High-Power Ceiling Mount Wireless 300N PoE Access Point

User Manual

Model 525800

INTELLINET NETWORK SOLUTIONS

INT-525800-UM-0316-1

Table of Contents

1. PRODUCT INTRODUCTION 1

1.1 PRODUCT FEATURES 1
1.2 PACKAGE CONTENTS 1
1.3 HARDWARE DESCRIPTION 2

2. HARDWARE INSTALLATION 3

2.1 WALL BRACKET INSTALLATION 3
2.2 CABLE CONNECTIONS 4
2.3 CONNECTING TO ACCESS POINT WEB CONFIGURATION INTERFACE 5
2.3.1 Set up the IP address of your computer 5
2.3.2 Connect to the Intellinet Access Point 5

3. CONFIGURATION OPTIONS 6

3.1 LOGIN TO THE DEVICE MANAGEMENT INTERFACE 6
3.2 PREREQUISITES 7
3.2.1 Firmware 7
3.2.2 Using the Web Interface 7
3.3 STATUS MENU 8
3.3.1 Overview 8
3.3.2 System and Kernel Log 10
3.3.3 Processes 10
3.3.4 Realtime Graphs 11
3.4 SYSTEM MENU 12
3.4.1 System 12
3.4.2 Administration (Changing of Administrator Password) 13
3.4.3 Backup, Hardware Reset and Firmware Upgrade 14
3.4.4 Reboot 15
3.5 NETWORK MENU 16
3.5.1 Interfaces 16
3.5.2 Wi-Fi 21
3.5.3 DHCP and DNS 29
3.6 LOGOUT 32

4. HOW TO 33

4.1 HOW TO CHANGE THE IP ADDRESS OF THE ACCESS POINT? 33
4.2 HOW TO SECURE THE WIRELESS NETWORK WITH A PASSWORD? 34
4.3 HOW TO RESTORE FACTORY DEFAULT SETTINGS? 35
4.3.1 Factory Reset via Web Interface 35
4.3.2 Factory Reset via Hardware Button 35
4.4 HOW TO SET UP THE ACCESS POINT AS A WIRELESS REPEATER? 36
4.5 HOW TO SET UP THE ACCESS POINT AS AN AP CLIENT? 43
4.6 HOW TO ACCESS THE CONFIGURATION VIA SSH? 47

4.7 HOW TO GET THE MAXIMUM WI-FI PERFORMANCE? 49

5. APPENDIX 51

5.1 CHANGING THE IP ADDRESS OF A NETWORK ADAPTER 51

5.1.1 Windows 8 51

5.1.2 Windows 7 and 10 53

5.1.3 Windows XP: 54

5.1.4 Mac OS X 55

5.2 TECHNICAL SPECIFICATIONS 56

5.3 GNU GENERAL PUBLIC LICENSE 57

6. WARRANTY 62

7. COPYRIGHT 63

8. FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT 64

1. Product Introduction

Wireless networking with three times the speed and five times the flexibility. The Intellinet Network Solutions High-Power Ceiling Mount Wireless 300N PoE Access Point, Model 525800, is the latest in wireless networking. Taking advantage of new technology, a wireless network can now see greatly enhanced network speeds. The High-Power Ceiling Mount Wireless 300N PoE Access Point comes with a PoE PD port. This port can be used to power the device from a PoE-compliant LAN switch, which is very convenient in situations where AC power is not readily available.

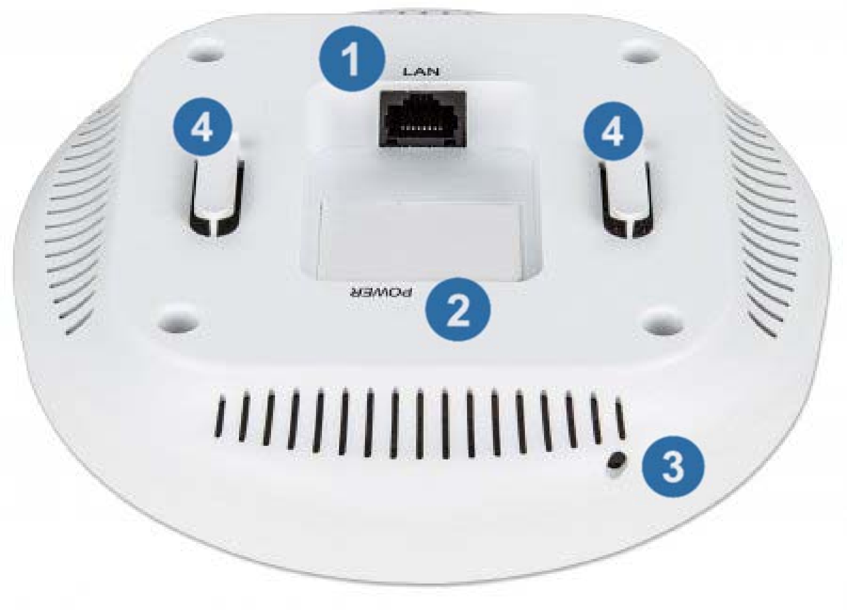
1.1 Product Features

- Up to 300 Mbps network link speed
- Smoke detector design
- Complies with 2.4 GHz IEEE 802.11n standard and is backward compatible with IEEE 802.11g/b standards
- 2T2R MIMO technology for enhanced throughput and coverage
- Supports WMM function to meet the multimedia data bandwidth requirement
- Supports WEP and WPA/WPA2 (TKIP and AES) data encryption
- IEEE 802.3af-compliant PoE-powered device with one PoE (PD) port
- DHCP server assigns IP addresses for all LAN users
- Easy installation through Web-based user interface
- Based on OpenWrt (open source) and LuCI

1.2 Package Contents

- High-Power Ceiling Mount Wireless 300N PoE Access Point
- Installation accessories
- Quick Installation Manual

1.3 Hardware Description



1 **Ethernet Port:** Ethernet port jack (RJ45) for wired Ethernet connections. The port supports 10 and 100 Mbps connections. It also acts as a IEEE802.3 af/at compliant PD port, so you can connect it to a PoE injector or PoE switch.

2 **Power Interface:** For non-PoE applications you can use this port to connect the power adapter (included).

3 **Reset Button:** If you need to restore the access point to the factory default settings, you can use a sharp object to push in the reset button. Do that for about 6 seconds and the Access Point will automatically restore the factory settings and restart.

4 **Bracket Attachment Points:** Wall or ceiling mount installation requires affixing the bracket (Figure 1) to the wall or ceiling, and then slide the bracket onto these two hooks.

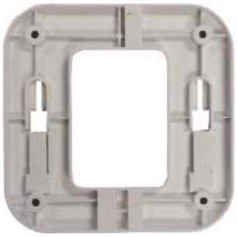


Figure 1

2. Hardware Installation

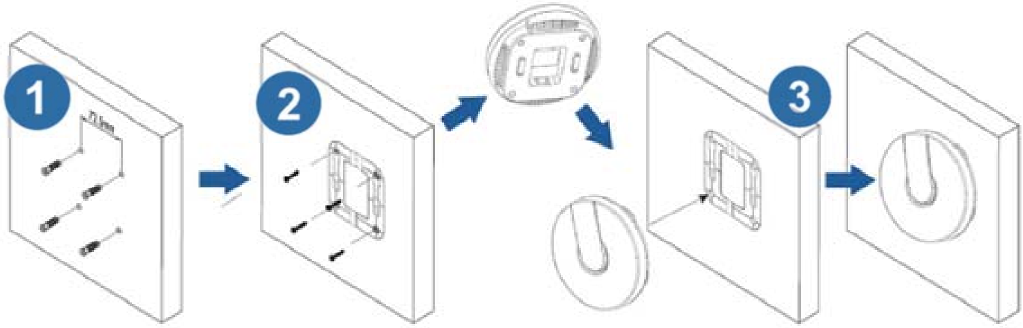
2.1 Wall Bracket Installation

1. Place the mounting bracket against a wall or the ceiling, and mark the positions of the holes with a pen. Remove the bracket and then use a drill on the four marked locations.

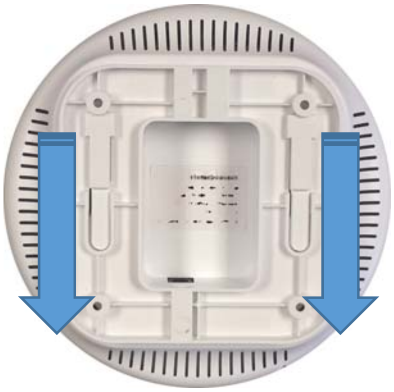
2. Insert the anchors into the holes – see image ❶

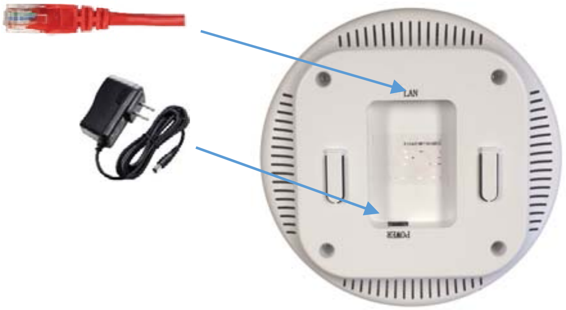
3. Line up the mounting bracket against the wall and the screw holes.
   Insert the screws into the mounting bracket and tighten the screws with a Phillips head screw driver. ❷

4. Connect the cables to the access point, and then slide the Access Point onto the attachment points on the bracket. ❸



2.2 Cable Connections

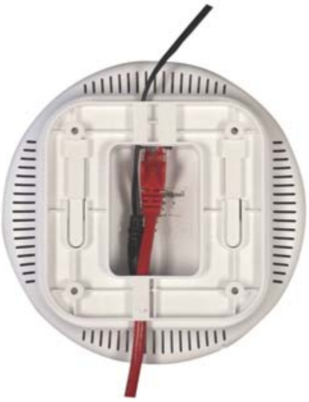




Connect an Ethernet cable to the RJ45 LAN port on the access point. Connect the other end of the cable to either a PoE injector (which connects to your network), a regular LAN switch.

Use the power adapter if you don’t use a IEEE802.3 af/at rated PoE injector or PoE switch.

Threat the cables through the ‘channels’ in the mounting brackets and put the mounting bracket back in place.



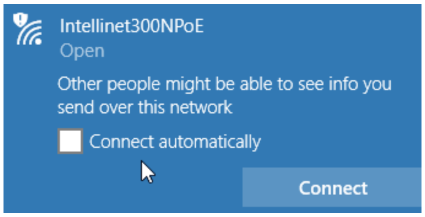
2.3 Connecting to Access Point Web Configuration Interface

2.3.1 Set up the IP address of your computer

Configuration of the access point is done with any standard web browser. In order to access the web interface of the access point, the IP address of your computer must be in range of 192.168.2.2 – 192.168.2.254. Refer to the section “Changing the IP Address of a Network Adapter” in the appendix for details.

2.3.2 Connect to the Intellinet Access Point

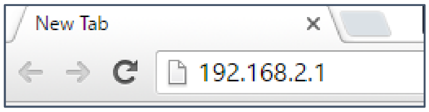
You can either connect wirelessly to SSID “Intellinet300NPoE”, or you connect via a wired network connection. In either case make sure that the IP address is set up correctly as per section 2.3.1.

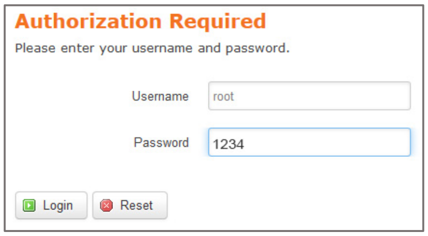


Intellinet300NPoE
Open
Other people might be able to see info you send over this network

□ Connect automatically

Open your web browser and connect to http://192.168.2.1. The default administrator password is ‘1234’.





Authorization Required

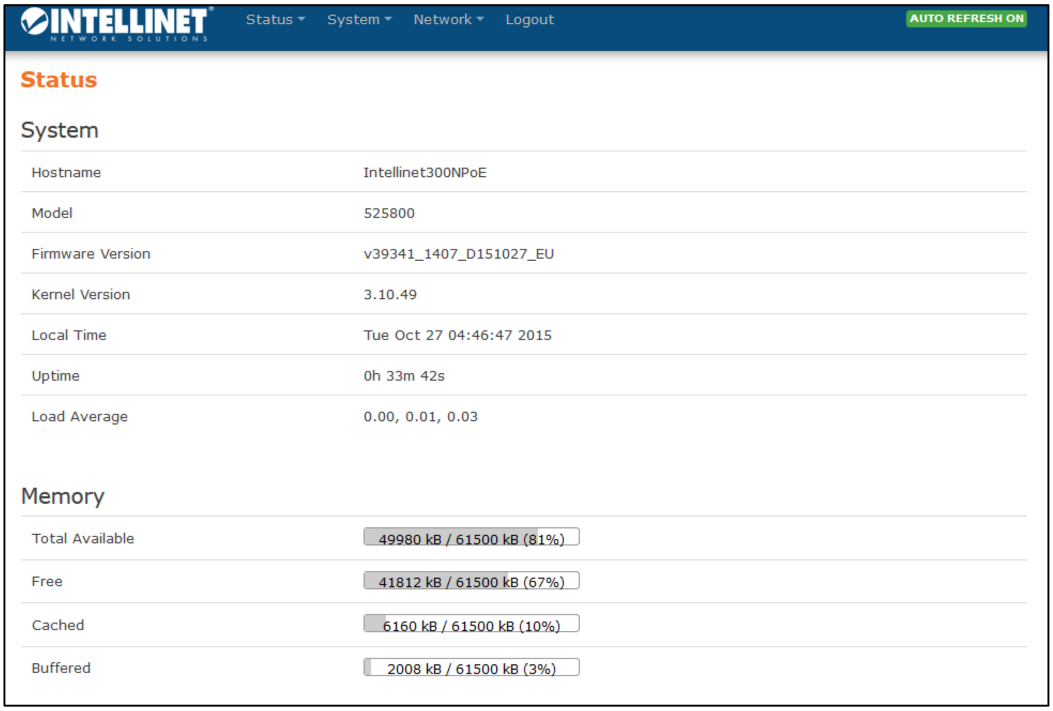
Please enter your username and password.

Username: root

Password: 1234

3. Configuration Options

3.1 Login to the device management interface



Status

System

Hostname	Intellinet300NPoE
Model	525800
Firmware Version	v39341_1407_D151027_EU
Kernel Version	3.10.49
Local Time	Tue Oct 27 04:46:47 2015
Uptime	0h 33m 42s
Load Average	0.00, 0.01, 0.03

Memory

Total Available	49980 kB / 61500 kB (81%)
Free	41812 kB / 61500 kB (67%)
Cached	6160 kB / 61500 kB (10%)
Buffered	2008 kB / 61500 kB (3%)

Access to the web interface is provided by the URL http://192.168.2.1. The default user name is 'root', and the default password is '1234.' The administrator menu provides access to the following main sections:

- **Status**
  Provides information about the device status, such as memory usage, error logs, running processes and real-time graphs.

- **System**
  Access to system settings, administrator password, tools to backup and restore the configuration, update the firmware, and more.

- **Network**
  All network related settings, wireless and wired, are controlled in this menu. Most of the key configurations are to be done here.

- **Logout**
  When you are done working on the configuration, clicking this button will end the session.

3.2 Prerequisites

3.2.1 Firmware

The Intellinet High-Power Ceiling Mount Wireless 300N PoE Access Point model 525800 is based upon the firmware OpenWRT Barrier Breaker 14.07, with LuCI utilized as the front end. These components are open source.

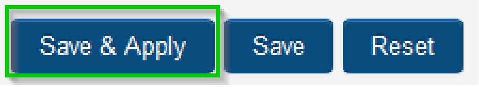
About OpenWRT:
OpenWrt is a highly extensible GNU/Linux distribution for embedded devices (typically wireless routers). Unlike many other distributions for these routers, OpenWrt is built from the ground up to be a full-featured, easily modifiable operating system for your router. In practice, this means that you can have all the features you need with none of the bloat, powered by a Linux kernel that's more recent than most other distributions.
(Excerpt from wiki.openwrt.org)

About LuCI:
This open source project resides at https://github.com/openwrt/luci/wiki. LuCI is an open source front end and a "[…] collection of several libraries, applications and user interfaces with general purpose for Lua programmers while the focus still remains on the web user interface which also became an official part of OpenWrt Kamikaze. […]

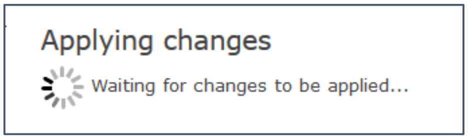
Note that the Intellinet firmware is set to use the BOOTSRAP theme. You cannot change this.

3.2.2 Using the Web Interface

Whenever you want to save the configuration and activate the new settings, you must click on "Save & Apply".

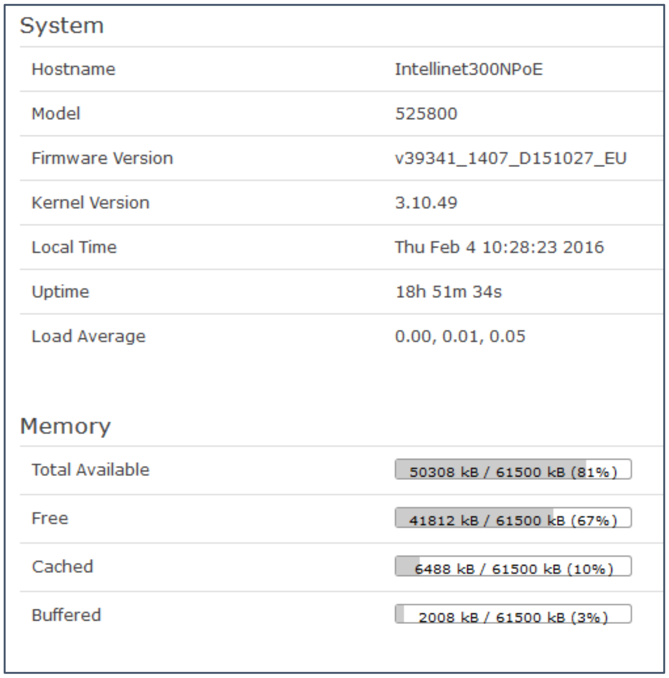


The access point will then save the settings and activate them right away.


Applying changes
Waiting for changes to be applied...

3.3 Status Menu

3.3.1 Overview



System

Hostname	Intellinet300NPoE
Model	525800
Firmware Version	v39341_1407_D151027_EU
Kernel Version	3.10.49
Local Time	Thu Feb 4 10:28:23 2016
Uptime	18h 51m 34s
Load Average	0.00, 0.01, 0.05

Memory

Total Available	50308 kB / 61500 kB (81%)
Free	41812 kB / 61500 kB (67%)
Cached	6488 kB / 61500 kB (10%)
Buffered	2008 kB / 61500 kB (3%)

The overview screen provides an at-a-glance overview of various system parameters. Most of the parameters are self-explanatory.

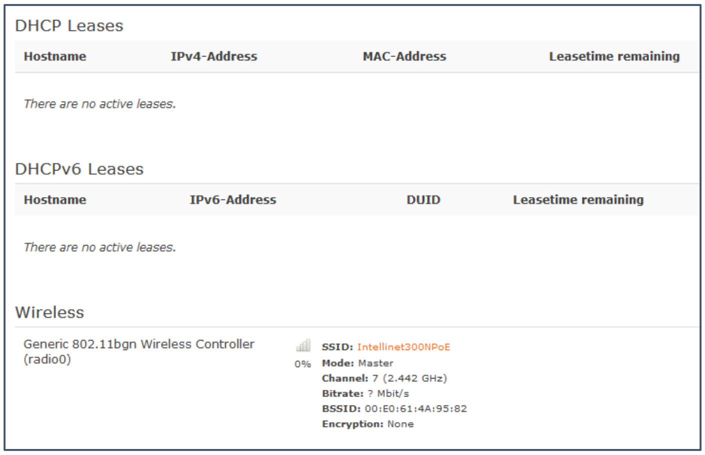
Firmware and Kernel Version:
If you ever need to contact the Intellinet technical support, make sure you include the firmware and kernel version in your message to the support team.

Load Average:
This parameter indicates the CPU load on the access point. If you experience slow-downs either when configuring the device, or during normal operations, you should check the load average. Any value approaching 1.00 is a cause for concern. Any value greater than 1.00 and your users will experience a lot of slow-downs and a reboot of the access point may be advisable. If you want to find out exactly which process is causing the high CPU load, click on 'Status -> Processes' to find out.

