GratWiFi

USER MANUAL

Version 2011-07-28

Content

A word from the developers 4

Introduction 4

Hotspot routers 4

Extending coverage 4

PORTAL 5

Introduction 5

Dashboard 5

Hotspot 5

Managing online users 6

Whitelisting, Blacklisting 8

Whitelist 8

Blacklist 9

Opening Hours 9

Modify settings 10

Landing page 10

E-mail redirection 10

WPA2 10

Port restrictions 10

Filtered websites and OpenDNS 10

Traffic Limit 11

Receive statistics 11

Authentication schemes 13

Accept and Surf 13

One-Time Code 14

Username/Password 14

One-Time Code and Username/Password 14

Managing One-Time Codes 15

Generating codes 15

Printing codes 15

Code usage 16

Managing Users and Passwords 16

Add a new user 16

Edit an existing user 16

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Remove a user 16
Troubleshooting 17
Routers 17
Linksys 17
Buffalo 17
Small Form Factor Server 18
Campsite Server 18
1U Rack Server 19
Flowchart 20
Glossary 21

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

A word from the developers

Hi,

My name is Herman verschooten and I am the lead developer of the GratWiFi® Hotspot System.
We have worked hard the past 3 years to create a system that is both user-friendly and stable.
I hope you will be enjoying the system as much as we had creating it.

March 3rd, 2011

Introduction

Welcome to GratWiFi®, we have tried to make this manual meaningful and comprehensive, but sometimes the additions and improvements outpace our documentation efforts. If you need some assistance on a topic not (yet) covered in this manual, do not hesitate to drop us a note at support@gratwifi.eu.

We will be covering both the portal and some general troubleshooting, but first let me introduce you to our trusty friend, the hotspot router in its different flavors.

Hotspot routers

To allow your customers to access the internet a device is installed at your premises that broadcasts a wireless signal; the hotspot router. We are currently deploying several types of routers

- A wireless router
- A small form factor server
- A 1U Rack based model

Extending coverage

If you have a large location, it is possible that some extra antennas have been installed; these will most likely be referred to as repeaters or access points. It is important to know the difference between the 3 terms usually used to name these extenders. When we add an antenna to a box using coaxial wiring, then these are referred to as antennas. The antenna is a passive item, meaning it has no logic inside to perform any actions. Access points are active devices added to the network and connected to the main hotspot router by Ethernet cabling. They each broadcast a wireless network, this allows a greater coverage and the use of separate channels (frequencies). Repeaters are active devices that are connected to the network by picking up the wireless signal, broadcast from the hotspot router (or an access point). They also include an access point that will be used to extend the range. Depending on make and model, they come with one or more radios. The number of radios is important as this will determine the speed of the wireless network. A single radio repeater has to use this one radio to receive packets sent to it, and to resend these packets to either the user's computer or it's uplink, it is easy to understand that this about halves the speed of the network. A dual radio repeater can be configured to have one radio perform the uplink and the other radio to communicate with the clients, both on different frequencies and even using different wireless technology (802.11a vs 802.11b/g/n).

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

PORTAL

Introduction

The place where you perform all configurations for the hotspot you manage is the portal, https://www.gratwifi.eu. After signing in, you will be redirect to your dashboard.

Dashboard

The dashboard is the central part of the portal and is available to all users. It contains a list of all your hotspot locations; it shows you the on/offline state together with the date and time of the last visitor and heartbeat. To be able to monitor your system, your hotspot router talks to our backend server every minute, this is what we call the heartbeat. If we haven't received a heartbeat in 5 minutes, we assume the hotspot is offline and it will be marked red.

Figure 1. Dashboard

Hotspot

After selecting one of our hotspots we are presented with a page containing information about the configuration and usage of this hotspot. On top you will find some general information, such as the address, followed by a list of users currently online.

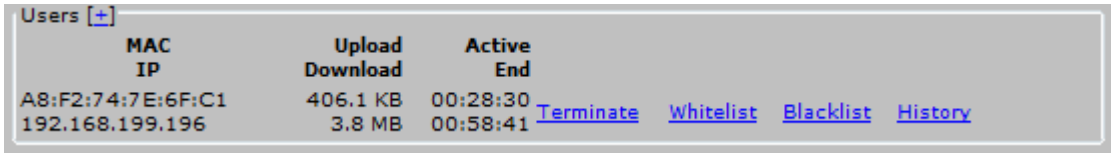


Figure 2. Online users

This list tells us the MAC address, the unique address of the network adapter the user is using to connect, the currently assigned IP address, the amount of data up and downloaded how long they have been online in this session as well as the time remaining. The actions that can be performed on the online users will be explained in one of the following chapters.

Figure 3. Users in penalty

As we will explain in the topic on Traffic Limit, a user can be penalized for surpassing the set volume of data within a certain timespan. Here we can see the MAC address, the moment they were blocked, and the time at which they can access the internet again. The actions will be explained in one of the following topics.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Next comes a block with configuration details, containing such things as the web address of the landing-page, session length in minutes, … It is followed by a representation of the hours our hotspot will be available for use.

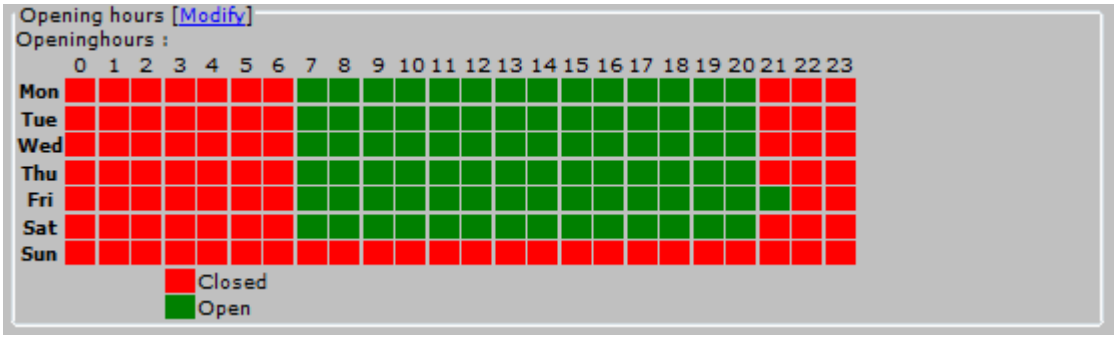


Figure 4. Opening hours

The remainder of the page contains usage statistics (figure 5). Every statistics can be exploded by clicking on it. A visitor is a computer connecting to the network, every time this computer starts a new session it counts as a visit. If the same computer starts 2 sessions within the same day, e.g. at 9 in the morning and at 2 in the afternoon, it will count as 1 visitor with 1 visit at 9h and 1 visitor, 1 visit at 14h, but it will count as 1 visitor with 2 visits for that day. The pie charts show the different types of operating systems, device types and browsers that have been used in the previous month. Click on the graphs to see more days, months or years.

