This will separate the ports on the back of your router and allow you to create individual networks that can?t see each other but that can still browse the internet. Note: Anything with < > around it needs supplemental information? Note: Anything with ? ? around it needs to be typed exactly as stated, except items in < >?

Contents

New Instructions

The following instructions were written specifically for DD-WRT v24 preSP2 running on the WRT54GS 1.0, but they should work fine on any router that supports VLANs.

2018: Instructions updated to work with routes that have vlan1 and vlan2 as default, instead of vlan0 and vlan1. There are additional nvram corrections needed based on your router. Do everything listed here, then Telnet or SSH into the router and take care of necessary NVRAM detail. See Switched Ports.

Preparation (OPTIONAL)

1. Reset router to Factory Default settings. Reset either by using the web interface or by doing a 30-30-30 Hard Reset.
2. Go to http://192.168.1.1/ in your web browser and set the Username and Password.
3. Configure Internet access as necessary.
4. Go to Setup -> Basic Setup.
5. Set the "Router Name" to whatever you desire.
6. Set the "Time Settings" appropriately.
7. Click Save, then Apply Settings.
8. Unplug the power for 30 seconds and then plug it back in. Wait for the lights to return to normal.
9. Ensure that Internet access is working properly.

VLAN configuration of ports 1, 2, and 3

1. Go to http://192.168.1.1/ in your web browser.
2. Go to Setup -> VLANs.
3. Uncheck ports 1, 2, and 3. Place port 1 into VLAN3, port 2 into VLAN4, and port 3 into VLAN5.
4. Your configuration page should look like this.
5. Click Save, then Apply Settings.
6. Plug your Ethernet cable into port 4 on the router if it is not already there.
7. Unplug the power for 30 seconds and then plug it back in. Wait for the lights to return to normal.
8. Go to Setup -> Networking.
    - NOTE: Do not set the following IP addresses to any subnets that already exist. In the 192.168.x.x address range, the third octet (the first "x") designates the subnet. In this tutorial, I'll assume that you are only using the 192.168.1.x subnet up to this point.
9. Under "Port Setup" set VLAN3 to Unbridged.
10. Set the IP Address to 192.168.2.1
11. Set the Subnet Mask to 255.555.255.0
12. Under "Port Setup" set VLAN4 to Unbridged.
13. Set the IP Address to 192.168.3.1
14. Set the Subnet Mask to 255.555.255.0
15. Under "Port Setup" set VLAN5 to Unbridged.
16. Set the IP Address to 192.168.4.1
17. Set the Subnet Mask to 255.555.255.0
18. Click Save.

The "Port Setup" section

1. Under DHCPD click Add.
2. Set DHCP 0 to vlan3 with a Leasetime of 1440 (24 hours).
3. Click Save.
4. Under DHCPD click Add.
5. Set DHCP 1 to vlan4 with a Leasetime of 1440 (24 hours).
6. Click Save.
7. Under DHCPD click Add.
8. Set DHCP 2 to vlan5 with a Leasetime of 1440 (24 hours).
9. Click Save.
10. Click Apply Settings.
11. The DHCPD section should look like this.
12. Plug your Ethernet cable into any port on the router aside from port 4 or the WAN port.
13. Unplug the power for 30 seconds and then plug it back in. Wait for the lights to return to normal.

VLAN configuration of port 4

1. Go to http://192.168.1.1/ in your web browser.
2. Go to Setup -> VLANs.
3. Uncheck port 4 and place it into VLAN6.
4. Click Save, then Apply Settings.
5. Unplug the power for 30 seconds and then plug it back in. Wait for the lights to return to normal.

6. Go to Setup -> Networking.
7. Under "Port Setup" set VLAN6 to Unbridged.
8. Set the IP Address to 192.168.5.1
9. Set the Subnet Mask to 255.555.255.0
10. Click Save.
11. Under DHCPD click Add.
12. Set DHCP 3 to vlan6 with a Leasetime of 1440 (24 hours).
13. Click Save, then Apply Settings.

