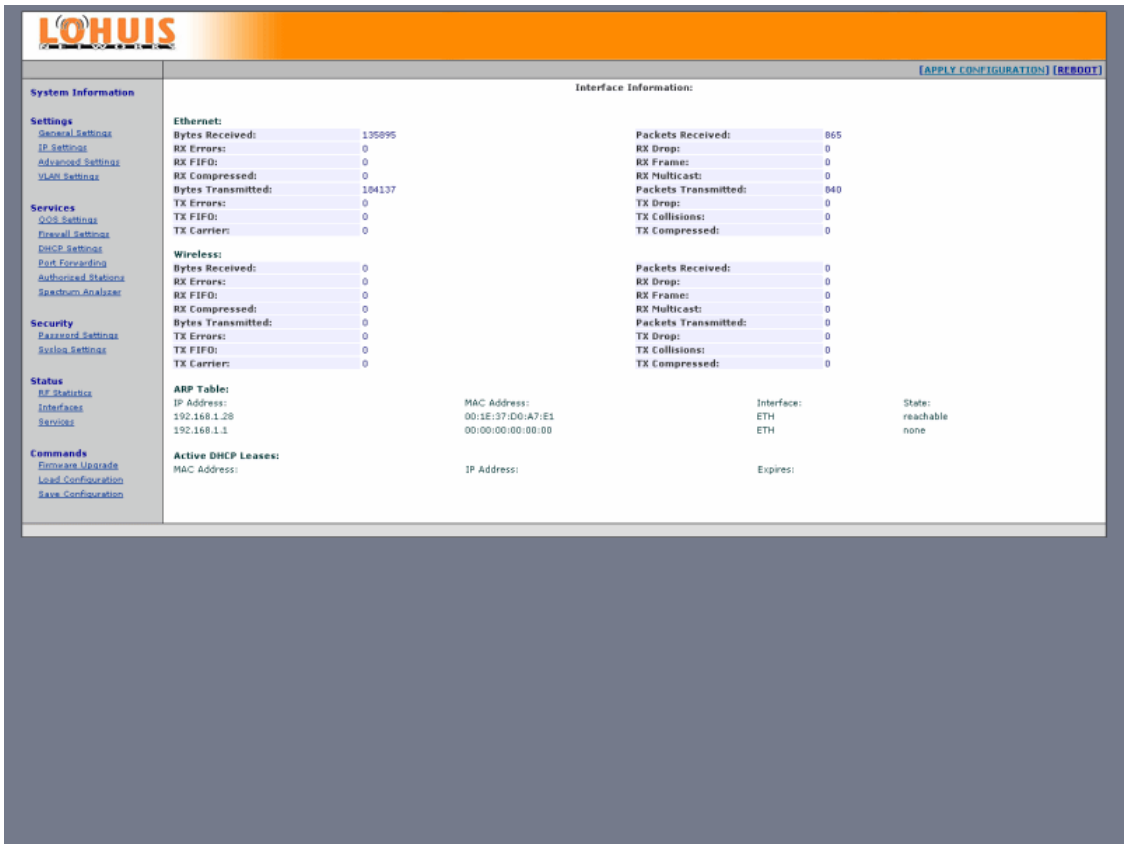
Device Startup - save an event when the device has started.
Firmware Upgrade - save an event when firmware upgrade was performed on the device.
Device Reboot - save an event when device is rebooting.
Admin Log In - save an event when user admin logged to device via WWW.
DHCP Server Lease - save an event when the built in DHCP server leased an IP address to the client (event will contain MAC address of the network card build into computer that obtained the lease).

