

Wireless network connections

Ligiu A. Uiorean

IT Lead – Autostrada Transilvania

December 2006

RNZN Guides

Index

0. Introduction.....	4
1. Safety	5
2. Equipment.....	6
a. Hardware	6
b. Software	7
c. Procedures	7
3. Planning	18
a. General Considerations	18
b. Mathematical estimations	18
d. Extending the range	22
4. Configuring the devices	23
a. Access point	23
c. Repeater.....	26
d. WDS.....	29
5. Deployment.....	31
a. Testing.....	31
b. Other issues	32
6. Wireless links at the RMW project.....	33
a. Long Range	33
b. On camp	37

0. Introduction

In this document I will try to describe a method of providing wireless data links to local and remote location using cost effective off the shelf equipment. It contains both the theoretical description of the problem and the practical guide in setting up the devices.

While this document has yet to be improved, all of the information has been tested in the field at the Romanian Motorway Project. The solutions described are able to provide reliable links if realistically planned. All solutions have been used at least one month in the field.

Savadisla, 20.December 2006

1. Safety

When installing an antenna, follow these general tips:

- For most elevated antenna installations, it is recommended that you use professional installers for proper installation and safety.
- For safety reasons, never touch a high-gain antenna when it is transmitting or point it at any part of your body.
- Carefully follow the instructions provided with your antenna.
- Keep antennas away from metal obstructions (heating and air-conditioning ducts, large ceiling trusses, building superstructures, and major power cabling runs).
- Use a directional antenna when connecting a link between two buildings. A directional antenna must be properly aligned to directly point at the other antenna.
- Antenna towers should be a safe distance from overhead power lines. The recommended safe distance is twice the tower height but not less than 15m
- To prevent moisture entry into the antenna cable, seal all external cable connectors using commercial products such as coax compatible electrical tape and Coax-Seal.
- Be aware that outdoor antennas are prone to lightning strikes. While a surge arrestor might protect the equipment in case of an indirect hit, never install or work on an antenna in bad weather.

2. Equipment

a. Hardware

We are trying to use standard of the shelf equipment in order to keep the price down. Compatible equipment is bellow:

- Linksys WRT54G 1.0 CDF0xxx or CDF1xxx
- Linksys WRT54G 1.1 CDF2xxx or CDF3xxx
- Linksys WRT54G 2.0 CDF5xxx
- Linksys WRT54G 2.2 CDF7xxx
- Linksys WRT54G 3.0 CDF8xxx
- Linksys WRT54G 3.1 CDF9xxx
- Linksys WRT54G 4.0 CDFAx
- Linksys WRT54G 5.0
- Linksys WRT54G 6.0
- Linksys WRT54GL 1.0 CL7Axxx (**recommended**)
- Linksys WRT54GL 1.1 CL7Bxxx (**recommended**)
- Linksys WRT54GS 1.0 CGN0xxx or CGN1xxx
- Linksys WRT54GS 1.1 CGN2xxx
- Linksys WRT54GS 2.0 CGN3xxx
- Linksys WRT54GS 2.1 CGN4xxx
- Linksys WRT54GS 3.0 CGN5xxx
- Linksys WRT54GS 4.0 CGN6xxx
- Linksys WRT54GS 5.0
- Linksys WRTSL54GS
- Linksys WRT300N v1 (v24 beta)
- Linksys WAP 1.0
- Linksys WAP 2.0
- Linksys WAP 3.0
- Allnet ALL0277
- Buffalo WHR-G54S
- Buffalo WHR-HP-G54
- Buffalo WBR-G54
- Buffalo WLA-G54
- Buffalo WBR2-G54
- Buffalo WBR2-G54S
- Belkin F5D7130/7330 (2mb flash)
- Belkin F5D7230-4 v1444 (2mb flash)
- ASUS WL500G (**recommended**)
- ASUS WL500G-Deluxe (**recommended**)
- ASUS WL500G-Premium (**recommended**)
- Mitsubishi R100 Diamond Digital Wireless Gateway (v23 SP2. Rebadged ASUS WL500G)
- Motorola WR850G
- Motorola WR850GP
- Siemens Gigaset SE505
- Ravo W54-RT
- Askey RT210W

I used WRT54GL because of availability.

b. Software

The stock firmware on the wireless router is suited for home use but we need advanced features for our setup. For this purpose we are using the DD-WRT open source firmware. The website can be downloaded from: <http://www.dd-wrt.com/>.

The main advantages of this firmware over the stock firmware are:

- possibility to adjust the RF output power
- support for repeater mode
- advanced monitoring and administration

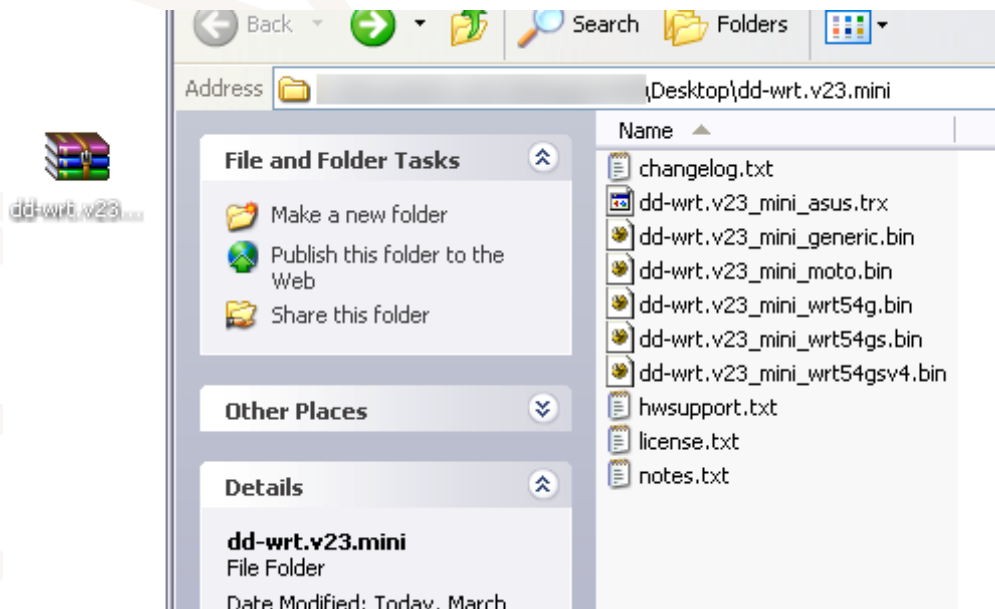
c. Procedures

The main challenge before we start is flashing the devices with the new firmware. Please note that the procedure below refers to the WRT54GL (identical to the WRT54G v4). In order to upgrade other types of routers please refer to the dd-wrt documentation or contact the author of this document.

Firmware update procedure:

1) Download the DD-WRT v23 firmware

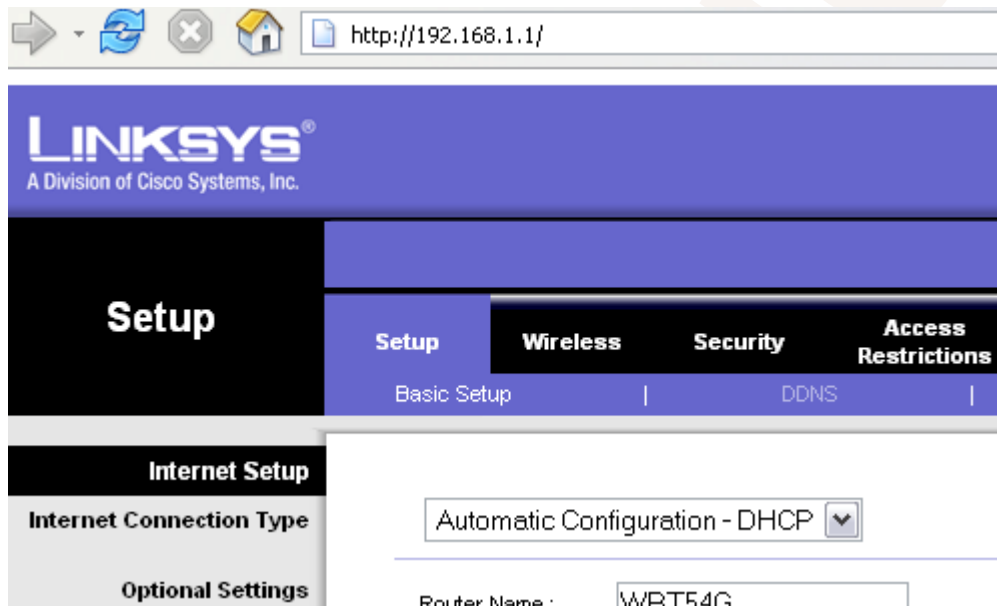
- You must use the **mini** version when upgrading from original linksys firmware!
- Download the Mini Version 23 [HERE \(dd-wrt.v23.mini.zip\)](http://www.dd-wrt.com/dd-wrtv2/downloads/index.php?path=dd-wrt.v23%2F&download=dd-wrt.v23.mini.zip) (<http://www.dd-wrt.com/dd-wrtv2/downloads/index.php?path=dd-wrt.v23%2F&download=dd-wrt.v23.mini.zip>) or go to the DD-WRT downloads section at <http://www.dd-wrt.com/dd-wrtv2/index.php?link=downloads>
- Extract the archive. Once it is downloaded and extracted from the zip archive it should look something like this:



2a) Reset through the Web Interface

if you forgot the password or IP of your router, proceed to step 2b.