Managing online users

Depending on your permissions you will see some links with actions (figure 2) for each online user.

- Terminate
  Disconnect the current session.
- Whitelist
  Add the current MAC to the whitelist.
- Blacklist
  Disconnect the current session and add the MAC to the blacklist.
- History
  Show a popup with a history of this MAC address.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

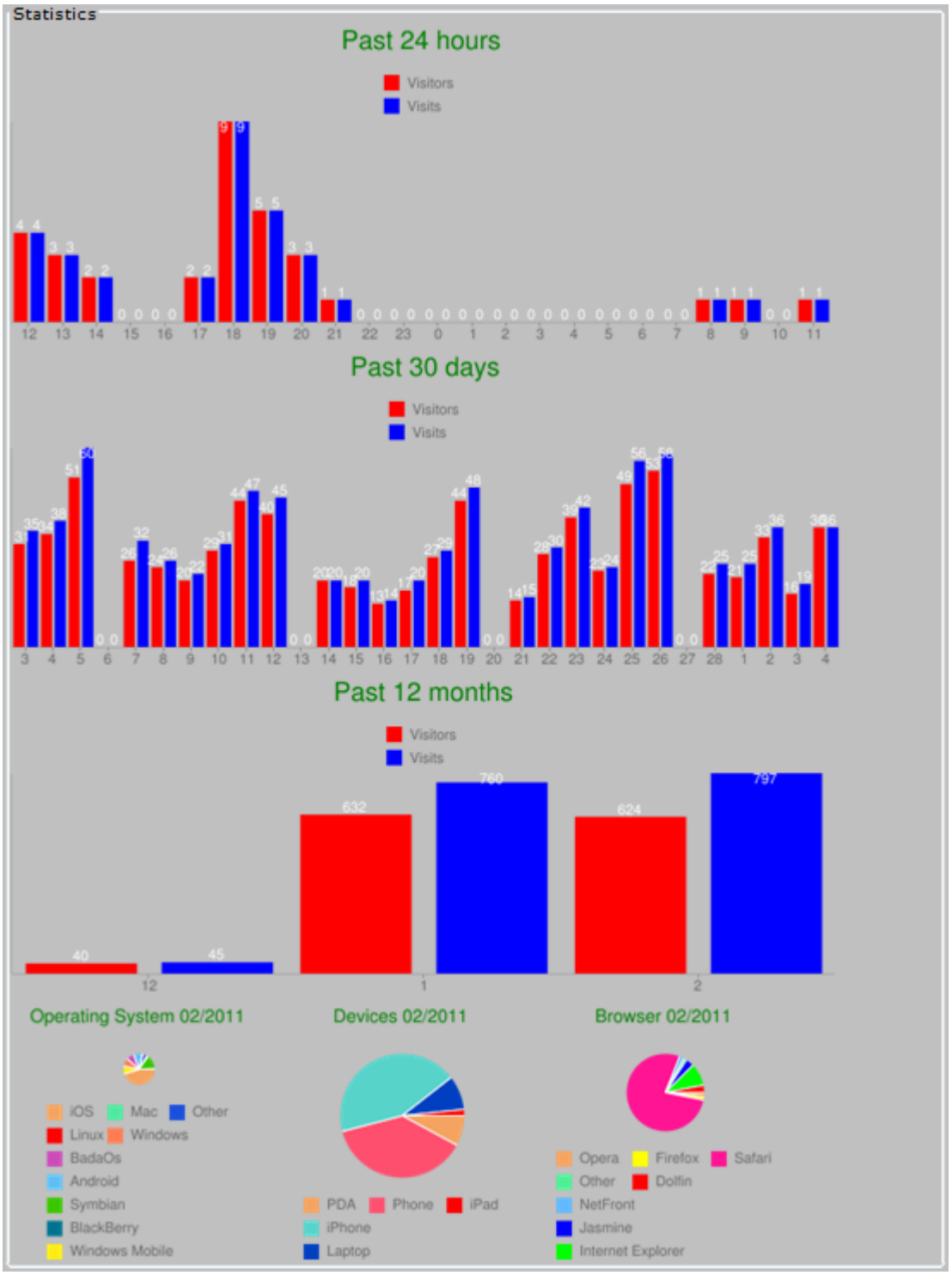


Figure 5. Statistics

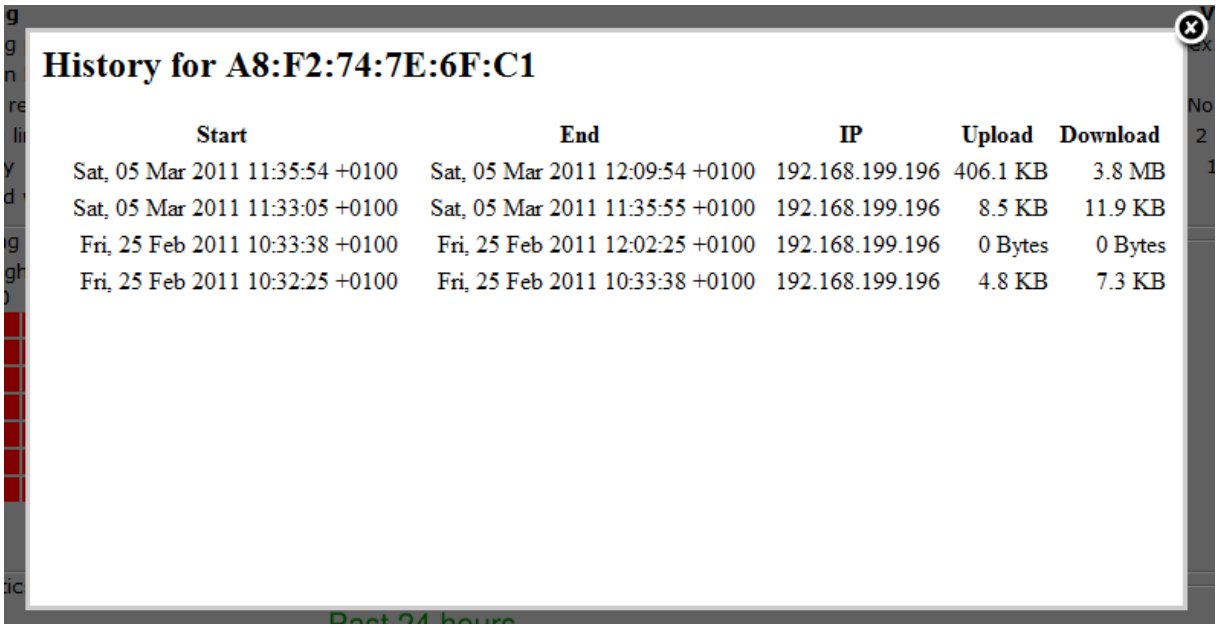


Figure 6. History

Whitelisting, Blacklisting

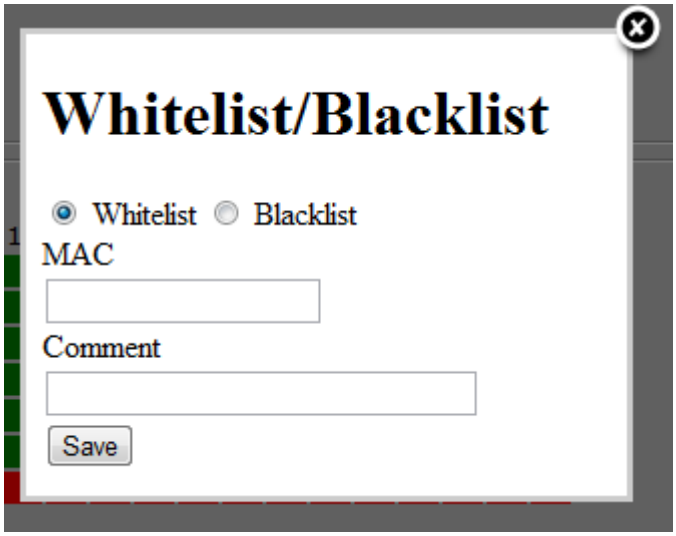


Figure 7. Add to whitelist/blacklist

Whitelist

Adding a computer to the whitelist of your hotspot is not something you do lightly. It allows this computer not only to bypass the accepting of the terms and conditions and have unrestricted access to the internet, but it will also NOT record any history, statistics or other logs for this computer. Fill in the MAC address (already filled in if you click the whitelist link) and give a comment, so you can later on remember which computer this is, and press save. The whitelisted computers will be listed on the hotspot page with a delete and edit link.

This is only to be used for your own computers, never for a computer belonging to third parties.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Blacklist

Adding a computer to the blacklist will cause the hotspot router to deny all access to this router. It effectively bans this computer from the network. As with the whitelist enter the MAC address and a comment.

Opening Hours

Some hotspots like hotels like to be available 24 hours to their customers. But others like a pub or restaurant, may want to limit access to their opening hours. During the 'closed' hours the users will be presented with a page telling them to come back during opening hours. Clicking the modify link (figure 4) takes us to edit page. The upper half of this page contains the regular opening hours; the lower half enables us to add exceptions. If you check the 'Hotspot closed' box, your users will be presented with a page telling them the hotspot is closed. The "opening hours" grid is divided horizontally in 24 hours and vertically in the 7 days of the week. Clicking on a green 'open' hour will turn it red 'closed'; clicking again will turn it green again. Don't forget to press "Save" when you are done. If you normally close on Sunday, but are open some Sundays in the year, you can add them using the exceptions. Select the date and click this will add a line to the right of the calendar.

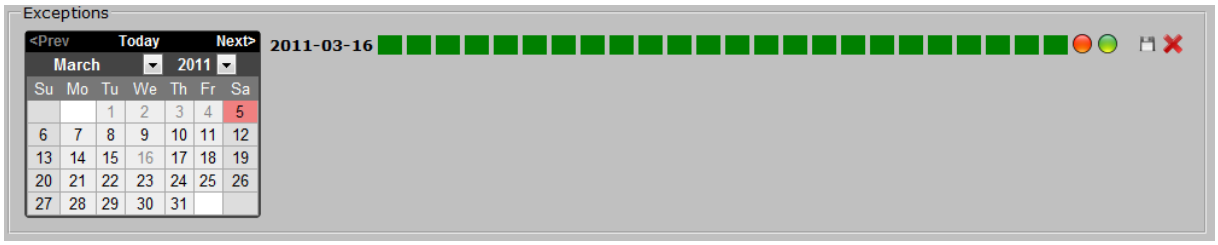


Figure 8. Exceptions for opening hours

The same method as with the regular opening hour applies. Pressing the red or green button at the end will turn the whole day closed or open, click when done, or to remove this exception. The opening hours on the hotspot information page will reflect these exceptions if the date is within the current week. Click Back on the top of the page to return to the hotspot information page.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Modify settings

Clicking the 'Modify settings' link in the hotspot information page, takes us to a page where we can modify most settings. Depending on your permissions, you will be able to change the name of your location, the address, telephone and type. Some options become available by clicking the checkbox in front of them, if unchecked they are set to the system default, e.g. the default Session Length is 60 minutes. Some settings require a little explication.

Do not forget to press the Save button to make your changes permanent. If you are not redirected to the hotspot information page after pressing Save, then look for fields that have a red border and correct the information.