Memory:
This is a quick overview of the memory situation on the access point. Ideally, you will see plenty of free memory. If the system has been running for a long time, the amount of free memory may have come down. Eventually you may need to reboot the access point to free up some memory, just like you sometimes need to reboot a PC or server.

DHCP Leases:

If you enable the DHCP server in the Intellinet access point, and network clients have joined the wireless network, you can see the list of clients that have obtained an IP address from the access point here. Next tgo the host name you can see the IP address, MAC address, and also the remaining lease time, which indicates when that IP address is due to expire. DHCP lease information is provided for both IPv4 and IPv6 IP addresses.



DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining

There are no active leases.

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

Wireless

Generic 802.11bgn Wireless Controller (radio0)

0%

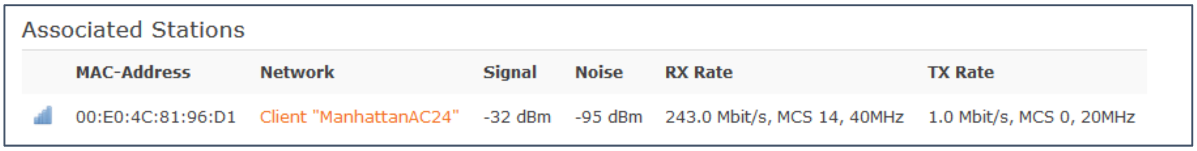
SSID: Intellinet300NPoE
Mode: Master
Channel: 7 (2.442 GHz)
Bitrate: ? Mbit/s
BSSID: 00:E0:61:4A:95:82
Encryption: None

Wireless:

Information about the current state of the wireless operation is shown in this section. Note that the signal strength indicator will show 0 % when running the standard access point mode (‘master’). That is perfectly normal behavior.

Associated Stations:

All connected WLAN clients are shown here, along with their MAC address, signal strength, data rates, etc.

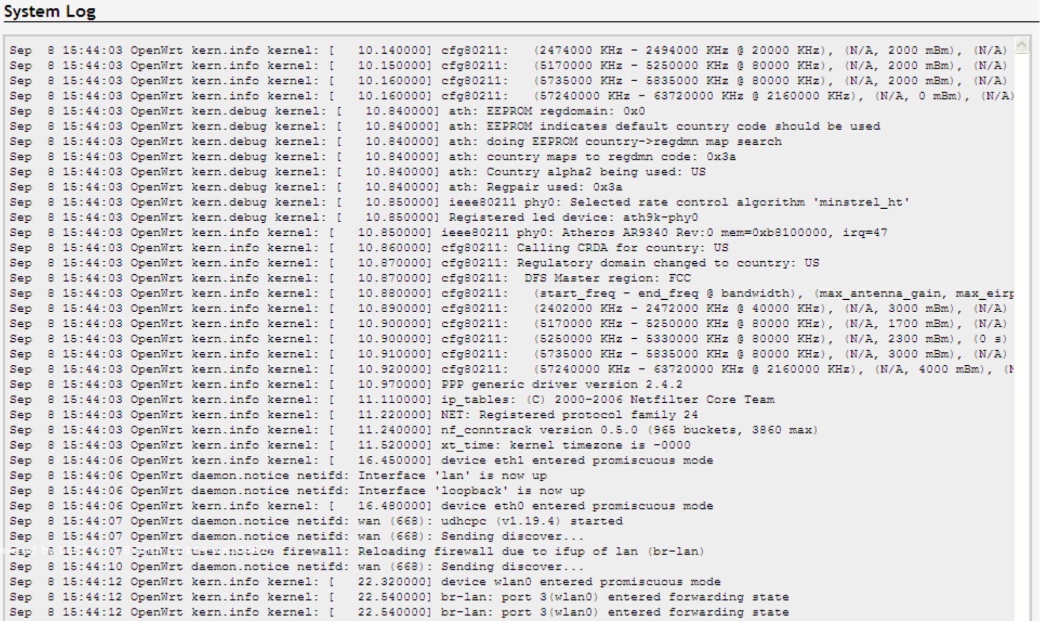


Associated Stations

	MAC-Address	Network	Signal	Noise	RX Rate	TX Rate
	00:E0:4C:81:96:D1	Client "ManhattanAC24"	-32 dBm	-95 dBm	243.0 Mbit/s, MCS 14, 40MHz	1.0 Mbit/s, MCS 0, 20MHz

3.3.2 System and Kernel Log

The Intellinet access point provides to very detailed logs, which can be useful in case you ever need to contact the technical support department.t

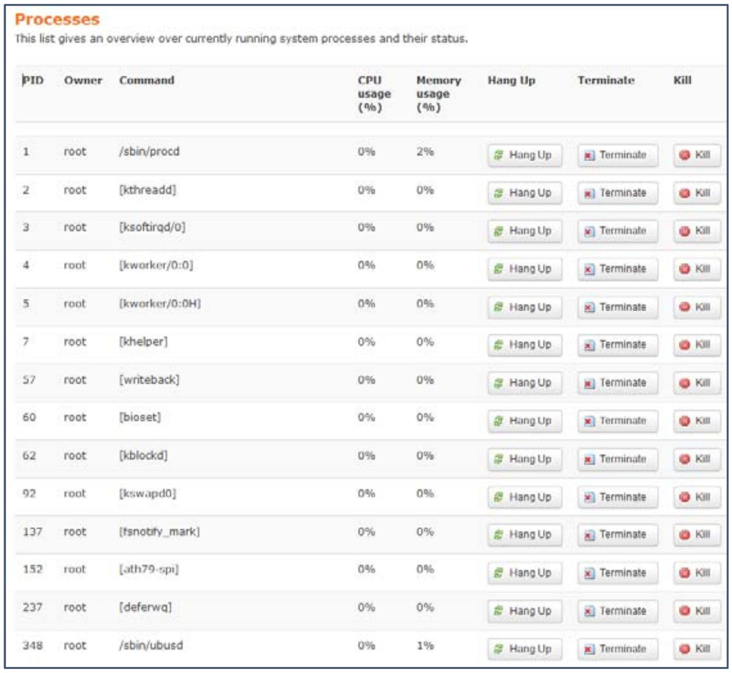


System Log

```
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.140000] cfg80211:   (2474000 KHz - 2494000 KHz @ 20000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.150000] cfg80211:   (5170000 KHz - 5250000 KHz @ 80000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.160000] cfg80211:   (5735000 KHz - 5835000 KHz @ 80000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.160000] cfg80211:   (57240000 KHz - 63720000 KHz @ 2160000 KHz), (N/A, 0 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: EEPROM regdomain: 0x0
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: EEPROM indicates default country code should be used
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: doing EEPROM country->regdmn map search
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: country maps to regdmn code: 0x3a
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: Country alpha2 being used: US
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: Regpair used: 0x3a
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.850000] ieee80211 phy0: Selected rate control algorithm 'minstrel_ht'
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.850000] Registered led device: ath9k-phy0
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.850000] ieee80211 phy0: Atheros AR9340 Rev:0 mem=0xb8100000, irq=47
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.860000] cfg80211: Calling CRDA for country: US
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.870000] cfg80211: Regulatory domain changed to country: US
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.870000] cfg80211:  DFS Master region: FCC
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.880000] cfg80211:   (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.890000] cfg80211:   (2402000 KHz - 2472000 KHz @ 40000 KHz), (N/A, 3000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.900000] cfg80211:   (5170000 KHz - 5250000 KHz @ 80000 KHz), (N/A, 1700 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.900000] cfg80211:   (5250000 KHz - 5330000 KHz @ 80000 KHz), (N/A, 2300 mBm), (0 s)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.910000] cfg80211:   (5735000 KHz - 5835000 KHz @ 80000 KHz), (N/A, 3000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.920000] cfg80211:   (57240000 KHz - 63720000 KHz @ 2160000 KHz), (N/A, 4000 mBm), (N
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.970000] PPP generic driver version 2.4.2
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.110000] ip_tables: (C) 2000-2006 Netfilter Core Team
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.220000] NET: Registered protocol family 24
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.240000] nf_conntrack version 0.5.0 (965 buckets, 3860 max)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.520000] xt_time: kernel timezone is -0000
Sep  8 15:44:06 OpenWrt kern.info kernel: [   16.450000] device eth1 entered promiscuous mode
Sep  8 15:44:06 OpenWrt daemon.notice netifd: Interface 'lan' is now up
Sep  8 15:44:06 OpenWrt daemon.notice netifd: Interface 'loopback' is now up
Sep  8 15:44:06 OpenWrt kern.info kernel: [   16.480000] device eth0 entered promiscuous mode
Sep  8 15:44:07 OpenWrt daemon.notice netifd: wan (668): udhcpc (v1.19.4) started
Sep  8 15:44:07 OpenWrt daemon.notice netifd: wan (668): Sending discover...
Sep  8 15:44:07 OpenWrt user.notice firewall: Reloading firewall due to ifup of lan (br-lan)
Sep  8 15:44:10 OpenWrt daemon.notice netifd: wan (668): Sending discover...
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.320000] device wlan0 entered promiscuous mode
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.540000] br-lan: port 3(wlan0) entered forwarding state
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.540000] br-lan: port 3(wlan0) entered forwarding state
```

3.3.3 Processes

This screen shows a complete list of all running processes on the Intellinet access point. This list can be useful if you need to examine performance slow-downs, which may be caused by a higher CPU load. Each process is shown with its current CPU usage (%) and memory usage (%). If you wish to end a process, you have three choices to do so.



Processes

This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	2%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
4	root	[kworker/0:0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/0:0H]	0%	0%	Hang Up	Terminate	Kill
7	root	[khelper]	0%	0%	Hang Up	Terminate	Kill
57	root	[writeback]	0%	0%	Hang Up	Terminate	Kill
60	root	[bioset]	0%	0%	Hang Up	Terminate	Kill
62	root	[kblockd]	0%	0%	Hang Up	Terminate	Kill
92	root	[kswapd0]	0%	0%	Hang Up	Terminate	Kill
137	root	[fsnotify_mark]	0%	0%	Hang Up	Terminate	Kill
152	root	[ath79-spi]	0%	0%	Hang Up	Terminate	Kill
237	root	[deferwq]	0%	0%	Hang Up	Terminate	Kill
348	root	/sbin/ubusd	0%	1%	Hang Up	Terminate	Kill

1. Hang Up

The safest and least aggressive command will try to end the process by 'asking nicely'. Most daemons will adhere to this command and close the process without disrupting anything or losing data.

2. Terminate

This commands orders the process to stop whatever it is doing and end itself. This is no longer ‘asking nicely’. This is ‘telling’. Since ending the process is still in the hand of the daemon for the process, this is also fairly safe to execute.

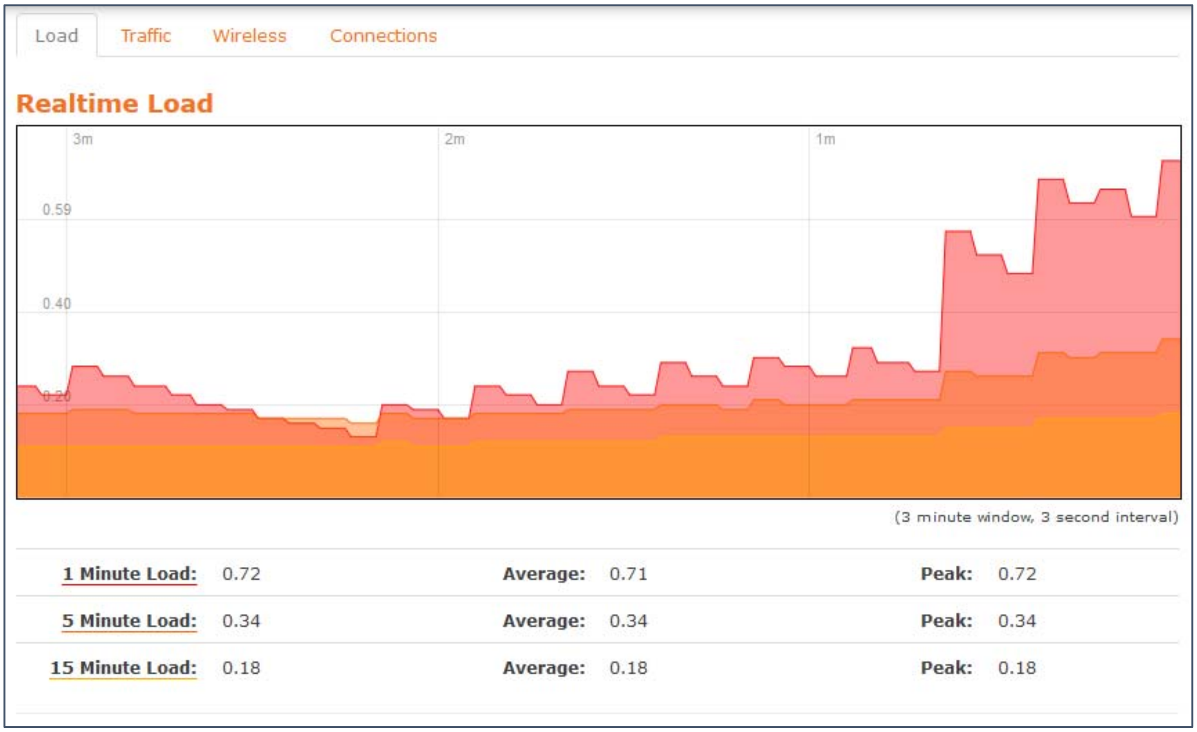
3.

When all other options fail and you cannot get a process to shut down by any of the two other means, the kill command is the last resort. It’s the toughest kill signal available as it shuts down the process rather than let the daemon shut it down properly.

Note: Under normal circumstances there is no need to end, terminate or kill a process. All of these processes server a specific purpose, and shutting down processes can bring down the entire system. In that case a power cycle of the access point may become unavoidable.

3.3.4 Realtime Graphs

The Intellinet access point provides you with detailed runtime data about the CPU load, traffic, wireless signal quality and the amount of connections.



Realtime Load

(3 minute window, 3 second interval)

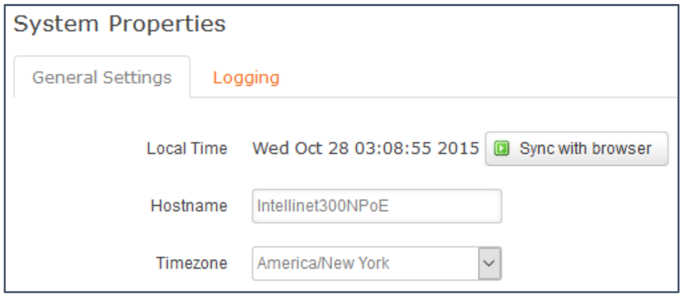
1 Minute Load:	0.72	Average:	0.71	Peak:	0.72
5 Minute Load:	0.34	Average:	0.34	Peak:	0.34
15 Minute Load:	0.18	Average:	0.18	Peak:	0.18

3.4 System Menu

3.4.1 System

On this screen you can define parameters related to error logging, time settings and the network name of the Intellinet access point.

General Settings:
Displays the current system time, allows to synchronize the time with your computer's web browser, displays the current network name of the access point (default 'Intellinet300NPoE'), as well as the time zone.

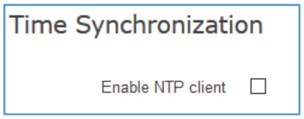

System Properties

Local Time: Wed Oct 28 03:08:55 2015

Hostname: Intellinet300NPoE

Timezone: America/New York

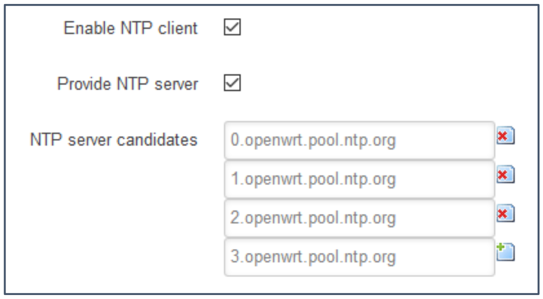
Time Synchronization:
The Intellinet access point doesn't have a real-time clock or a CMOS battery, and because of this, every time it loses power, the clock resets to a default date. To prevent this from happening, ,you can use NTP to get the time from the internet. Note that setting up NTP is not required for the Intellinet access point to function, but it can make troubleshooting easier when you're looking at timestamped log files.


Time Synchronization

Enable NTP client ☐

Enable the NTP client to activate this feature. When activated, the Intellinet access point will provide you with a list of four possible NTP servers. These are good choices in general.

The option "Provide NTP server" can be activated, to turn the Intellinet access point into an NTP relay SERVER. That means, it'll forward NTP requests from clients in your network to an external NTP server.


Enable NTP client ☑

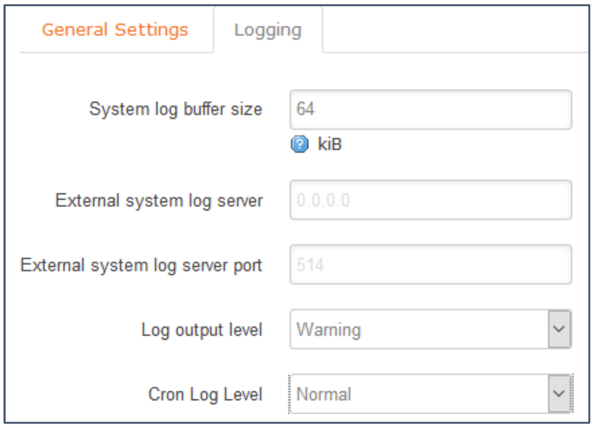
Provide NTP server ☑

NTP server candidates: 0.openwrt.pool.ntp.org
1.openwrt.pool.ntp.org
2.openwrt.pool.ntp.org
3.openwrt.pool.ntp.org

Logging:
The Intellinet access point has the ability to create a history log of important events. These logs can be stored either in the device own memory, or on an external server using the Syslog protocol, which is a standard for forwarding log messages in an IP network.

System log buffer size:
The default value is 16 kiB (kibibyte, or kilobyte). Once that buffer is used up, the log will be overwritten. You can assign a larger value here, but be mindful of the total available memory of your system.

External system log server:
Syslog is a client/server protocol. The Syslog sender (the access point) sends a small (less than 1KB) textual message to the Syslog server. Enter the IP address of your Syslog server here.



System log buffer size: 64 kiB

External system log server: 0.0.0.0

External system log server port: 514

Log output level: Warning

Cron Log Level: Normal

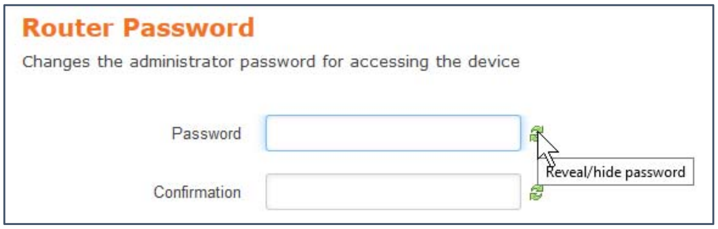
External system log server port:
The standard port for Syslog servers is 514. You can make adjustments to that value here, if necessary.

Log Output level:
You can define, how much information you want to include in the log file. “Debug” creates messages about virtually everything that is going on whereas “Emergency” only logs messages of the utmost importance.

Cron Log Level:
This parameter controls the log level for the kernel log.

3.4.2 Administration (Changing of Administrator Password)

On this page you can change the administrator password for the web interface. Provide a new password, and repeat it in the confirmation field.



Router Password

Changes the administrator password for accessing the device

Password:

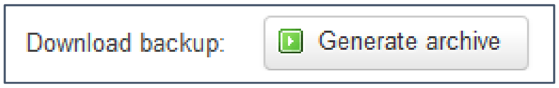
Confirmation:

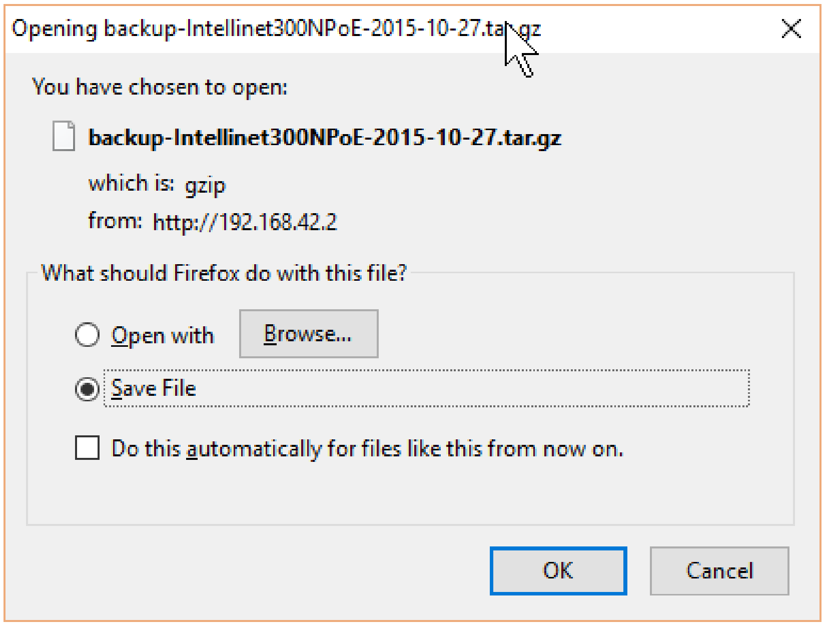
3.4.3 Backup, Hardware Reset and Firmware Upgrade

3.4.3.1 Backup / Restore

This page enables you to save the access point’s current settings as a file to your local computer, and also restore the access point to previously saved settings.