RF Statistics



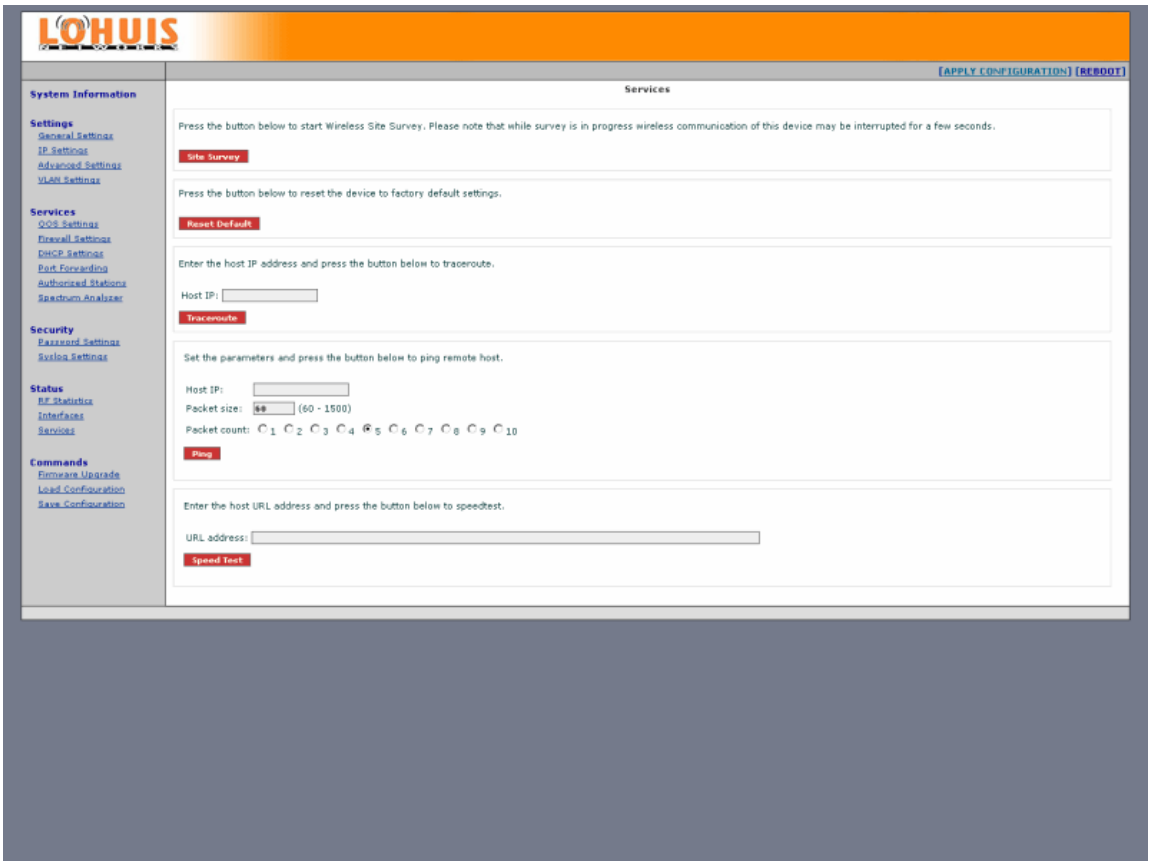
This page shows counters for various RF related hardware variables. One of the most important counters to look at here is PHY Errors counter which if increases rapidly over short time shows that there is interference on the channel you are using.