Add Firewall rules to isolate the VLANs

1. Go to Administration -> Commands. Or enter them via SSH.
2. Copy and paste the following commands into the textbox:
```
iptables -I FORWARD -i vlan+ -o vlan+ -j DROP
iptables -I FORWARD -i vlan+ -o vlan1 -j ACCEPT
iptables -I FORWARD -i vlan1 -o vlan+ -j ACCEPT
```
3. Click "Save Firewall".
    - Command 1 Notes
      This command blocks communication between all VLANs.
    - Commands 2 and 3 Notes
      These commands allow all VLANs to communicate with VLAN1. VLAN1 contains the WAN port making communication with it necessary for Internet access (under most Internet access configurations). Please note that these commands may not do the trick, as I was unable to test them due to my Verizon FiOS setup.
    - Additional Commands Notes
      This command blocks all communications with the 192.168.6.x subnet. This command should be alerted and/or duplicated to block each subnet used by any additional routers on your LAN.
      ```
      iptables -I FORWARD -s 192.168.6.0/255.255.255.0 -j DROP
      ```
4. Finalize Settings
5. Go to Setup -> Basic Setup.
6. Click Save, then Apply Settings.
7. Unplug the power for 30 seconds and then plug it back in. Wait for the lights to return to normal.

http://www.dd-wrt.com/phpBB2/viewtopic.php?p=637106#637106

Old Instructions

Assumptions:

1. You have DD-WRT v23 SP2 installed and working to your liking.
2. You know the Login & Password for web administration.
3. You're running a Microsoft based operating system, Mac or Linux box.

How will this work?

1. First it separates the ports from each other.
2. It activates a DHCP server for each network.
3. We tell the DD-WRT that we have changed the VLANs.

Procedure:

1. Telnet into the router.

Note: You don?t have to separate all of the ports, remove the sections that don?t apply to your needs and make sure to add that port in to the very first line of text to copy. Example: if you don?t want port 2 to be on its own network and would like to share that port with port 1 then the first line would read: ***?nvram set vlan0ports=?1 2 5*?****, and just delete the sections that apply to* ***vlan2****.*

2. Text to copy:

(Added by tetech: For the uninitiated, its worth noting that the port numbers don't necessarily correspond with how they are numbered on the back of the device. For me, "port 4" was the WAN port, and ports 0-3 corresponded to the labels 1-4 on the back of the device.) (Added by Wayland: actually I believe on the WRT54GL and V4 the ports are actually numbered 4 3 2 1 0 corresponding to WAN 1 2 3 4. Just to confuse further the VLAN settings on the web interface the numbers should read W 4 3 2 1. See http://wifi.frubsd.org/_media/wrt54_sw2_internal_architecture.png)

```
nvram set vlan0ports="1 5*"
nvram set vlan2ports="2 5*"
nvram set vlan3ports="3 5*"
nvram set vlan4ports="4 5*"

nvram set rc_startup='
#!/bin/ash
PATH="/sbin:/usr/sbin:/bin:/usr/bin:${PATH}"

ifconfig vlan2 <router address on vlan> netmask 255.255.255.0
ifconfig vlan3 <router address on vlan> netmask 255.255.255.0
ifconfig vlan4 <router address on vlan> netmask 255.255.255.0

ifconfig vlan2 up
ifconfig vlan3 up
ifconfig vlan4 up
'

nvram set rc_firewall='
iptables -I INPUT -i vlan2 -j ACCEPT
iptables -I FORWARD -i vlan2 -o vlan1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i vlan2 -o ppp0 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i br0 -o vlan2 -j logdrop

iptables -I INPUT -i vlan3 -j ACCEPT
iptables -I FORWARD -i vlan3 -o vlan1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i vlan3 -o ppp0 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i br0 -o vlan3 -j logdrop

iptables -I INPUT -i vlan4 -j ACCEPT
```

```
iptables -I FORWARD -i vlan4 -o vlan1 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i vlan4 -o ppp0 -m state --state NEW -j ACCEPT
iptables -I FORWARD -i br0 -o vlan4 -j logdrop
'
nvram commit
```

Notes:

a) If you have your WLAN detached, you should write new rules for eth1 (WLAN port), not allowing traffic from br0 to eth1, and from eth1 to br0 (for your bridged vlans); and so on for all detached vlans you have, but vlan1 (default WAN port).

b) Probably you don't have ppp0 port, so don't write rules related with.

3. Open the Web Administration of the router by going to its IP address then:

4. Administration Tab --> Services Tab --> Under DNSMasq paste the following:

```
interface=vlan2
dhcp-option=vlan2,3,<router address on vlan>
dhcp-range=vlan2,<start ip>,<end ip>,<net mask>,<lease time>
interface=vlan3
dhcp-option=vlan3,3,<router address on vlan>
dhcp-range=vlan3,<start ip>,<end ip>,<net mask>,<lease time>
interface=vlan4
dhcp-option=vlan4,3,<router address on vlan>
dhcp-range=vlan4,<start ip>,<end ip>,<net mask>,<lease time>
```

Notes:

a) Take care of setting the correct vlan for each dhcp-option and dhcp-range, because if you don't say which parameter is for, DNSMasq couldn't know how set up more than one DHCP server (it doesn't depend on the order you write those lines).

b) When you set up router address and range with dhcp-option and dhcp-range, vlan address is set up automaticly without using ifconfig command (I've seen v24sp1 makes for you).