Backup:

1. 
Download backup: Generate archive

2. 
Opening backup-Intellinet300NPoE-2015-10-27.tar.gz

You have chosen to open:

backup-Intellinet300NPoE-2015-10-27.tar.gz

which is: gzip

from: http://192.168.42.2

What should Firefox do with this file?

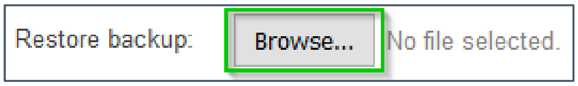
○ Open with Browse...

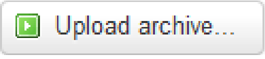
● Save File

□ Do this automatically for files like this from now on.

OK Cancel

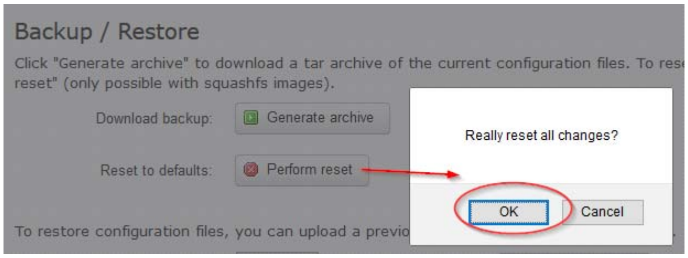
Restore:

1. 
Restore backup: Browse... No file selected.

2. 
Upload archive...

3.4.3.2 Factory Reset:

In order to set back the Intellinet access point to the factory default settings, you need to click on the “perform reset“ button, and then confirm the second question by clicking “OK”.



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To res
reset" (only possible with squashfs images).

Download backup:

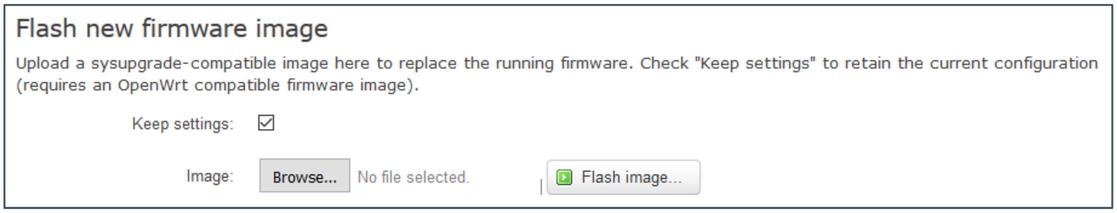
Reset to defaults:

To restore configuration files, you can upload a previo

Really reset all changes?

3.4.3.3 Firmware Upgrade:

This function allows updating the system firmware to a more recent version. Updated firmware versions can offer increased performance and security, as well as bug fixes. You can download the latest firmware from the Intellinet website at www.intellinetnetwork.com/search?q=525800.



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ☑

Image: No file selected.

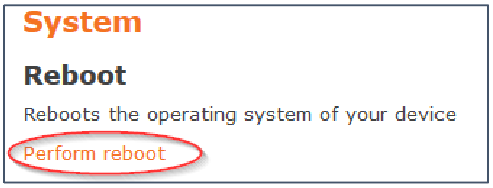
Keep Settings: Activate this option if you want to keep the current system configuration of your access point. If you uncheck this option, the access point will perform a reset to factry default values after the firmware upgrade.

Image: Click “Browse …” to select the firmware file on your hard drive.
Flash Image: Click here to begin the firmware upgrade process.

Note: Installing an incorrect firmware file, or interrupting the firmware upgrade process, i.e., by disconnecting the access point from power or the network, can lead to the destruction of the access point. PROCEED WITH CAUTION.

3.4.4 Reboot

In order to reboot the access point without physically disconnecting it from the power source, you can use this function. A reboot may be necessary from time to time in order to free up system resources, such as memory.



System

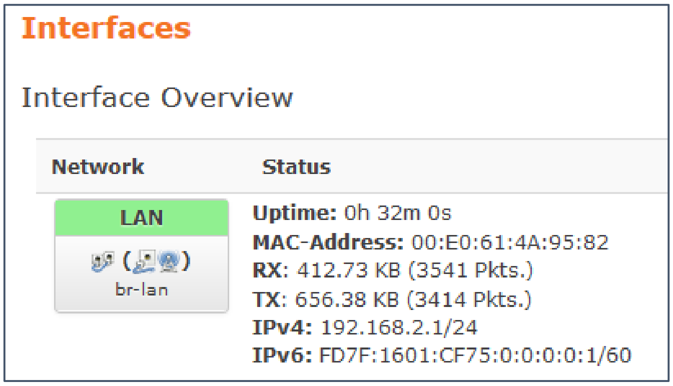
Reboot

Reboots the operating system of your device

3.5 Network Menu

3.5.1 Interfaces

The interfaces screen allows customization of the LAN interface. It provides access to many advanced features which require a good knowledge about TCP/IP and wireless networks. This user guide will therefore limit itself to those tasks, that most users are going to have to deal with.



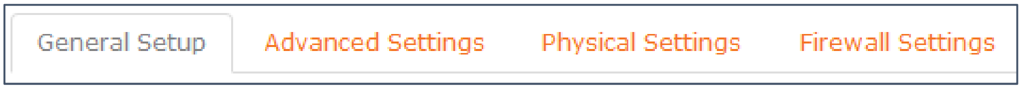
Interfaces

Interface Overview

Network	Status
LAN br-lan	**Uptime:** 0h 32m 0s **MAC-Address:** 00:E0:61:4A:95:82 **RX:** 412.73 KB (3541 Pkts.) **TX:** 656.38 KB (3414 Pkts.) **IPv4:** 192.168.2.1/24 **IPv6:** FD7F:1601:CF75:0:0:0:0:1/60

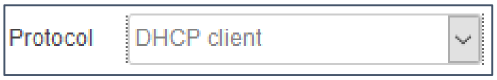
Above: Interface Statistics

Clicking the "Edit" button opens a new screen, which is divided into four screens.



General Setup:
The most important feature here is the protocol selection. You will either set this to "Static address", which is the default value, or to "DHCP client". All other options don't apply to the Intellinet access point.

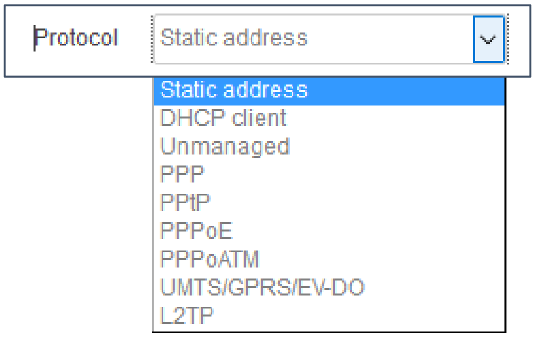
DHCP client:
If you want the Intellinet access point to receive its IP information from a DHCP server in your network, i.e., a router, then you can enable this option. With this option enabled, the IP address of the Intellinet access point will depend on the DHCP server in your network. You will need to check with the DHCP server log in order to find out which IP address the Intellinet access point can be reached at.



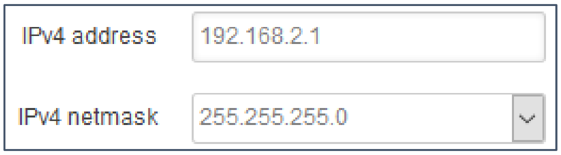
Protocol: DHCP client

Static address:

You need to set up the IP address of the access point manually. When you select this option, you will need to specify the IPv4 IP address and the IPv4 netmask.



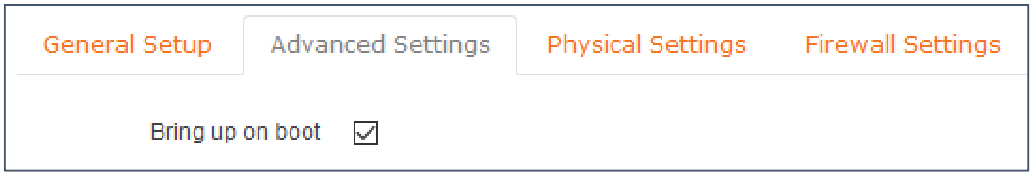
Protocol: Static address



IPv4 address: 192.168.2.1

IPv4 netmask: 255.255.255.0

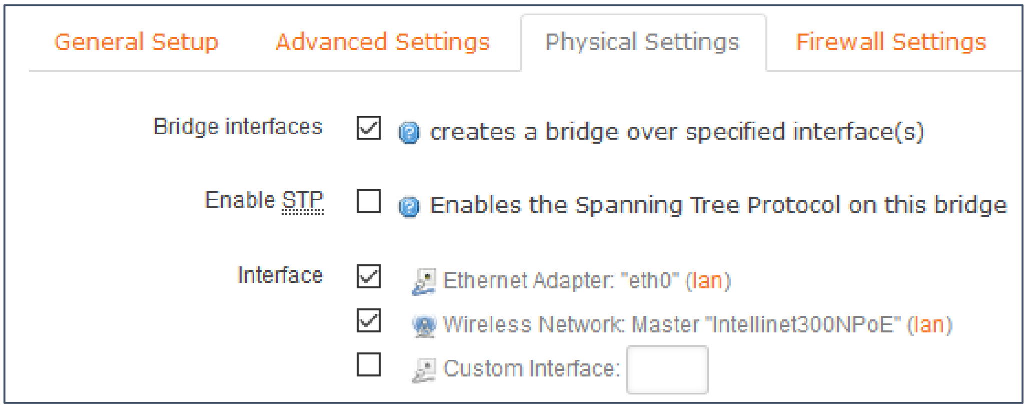
You can also set up the IPv6 address, in case you run an IPv6 address scheme in your local network. Set the IPv6 assignment length, i.e., 64 and the prefix (hint). All other options (IPv4 broadcast, custom DNS servers, etc.) do not apply.



Bring up on boot ☑

Advanced Settings:

Largely irrelevant to the Intellinet Access Point, however you do want to make sure that the “bring up on boot” option is activated.



Bridge interfaces ☑ creates a bridge over specified interface(s)

Enable STP □ Enables the Spanning Tree Protocol on this bridge

Interface ☑ Ethernet Adapter: "eth0" (lan)

☑ Wireless Network: Master "Intellinet300NPoE" (lan)

□ Custom Interface:

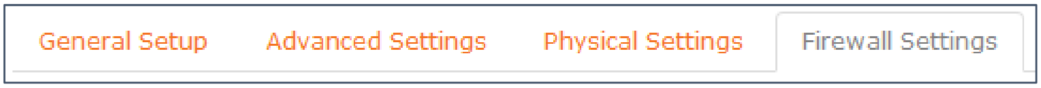
Physical Settings:

Under normal circumstances there is no need to make any adjustments here. Above shows the default configuration of the Intellinet access point.

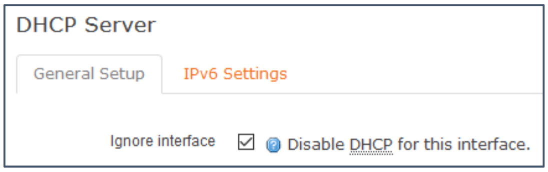
Bridge interfaces: Activate this option and the interfaces selected below will be able to communicate with each other (i.e., “eth0” and “Intellinet300NPoE”. Normally, this is what you would want.

Enable STP: The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Even if you don't think you will be running into a situation where loops may be created in your network, activating this option is still considered best practice.

Interface: This are the interfaces of your Intellinet access point. By default you will only see the two "physical" interfaces, which are the LAN port eth0 and the Wi-Fi radio "Intellinet300NPoE". If you have added other interfaces, they, too, will show up in this section.



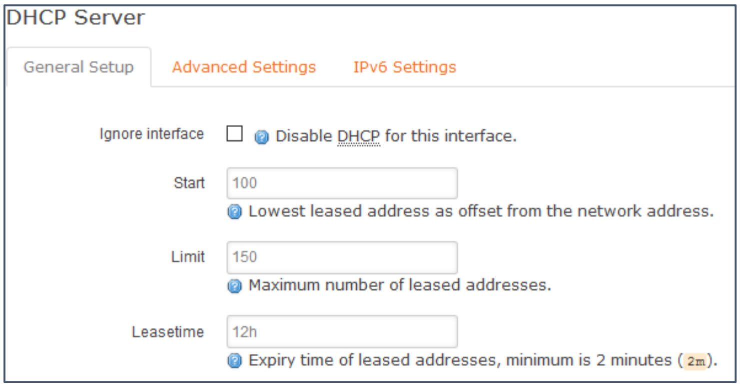
The Firewall Settings do not apply to the function of the Intellinet access point. The default setting is "lan".



Ignore interface ☑ Disable DHCP for this interface.

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually. The most common example of a DHCP server is a router, which connects local network clients to the Internet.

Ignore interface: Enable or disable this option to activate or deactivate the DHCP service for the interface.



Ignore interface ☐ Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 minutes (`2m`).

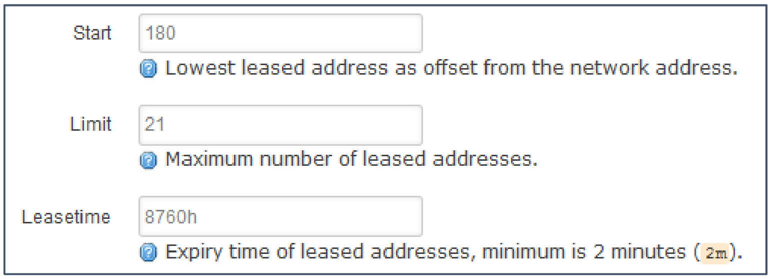
If you enable DHCP, then you need to provide three additional parameters:

1. Start:
What is the lowest IP address of the block of IP addresses the DHCP will hand out.

2. Limit
How many IP addresses are being handed out by the DHCP server.

3. Lease Time
Specify the lease time for each of the IP addresses given out to network clients. Possible values range from “2m” (two minutes) to a very high number of hours, for example “8760h”, which is as much as one year.

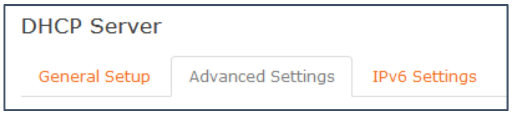
Example: If you want to set up the Intellinet access point to act as a DHCP server and provide IP addresses for clients in range of 192.168.2.180 – 192.168.2.200, which are valid for one week, then you would set up the parameters as shown below:



Start 180
Lowest leased address as offset from the network address.

Limit 21
Maximum number of leased addresses.

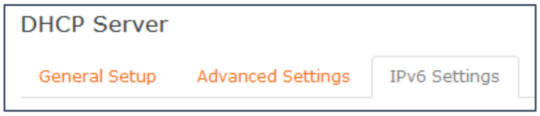
Leasetime 8760h
Expiry time of leased addresses, minimum is 2 minutes (2m).



DHCP Server

The advanced settings for the DHCP server are best to be left alone, unless you know exactly what you are doing.

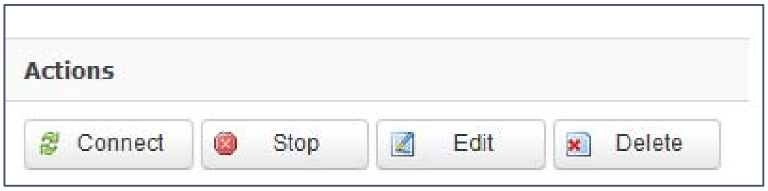
Parameter	Description
Dynamic DHCP	Dynamically allocate DHCP addresses for clients. If disabled, only clients with static leases will be served. A static lease, also referre3d to as static DHCP, is the process, where a certain IP address is reserved for a certain network client by means of assigning the IP address to that client’s MAC address.
Force	Force DHCP on this network even if another server is detected.
IPv4-Netmask	If specified, the Intellinet access point will provide this network mask to all clients. Normally it is calculated from the subnet that is served, but this option, when activated, overrides the netmask sent to clients.
DHCP-Options	This field can be used for any number of things. The Bootstrap Protocol (BOOTP) knows a number of DHCP related parameters. Refer to the ‘Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) Parameters’ on *iana.org* for further information.



IPv6 related DHCP settings are as follows:

Parameter	Description
Router Advertisement-Service	Set to disabled, relay, server or hybrid mode.
DHCPv6-Service	Set to disabled, relay, server or hybrid mode.
NDP-Proxy	Set to disabled, relay, server or hybrid mode.
Announced DNS servers	DNS servers to be announced to clients.
Announced DNS domains	DNS domains to be announced to clients.

Before we move on, let’s take a look at the remaining actions on the interface settings page:



Connect: Clicking this button will re-initialize the interface.

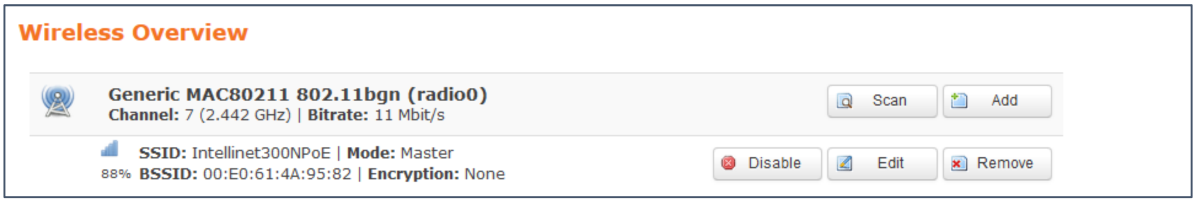
Stop: Clicking this button will shut down that interface. Be careful not to shut down the interface, which you use in order to access the configuration menu, or else …

Edit: Discussed on preceding pages at length.

Delete: Completely removed the interface from the Intellinet access point configuration. Be careful not to delete the interface, which you use in order to access the configuration menu, or else … see above.

3.5.2 Wi-Fi

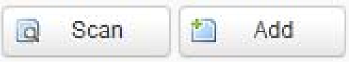
This section deals with the wireless function of the Intellinet access point. The image below shows the default state of the wireless settings. On the following pages we are going to discuss some core settings of the wireless interface. More specific tasks related to the wireless configuration are covered in the HOW TO section of this user guide.



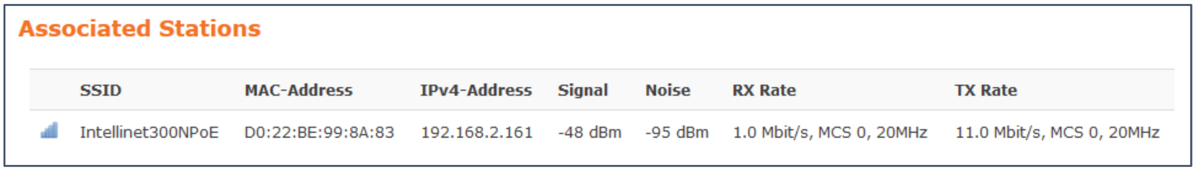
Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | **Bitrate:** 11 Mbit/s

SSID: Intellinet300NPoE | **Mode:** Master
88% **BSSID:** 00:E0:61:4A:95:82 | **Encryption:** None



These two options are used to connect the Intellinet access point with another wireless network, or to add another wireless SSID to the existing configuration. You can find more information in the HOW TO section of this user guide.