Landing page

When a customer visits your hotspot they will be presented with a terms of services page, after accepting they are redirected to your landing page, if set, else they will go to the site they originally requested. Make sure you enter a correct URL. We offer you 2 macro's you can use in the web address; MAC will be replaced with the MAC address of the user and LNG will be replaced with the chosen language (nl, fr or en).

E-mail redirection

If your users want to send e-mail using an e-mail client on their computer, they will have configured an outgoing mail server (SMTP) in their client. Some Internet Service Providers however do not allow access to SMTP-servers outside of their network. If you want to enable outgoing e-mail for your users in such a case, you can fill in the outgoing mail server for your internet connection, or you can enter our relay-server; relay.gratwifi.eu:17125. If you do not want people to be able to send e-mail, you can fill in 127.0.0.1.

WPA2

A hotspot rarely uses an encrypted wireless network but for those who want to, you can fill in a key or have the system generate one for you. You'll be responsible for supplying this key to your users.
The WPA2-key will only be applied to our router, not to any extra access points or repeaters.

Port restrictions

Some owners want to restrict the internet access to certain ports or protocols, e.g. web browsing only. Enter a list of ports and access will only be available to these. Commonly used ports are;

- 80 : HTTP, web browsing
- 443: HTTPS, secure web browsing
- 25: SMTP, outgoing e-mail
- 110: POP3, e-mail retrieval
- 143: IMAP4, e-mail retrieval

Filtered websites and OpenDNS

Most people do not want their customers to access porn or other explicit material while surfing in their establishment. To filter these, you can enter some web addresses (e.g. playboy.com,), that will be denied. If you have a fixed IP address, you can create an account with OpenDNS (http://www.opendns.net); they offer an easy to use interface that allows you to choose which

categories you want to block. If you do not have a fixed IP, contact your GratWiFi® partner, they will be able to configure this for you.

Traffic Limit

To discourage people from abusing your internet connection, you can apply limits on the amount of data they can transmit or receive during a certain period of time.

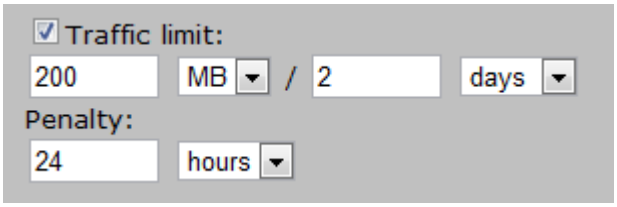


Figure 9. Traffic limit

Enable the traffic limit option, and enter how many megabytes (MB) or gigabytes (GB) of traffic you want to allow. Next choose the amount of time they have to consume this, and lastly you can add a penalty, expressed in hours or days. Let's explain this by example:

- Limit: 200MB / 1 Day, Penalty 0 hours
  If someone starts surfing at 10:00 and surpasses the 200MB at 14:00, the session will be terminated, and a message will be displayed to tell them that the internet will be available again at 10:00 the next morning.
- Limit: 200MB / 1 Day, Penalty 6 hours
  If someone starts surfing at 10:00 and surpasses the 200MB at 14:00, the session will be terminated, and a message will be displayed to tell them that the internet will be available again at 16:00 the next day.
- Limit: 500MB / 5 Day, Penalty 2 days
  If someone starts surfing Monday morning at 10:00 and surpasses the 500MB Tuesday at 14:00, the session will be terminated, and a message will be displayed to tell them that the internet will be available again at Sunday 10:00.

If you do not want to add extra penalty time enter a 0 (zero).

If someone surpasses the limit, he will be disconnected and blocked until the current period has ended. The penalty time is added to the end of the period. Computers in 'penalty' will be listed on the hotspot information page (see figure 3), with a link to cancel the penalty, a link to see the history (see figure 6), and a link to show the volumes of the past period (figure 10).

Receive statistics

At the bottom of the page there are some checkboxes that enable you to receive daily, weekly and monthly statistics of your hotspot by e-mail. Weekly statistics are sent on Monday, Monthly on the 1st of the month.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

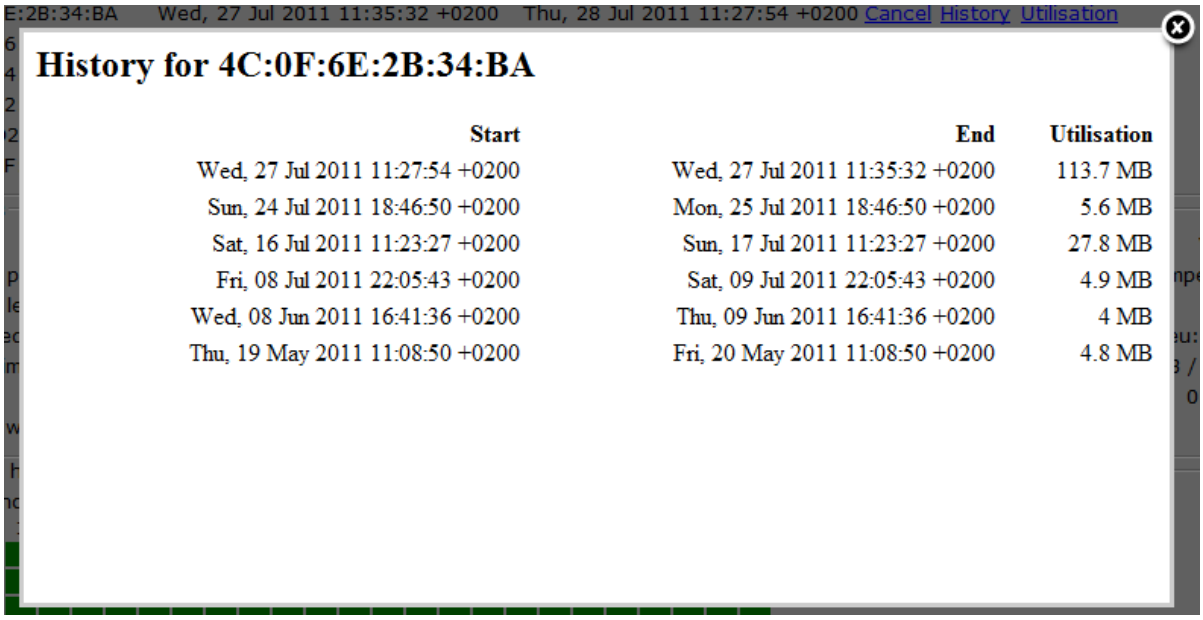


Figure 10. Volume history

Authentication schemes

When a customer wants to access the internet using your hotspot, he will be presented with the terms and conditions. Accepting these can be as easy as clicking a button or it may require authentication. The different authentication schemes available are explained below.