- From a PC connected to one of the 4 LAN ports on the router open a web browser and go to the IP of the router (default IP is 192.168.1.1).
- You will be prompted for username and password. Username is not required. Enter password (default password is *admin*) and you should be at the Web Interface of your WRT54G v4



- Click the "Administration" tab.

Firmware Version : v4.20.6

Wireless-G Broadband Router **WRT54G**

Security **Access Restrictions** **Applications & Gaming** **Administration** **Status**

| Diagnostics | Factory Defaults | Firmware Upgrade | Config Management

Local Router Access : You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access : Allows you to configure access options to the

- Click the "Factory Defaults" sub-tab.
- Select "Yes".

Wireless-G Broadband Router

Setup **Wireless** **Security** **Access Restrictions** **Applications & Gaming** **Administration**

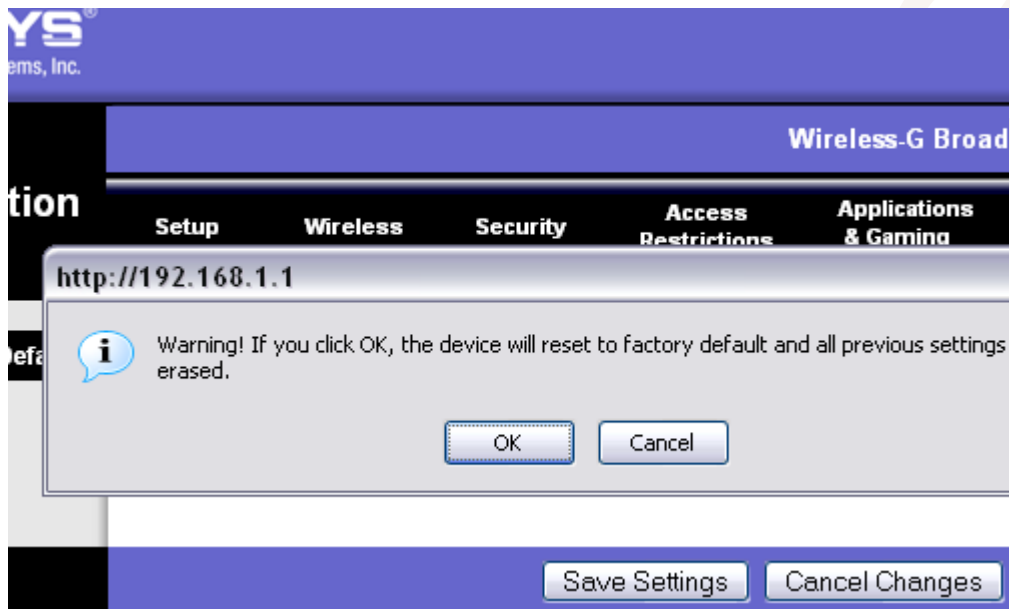
Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management

Restore Factory Defaults : ☒ Yes ☐ No

Save Settings Cancel Changes

This will restore the Router to factory default settings. More...

- Click the "Save Settings" button.
- A warning will pop up, click "ok".



2b) Reset to factory defaults

- Press and hold the reset button on the back of the router for 30 seconds. This will clear your NVRAM, the configuration and reset the password to *admin*.

Be aware that if your router currently has an OpenWRT firmware running on it, then using the reset button may brick your router. Research your current firmware to be safe.

3) Upgrade Firmware

Do not turn off the computer, close the web browser, or turn off the router during this process!!!!

- From a PC connected to one of the 4 LAN ports on the router open a web browser and go to the IP 192.168.1.1.

The screenshot shows a web browser window with the address bar displaying `http://192.168.1.1/`. The page header features the Linksys logo and the text "A Division of Cisco Systems, Inc.". The main navigation bar includes tabs for "Setup", "Wireless", "Security", and "Access Restrictions". The "Setup" tab is active, and the "Basic Setup" sub-tab is selected. On the left, a sidebar menu shows "Internet Setup" as the current section, with "Internet Connection Type" and "Optional Settings" as sub-sections. The main content area displays "Internet Connection Type" set to "Automatic Configuration - DHCP" via a dropdown menu. Below this, the "Router Name" is set to "WRT54G".

- You will be prompted for username and password. Leave username blank, enter password *admin*. Now you should be at the Web Interface of your WRT54G v4.

This is a duplicate of the screenshot above, showing the Linksys WRT54G v4 web interface. The browser address bar shows `http://192.168.1.1/`. The "Setup" tab is active, and the "Basic Setup" sub-tab is selected. The sidebar menu shows "Internet Setup" as the current section. The main content area displays "Internet Connection Type" set to "Automatic Configuration - DHCP" and "Router Name" set to "WRT54G".

- Click the "Administration" tab

Firmware Version : v4.20.6

Wireless-G Broadband Router

WRT54G

Security	Access Restrictions	Applications & Gaming	Administration	Status
Diagnostics	Factory Defaults	Firmware Upgrade	Config Management	

Local Router Access : You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access : Allows you to configure access options to the

Local Router Access : You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access : Allows you to configure access options to the

- Click the "Firmware Upgrade" sub-tab.

Setup	Wireless	Security	Access Restrictions	Applications & Gaming	Administration
Management	Log	Diagnostics	Factory Defaults	Firmware Upgrade	Config Management

Firmware Upgrade

Please select a file to upgrade :

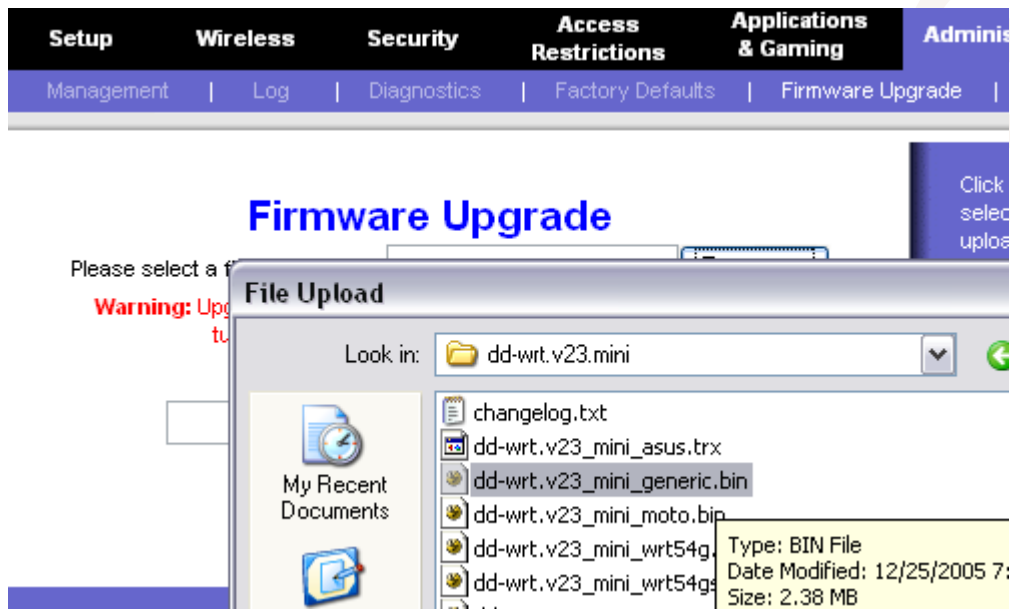
Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted !

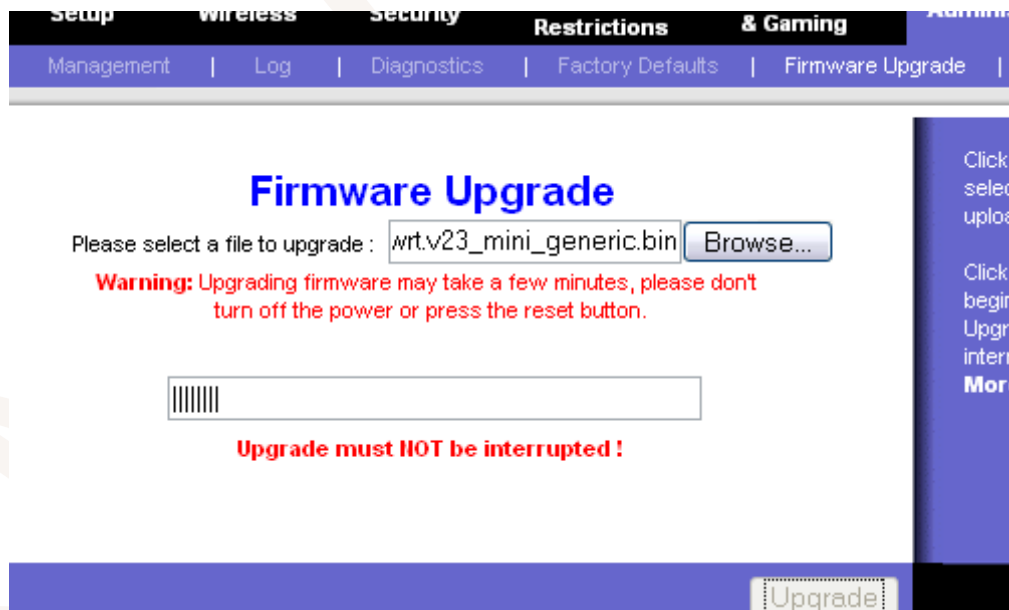
Click on the select the uploaded t

Click the U begin the u Upgrade m interrupted **More...**

- Click the "Browse" button and select "dd-wrt.v23_mini_generic.bin" file you extracted in step 1.

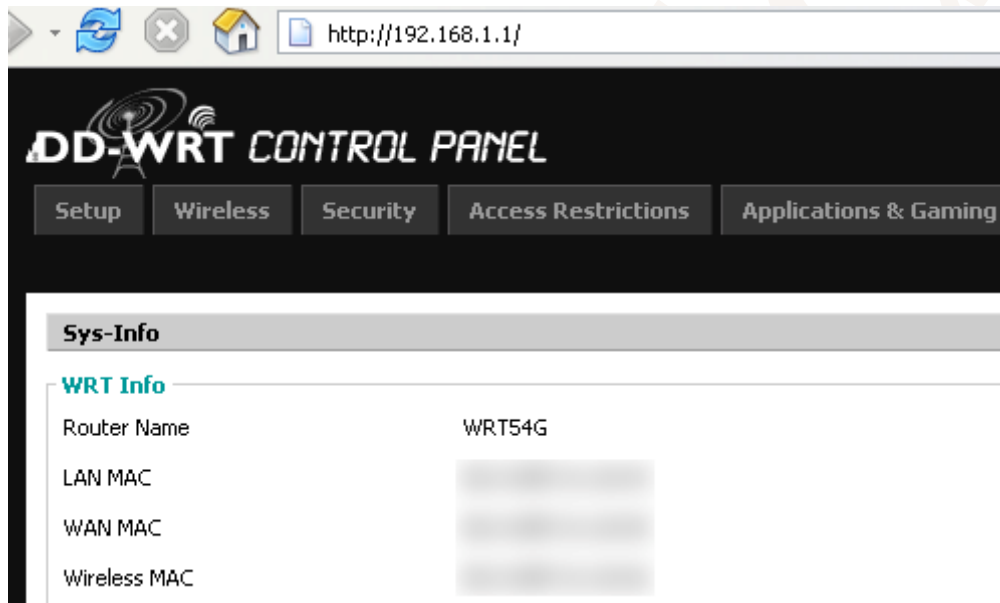


- Click the "Upgrade" button.
- The router will take a few minutes to upload the file, flash the firmware, and then reset.



Now you should receive an "Upgrade successful" message. Wait for the router to reboot and connect to <http://192.168.1.1>. You should be able to access the new firmware. Please note that the default login username/password has changed from <blank>/admin to root/admin.

If flashed successfully you will now be at the DD-WRT web interface and the Router Name will be DD-WRT.



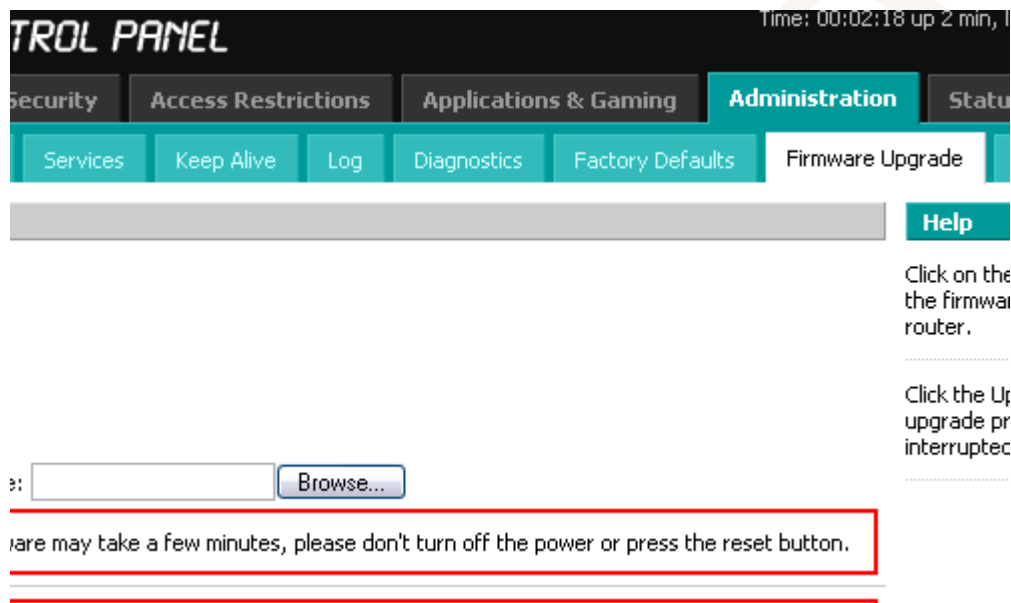
4) Reset to factory defaults AGAIN

- Repeat step 2 above. Note: step 2b (the manual way of clearing the NVRAM) is recommended to make sure the radio gets the correct parameters.

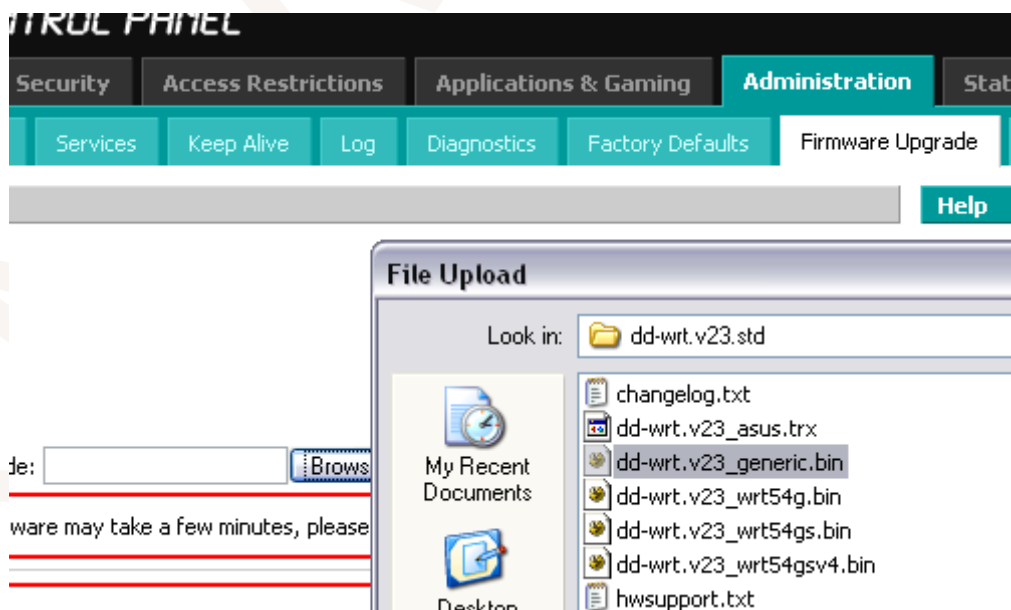
5) Upgrade the Firmware to DD-WRT STD v23

- It is strongly advised that you enable the "Boot Wait" option under the "Administration" tab before continuing. This will help you recover in the future should you flash your router improperly. If you use v23 or higher the "Boot Wait" option is enabled by default.
- Download the STD Version 23 [HERE \(dd-wrt.v23.std.zip\)](http://dd-wrt.gruftie.com/dd-wrtv2/downloads/index.php?path=dd-wrt.v23%2F&download=dd-wrt.v23.std.zip) (<http://dd-wrt.gruftie.com/dd-wrtv2/downloads/index.php?path=dd-wrt.v23%2F&download=dd-wrt.v23.std.zip>) or go to the DD-WRT downloads section at <http://www.dd-wrt.com/dd-wrtv2/index.php?link=downloads>
- Extract it

- Click the "Administration" tab
- Click the "Firmware Upgrade" sub-tab.