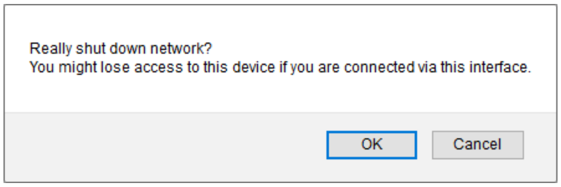


Associated Stations

	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
	Intellinet300NPoE	D0:22:BE:99:8A:83	192.168.2.161	-48 dBm	-95 dBm	1.0 Mbit/s, MCS 0, 20MHz	11.0 Mbit/s, MCS 0, 20MHz

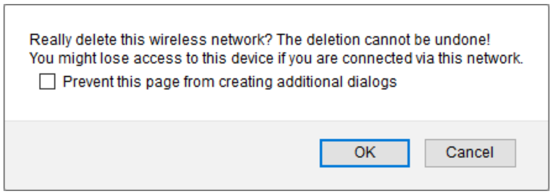
All clients that are currently connected to the Intellinet wireless access point are listed here. The SSID identifies to which SSID the station is connected. When you have a setup with multiple SSIDs, the SSID information will be helpful as it allows you to quickly ascertain to which wireless network a certain client is connected to. The other information about the given is pretty self-explanatory.

Disable: If you want to disable wireless service, you can click on this button. A security message (below) will remind you about the possible implications of this action.



Really shut down network?
You might lose access to this device if you are connected via this interface.

Remove: Similar to “Disable”, but this action is permanent as it deletes the current wireless setup from the access point configuration. As before, a warning message needs to be confirmed by clicking on “OK”, before this action will be performed.

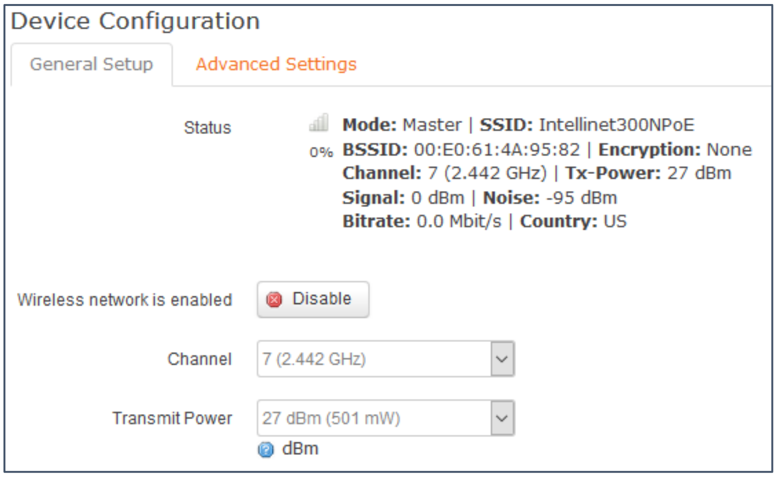


Really delete this wireless network? The deletion cannot be undone!
You might lose access to this device if you are connected via this network.

☐ Prevent this page from creating additional dialogs

This lets you make changes to the wireless configuration.

3.5.2.1 Device Configuration - General Setup:



Device Configuration

Status: 0% **Mode:** Master | **SSID:** Intellinet300NPoE
BSSID: 00:E0:61:4A:95:82 | **Encryption:** None
Channel: 7 (2.442 GHz) | **Tx-Power:** 27 dBm
Signal: 0 dBm | **Noise:** -95 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

Wireless network is enabled

Channel: 7 (2.442 GHz)

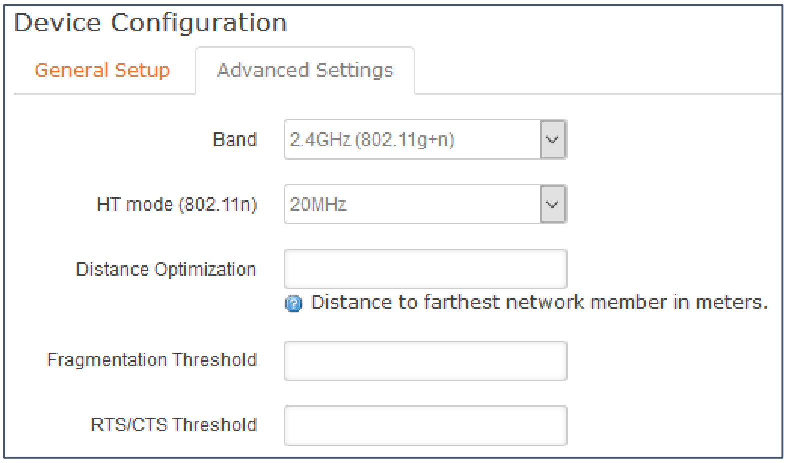
Transmit Power: 27 dBm (501 mW)

dBm

Parameter	Description
Status	All information about the current wireless configuration at a glance. Note that if no wireless connection has been established by any WLAN client, the signal strength will be indicated as 0 dBm, and the Bitrate will show as 0.0 Mbit/s. once connections are made, these numbers will change.
Disable button	You can disable the wireless function by clicking this button. This is very much the same as the disable function described on the previous page, but when you click the disable button here, there will not be any warning message for you to confirm. So proceed with caution, or you might accidentally disable Wi-Fi service for all your users.
Channel	Wireless channels EU (ETSI): 1-13, U.S. (FCC): 1-11. Set the channel to a value that puts this wireless network at least four channels apart from an existing wireless network that might be in close proximity. For example, if another 2.4 GHz wireless network in range is set to channel 2, then it’d be best to set your Intellinet access point to channel 6 or higher.

Transmit Power	With this parameter you can control how strong the wireless signal is that the Intellinet access sends out. If you want to maximize wireless signal range and performance, you want to set this value to the highest setting, however there might be situations where you want to reduce the signal strength, because you do not want your Wi-Fi signal to travel too far. There are two variants of the Intellinet access point. The EU (ETSI) version provides a maximum power output of 17 dBm, which in combination with the 3 dBi internal antenna equates to 20 dBm EIRP power. The US version (FCC) of the Intellinet access point provides up to 27 dBm output power for a total EIRP power output of 30 dBm.

3.5.2.2 Device Configuration – Advanced Settings


Device Configuration

Band: 2.4GHz (802.11g+n)

HT mode (802.11n): 20MHz

Distance Optimization:

Distance to farthest network member in meters.

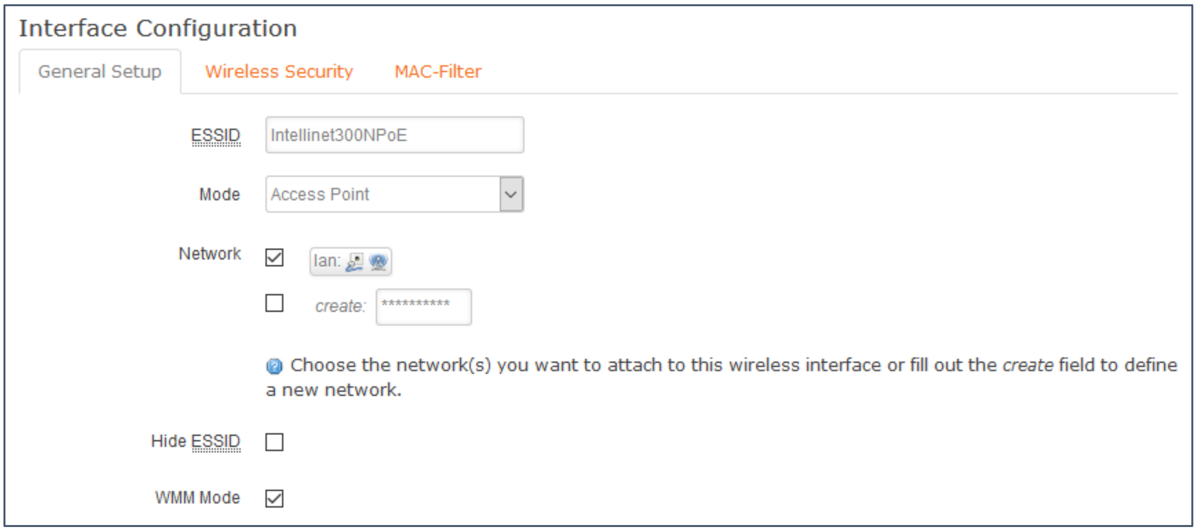
Fragmentation Threshold:

RTS/CTS Threshold:

Parameter	Description
Band	Set to 2.4 GHz for wireless IEEE 802.11g and N devices. This value cannot be changed.
HT mode (802.11n)	HT stands for high throughput. The IEEE 802.11n standard knows two HT modes, HT20 and HT40. The number references the width of the channel used by the access point. Possible values are disabled, 20 MHz, and 40 MHz. Disabled: This disables wireless N connections. The fastest link speed achievable is 56 Mbps (Wireless G). 20 MHz: HT20 mode with a 20 MHz wide channel for link speeds of up to 150 Mbps. 40 MHz: Two neighboring 20 MHz channels are bundled to form a 40 MHz channel - for link speeds of up to 300 Mbps with a 2T2R WLAN adapter.

Force 40MHz mode	When you activate the 40 MHz HT mode, this option appears. If this option is deactivated, you run the Intellinet access point in the proper 20/40 MHz coexist model. When activated, the access point will always use 40MHz channels even if the secondary channel overlaps with other wireless networks. Using this option does not comply with IEEE 802.11n-2009, and since using 40 MHz can actually be detrimental to the performance in busy network environments, activating this open is rarely a good idea.
Distance Optimization	This parameter controls the sensitivity range. When a packet is sent out from the access point, it waits for an acknowledgement frame from the other end. The access point will wait for a response until a certain amount of time has elapsed, called the "ACK timeout". When you enter the maximum distance to the furthest member of the wireless network, you optimize the ACK timeout for your network. Enter the value in meters. If you are used to using “feet”, simply divide the approx. distance by three. Keep in mind that the higher the ACK timing, the lower the throughput will be. If the value is set too high, packets could be lost as the access point waits for the ACK window to timeout. On the other hand, if the ACK value is set too low, the window could expire too soon and returning packets could be dropped, also lowering throughput.
Fragmentation Threshold	The fragmentation threshold is used to set the maximum packets size that a client will send. The smaller the maximum sizes the better the reliability of the wireless connection, but the performance is likely to decrease. Possible values range from 256 to the default value of 2346 (bytes). So when should you change this value? Only if you need to improve the reliability of a wireless connection where performance is secondary. Usually you do more harm than good if you lower the fragment threshold.
RTS/CTS Threshold	RTS/CTS (request to send / clear to send) packets are sent by wireless clients to access points. The clients essentially ask for permission to send the next data packet. The lower the threshold, the more stable your wireless network, since it essentially asks more often when sending packages. The default value is 2347, and you are well advised to leave this value unchanged.

3.5.2.3 Interface Configuration – General Setup



Interface Configuration

ESSID: Intellinet300NPoE

Mode: Access Point

Network: ☑ lan:
☐ create: **********

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

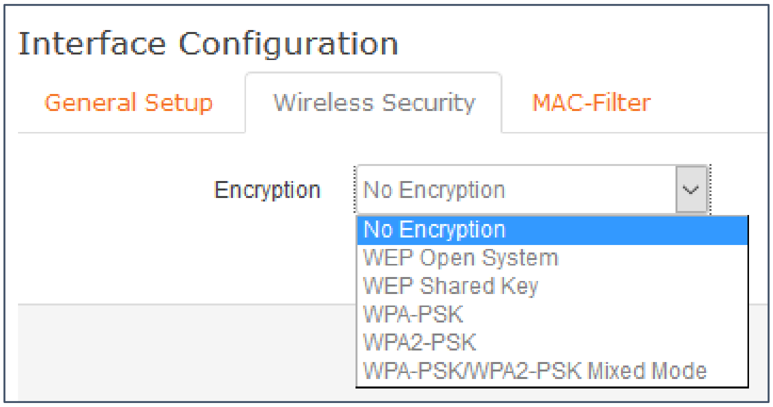
Hide ESSID ☐

WMM Mode ☑

Parameter	**Description**
ESSID	The name of the wireless network.
Mode	Access Point: Default operation mode, which you will use most of the time. It is used to connected wireless clients to the wired network. It's also referred to as the 'Master' mode. Client: Also referred to as AP Client, or station mode. Normally the Intellinet device acts as a full-fledged wireless access point, however in client mode, things are different. In client mode, the Intellinet access point does not offer itself as a wireless access point to wireless clients. Instead it uses its wireless radio to connect to another wireless network, and any station connected to the LAN port of the access point can communicate with the wireless network. In client mode, the Intellinet access point acts as if it were a wireless network adapter. Access Point (WDS): WDS stands for wireless distribution system. A wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client frames across links between access points. One disadvantage is that the maximum wireless effective throughput may be halved after the first retransmission (hop) being made. For example, in the case of two APs connected via WDS, and communication is made between a computer which is plugged into the Ethernet port of AP A and a laptop which is connected wirelessly to AP B. The throughput is halved,

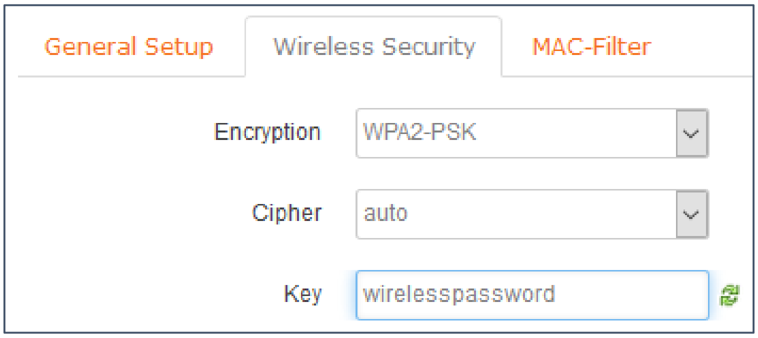
	because AP B has to retransmit the information during the communication of the two sides. Client (WDS): In this mode the access point acts as a client, similar to the regular client mode, but in this case it will connect to access points in WDS mode. When activated, you need to enter the WDS access point's ESSID and BSSID into the configuration.
Network	This option is used to connect the wireless network interface to another interface. By default this is the LAN interface, which is what you need if you want wireless clients to be able to communicate with the rest of the network that is connected to the access point's LAN port.
Hide ESSID	Enable or disable the broadcast of the SSID.
WMM Mode	WMM stands for Wi-Fi Multimedia. WMM prioritizes network traffic in four categories: 1. Voice 2. Video 3. Best effort (this is the majority of traffic from applications other than video and voice) 4. Background jobs such as printing, file downloads and other non-latency sensitive applications. Simply by activating WMM for the SSIDs of the Intellinet Access Point you can already achieve a noticeable improvement of the quality of service.

3.5.2.4 Interface Configuration – Wireless Security


Interface Configuration

Encryption: No Encryption

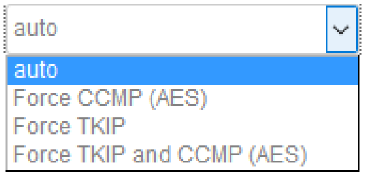
In order to secure access to the wireless network, you can enable encryption. WPA2-PSK is recommended as it provides the best security, while WEP should not be used anymore, unless you have some legacy equipment that does not support WPA or WPA2.
WPA-PSK and WPA/2-PSK Mixed Mode can be used, if you have equipment that does not support WPA2-PSK, other than that, WPA2-PSK is the best option.



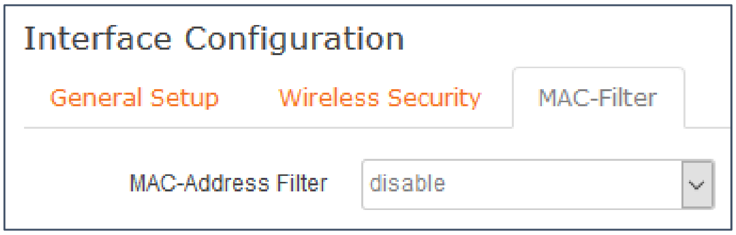
Encryption: WPA2-PSK

Cipher: auto

Key: wirelesspassword

Parameter	Description
Encryption	Select the encryption type you wish to use for the wireless network.
Cipher	In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption. In this case, the cipher is the method used to secure the wireless key.  auto auto Force CCMP (AES) Force TKIP Force TKIP and CCMP (AES) The most secure cipher is CCMP (AES). If security matters to you more than potential problems caused by incompatibilities to older Wi-Fi devices, then you should select “Force CCMP (AES)” mode. TKIP is designed for hardware which does not support CCMP. It provides better compatibility at the cost of reduced security. Auto is the default mode, and for most users, it provides a good compromise between security and compatibility.
Key	Type in the wireless password you intend to use for your network. Be sure to type in a secure password, because the best security mechanisms, i.e. WPA2, mean nothing, if the key you use is too short, too simple, or too generic. Clicking the 🔄 button will show the password in clear text.

3.5.2.5 Interface Configuration – MAC Filter

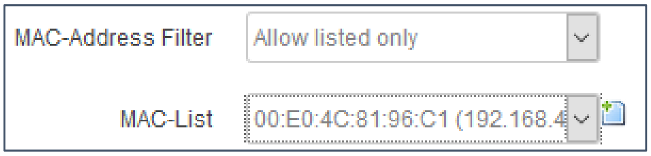


Interface Configuration

General Setup | Wireless Security | MAC-Filter

MAC-Address Filter: disable

The MAC filter option is visible when the mode is set to “Access Point” or “Access Point (WDS)”. A media access control address (MAC address), also called physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment. With the Intellinet access point you can limit or grant access to the wireless network based on the MAC address of the client.

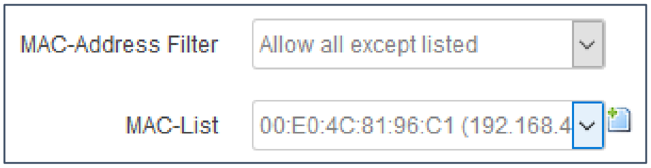


MAC-Address Filter: Allow listed only

MAC-List: 00:E0:4C:81:96:C1 (192.168.4

In this mode you grant access to the wireless network for users listed in the field MAC-List. Any client that is not listed, will not be able to access the network.

Click ⌄ to open up a list of stations that recently connected to the Intellinet access point to quickly add them to the allow list. Select custom to manually enter a MAC address.
Click ⊞ to add a new field for a new MAC address.



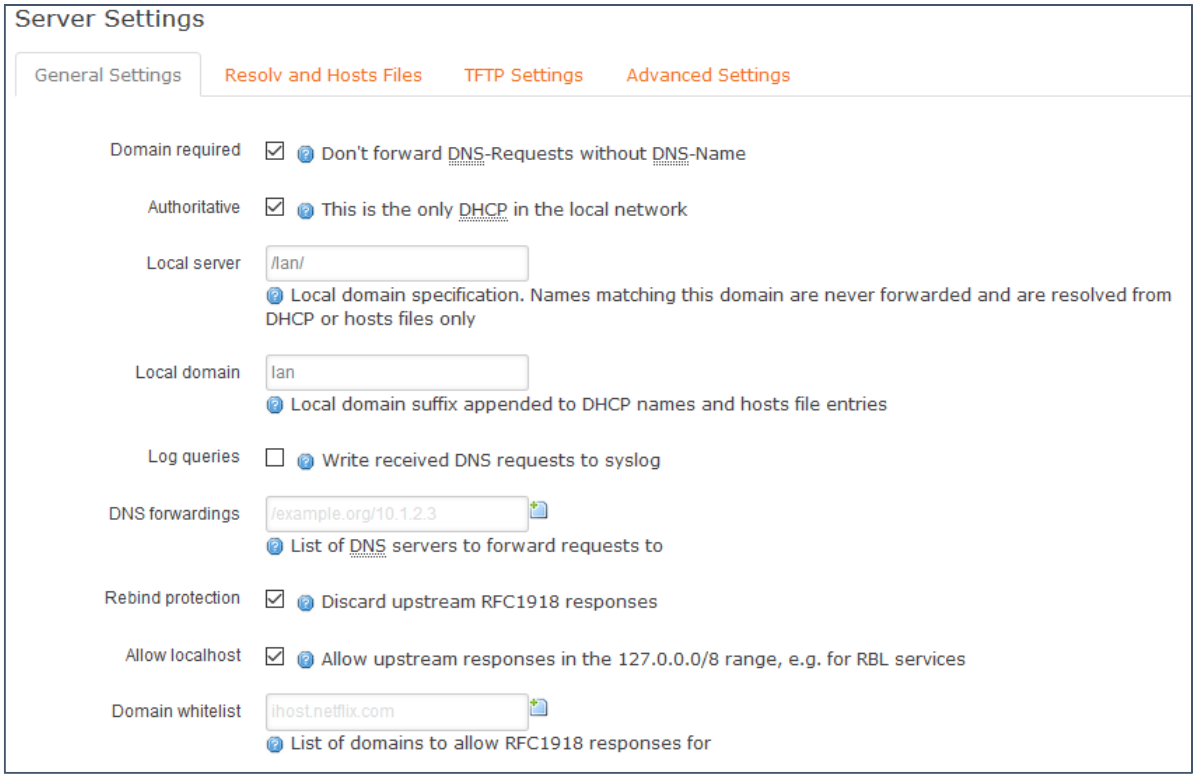
MAC-Address Filter: Allow all except listed

MAC-List: 00:E0:4C:81:96:C1 (192.168.4

On this mode you only enter those MAC addresses that you want to forbid access to your network. Any other wireless client will be able to connect to the network.