Your local partner will help you choose the right authentication scheme, and set it up.

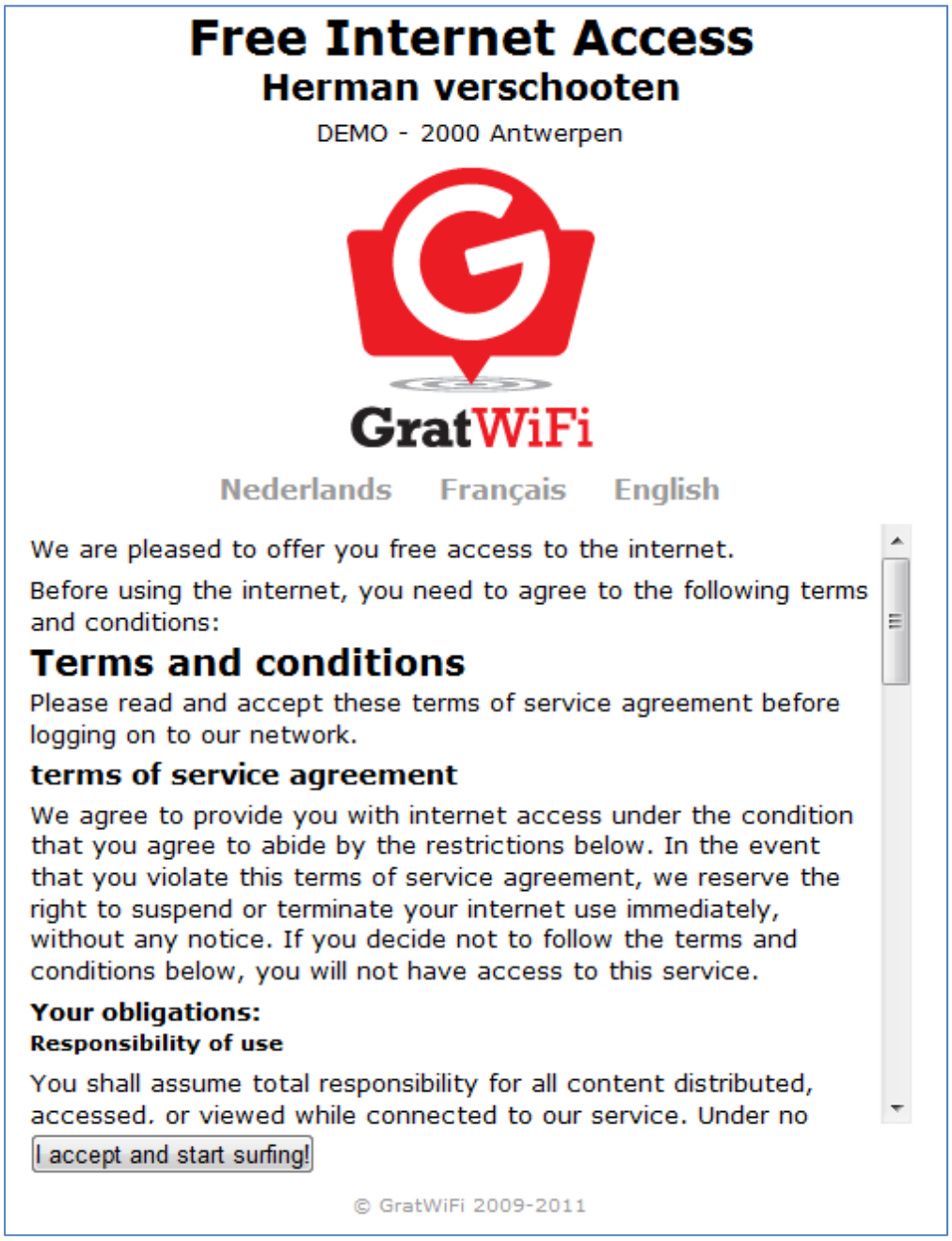


Figure 11. Terms and conditions

Accept and Surf

The customer is presented with a button to accept the terms and conditions (figure 11). After clicking he is redirected to your landing page or the internet if no landing page was set.

One-Time Code

The customer is presented with a field to fill in the code, you supplied, and a button to accept the terms and conditions. This allows you to restrict usage of the hotspot to actual customers. See "Managing One-Time Codes" for more information.

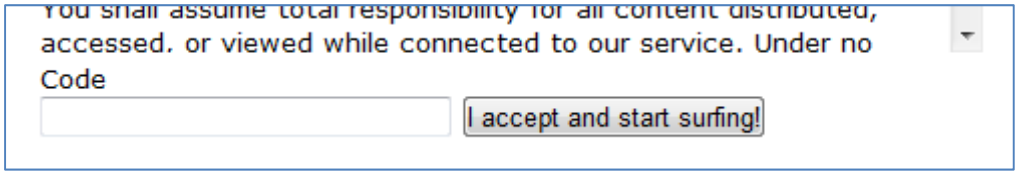


Figure 12. One-time code

Username/Password

The customer is presented with fields to fill in his username and password, and a button to accept the terms and conditions. See "Managing Users and Passwords" for more information.