- Hit the browse button and select dd-wrt.v23_generic.bin that you just extracted.



-
- You should see the progress of the flash like so:

Firmware Upgrade

Reset after flashing to:

☒ No reset

☐ Firmware Defaults

☐ Factory Defaults

Please select a file to upgrade:

Warning: Upgrading firmware may take a few minutes, please don't turn off the power or press the reset button.

Upgrade must NOT be interrupted ! (please wait 2 mins.)

-
- If the upgrade went well then you should see a success message. You're done!



6) Troubleshooting

- If your router fails to reboot (power light doesn't stop flashing, no web interface, etc) you will need to consult the online DD-WRT documentation or contact the author of this document.

3. Planning

a. General Considerations

When planning a wireless link there are several factors that need to be taken into consideration:

- link length
- terrain height, obstacles
- terrain type
- needed bandwidth
- local regulations

All of these factors affect the odds of the link to be achievable. To give you an overview of how these factors affect your link here are some generally accepted ideas:

- very good links can be achieved up to 10km, reasonable links up to 20km
- generally only line of direct sight links can be achieved (non line of sight or obstructed line of sight links are possible only over short distances)
- Wireless links work better over hard rock than over wet terrain or water
- Always consider that the effective bandwidth is about half the raw bandwidth
- Always check your local regulations before deploying a long range wireless link

b. Mathematical estimations

In calculating a long distance link we have to take into account at least the following factors:

Transmitting equipment power (+)
Transmitting antenna gain (+)
Free space loss (-)
Receiving antenna gain (+)
Receiving equipment sensitivity (+)

The factors marked with (+) contribute to the range, the factors marked with (-) reduce the range. There are other factors to take into account (like cable loss, connector loss, terrain) but they can be neglected for an ideal model. The ideal model should have about 10db to 20db to spare above the theoretical limit. Please also note that the maximum radiated power (equipment power + antenna gain) might be regulated, however the receiving gain is not regulated so it is important to have a high gain antenna and adjust the power output to match local regulations.

The transmitting equipment power for the WRT54GL is adjustable between 1 and 250 mW which translates into 0 to 24 dbm.

The receive sensitivity is not specified but it is estimated at around -85 db. High quality equipment has better sensitivity.

A sample calculation for a 12 km link follows:

Highest transmitted frequency: 2483.000 MHz (2.483 GHz)
Wavelength : 4.753 inches (12.074 centimeters)
Transmitter RF power output : 3.000 dBm (1.995 milliwatts)

Transmit cable type : Times Microwave LMR-600
Transmit cable length : 3.000 feet (0.914 meters)
Total transmit cable loss : 0.132 dB (0.044 dB/foot 0.145 dB/meter)
Total transmit connector loss : 0.500 dB through 2 connectors
Total transmit cable loss : 0.632 dB
Transmit miscellaneous losses : 2.000 dB

Transmit antenna peak gain : 24 dBi
RF input power to the antenna : 2.368 dBm (1.725 milliwatts)
Allowed input power to antenna : 24.000 dBm (251.189 milliwatts)
Transmit antenna height : 60.000 feet (18.288 meters)
Distance to the radio horizon : 10.629 miles (17.106 kilometers)

Receive cable type : Times Microwave LMR-400
Receive cable length : 3.000 feet (0.914 meters)
Total receive cable loss : 0.202 dB (0.067 dB/foot 0.221 dB/meter)
Total receive connector loss : 0.500 dB through 2 connectors
Total receive cable loss : 0.702 dB
Receive miscellaneous losses : 1.000 dB

Receive antenna peak gain : 24 dBi
Receive antenna height : 25.000 feet (7.620 meters)
Distance to the radio horizon : 6.861 miles (11.042 kilometers)

Received power level : -73.268 dBm (48.541 μ V)
Receiver's threshold : -85.000 dBm (12.574 μ V)
Operating margin : 11.732 dB
Probability of outage : 1 %
Total free space path loss : 121.933 dB over a path length of 7.456 miles (12.000 kilometers)
Peak transmitted EIRP : 24.368 dBm (273.386 mW)

Midpoint 0.6 Fresnel zone boundary : 48.354 feet (14.738 meters)
Maximum space wave communications distance : 17.490 miles (28.148 kilometers)

Apparently the link is viable. Please note that this calculation is valid for DIRECT LINE OF SIGHT links.

While most of the coefficients are constant for a particular setup, the free space loss seems to be the defining factor. Free space loss can be calculated using the following formula:

$$free\ space\ loss = \left(\frac{4\pi R}{\lambda} \right)^2 = \left(\frac{4\pi Rf}{c} \right)^2$$

The equation for free-space loss is below where λ is the signal wavelength, f is the signal frequency, R is the distance or radius of the signal from the transmitter, and c is the speed of light in the signal transmission medium. Note that the units used should be consistent, e.g., λ and R in meters, and c in meters per second.

There are many utilities on the internet that do the calculation automatically but I discovered that some are wrong. One that I have verified and apparently gets it right can be found at <http://my.athenet.net/~multiplex/cgi-bin/wireless.main.cgi>

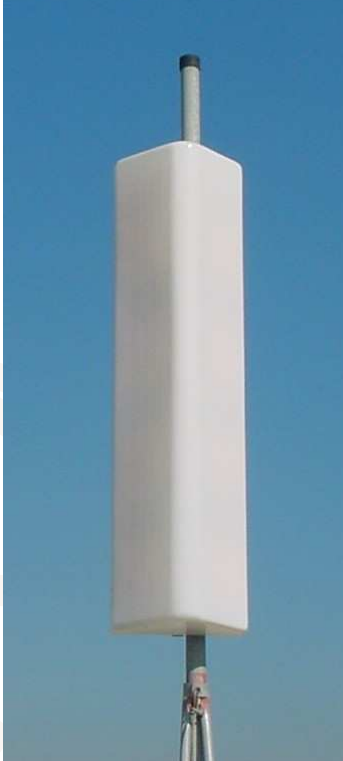
For indoor wireless links usually it is easier to test the wireless signal propagation than to calculate it. Just as a general reference:

Obstacle Attenuation	[dB]
Floor	30
Brick wall with window	2
Office wall	6
Metal door in office wall	6
Cinder block wall	4
Metal door in brick wall	12
Brick wall next to metal door	3

c. Choosing an antenna

For the reasons explained before, you should always use the highest gain antenna available while still remaining within legal limits.

Below are a few antenna types presented and their typical recommended scenarios:

	Omni directional Antennas Gain: 5-12dbi Recommended for camp coverage and indoor office applications. High gain omni antennas reduce signal radiation in the vertical plane so it is important to provide them the necessary tilt for a specific application. Ideally placed in the middle of the desired coverage area.
	Sectorial antennas Gain: 17-19 dbi Recommended for camp coverage (when you just can't place an omni in the middle), and for point to point links where you have a strong interfering signal at the "back" of the antenna.

	Parabolic grid antenna Gain: 19-27dbi Ideal for very long range links. Need careful aiming and are prone to interference.
---	---

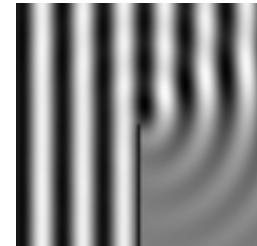
d. Extending the range

In real life situations you will discover that most of the situations are non line sight or the sight is obstructed. Non line of sight links are possible maybe up to 5 km depending on terrain. Longer non line of sight links are realizable only using repeaters.

Non line of sight link

A phenomenon called “knife edge diffraction” allows radio waves to propagate behind an obstacle (but with considerable loss). To better understand how signal propagates over an obstacle the attached image is relevant.

The estimated loss behind a 10m obstacle at 5 km is 8db (additional to the path loss).