3.5.3 DHCP and DNS

This section is only relevant if you are using the access point’s DHCP server, want to configure DNS related settings and setup TFTP.



Domain required ☑ Don't forward DNS-Requests without DNS-Name

Authoritative ☑ This is the only DHCP in the local network

Local server: /lan/
Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain: lan
Local domain suffix appended to DHCP names and hosts file entries

Log queries ☐ Write received DNS requests to syslog

DNS forwardings: /example.org/10.1.2.3
List of DNS servers to forward requests to

Rebind protection ☑ Discard upstream RFC1918 responses

Allow localhost ☑ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

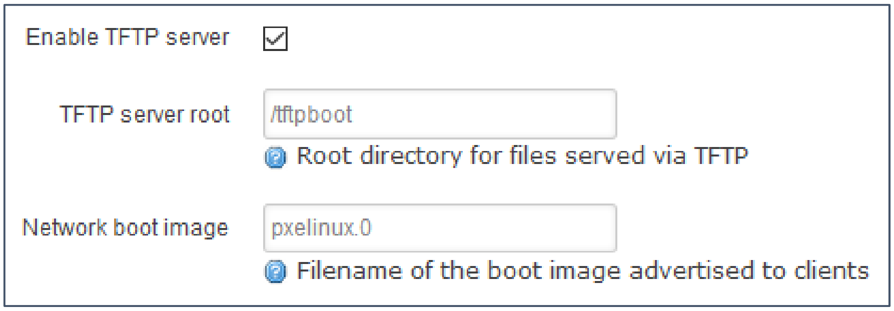
Domain whitelist: ihost.netflix.com
List of domains to allow RFC1918 responses for

3.5.3.1 General Settings / Resolv and Hosts Files

All of these options are for advanced users with good knowledge about the inner workings of TCP/IP in general, and DNS in particular. Most users are well advised to give this entire section a wide berth.

3.5.3.2 TFTP Settings

OpenWRT uses Dnsmasq as its default DNS forwarder and DHCP server. It is also has a built-in TFTP server. Dnsmasq allows you to host the TFTP files on your router. In order to do that, you need to specify the TFTP root folder, and the name of the network boot image.



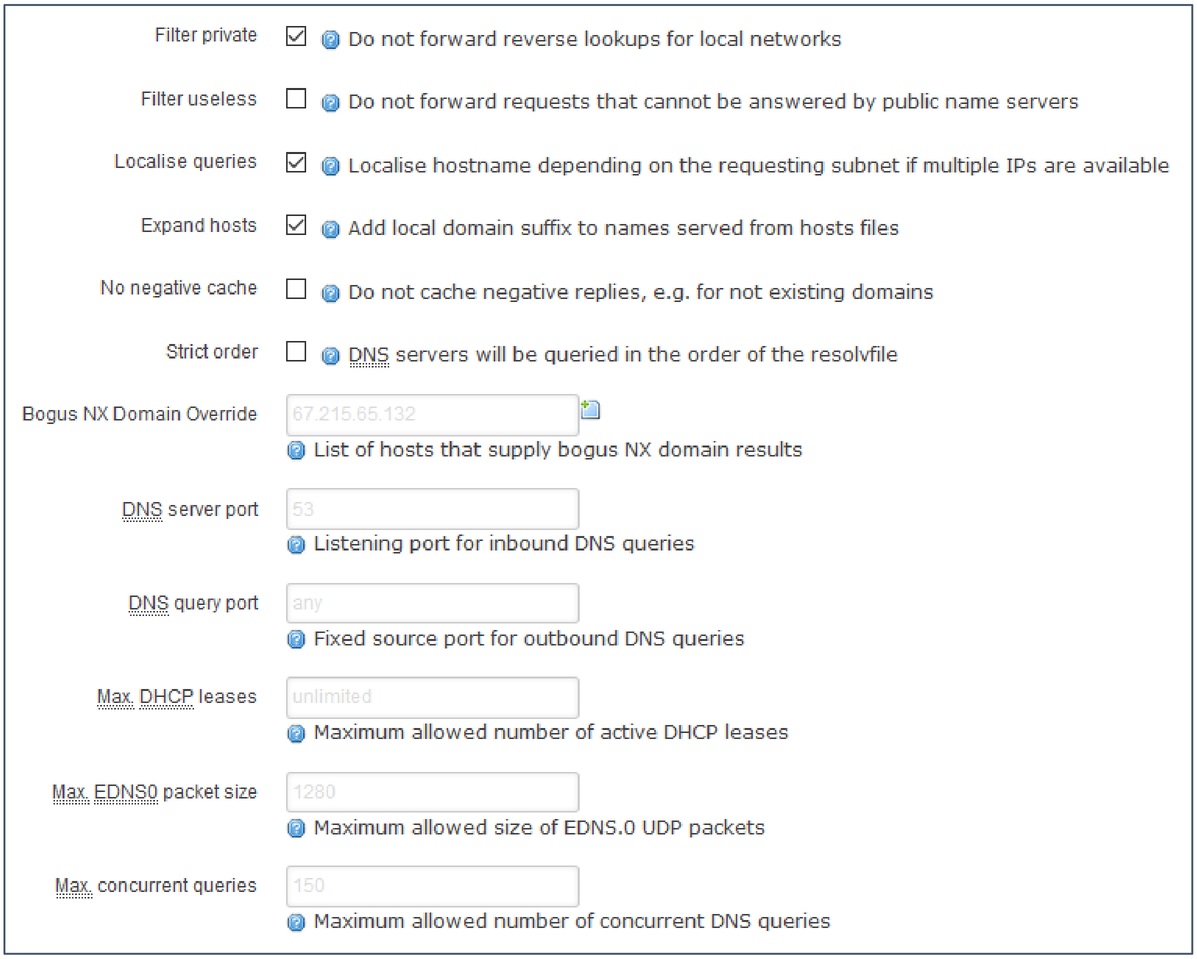
Enable TFTP server ☑

TFTP server root: /tftpboot
Root directory for files served via TFTP

Network boot image: pxelinux.0
Filename of the boot image advertised to clients

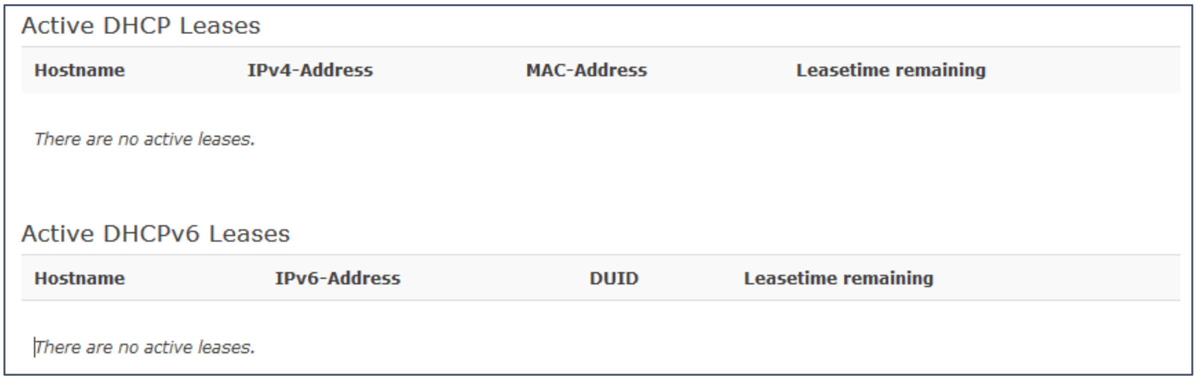
3.5.3.3 Advanced Settings

A variety of advanced parameters concerning DNS and DHCP. Under normal circumstances there is no need to make any changes to any of these parameters, and that includes when running the Intellinet device as a classic access point, or a wireless repeater.



Filter private	☑ Do not forward reverse lookups for local networks
Filter useless	□ Do not forward requests that cannot be answered by public name servers
Localise queries	☑ Localise hostname depending on the requesting subnet if multiple IPs are available
Expand hosts	☑ Add local domain suffix to names served from hosts files
No negative cache	□ Do not cache negative replies, e.g. for not existing domains
Strict order	□ DNS servers will be queried in the order of the resolvfile
Bogus NX Domain Override	67.215.65.132 List of hosts that supply bogus NX domain results
DNS server port	53 Listening port for inbound DNS queries
DNS query port	any Fixed source port for outbound DNS queries
Max. DHCP leases	unlimited Maximum allowed number of active DHCP leases
Max. EDNS0 packet size	1280 Maximum allowed size of EDNS.0 UDP packets
Max. concurrent queries	150 Maximum allowed number of concurrent DNS queries

3.5.3.4 DHCP – Active and Static Leases



Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining

There are no active leases.

Active DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

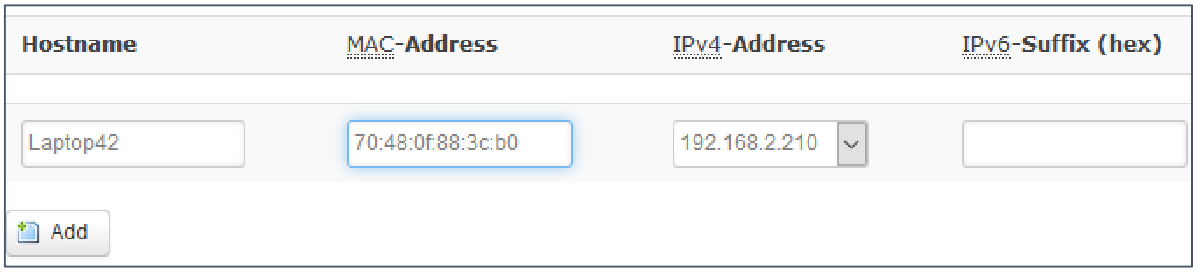
There are no active leases.

This section provides an overview of all clients that are currently connected to the access point and have obtained an IP address (IPv4 or IPv6). Shown are the host name, the IP address, and MAC address and the remaining lease time.

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.



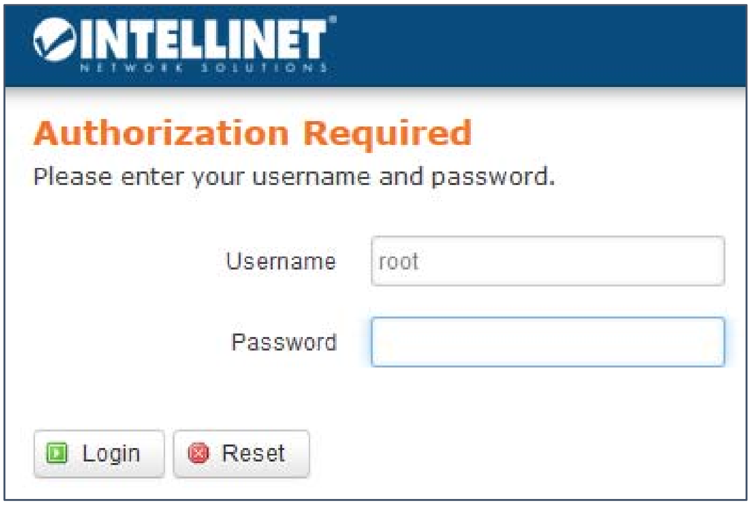
Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
Laptop42	70:48:0f:88:3c:b0	192.168.2.210	

Click Delete in order to delete a static lease.

3.6 Logout

When you are done making changes to the configuration, you can end the browser session by clicking on logout.

After this, you will be re-directed to the login page of the web admin menu.



Authorization Required

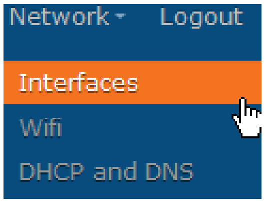
Please enter your username and password.

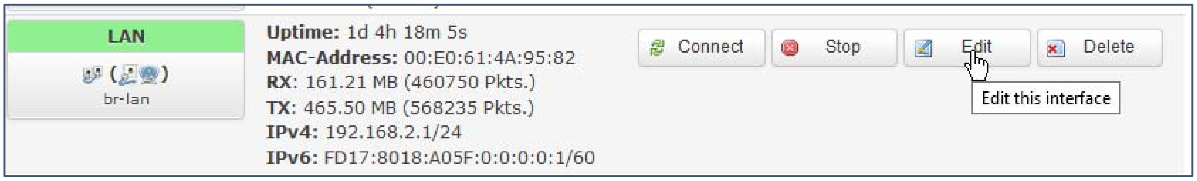
Username	root
Password	

4. How To

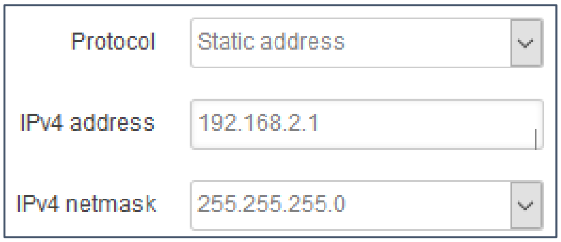
4.1 How to change the IP address of the access point?

The default IP address of the Intellinet access point is 191.168.2.1 with a subnet 255.255.255.0. If you want to make an adjustment to that IP address, proceed as follows:



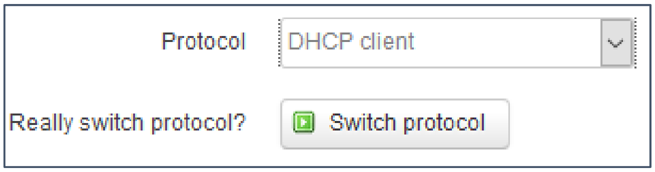


Uptime: 1d 4h 18m 5s
MAC-Address: 00:E0:61:4A:95:82
RX: 161.21 MB (460750 Pkts.)
TX: 465.50 MB (568235 Pkts.)
IPv4: 192.168.2.1/24
IPv6: FD17:8018:A05F:0:0:0:0:1/60



Protocol	Static address
IPv4 address	192.168.2.1
IPv4 netmask	255.255.255.0

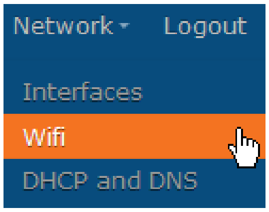
You can either make changes to the IPv4 address to assign a different static IP address, or you can change the IP address from static to DHCP. When set to DHCP, the access point receives its IP address from a router in your network. To enable DHCP, you need to select “DHCP client” from the drop-down list, then click on Switch protocol.

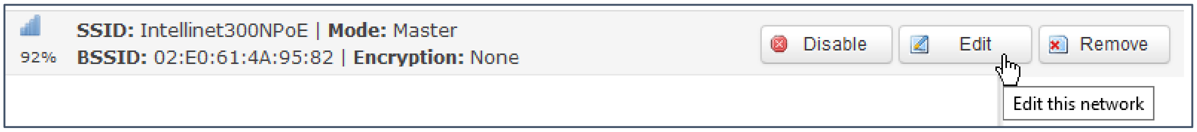


Protocol	DHCP client
Really switch protocol?	Switch protocol

4.2 How to secure the wireless network with a password?

In order to secure the wireless network with a password, proceed as follows:

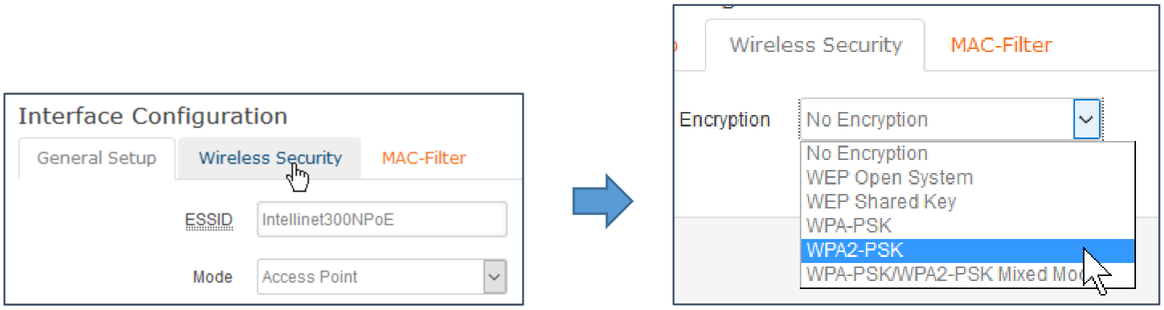




92%

SSID: Intellinet300NPoE | **Mode:** Master

BSSID: 02:E0:61:4A:95:82 | **Encryption:** None

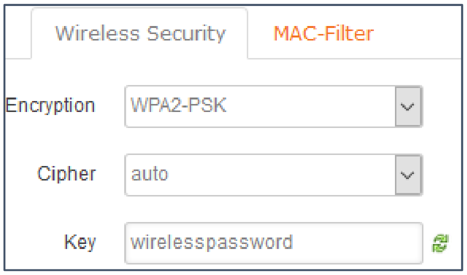


Interface Configuration

ESSID: Intellinet300NPoE

Mode: Access Point

Encryption: No Encryption



Encryption: WPA2-PSK

Cipher: auto

Key: wirelesspassword

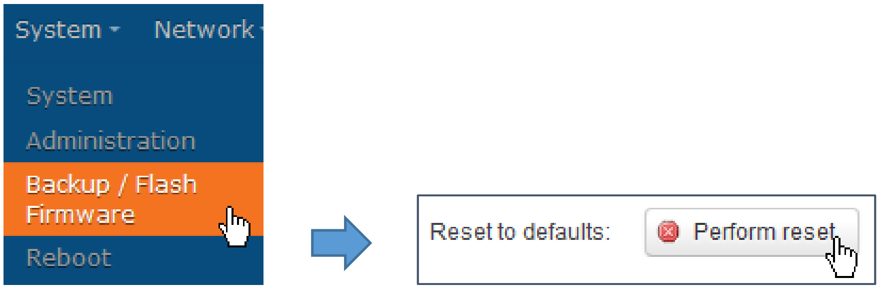
The Intellinet access point supports various encryption methods (WEP, WPA and WPA2), the different cipher types (TKIP or AES) and the wireless key itself, called pre-shared key.

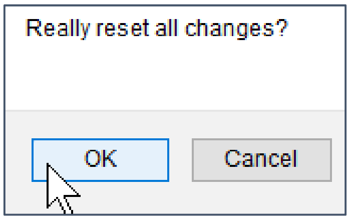
For maximum security, we recommend using WPA2 with CCMP AES as the cipher. Activating the less secure “TKIP” instead of “AES”, or “WPA” instead of “WPA2” should only be done, if older wireless clients experience difficulties connecting to the wireless network. WEP should really only be used if you have legacy equipment so old it won’t even support WPA encryption.

4.3 How to restore factory default settings?

There are two ways to reset the Intellinet access point to factory default settings.

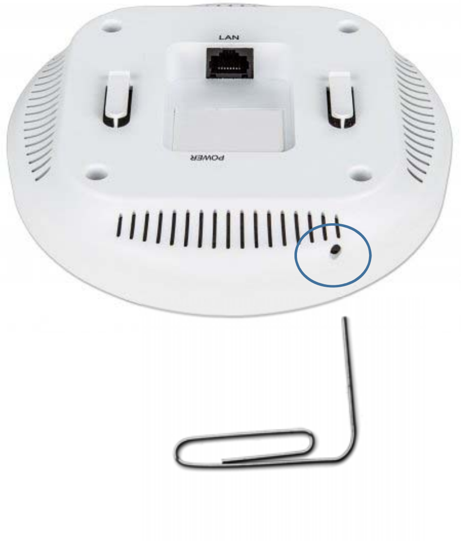
4.3.1 Factory Reset via Web Interface




Really reset all changes?