Interface Status



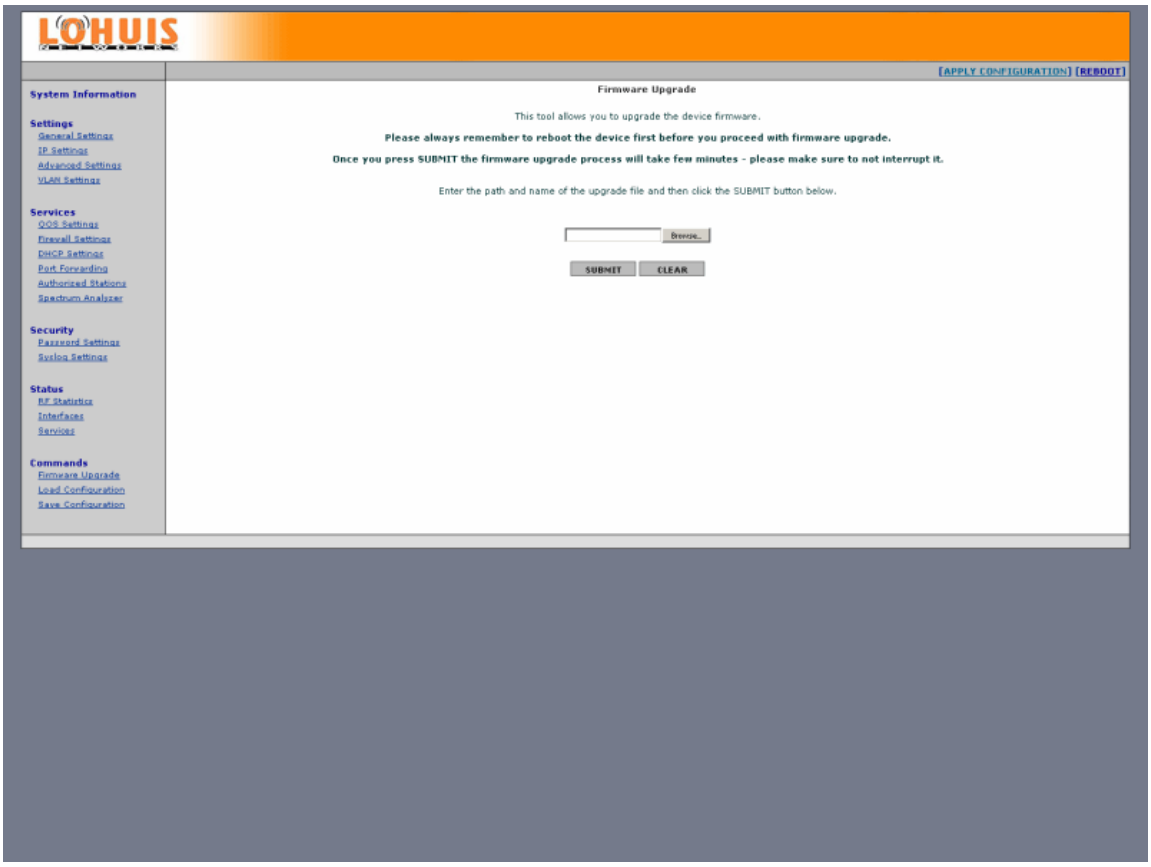
This page shows information about packets that traversed the bridge/router. In IP Bridge mode there is also Bridge Learn Table shown, in IP Router mode there is device ARP table shown, containing it's neighbors MAC addresses. Currently active DHCP leases are also displayed here.

Services



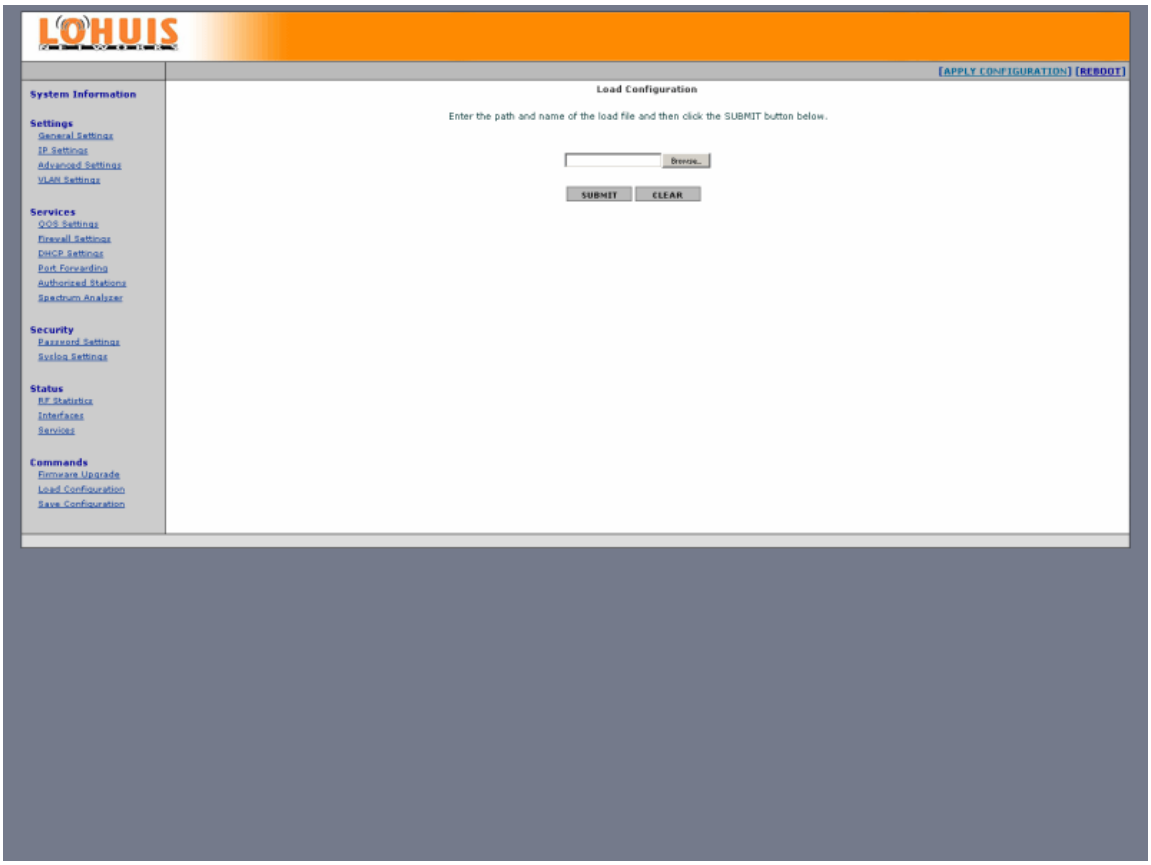
Site Survey – Allows to see other Access Points in range.
Reset Default – Allows to reset device to factory default settings.
Traceroute – This command is used to determine the route taken by packets across an IP network.
Ping – This command is used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP "echo request" packets to the target host and listening for ICMP "echo response" replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