Repeaters

A repeater is a device that receives a signal and retransmits it. It can be used to pass over obstructions. A typical receiver would sit on top of a hill and provide signal in a nearby valley. Using DD-WRT it is possible to use a WRT54GL for this purpose.

4. Configuring the devices

There are 3 basic operation modes for the wireless router:

- a. Access Point – provides link to a wired network, accepts wireless clients
- b. Client – Links a remote wired network to a wireless network, accepts only wired clients
- c. Repeater or WDS – Links two wireless networks, acts both as an AP (accepting wireless clients) and as a Client (connecting to a wireless network)

Repeater mode and WDS mode are recommended for specific situations. WDS (wireless distribution system) is recommended in situations with pretty strong signal (high capacity links) between the routers. Using WDS you can create a mesh of routers that can cover a wider area with wireless signal. It is suitable for scenarios where for example you wish to cover a camp with wireless signal and allow laptop users to roam between routers. The downside of this setup is that for every hop the capacity of the link is cut in half.

Repeater mode is suitable in situations where you wish to provide a link in a very remote location. Repeater mode has no major impact on bandwidth but it is harder to set up and does not permit roaming between. A suitable scenario for this setup is a standalone unit on top of a hill, providing wireless coverage into a valley.

a. Access point

There are five basic configuration changes required to set up your router as an access point.

Turn off DHCP

If you do not turn off DHCP, when you plug your router into the network (later) you will give other clients on the wired network ip addresses which are inappropriate for that network.

Set the IP address of the LAN Interface

Preferably immediately after turning off DHCP, while you still have the ip address the AP gave you, set the ip address of the LAN interface to the ip address you want the AP to use. Alternatively you can use the instructions below to set the APs ip address via DHCP.

If you can't connect to the AP to set the ip address, it is probably because your computer no longer has an IP address on the same subnet. Simply set your computer's ip address and subnet to 192.168.1.2 and 255.255.255.0 respectively. You should then be able to point your browser at 192.168.1.1.

LAN uplink through WAN port

If you use your DD-WRT router as AP only, you may use your DD-WRT router's WAN port to connect it to your existing LAN. To do this, you need to disable the Internet Connection and "assign WAN Port to Switch".

Normally, your router does layer 3 IP routing. By "assigning WAN Port to Switch", your DD-WRT router will bypass that functionality and just pass on the layer 2 ethernet packets from your wired network to the wireless network and vice versa.

Alternatively, if you have a router that supports assigning the WAN port to the switch:
Setup -> Basic Setup -> Internet Connection Type -> Connection Type = Disabled
Setup -> Basic Setup -> Network Setup -> WAN Port -> Assign WAN Port to Switch

Choose a channel and an operation mode

From Wireless->Basic Settings choose:

- AP mode
- Wireless Mode: B-only (for very long links), Mixed (for local links)
- Wireless channel 1 through 14 (according to your local regulations not all channels might be available)
- Sensitivity range 0 (needed just in case of long range links)

Encryption

From Wireless-> Wireless Security you have to choose an encryption mode. WEP is not recommended since it is flawed.

The easiest security mode to set up is WPA-Pre Shared key and it is considered secure with long keys. Use the same key on all the clients.

b. Client

Client mode wireless is generally used to "retrieve" an Internet connection (using the Wireless portion of the router) from another router, and then share it out to the LAN (wired switch ports). If you have a wireless router connected to the Internet in one location and would like to connect wired clients in a remote location to allow shared Internet, one solution is to use **Client Mode Wireless**. This will not require the host router to be running DD-WRT firmware. The WRT running DD-WRT firmware and configured to run in Client Mode will connect to the host router as though it were any other wireless client, and will share the wireless connection out the LAN (wired switch ports) as though the host router were connected directly to its WAN port. This means that the host router and the Client Mode router will be on separate subnets. NAT will be used between the routers, so when port forwarding is needed, it will need to be configured at both routers, not just the host router. Devices connected to the Client Mode router will not be able to use the DHCP server from the host router. Also, a device connected to the Client Mode router should use the Client Mode router as its gateway and DNS server.

Step 1

1. Select Wireless > Basic Settings tab
2. Set Wireless Network. Wireless Mode = Client
3. Set Wireless Network. Wireless Network Mode = Mixed (or B-Only if this is a very long range link)
4. Set Wireless Network. Wireless Network Name (SSID) = SUBSTITUTE_YOUR_ROUTER_SSID
5. Click Save Setting button

Step 2

The settings in this tab will vary depending on what security settings are configured on the ROUTER. Basically it is the same as you enter when connecting a laptop or any other wireless device with the ROUTER. I will use the example of WEP based encryption with a 64 bit hex key. If your ROUTER doesn't have any security settings, then this step can be skipped.

1. Select Wireless > Security tab
2. Set Wireless Security.Security Mode = WPA-Preshared (matching your AP)
3. Click Save Setting button

Step 3

1. Select Setup > Basic Setup tab
2. Set Wireless Setup.Internet Connection Type = Static IP
3. Set Wireless Setup.Internet IP Address = 192.168.1.2 (or whatever ip address you identified in step 2 of preparation)
4. Set Wireless Setup.Subnet Mask = 255.255.255.0 (same as assumption #3)
5. Set Wireless Setup.Gateway = 192.168.1.1 (Same as assumption #2)
6. Set Wireless Setup.Static DNS 1 = 192.168.1.1 (Same as assumption #2)
7. Set Wireless Setup.Static DNS 2 = aaa.bbb.ccc.ddd (Same as assumption #4)
8. Set Wireless Setup.Static DNS 3 = aaa.bbb.ccc.eee (Same as assumption #5)
9. Set Wireless Setup.Router Name = BRIDGE (doesn't matter what you name it)
10. Set Wireless Setup.Host Name = BRIDGE (doesn't matter what you name it)
11. Set Wireless Setup.Domain Name = Blank (unless you have a reason to enter it)
12. Set Wireless Setup.MTU = Auto
13. Set Network Setup.Local IP Address = 192.168.2.2 (increment the 3rd octet of the Wireless Setup.Internet IP Address field by 1, e.g 192.168.1+1.2. So now 192.168.1.2 is your ROUTER facing IP and 192.168.2.2 is your CLIENT network facing IP.
14. Set Network Setup.Subnet Mask = 255.255.255.0 (Same as assumption #3)
15. Set Network Setup.Gateway = 192.168.2.2 (Same as #13 above)
16. Set Network Setup.Local DNS = 192.168.1.1 (Same as #6 above)
17. Set Network Setup.DHCP Server = Enabled (To let the CLIENT issue dynamic IPs to the devices hooked up to it)
18. Set Network Setup.Starting IP Address = 192.168.2.100 (You may have to click on Save Settings button before you see 192.168.2 written in this field. If you do, make sure you connect back to the CLIENT using the ip address is #13 above)
19. Set Network Setup.WINS = 0.0.0.0
20. Click on Save Settings button. Notice that after this configuration, your CLIENT bridge/router has a different IP address for administration. So if you are not automatically redirected to the new IP, you may have to connect to the administration web page by typing 192.168.2.2 yourself. Also note that at this stage, you may not be able to connect to the new IP unless you are using a computer hooked up to one of the LAN ports of the CLIENT itself. And you may need to temporarily setup your computer's TCP/IP config to use a static IP in the 192.168.2.* subnet.

Step 4

These steps are temporary so that you don't run into any issues during setup. Once you have everything working, you can undo these settings one by one as long as your setup keeps working. Theoretically speaking, you shouldn't need to because your internal network is protected by the firewall of your ROUTER from the internet anyway. But if you are security conscious then you may want to undo these.

1. Select Security > Firewall
2. Set Firewall.Firewall Protection = Disabled
3. Set Firewall.Block Anonymous Internet Requests = unchecked
4. Click Save Settings button

At this point, you should be able to Click on Status > Wireless tab and see that you are connected to the ROUTER. You should also be able to hook up a device or computer to one of the four LAN ports of the CLIENT and notice that it obtains a dynamic IP like 192.168.2.100 or some number greater than 100. You should also be able to ping your ROUTER, i.e. ping 192.168.1.1.

c. Repeater

1. Install [DD-WRT v24 beta](http://www.dd-wrt.com/dd-wrtv2/downloads.php) (<http://www.dd-wrt.com/dd-wrtv2/downloads.php>)(v23 will not work).

- Build 2006-0911 is known to be stable for repeater mode. Users also report success with newer builds like 2006-1216.
- Keep ethernet cable connected for these instructions (to have connectivity across wireless network changes).