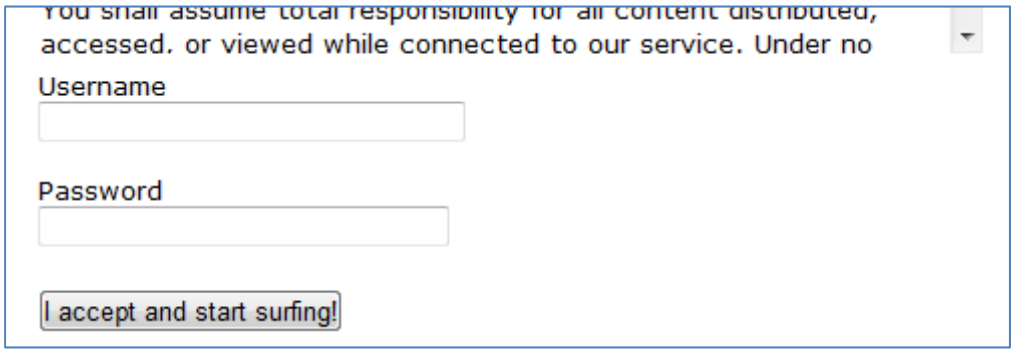


Figure 13. Username and password

One-Time Code and Username/Password

This is a combination of both the One-Time Codes and Username/Password options explained above. The user will see a field to fill in the one-time code and 2 fields for Username/Password. This allows you to create a username/password for regular users, staff, and longtime residents and have the flexibility of one-time codes for other users.

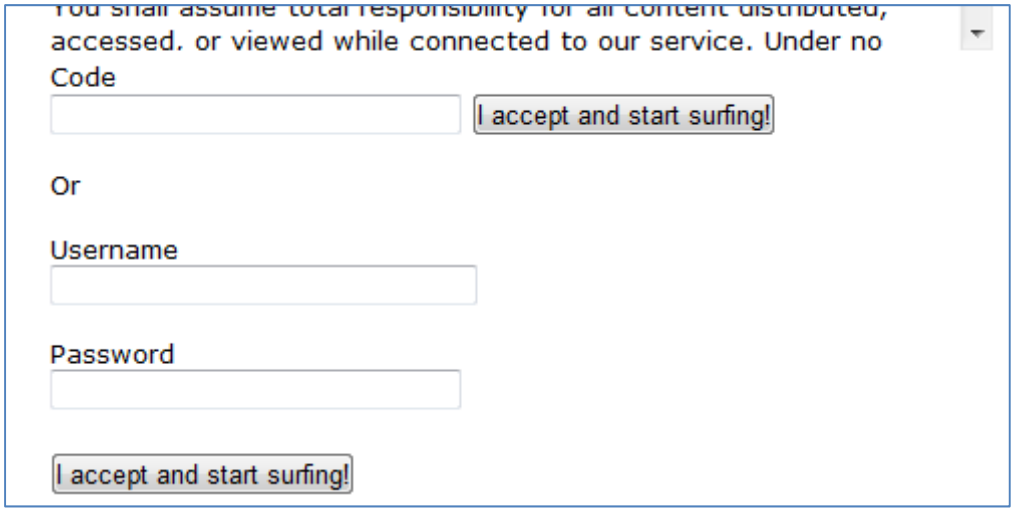


Figure 14. Combination One-time code with Username and password

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Managing One-Time Codes

To manage the One-Time code, click the “One-time code” link in the menu at the top of hotspot information page. The screen is divided into 2 sections, “Generate” and “Code Usage”. The former allows you to generate and print codes, the latter enables you to see if a certain code has already been used.

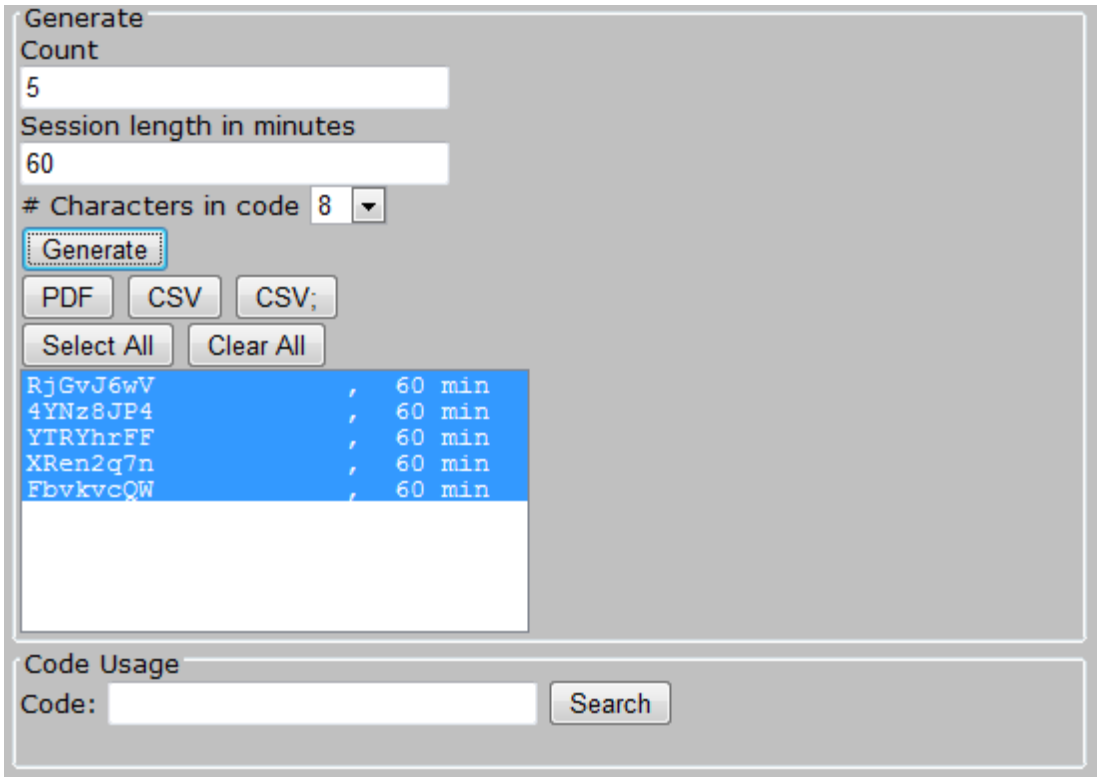


Figure 15. One-Time Codes

Generating codes

Follow these steps to generate new codes:

- Enter the number of codes you want to generate.
- Enter the session length in minutes.
- Choose the length in characters of the code from the dropdown.
- Press Generate

The newly generated code will be added to list, and will be selected (in blue). When a code has been used, it will disappear from the list.