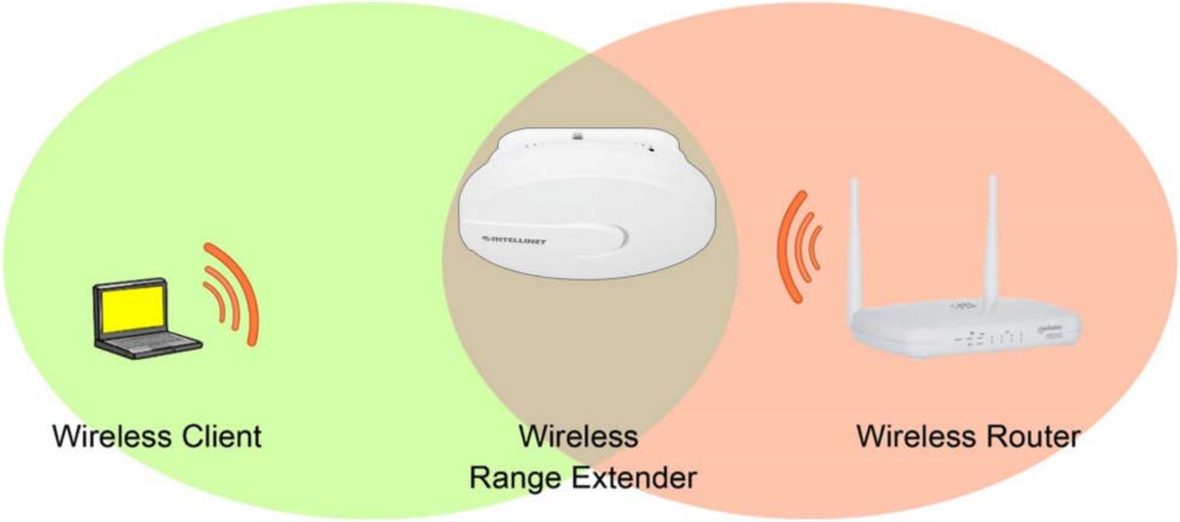
4.3.2 Factory Reset via Hardware Button

If the web interface can no longer be reached, i.e., because the administrator password was lost or forgotten, the only way to re-gain access is to do a factory reset via the reset button.



Use a sharp object like a paper clip to push in the reset button. Do that for about 6 seconds while the device is powered on and the access point will automatically restore the factory settings and restart.

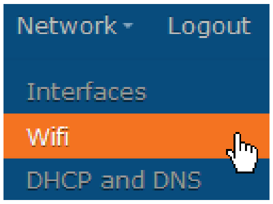
4.4 How to set up the access point as a wireless repeater?

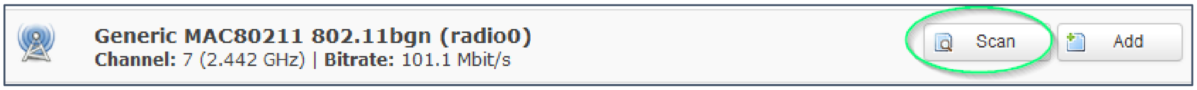


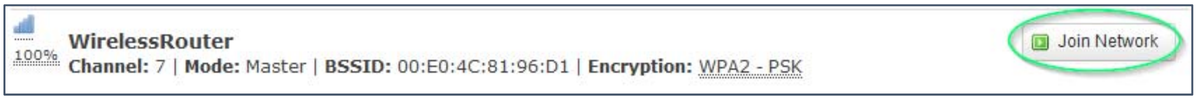
A wireless repeater (also called wireless range extender) takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network. The effect is that the range of the wireless network is increased. The other function of the wireless repeater is that it creates a bridge to another wireless network for all clients that are connected to the LAN port on the access point. In summary, there are two functions that the access point needs to do:

1. Create a wireless bridge connection to another wireless network
2. Create a local wireless network for Wi-Fi clients to connect to.

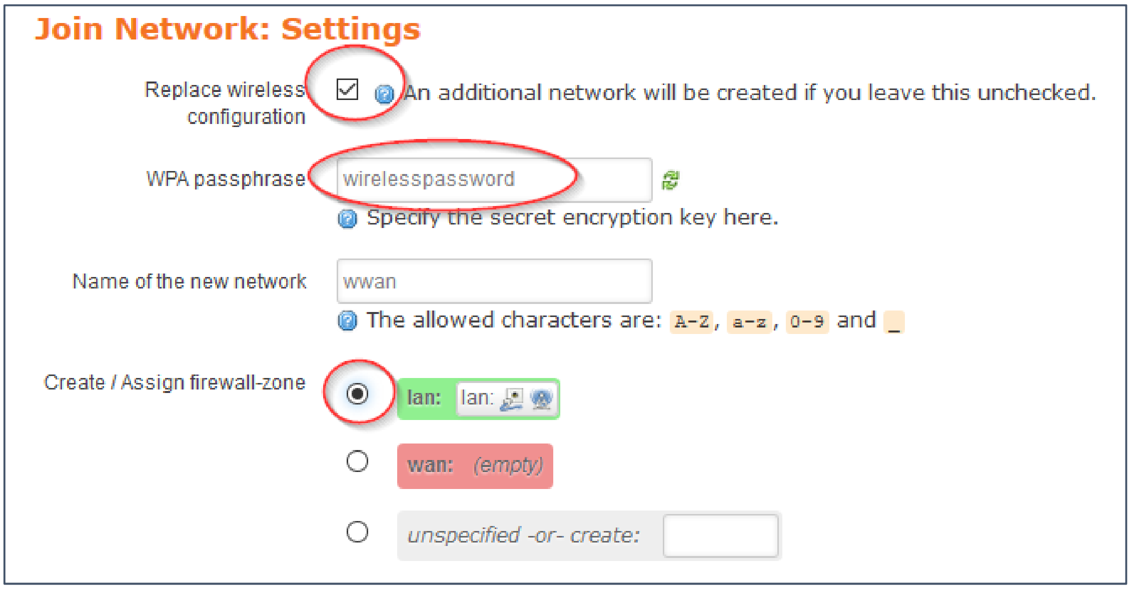
In order to set up the Intellinet access point as a wireless repeater, you need to perform a series of steps. We are using an access point that is set to the factory default settings, and we are repeating the signal of a wireless network with the SSID "WirelessRouter", which is secured with WPA2 encryption.




Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | **Bitrate:** 101.1 Mbit/s



WirelessRouter
Channel: 7 | **Mode:** Master | **BSSID:** 00:E0:4C:81:96:D1 | **Encryption:** WPA2 - PSK



Join Network: Settings

Replace wireless configuration ☑ An additional network will be created if you leave this unchecked.

WPA passphrase: wirelesspassword
Specify the secret encryption key here.

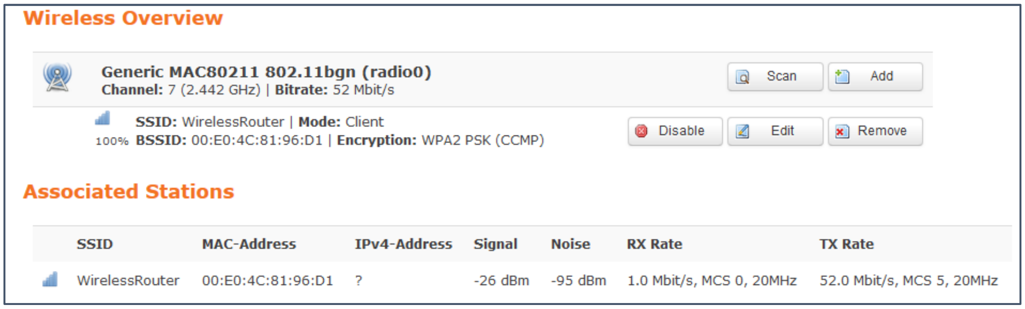
Name of the new network: wwan
The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone:
● lan: lan:
○ wan: (empty)
○ unspecified -or- create:

Parameter	Description
Replace wireless configuration	Make sure this option is selected when setting up a wireless repeater. You want to replace the current Wi-Fi configuration (Access Point mode) with a new one (client mode). Later on in the configuration the access point will be re-created.
WPA passphrase	Type in the wireless password for the wireless network you are about to connect to.
Name of the new network	This sets the name of the new interface. Recommend leaving “wwan”.
Create / Assign firewall-zone	Select “lan”.

Click on Submit to save the settings. Then on the next page, scroll to the bottom and click on Save & Apply.

Go to Network -> WiFi and verify the connection on the wireless overview screen. It should be looking like this:



Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | Bitrate: 52 Mbit/s

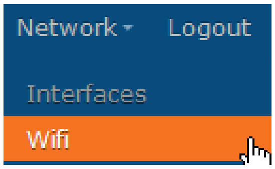
100% SSID: WirelessRouter | Mode: Client
BSSID: 00:E0:4C:81:96:D1 | Encryption: WPA2 PSK (CCMP)

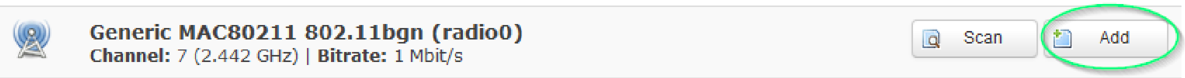
Associated Stations

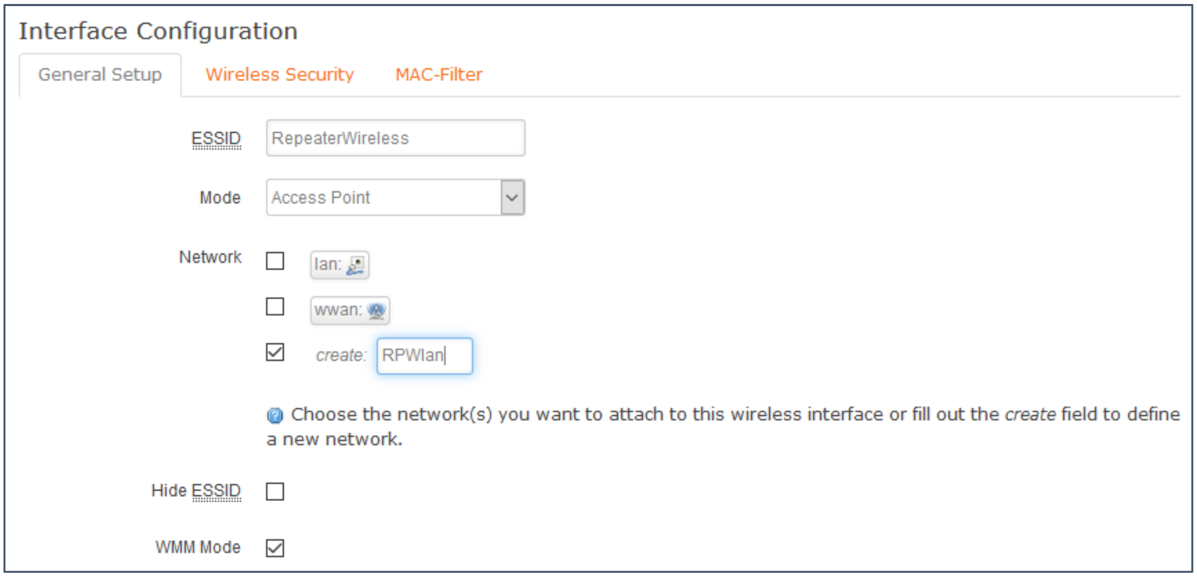
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
WirelessRouter	00:E0:4C:81:96:D1	?	-26 dBm	-95 dBm	1.0 Mbit/s, MCS 0, 20MHz	52.0 Mbit/s, MCS 5, 20MHz

This concludes the setup of the wireless bridge connection.

Next, create a wireless network to which local Wi-Fi clients can connect to. The example shows the creation of a WPA2 encrypted network.




Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | **Bitrate:** 1 Mbit/s


Interface Configuration

ESSID: RepeaterWireless

Mode: Access Point

Network: □ lan: □ wwan: ☑ create: RPWlan

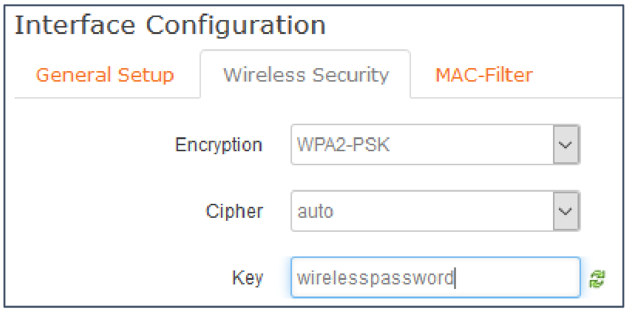
Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID □

WMM Mode ☑

Parameter	Description
ESSID	Type in the name of the new wireless network. This does not need to match the ESSID of the wireless network, of which you want to extend the range.
Mode	Set to Access Point
Network	Uncheck any existing options such as "lan" or "wwan", and check the option "create". Then type in a descriptive name for the new network interface.
Hide ESSID	If you don't want the Intellinet access point to broadcast the ESSID to nearby wireless clients, you can enable this option.
WMM Mode	Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. Recommendation is to enable this.

Next is the setup of the wireless security.



Interface Configuration

Encryption: WPA2-PSK

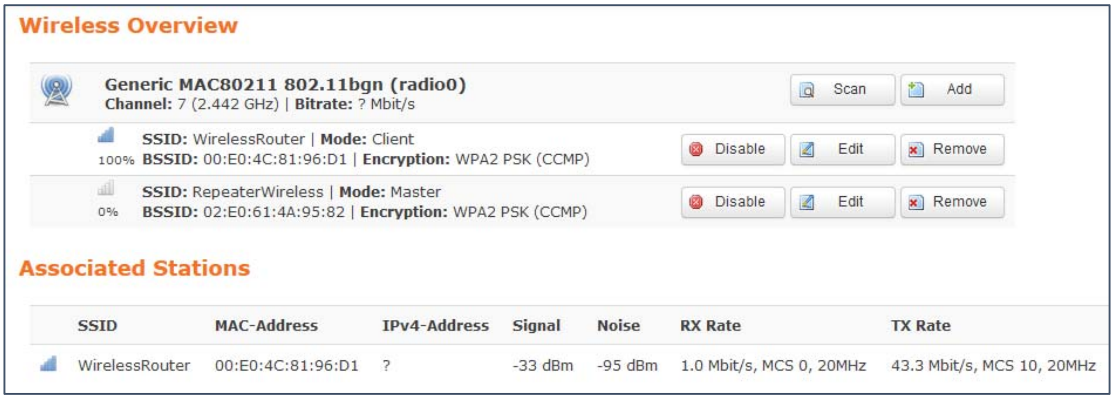
Cipher: auto

Key: wirelesspassword

Parameter	Description
Encryption	Set to WPA-PSK. The other options provide weaker security for your wireless network and are only recommended if you have equipment that can't connect to WPA2-secured wireless networks.
Cipher	Set to "auto".
Key	Type in the password for the wireless network. You can, but don't have to, use the same wireless password that the wireless network uses, of which you want to extend the range.

Click Save & Apply to create the new wireless network.

Verify the wireless setup on the wireless overview screen. It should be looking like this:



Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | **Bitrate:** ? Mbit/s

100% **SSID:** WirelessRouter | **Mode:** Client
BSSID: 00:E0:4C:81:96:D1 | **Encryption:** WPA2 PSK (CCMP)

0% **SSID:** RepeaterWireless | **Mode:** Master
BSSID: 02:E0:61:4A:95:82 | **Encryption:** WPA2 PSK (CCMP)

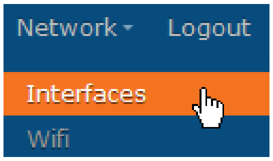
Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
WirelessRouter	00:E0:4C:81:96:D1	?	-33 dBm	-95 dBm	1.0 Mbit/s, MCS 0, 20MHz	43.3 Mbit/s, MCS 10, 20MHz

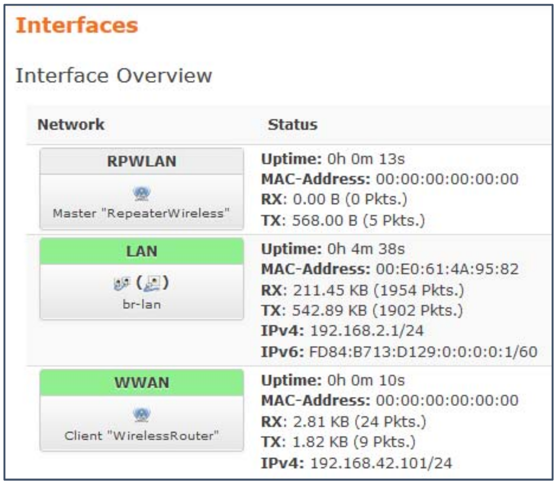
SSID "WirelessRouter", Mode "Client":
This is the wireless connection to the wireless network, of which you want to extend the range.

SSID "RepeaterWireless", Mode "Master"
This is the wireless network for Wi-Fi clients. Wi-Fi clients can connect to this network, and then communicate with the wireless router network via the bridge connection (mode 'client).

Next, open the Network -> Interfaces screen.



The screen should look as follows:

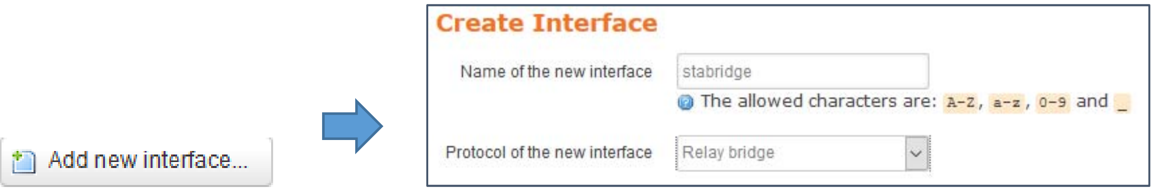


Interfaces

Interface Overview

Network	Status
RPWLAN Master "RepeaterWireless"	**Uptime:** 0h 0m 13s **MAC-Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 568.00 B (5 Pkts.)
LAN br-lan	**Uptime:** 0h 4m 38s **MAC-Address:** 00:E0:61:4A:95:82 **RX:** 211.45 KB (1954 Pkts.) **TX:** 542.89 KB (1902 Pkts.) **IPv4:** 192.168.2.1/24 **IPv6:** FD84:B713:D129:0:0:0:0:1/60
WWAN Client "WirelessRouter"	**Uptime:** 0h 0m 10s **MAC-Address:** 00:00:00:00:00:00 **RX:** 2.81 KB (24 Pkts.) **TX:** 1.82 KB (9 Pkts.) **IPv4:** 192.168.42.101/24

Now we create a new interface – a relay bridge. This interface is going to forward packets from the local LAN and RPWLAN to the wireless router network via the WWAN.



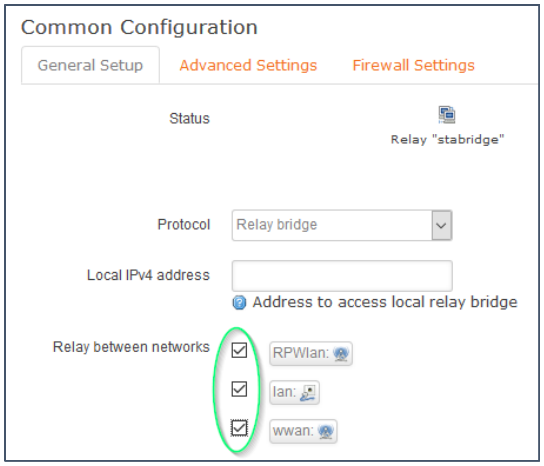
Create Interface

Name of the new interface: stabridge

The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Relay bridge

Type in "stabridge" for the name of the new interface, and select "Relay bridge" as the protocol. Click on Submit next.



Common Configuration

General Setup | Advanced Settings | Firewall Settings

Status: Relay "stabridge"

Protocol: Relay bridge

Local IPv4 address:

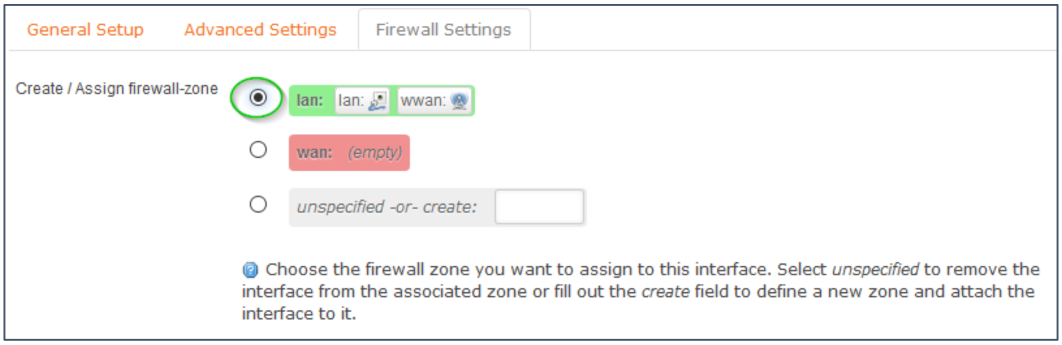
Address to access local relay bridge

Relay between networks:
☑ RPWlan:
☑ lan:
☑ wwan:

On the "General Setup" page, activate all three networks:
(x) RPWLan
(x) lan
(x) wwan

Click Save & Apply.