2. Go to tab "Setup", sub-tab "Basic Setup":

- Change "local IP address" to a unique subnet (different than device you wish to repeat), such as 192.168.69.1.
- Save settings.

DD-WRT CONTROL PANEL

Firmware: DD-WRT v24 Beta (09/10/0...)
Time: 09:08:38 up 3 days, 8:28, load average: 0.00, 0.00
WAN IP: 192.168...

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing | VLANs

Wireless Setup

Internet Connection Type

Connection Type: Automatic Configuration - DHCP

STP: ☒ Enable ☐ Disable (disable for COMCAST ISP)

Optional Settings (required by some ISPs)

Router Name: repeater

Host Name: repeater

Domain Name:

MTU: Auto 1500

Network Setup

Router IP

Local IP Address	192	168	69	1
Subnet Mask	255	255	255	0
Gateway	0	0	0	0
Local DNS	0	0	0	0

Help more...

Automatic Configuration - DHCP
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

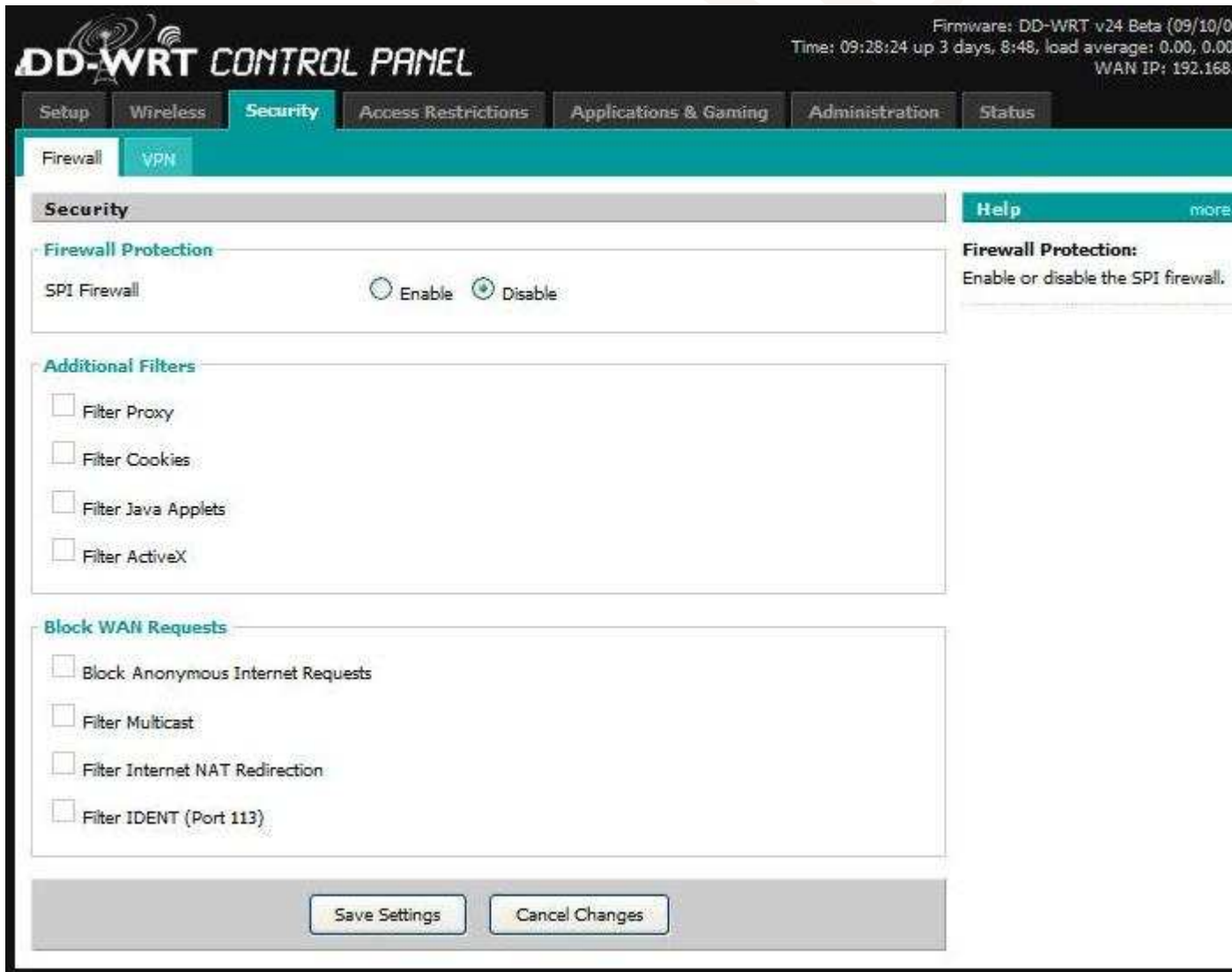
Subnet Mask:
This is the subnet mask of the router.

DHCP Server:
Allows the router to manage your addresses.

Start IP Address:
The address you would like to start with.

3. Go to tab "Security", sub-tab "Firewall":

- Disable all check boxes and set firewall to "disable".
- Save settings.



4. Go to tab "Wireless", sub-tab "Basic Settings":

- Set Wireless Mode to "Repeater"
- Click on "Add" under Virtual Interfaces, and enter an SSID (such as "repeater") and set "Wireless Network Name (SSID)" to the network you wish to repeat (and AP Isolation is "disabled" and Network Configuration is "Bridged"). If you want the source network (the one you're repeating) to be dynamically acquired, see steps below.
- Optional: Set Wireless Channel to "Auto" (or your preferred channel), and set Sensitivity Range to "0" for performance enhancements.
- Click "Save Settings".

DD-WRT CONTROL PANEL

Firmware: DD-WRT v24 Beta (09/10/0
Time: 09:32:06 up 0 min, load average: 0.53, 0.16
WAN IP: 192.168

Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status

Basic Settings
Radius
Wireless Security
MAC Filter
Advanced Settings
WDS

Wireless Physical Interface

Physical Interface wl0 - SSID [] HWAddr [00:16:01:2E:94:B6]

Wireless Mode

Repeater

Wireless Network Mode

Mixed

Wireless Network Name (SSID)

Wireless Channel

Auto

Wireless SSID Broadcast

☒ Enable
☐ Disable

Sensitivity Range (ACK Timing)

(Default: 2000 meters)

Wireless Network Mode:

If you wish to exclude Wireless-G clients, choose *B-Only* mode. If you would like to disable wireless access choose *Disable*.

Sensitivity Range:

Adjusts the ack timing. 0 disables a timing completely.

Virtual Interfaces

Virtual Interfaces wl0.1 SSID [repeater]

Wireless Network Name (SSID)