Printing codes

The next 3 buttons allow you to ‘print’ the codes selected in the list.

- PDF : Generate a PDF in GratWiFi layout with the selected codes.
- CSV : Generate a comma-separated file with the selected codes.
- CSV; : Generate a ‘;’-separated file with the selected codes.

The file generated by the 2 CSV-buttons differs only in the separation character, a comma “,” or a semi-colon “;”. The file can be opened with a spreadsheet program, such as Microsoft Excel, or used

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

in a mail merge to create a personalized layout. Depending on your locality you may need to choose the semi-colon separator, to make this work.

The file contains 2 columns:

- The code within quotation marks, e.g. “FbvkvcQW”
- The session length in minutes, e.g. 60

Code usage

It can happen that you need to see if a certain code has already been used. Fill in the code and press search. If the code has already been used, the date and time of the last session will be printed.

Managing Users and Passwords

If the “Username and Password” authentication scheme is active, an additional section will appear in the hotspot information page, labeled “Usernames”.

Figure 16. Usernames

Add a new user

Click on the ‘+’-sign to open the ‘add new user’ window. Fill in the username and password fields and select a date from and to. The user will only be able to use the system between the From and To dates.

Figure 17. Add new user

Edit an existing user

Click the user’s name to open the edit window.

Remove a user

Click the ‘X’ to remove the user.

⚠ Users that have expired will not be removed automatically.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Troubleshooting

As with all systems sometimes things go wrong, this little troubleshooting guide may help you resolve the issues, without having to call your local partner.

Routers

Linksys

Figure 18. Linksys router

A list of items to check If your hotspot is running on a Linksys router;

- The Power led should be on and fixed. It only blinks during booting.
- The DMZ led should be off.
- The WLAN is on and it blinks if there is wireless traffic.
- Ethernet Ports 1 to 4 are only on if a device is attached to one of these interfaces on the back of the router .
- The Internet led is on, if the router is attached to your internet modem or local network. This does not indicate that our router has an active internet connection.

Buffalo

Figure 19. Buffalo

A list of items to check If your hotspot is running on a Buffalo router;

- The Power led should be on and fixed.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

- The Wireless G is on and it blinks if there is wireless traffic.
- The BRIDGE led is off.
- The DIAG led should be off. It is only on during booting.
- The port labeled WAN on the back of the router should have cable and should be lit. This does not indicate that our router has an active internet connection.
- If a cable is attached to any of the ethernet ports, then it should be lit.

Small Form Factor Server

Figure 20. Small Form Factor Server

A list of items to check;

- The green power led should be lit.
- The orange hard disk led blinks occasionally.
- The left ethernet interface, labeled 1 or LAN, should be connected to the hotspot network.
- The right ethernet interface, labeled 2 or WAN, should be connected to the internet.

Campsite Server

Figure 21. Campsite Server

A list of items to check;

- The blue power led on the front should be up.
- The red hard disk led blinks occasionally.
- The left ethernet interface should be connected to the hotspot network.
- The right ethernet interface should be connected to the internet

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

1U Rack Server

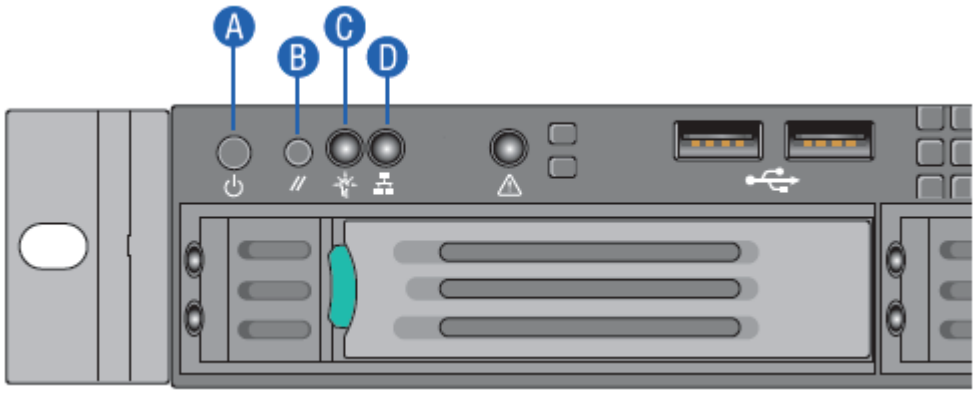


Figure 22. Server front

A) Power Button
B) System Reset Button
C) Power Led
D) System Nic 5 Activity LED.

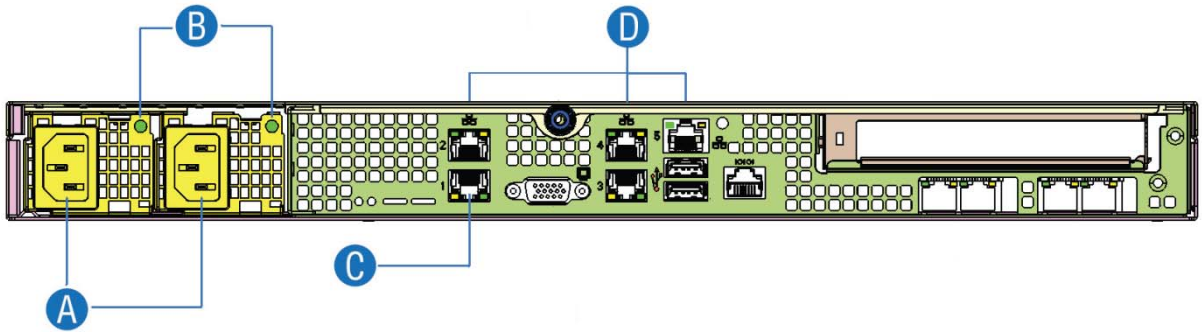


Figure 23. Server Back

A) Redundant Power Supply Units
B) Power Supply Status Led
C) WAN-connection
D) LAN-connections

Things to check:

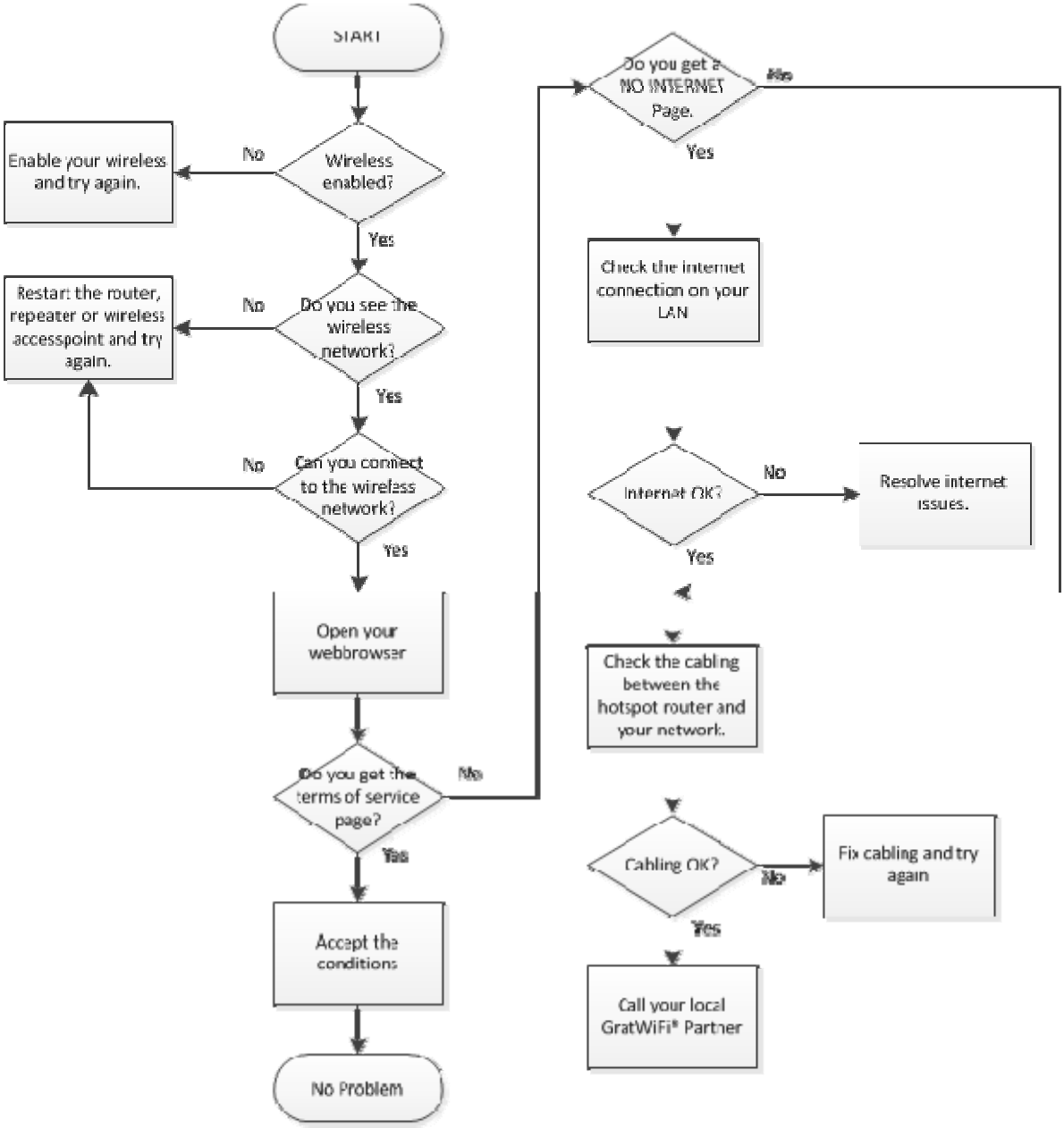
- Make sure the power led is on and not blinking.
- Make sure the WAN cable is correctly attached.
- Connect at least one extra devices to the ethernet ports.

⚠ It is possible that the images displayed here may not be for the device you have at your location. Consult your local partner for up to date information. These images are for the devices actually used by GratWiFi® in the Benelux area.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Flowchart

This flowchart starts from the user's perspective.



©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv

Glossary

- 802.11a/b/g/n
  In documents about wireless networking the term 802.11 followed by 1 or more characters, refers to the collection of standards for wireless networks developed by the IEEE (Institute of Electrical and Electronics Engineers).
- Blacklist
  The Blacklist contains a list of MAC addresses that are disallowed access to your hotspot.
- Browser
  The program you use to surf the internet, e.g. Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, Opera…
- Heartbeat
  A signal sent from your router to our servers every minute.
- Hotspot
  A location that offers internet access over a wireless network through the use of a router.
- LAN
  LAN or Local Area Network, is the name for the network you are connected to. Or in the case of the hotspot it is the network the clients connect to.
- Landing page
  The first page the user visits after accepting the terms and conditions. This can be your homepage or a promotional advert…
- MAC
  a Media Access Control –address is a unique identifier assigned to the network interface of a computer. Each network interface has its own MAC-address.
- Operating System
  Every computer needs a basic program to operate and interface with its users; this is called the operating system. Popular Operating systems or OS are Microsoft Windows, Apple OS X, and Linux for PC, iOS (iPhone, iPod, and iPad), Android and Blackberry for mobile devices.
- Router
  A device that regulates the traffic from your network to the internet, and vice versa.
- URL
  A Uniform Resource Locator is the term for what we generally call a web address, or server name. It generally starts with a protocol, followed by the address and some parameters, e.g. http://www.google.be?q=GratWiFi.
- Whitelist
  A list of MAC addresses that are allowed to use your hotspot as if it were an access point, without any restrictions, or logging.
- WAN
  WAN stands for Wide Area Network, and is generally the term used for the non-local network. For the hotspot users, it is the network the hotspot router takes its internet connection from, in most cases your LAN network.
- Wi-Fi
  The popular term for Wireless Fidelity or Wireless networking.

©2009-2011 Herman verschooten & Hotspot Service BeNeLux nv