Firmware Upgrade



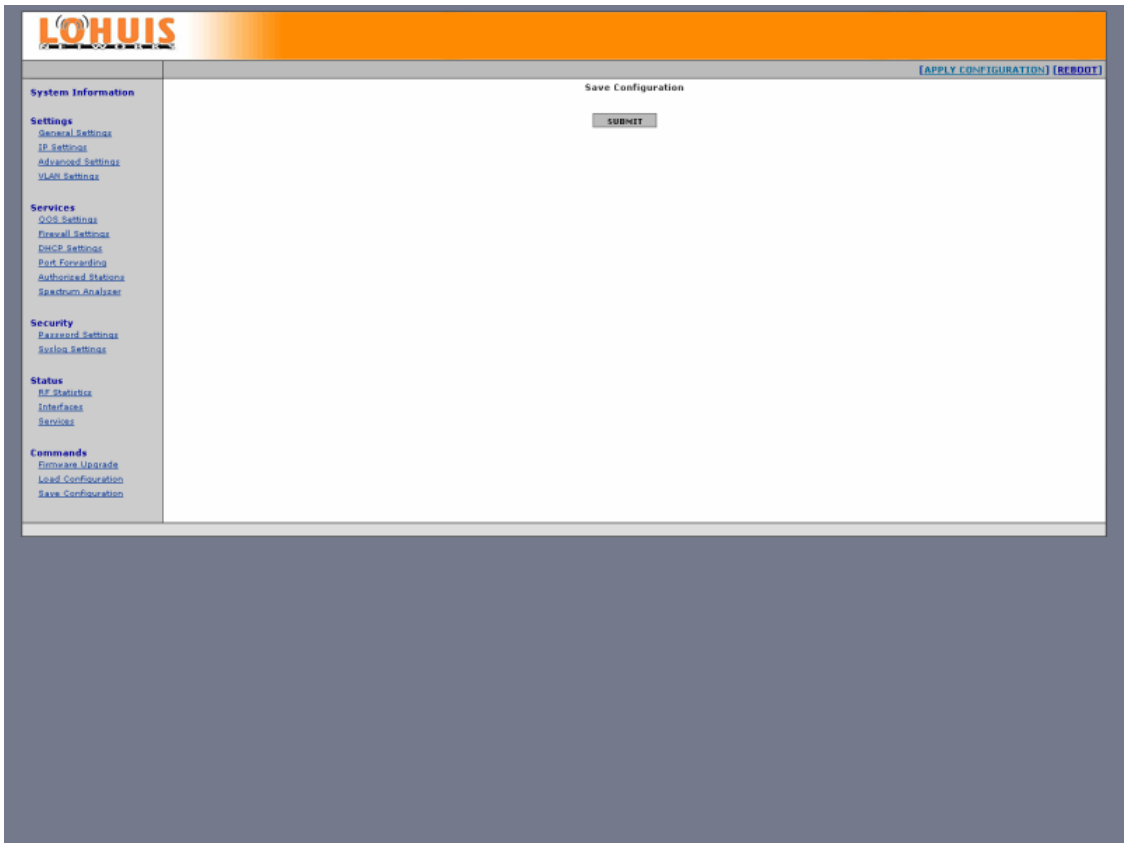
This page allows you to upgrade the device firmware.