repeater

Wireless SSID Broadcast

☒ Enable
☐ Disable

AP Isolation

Disabled

Network Configuration

☐ Unbridged
☒ bridged

Add

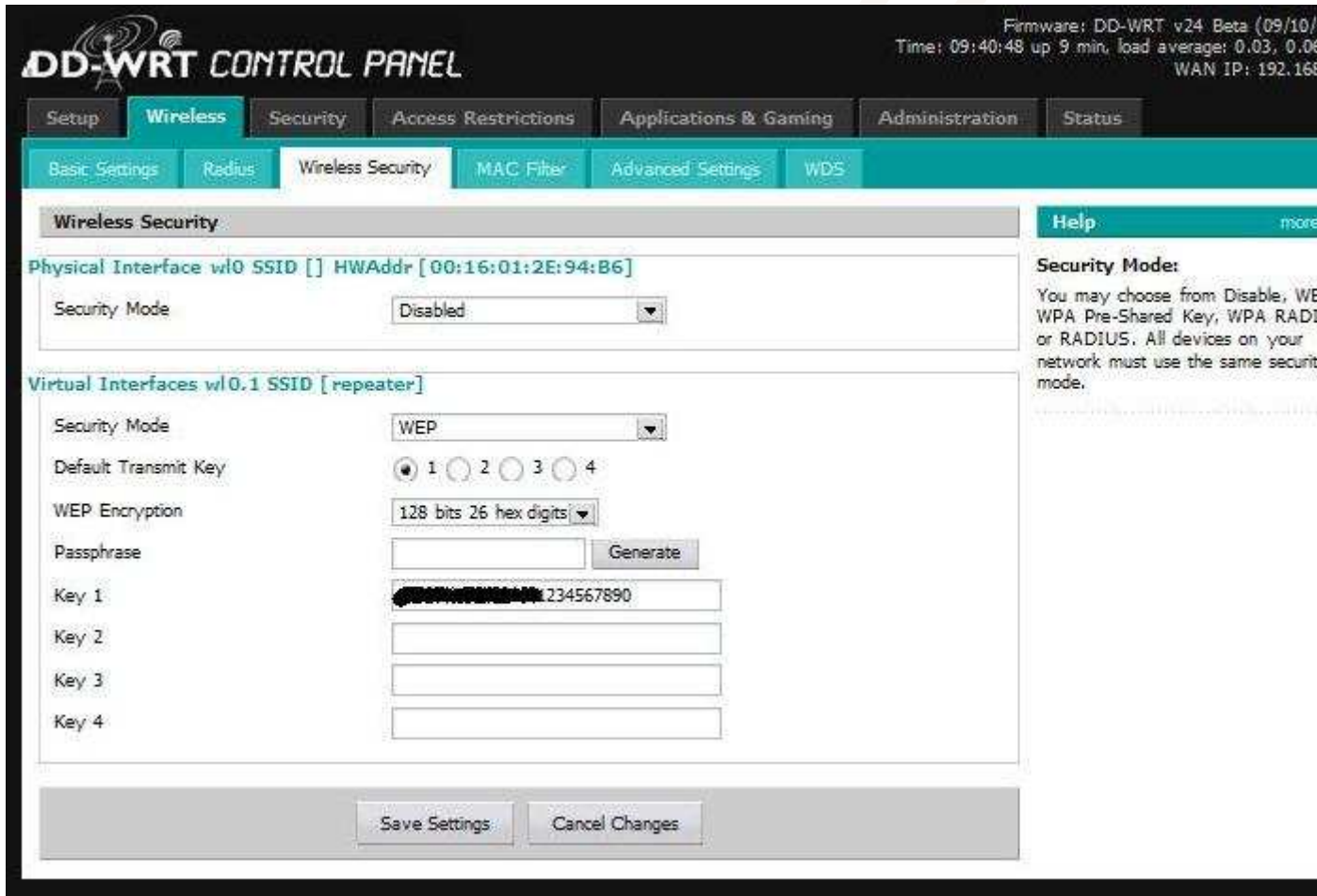
Remove

Save Settings

Cancel Changes

5. You may use security (WEP, WPA, etc) in repeater mode. An example application of this would be to make the repeated network private (for your use only).

- Go to tab "Wireless", sub-tab "Wireless Security".
- Setup WEP (or other security) under virtual interface.
- Configure your client/computer to use the same security.



- Notice in the screenshot above you may also configure security for the physical interface (source) network if you wish to repeat a secure network. In the example this is disabled. If you enable this, the dynamic repeating functionality may not work (since you're hard configuring the source network).
- Note: At this time, only one interface can have security - not both simultaneously. See "Known Issues" below.

6. The first time you connect to the repeater (wirelessly), or after disconnect, you may need to perform a "repair wireless network connection". For example, in XP, right click on the wireless icon and select "Repair".

d. WDS

WDS (Wireless Distribution Service) creates a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The WDS-enabled access points **can** accept wireless clients (e.g. wireless laptop users) just as traditional APs would. There is no free lunch, however: WDS consumes wireless bandwidth normally available to wireless clients.

Standard terminology for a two router setup:

- The **client router** is the router which does not have an internet connection.
- The **host router** is the router which does have the internet connection and is going to share it with other routers.

Two or more WRT54G / WRT54GS / WRT54GL boxes

Setup

1. Save the configuration on both routers: **Administration -> Backup**. Click "Backup" button and follow prompts so save nvram backup files, i.e. nvram_host.bin, and nvram_client.bin. The configurations can be restored if the setup doesn't work out and you need to quickly get back to a different (working) configuration.
2. Reset both routers to factory default settings so other settings will not have a possible conflict: **Administration -> Factory Default - select yes - click "Save Settings" button**.
3. Give both the routers a different IP address, i.e. 192.168.1.1 (host/internet gateway) and 192.168.1.2 ("client router") on the same subnet. **Setup -> Basic Setup**
4. Change the Internet Connection Type to Disable on the client router. **Setup -> Basic Setup -> Internet Setup -> Internet Connection Type -> Disable**
5. Set the Gateway IP address of the client router to the LAN IP address of the host router. **Setup -> Basic Setup -> Network Setup -> Router IP -> Gateway**
6. For each router, under **Setup -> Basic Setup -- Network Address Server Settings (DHCP) -- Start IP Address**, you may want to set different starting address for the different routers. For example host 192.168.1.1 starts DHCP at 100 and client 192.168.1.2 starts at 200. This will allow you to enable DHCP on both routers and know which router you are connecting to. This is helpful when connecting to your network with a wireless laptop so you know which router it is connecting to and for changing wireless power settings (both laptop and routers). Alternately, you can disable DHCP on the client router(s) and have only the gateway perform DHCP services.
7. On the client router, under **Setup -> Basic Setup -- Network Address Server Settings (DHCP) - - Static DNS 1,2,3** enter the DNS settings provided by your ISP. These can also be found from the host router under **Status -> Router -- Internet**.
8. Turn off the firewall on the client router. **Security -> Firewall -> Firewall Protection -> Disable**
9. Turn off security on both routers (this should already be done if you reset as above). Security can be re-enabled after all other steps are complete, but in order to minimize troubleshooting, it's best to get things setup with no security active. **Wireless -> Wireless Security -> Security Mode -> Disabled**
10. Put both routers into AP mode and on the same channel. **Wireless -> Basic Settings**
11. Under **Wireless -> Basic Settings**, set the SSID to your liking. For WPA WDS, the SSID for the routers needs to be the same. For WEP, different SSIDs can make troubleshooting easier.
12. If you plan to use WPA later, then select **G-only** in **Wireless -> Basic Settings**. You cannot use B-only with WDS.
13. Open WDS configuration on both routers. **Wireless -> WDS**
14. On each router, you will see its wireless MAC address at the top of the **Wireless -> WDS** page. Put each router's MAC into the table of the other router, and select **LAN** for the type. Note that this MAC address is different from the one that may be printed on your case!
15. There is no need to enable **Lazy WDS** or **WDS subnet** on either router.
16. Test that you can ping the gateway from the client. Note that it may take a short amount of time for the WDS to be established, and you may need to reboot both the gateway and the client.
17. Enable encryption now, if you like (highly recommended).

5. Deployment

Before deploying the equipment in the field, always test it locally.

Test the following:

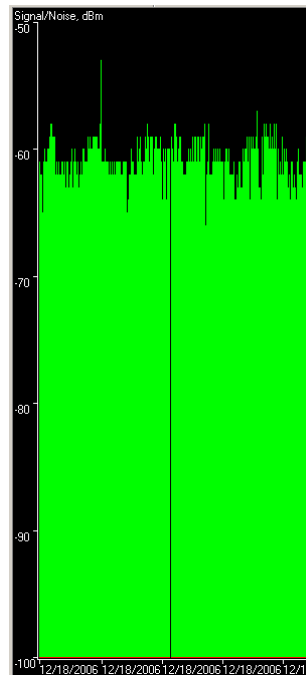
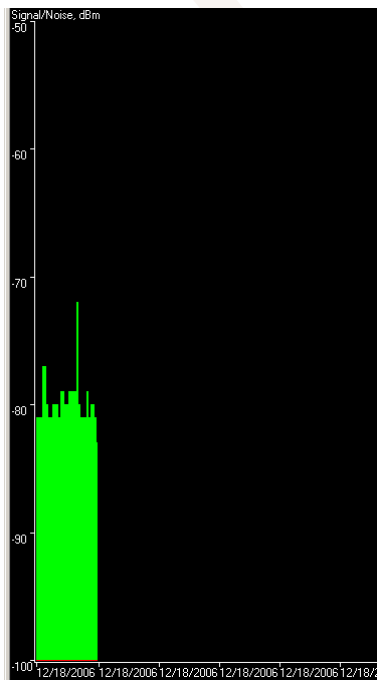
- working configuration
- working power supply
- proper interconnection with the antennas
- antenna gain
- stable configuration (power cycle the routers, see if they return to a working configuration with no intervention)

a. Testing

While most of the steps are fairly trivial I will detail the method for testing antenna gain. Without specialized equipment (like a RF signal meter or a high speed oscilloscope) this is not exact science but it can give you a very good idea if your antenna is working and properly connected.

Using software like netstumbler you can graphically display the strength of the RF signal as received by your wireless card in your computer.