Open the firewall settings and activate the “lan” option.



Create / Assign firewall-zone

● lan: lan: wwan:

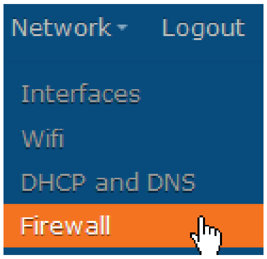
○ wan: *(empty)*

○ *unspecified -or- create:*

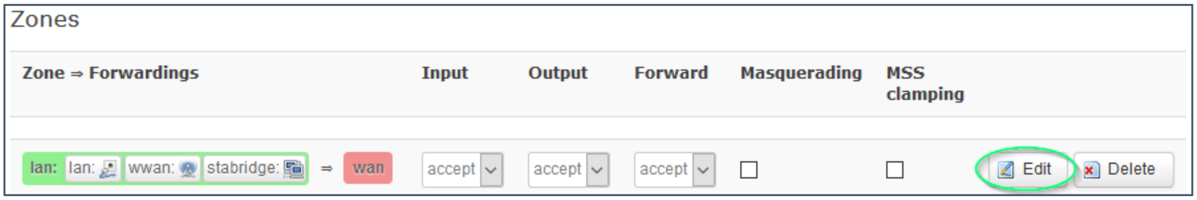
Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Click Save & Apply.

Next, open the firewall menu.



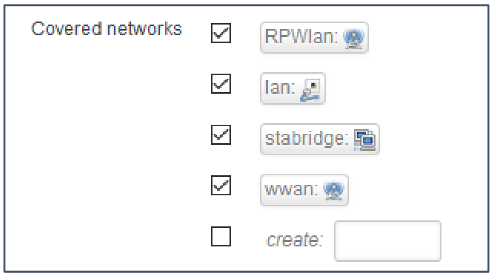
Under “Zones”, click “Edit” for the “lan” zone.



Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: wwan: stabridge: ⇒ wan	accept	accept	accept	□	□	Edit Delete

Make sure that these options are activated.



Covered networks

☑ RPWlan:

☑ lan:

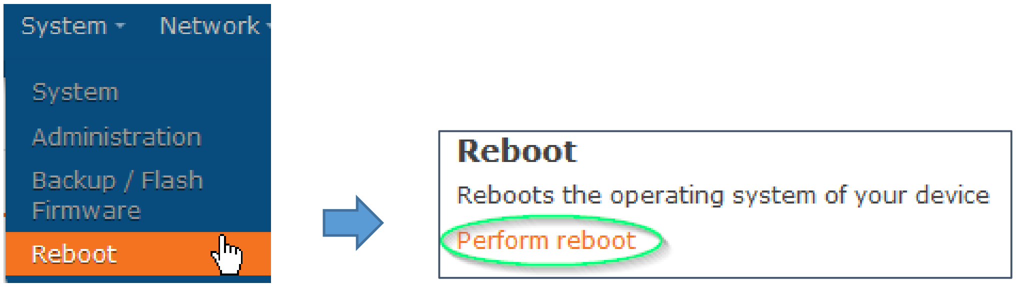
☑ stabridge:

☑ wwan:

□ *create:*

Click Save & Apply.

Finally, reboot the Intellinet access point.



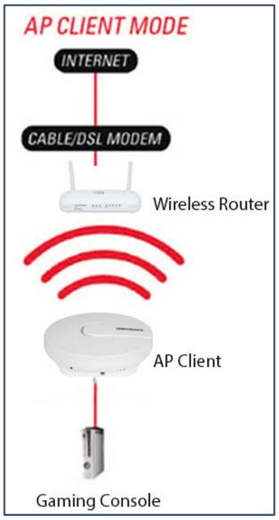
Reboot

Reboots the operating system of your device

This completes the setup of the wireless repeater.

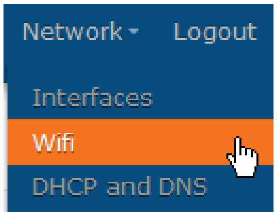
Note: If the administrator menu fails to load after the restart, wait for two minutes, and then manually reconnect to the web configuration URL at http://192.168.2.1.

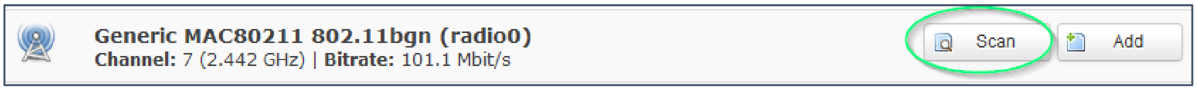
4.5 How to set up the access point as an AP client?



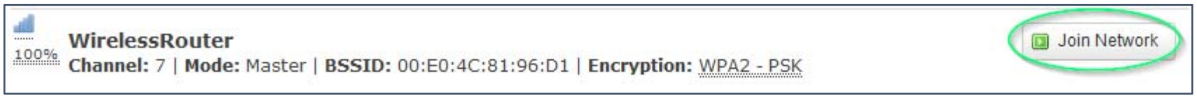
In this operational mode, the access point acts as a bridge between the a station (or stations) that are connected to the LAN port, and an existing wireless network. This mode can be used to connect a non-wireless device to a wireless network, for example, an Internet-ready TV that is equipped with a physical network port, but no Wi-Fi . The function of the AP client mode is quite similar to that of a wireless repeater, however, in AP client mode, the access point (designated "AP Client" in the image on the right) will not be available for connection from wireless clients. The wireless radio only connects to the root access point ("Wireless Router" in the example) and acts as a wireless bridge.

Here is how to set it up. In our example we are connecting to a wireless router with the SSID "WirelessRouter".

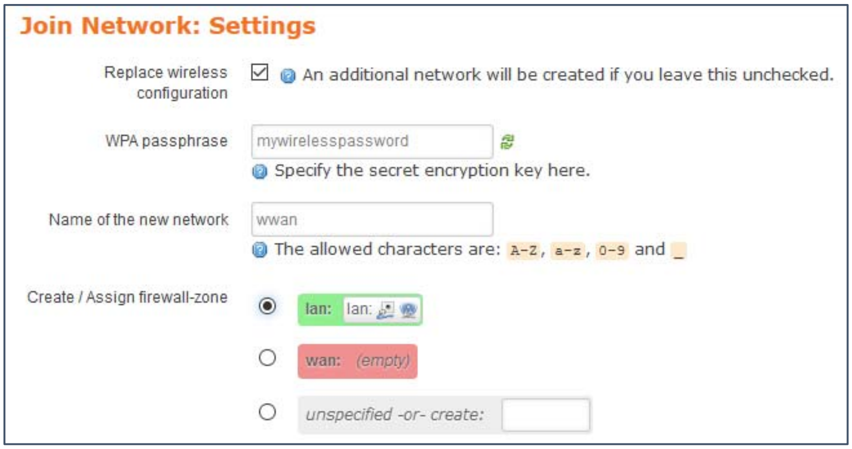




Generic MAC80211 802.11bgn (radio0)
Channel: 7 (2.442 GHz) | **Bitrate:** 101.1 Mbit/s



100%
WirelessRouter
Channel: 7 | **Mode:** Master | **BSSID:** 00:E0:4C:81:96:D1 | **Encryption:** WPA2 - PSK



Join Network: Settings

Replace wireless configuration ☑ An additional network will be created if you leave this unchecked.

WPA passphrase: mywirelesspassword
Specify the secret encryption key here.

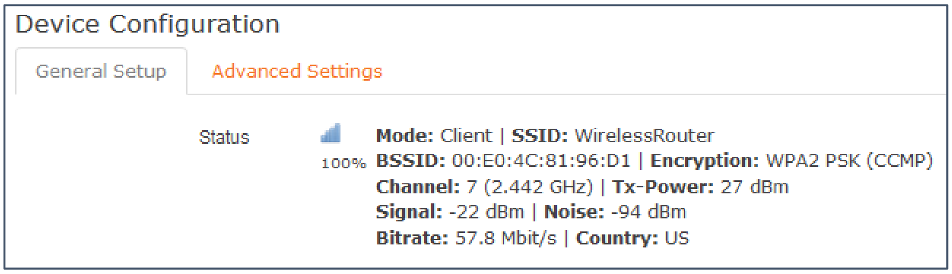
Name of the new network: wwan
The allowed characters are: `A-Z`, `a-z`, `0-9` and `_`

Create / Assign firewall-zone
● lan: lan:
○ wan: (empty)
○ unspecified -or- create:

Parameter	Description
Replace wireless configuration	Make sure this option is selected when using the client mode.
WPA passphrase	Type in the wireless password for the wireless network you are about to connect to.
Name of the new network	This sets the name of the new interface. Recommend leaving “wwan”.
Create / Assign firewall-zone	Select “lan”.

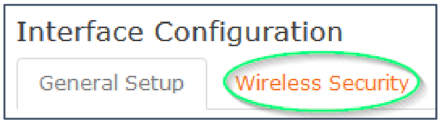
Click on Submit to save the settings. Then on the next page, scroll to the bottom and click on Save & Apply.

If all works well, you will see the following information on the “Device Configuration”:



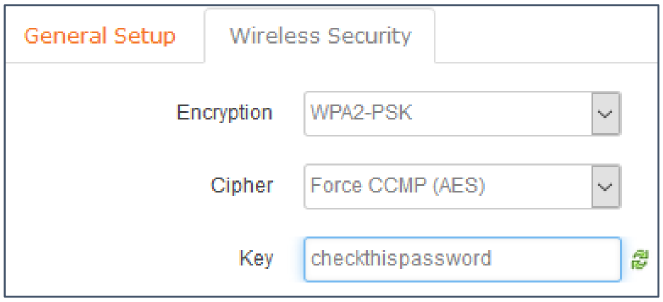
Mode: Client | **SSID:** WirelessRouter
BSSID: 00:E0:4C:81:96:D1 | **Encryption:** WPA2 PSK (CCMP)
Channel: 7 (2.442 GHz) | **Tx-Power:** 27 dBm
Signal: -22 dBm | **Noise:** -94 dBm
Bitrate: 57.8 Mbit/s | **Country:** US

Note that the signal strength indicator shows a value that is ideally greater than 70%. If it shows 0%, then something went wrong. Most likely the wireless password was not entered correctly, or does not match the wireless password of the wireless network you are connecting to. In order to fix that, on the same screen scroll down until you see the “Interface Configuration” section. Select “Wireless Security”.



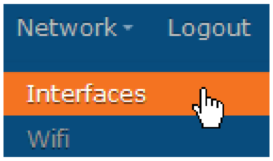
There make sure that password matches with the password of the wireless network. Click on ⟳ to reveal the password display in clear text for easier verification.

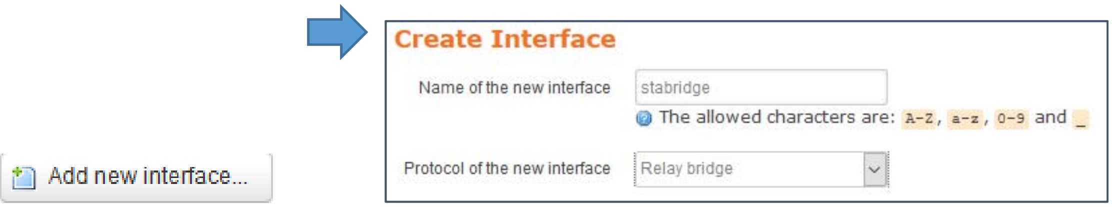
the cipher should usually be left to AUTO, however you may set it to “FORCE XXX” in case you encounter problems.



Encryption: WPA2-PSK
Cipher: Force CCMP (AES)
Key: checkthispassword

The last step is to create a relay bridge interface that connects the LAN port to the wireless network. Proceed as follows.



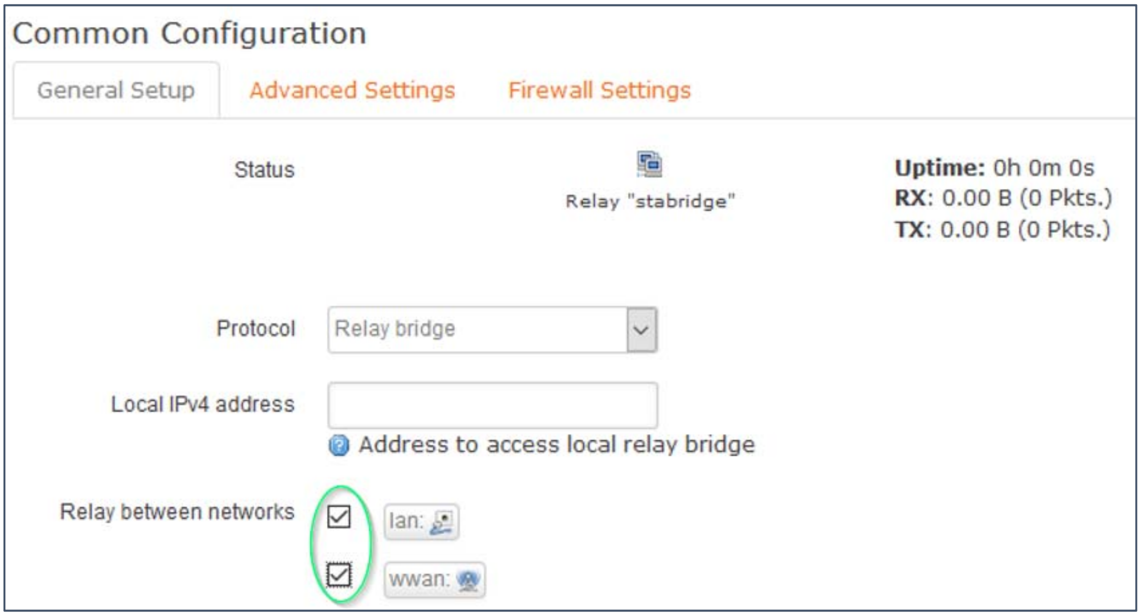


Name of the new interface: stabridge

The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Relay bridge

On the “General Setup” page, activate all three networks:
(x) lan
(x) wwan



Status: Relay "stabridge"

Uptime: 0h 0m 0s
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

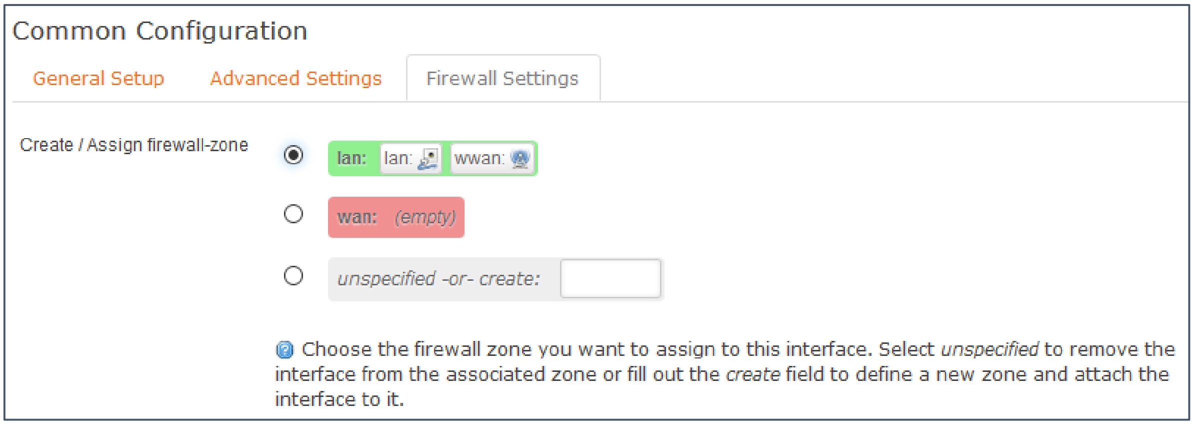
Protocol: Relay bridge

Local IPv4 address:

Address to access local relay bridge

Relay between networks: ☑ lan: ☑ wwan:

Click Save & Apply.



Common Configuration

Create / Assign firewall-zone

● lan: lan: wwan:

○ wan: *(empty)*

○ *unspecified -or- create:*

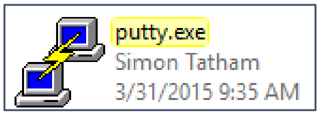
Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Activate “lan”, then Click Save & Apply.

4.6 How to access the configuration via SSH?

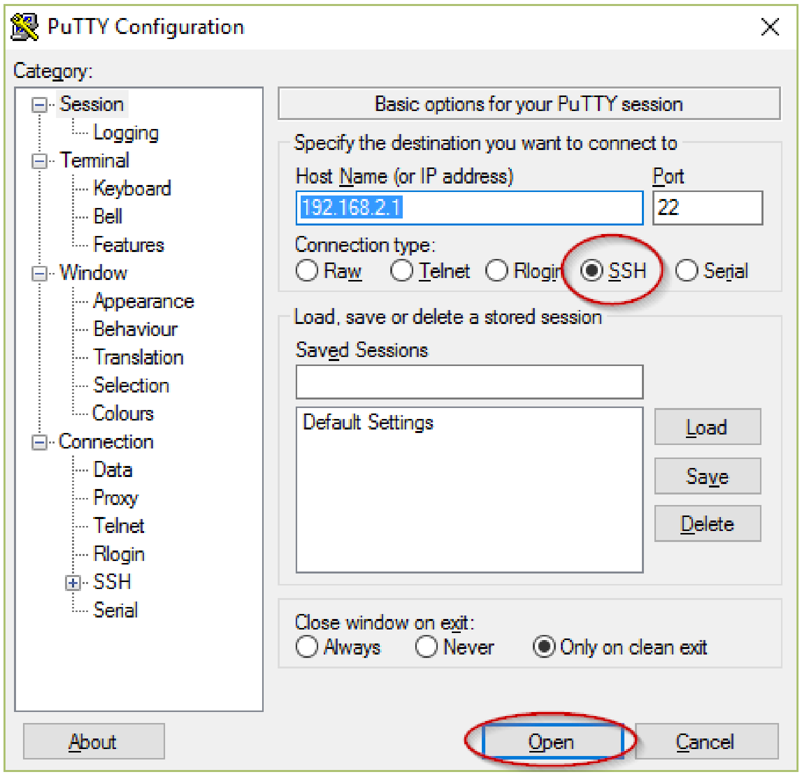
The instructions below are written for Windows systems and are based upon using the free utility PUTTY from putty.org. The instructions also assume that the Intellinet access point is set to default values as far as the IP address is concerned, and that your computer has a working network connection to the access point.

After you have downloaded and installed it, run putty.exe.



putty.exe
Simon Tatham
3/31/2015 9:35 AM

Type in the IP address of the access point into the host name field. Verify that the port number is 22 and the connection type is set to "SSH". Click 'Open' to establish the connection.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.2.1

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

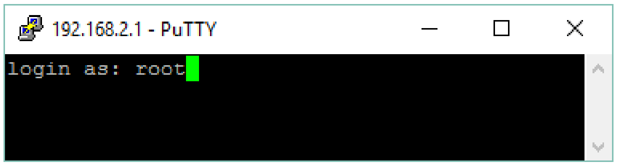
Load, save or delete a stored session

Saved Sessions

Default Settings

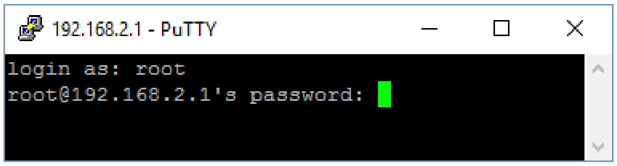
Close window on exit: ○ Always ○ Never ● Only on clean exit

Type in ‘root’, then press enter.