Load Configuration



This page allows you to load device configuration from file.

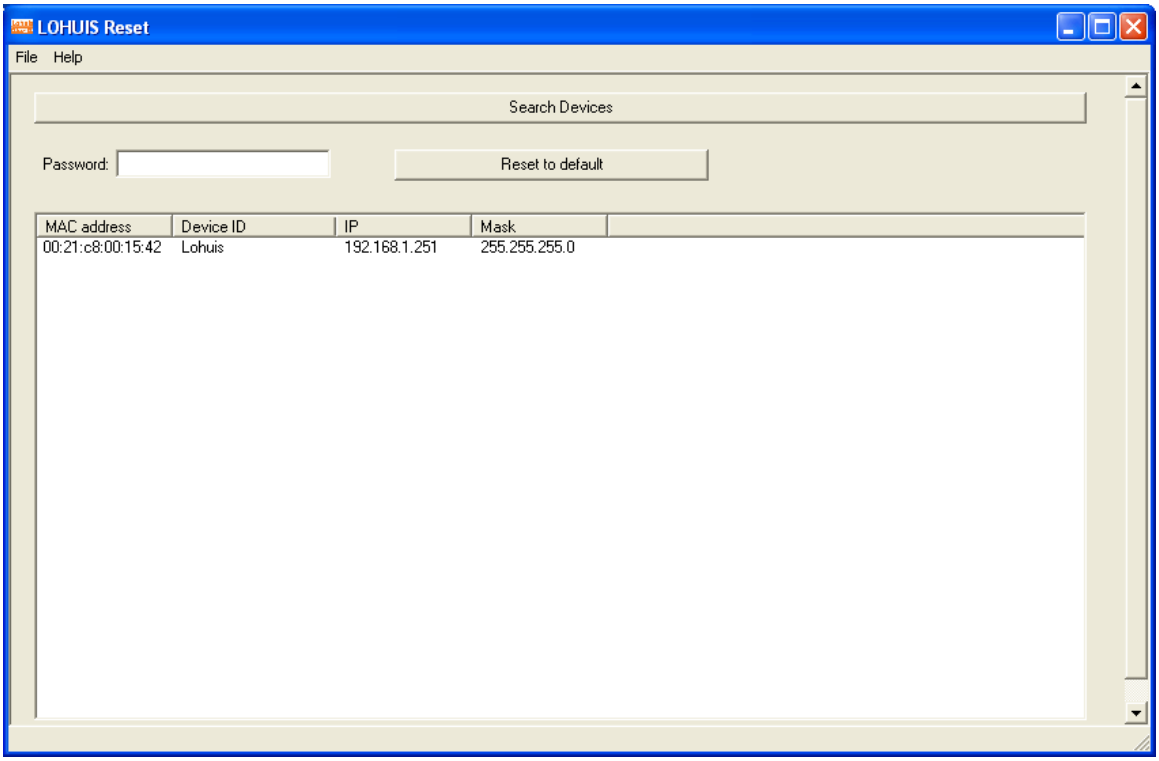
Save Configuration



This page allows you to save device configuration to file.

Resetting device to default settings.

In order to reset Lohuis device to factory default settings you need to use Lohuis Reset software .
Reset will locate any compatible Lohuis device regardless of its IP address located on the same physical subnetwork with the computer it is running on.



After selecting the device you want to reset enter "Reset to Default Password" in the Password: field and press button.

If you have changed Reset to Default Password to one you no longer remember then please email us at support@Lohuisnetworks.com stating device type and MAC Address and we will provide you one time, generated password that will let you reset the device to factory default settings.