Here is a sample output from a IBM T42 laptop about 100m away from a WRT54GL AP, using it's stock omni antenna, vs. the same setup but with a CalAmp 24dbi antenna connected to the AP:



As seen, there is a considerable gain in signal level. Even if the gain displayed is about 20 dbi (as expected) this values are not reliable and are highly dependent on the computer's wireless card firmware.

b. Other issues

In field deployment always involves a bit of experimenting, especially for long range links. Pointing antennas might be frustrating and involves time consuming fine adjustments. The ideal tool for aligning antennas is a GPS unit with an integrated electronic compass (a minimal unit would be the Garmin GEKO 301). A simple GPS unit is NOT enough as it will point direction only when moving.

Take your time in adjusting the antennas at both ends, double check the equipment configuration and connections.

Trust your calculations, if they say the link is possible, it will work.



Always use polycarbonate weather sealed boxes to host your equipment. The closer the equipment is placed to the antenna, the lower are the cable losses. You can power the equipment by using the pair 7 and 8 of the ethernet cable.

6. Wireless links at the RMW project

The current status (as of 18 December 2006) of the wireless links at the RMW project that are realized using the described technology is the following

a. Long Range

The long range links at the Savadisla camp are supported by a WRT54GL unit connected to a CalAmp 24dbi antenna facing EES. The system can provide link along the alignment for up to 20km (depending on the terrain). The current active links are:

- Camp to km29
- Camp to km26 (via repeater on top of hill)



Map of the links with simulated 12.5 degree beamwidth.

Note: Km32 has also been surveyed and a link can be provided there but it's not needed anymore.

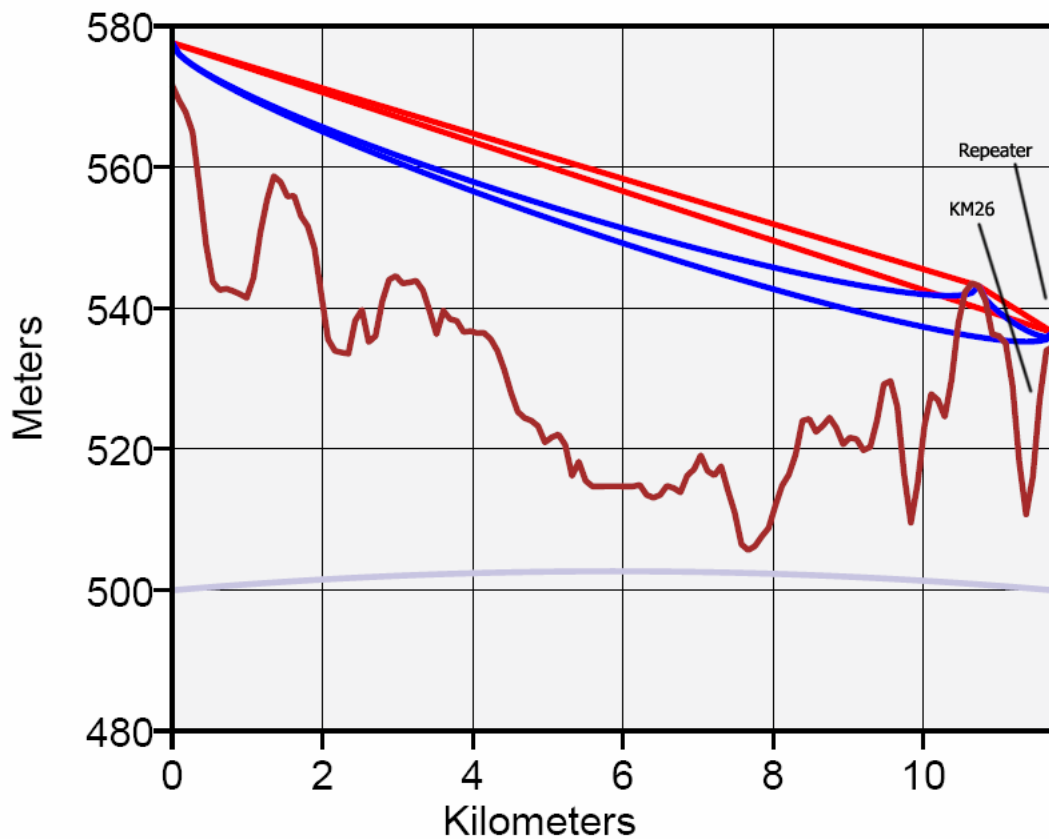
Camp to km29

This is an 8km link with direct line of sight. The average raw data rate is 5.5 Mbps.



Camp to km 25

This is a non line of sight link achieved via a repeater placed on the top of a hill further away than the actual camp. The distance from camp to repeater is about 12km. The profile of the terrain is displayed below:



As seen, it would have been impossible to connect KM26 directly due to the non line of sight situation.

The average raw data rate of the camp to km26 link is about 2Mbps. While theoretically a higher data rate could be achieved, the repeater is placed relatively close to high voltage power lines.

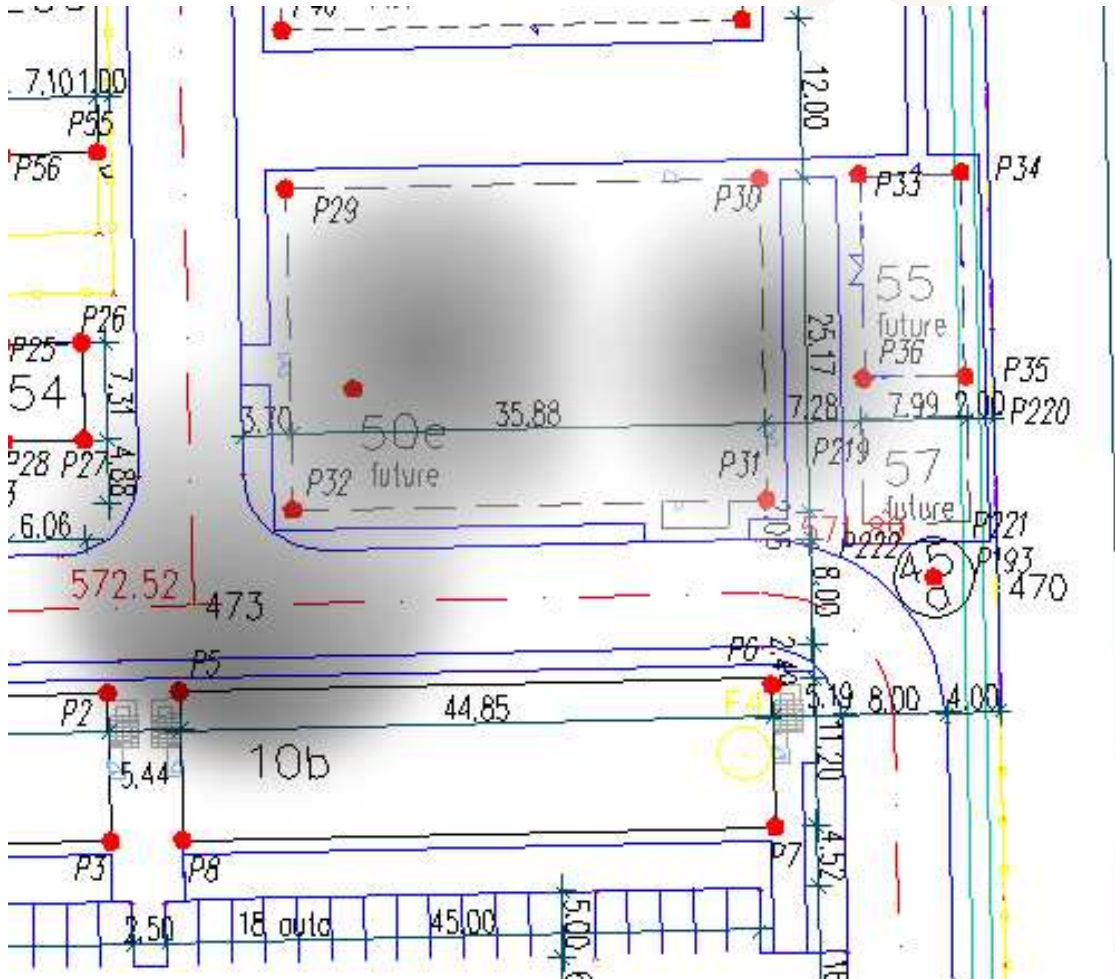




b. On camp

The construction of living quarters in the camp area required the introduction of internet access in the dorms. We decided to provide this access using wireless equipment, via the technology described here. The

service is provided by means of a root AP and WDS configured devices. This way, users have perfect signal over a wide area.



Simulated coverage area and router interaction.

Since the area is fairly small, we can use WDS even over 2 hops. The lowest raw speed achieved is at least 5.5 Mbps.