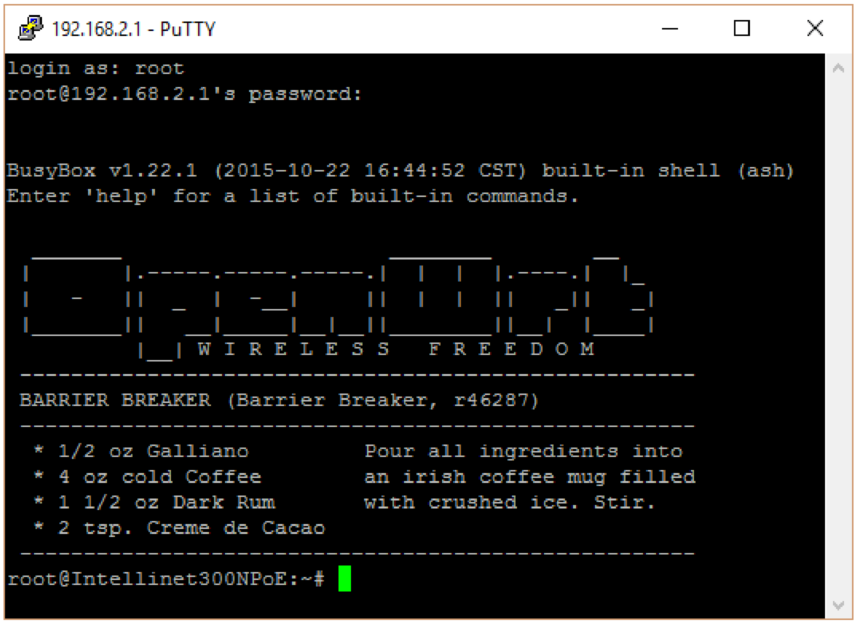


```
login as: root
```

Type in ‘1234’ as the password and press enter.



```
login as: root
root@192.168.2.1's password:
```



```
login as: root
root@192.168.2.1's password:


BusyBox v1.22.1 (2015-10-22 16:44:52 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 BARRIER BREAKER (Barrier Breaker, r46287)
 -----------------------------------------------------
  * 1/2 oz Galliano         Pour all ingredients into
  * 4 oz cold Coffee        an irish coffee mug filled
  * 1 1/2 oz Dark Rum       with crushed ice. Stir.
  * 2 tsp. Creme de Cacao
 -----------------------------------------------------
root@Intellinet300NPoE:~#
```

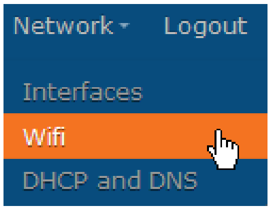
OpenWRT related instructions concerning editing the configuration with PUTTY can be found at wiki.openwrt.org.

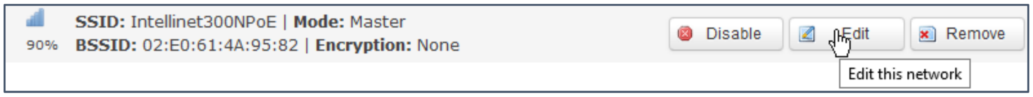
4.7 How to get the maximum Wi-Fi performance?

There are many factors that influence the wireless range and speed you can achieve. Some factors are related to the environment, others are related to the settings of the access point.

- Environmental Considerations
  - A direct line of sight between access point and wireless client provides best results. Obstacles of any kind will reduce the performance. That reduction can be small, or quite severe. Everything blocks wireless signals to a smaller or larger extend. Wood, plaster or glass don't interfere much, but brick, stone, and water (think of that big fish tank or water pipes) can be more problematic. Among the worst enemies of a wireless signal are ceramic, concrete, metal, and mirrors, which reflect visible light and radio waves alike.
  - Keep the distance between wireless client and access point below 100 feet (30 meter)
  - Install the access point on the ceiling for best signal propagation.

- Wireless Settings
  - Channel Selection: Set the channel to a value that puts this wireless network at least four channels apart from an existing wireless network that might be in close proximity. For example, if another wireless network in range is set to channel 2, then it'd be best to set your Intellinet access point to channel 6 or higher. You can set the channel here:

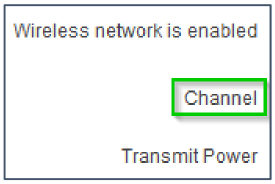




90%

SSID: Intellinet300NPoE | **Mode:** Master

BSSID: 02:E0:61:4A:95:82 | **Encryption:** None



  - Output Power:
    The Intellinet access point ships with the output power setting at maximum, which means 27 dBm for the US market, and 17 dBm for the ETSI (EU) region. The transmit power option can be found right underneath the channel parameter (see above). You should check and make sure that the settings is set to maximum for best signal strength and coverage.

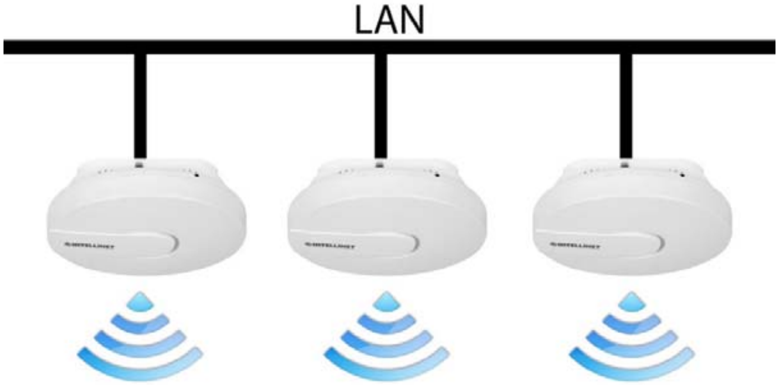
- Avoid wireless repeater setups:
  Repeating a wireless signal in order to increase the range of your wireless network without running a single network cable, that sounds like a great idea. It’s relatively easy to set up, and it requires no additional cables to be run.

  The primary disadvantage of a wireless repeater setup is that it effectively cuts the bandwidth in half for any computer that is connected to it. The reason for this is that the repeater receives the signal, processes the signal, and that takes time, and then rebroadcasts the signal – and does this in both directions, from the router to the computer and from the computer to the router.

  Other disadvantages:
  - Compatibility problems between different devices from different vendors using different chipsets
  - If the repeater is connected too far away from the access point, the AP Wi-Fi signal has already degraded too much, and even if the re-broadcasted signal appears strong for the wireless client that connects to the repeater, the seemingly great connection quality can yield results that are sub optimal.
  - Not good enough for serious gamers – wireless repeater setups can introduce additional packet loss to the wireless connection. While wireless connections by nature as not as robust as wired connections, connecting via a wireless repeater can compound the problem.

  What are the alternatives:
  If you need to cover an area that is too large for one access point alone and you want to maximize the stability and performance of your wireless network, and then the following setup is going to yield the best results:

  Each access point is connected to the wired backbone, and each access point is set up in access point mode.



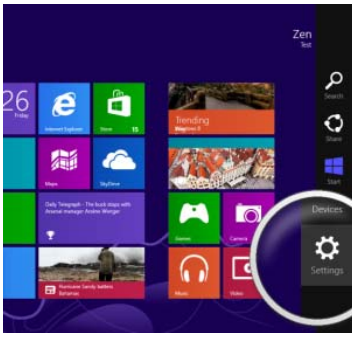
5. Appendix

5.1 Changing the IP Address of a Network Adapter

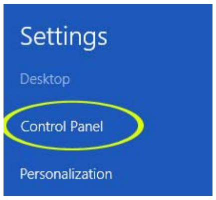
The Intellinet access point operates on the IP address 192.168.2.1. For your computer to access the administrator configuration interface, the IP address of the network adapter in your computer has to be in the same range; e.g., 192.168.2.50. Refer to the instructions that came with your computer for information on how to change the IP address on the network adapter in your computer for any operating system that is not explained in this user manual.

5.1.1 Windows 8

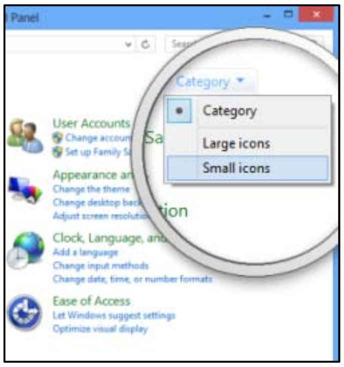
1. If you are using a PC, move the mouse cursor to the bottom or top right corner of the screen and select the cog icon for Settings. If you are using a tablet, swipe left from the right side of the screen and select Settings.



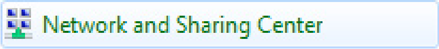
2. Click "Control Panel."



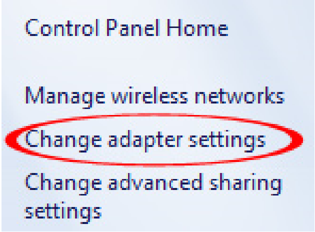
3. Select "Small icons."



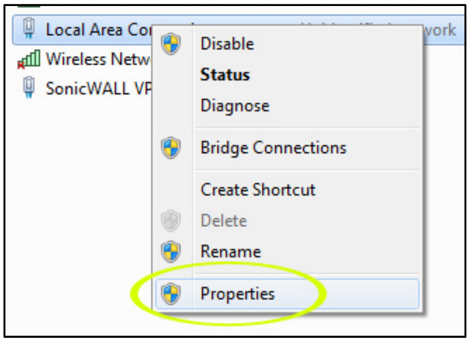
4. Open “Network and Sharing Center.”



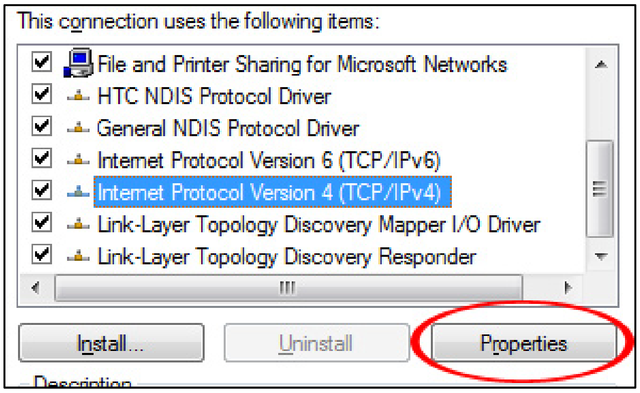
5. Click “Change adapter settings.”



6. Right-click your network adapter and select “Properties.”

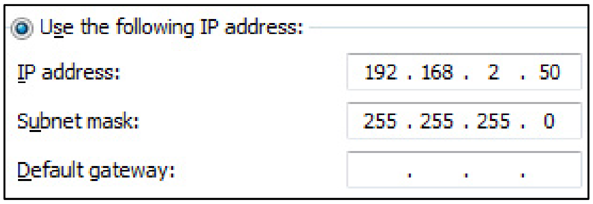


7. Select “Internet Protocol Version 4” from the list and click “Properties.”


This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- ☑ HTC NDIS Protocol Driver
- ☑ General NDIS Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

8. Enter the information as shown below, then click “OK” to save the settings.


● Use the following IP address:

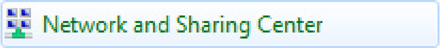
IP address: 192 . 168 . 2 . 50

Subnet mask: 255 . 255 . 255 . 0

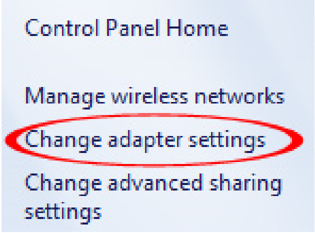
Default gateway: . . .

5.1.2 Windows 7 and 10

1. Open the Network and Sharing Center.

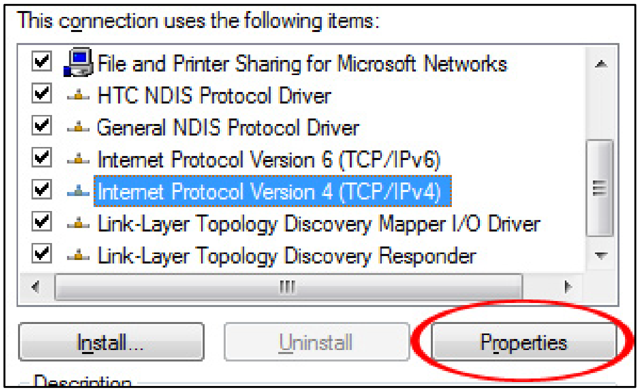


2. Click on “Change adapter settings.”



3. Right-click your network adapter and select “Properties.”

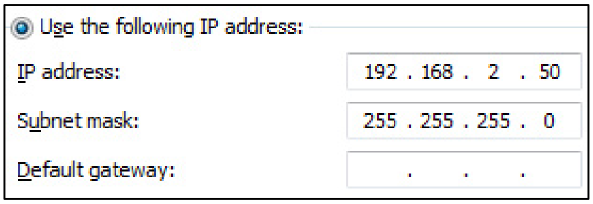
4. Select “Internet Protocol Version 4” from the list and click “Properties.”



This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- ☑ HTC NDIS Protocol Driver
- ☑ General NDIS Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

5. Enter the information as shown below, then click “OK” to save the settings.



● Use the following IP address:

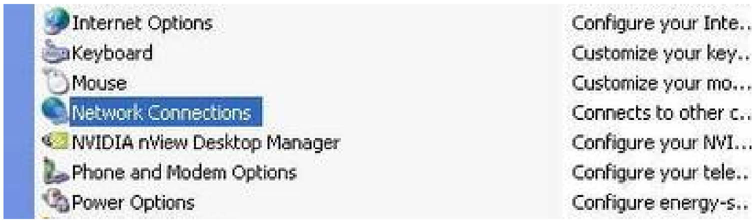
IP address: 192 . 168 . 2 . 50

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

5.1.3 Windows XP:

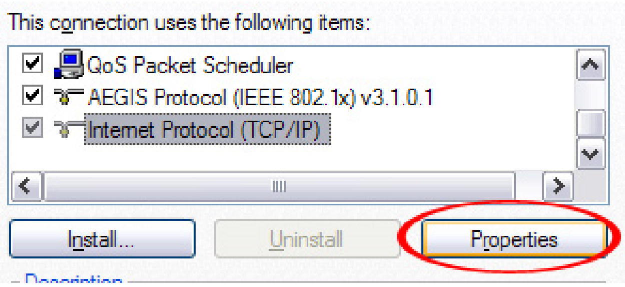
1. Double-click the “Network Connections” icon in the control panel.



Internet Options	Configure your Inte..
Keyboard	Customize your key..
Mouse	Customize your mo…
Network Connections	Connects to other c..
NVIDIA nView Desktop Manager	Configure your NVI…
Phone and Modem Options	Configure your tele..
Power Options	Configure energy-s..

2. Right-click the connection (e.g., Local Area Connection) and select “Properties.”

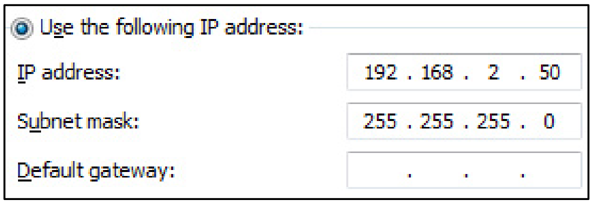
3. Select “Internet Protocol (TCP/IP)” from the list and click “Properties.”



This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.1.0.1
☑ Internet Protocol (TCP/IP)

4. Enter the information as shown below, then click “OK” to save the settings.



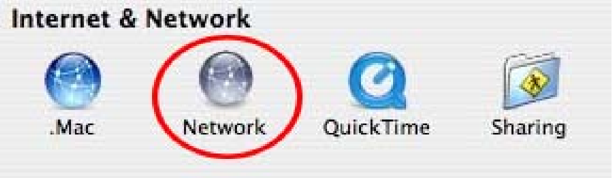
● Use the following IP address:

IP address:	192 . 168 . 2 . 50
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

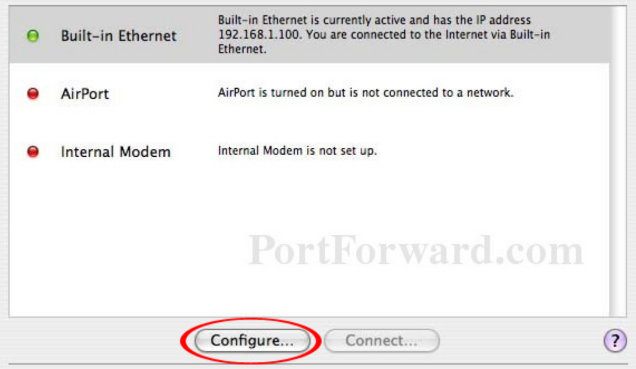
5.1.4 Mac OS X

1. Open the System Preferences page.

2. In the Internet & Network section, click the Network icon.

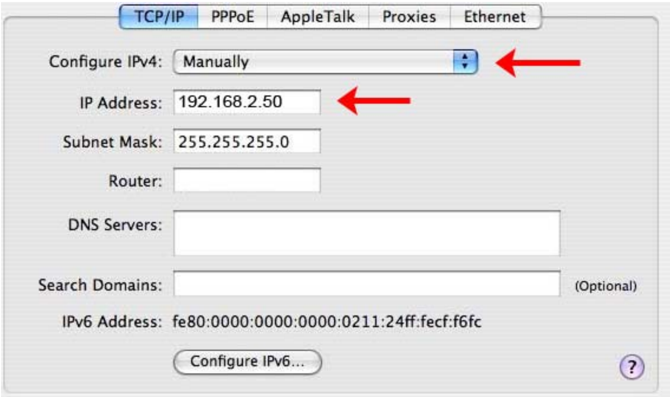


3. Select either Built-in Ethernet or AirPort, depending on how you connect to the wireless access point, then click "Configure… ."



●	Built-in Ethernet	Built-in Ethernet is currently active and has the IP address 192.168.1.100. You are connected to the Internet via Built-in Ethernet.
●	AirPort	AirPort is turned on but is not connected to a network.
●	Internal Modem	Internal Modem is not set up.

4. Set the value for Configure IPv4 to "Manually" and enter 192.168.2.50 in the IP Address field. Click "Apply Now" (not shown in screen shot) to save the settings.



Configure IPv4: Manually

IP Address: 192.168.2.50

Subnet Mask: 255.255.255.0

Router:

DNS Servers:

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:0211:24ff:fecf:f6fc

5.2 Technical Specifications

Specification			
ROM	RAM	4/8/16M	DDR1: 16/32/64M
Standards		IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u, IEEE 802.3af	
Interface Type		1-Port 10/100 RJ45 Ethernet interface, support the 802.3af standard	
RF Power		11b: 27dbm（max） 11g: 24dbm（max） 11n: 23dbm（max）	
Radio Data Rate		11n: Up to 300Mbps 11g: 54/48/36/24/18/12/9/6M 11b: 11/5.5/2/1M	

Sensitivity @PER		11N_MCS7_20M: -70dBm@10% PER;
		11N_MCS7_40M: -69dBm@10% PER;
		54M: -72dBm@10% PER;
		11M: -88dBm@8% PER;	

security		WEP, WPA2/WPA-PSK (AES, TKIP)	
Frequency range		2.4~2.4835GHz	
Antennas		2PCS 2.4G Omnidirectional 2dBi The built-in antenna 2dBi fixed Antennas	
Max. Consumption		9W (Max)	
Dimensions (D x H)		(144*42.5)mm	
Environment		Operating Temperature: -0°C - 40°C Storage Temperature: -40°C - 70°C Operating Humidity: 10% - 90% RH non-condensing Storage humidity: 5% - 95% RH non-condensing	

5.3 GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original
authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an

announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this

License. (Exception: if the Program itself is interactive but
does not normally print such an announcement, your work based on
the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable
source code, which must be distributed under the terms of Sections
1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three
years, to give any third party, for a charge no more than your
cost of physically performing source distribution, a complete
machine-readable copy of the corresponding source code, to be
distributed under the terms of Sections 1 and 2 above on a medium
customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer
to distribute corresponding source code. (This alternative is
allowed only for noncommercial distribution and only if you
received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that

is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component
itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not
excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

6. Warranty

Deutsch Garantieinformationen finden Sie hier unter intellinetnetwork.com/warranty.
English For warranty information, go to intellinetnetwork.com/warranty.
Español Si desea obtener información sobre la garantía, visite intellinetnetwork.com/warranty.
Français Pour consulter les informations sur la garantie, rendezvous à l'adresse intellinetnetwork.com/warranty.
Italiano Per informazioni sulla garanzia, accedere a intellinetnetwork.com/warranty.
Polski Informacje dotyczące gwarancji znajdują się na stronie intellinetnetwork.com/warranty.
México Póliza de Garantía Intellinet — Datos del importador y responsable ante el consumidor IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlan Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500

La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.
A. Garantizamos cámaras IP y productos con partes móviles por 3 años.
B. Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:
1. Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.
2. El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.
3. La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.
Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde ue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos n su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, numero de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese tilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

7. Copyright

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

8. Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

intellinetnetworkcom