5. Click on ?Save Settings?

6. Setup Tab --> VLANs

- Set ?Port 2? to ?VLAN 2?
- Set ?Port 3? to ?VLAN 3?
- Set ?Port 4? to ?VLAN 4?

7. Click on ?Save Settings?

8. Reboot the router.

9. Now test your networks?

A Word Document of this with an example can be found at Detached Networks By Ports.doc (Main webserver down, unknown return time for listed file...)

Created by: bordr415 Modified by: JC

GUI Tutorial

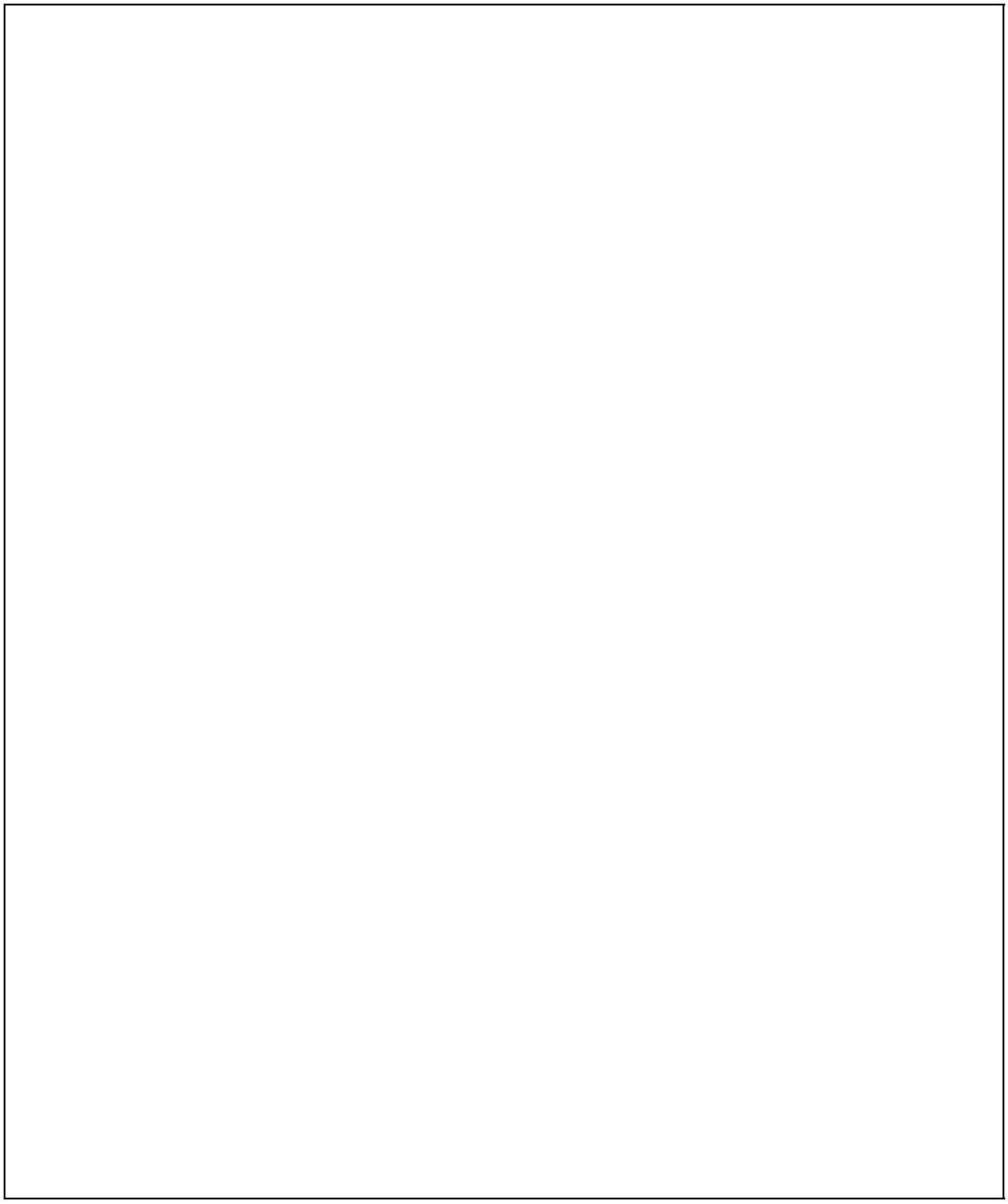
Tested with firmware DD-WRT v24-sp2 (01/02/09) std @ WRT54G V2.2
Thanks to pepe

Goal

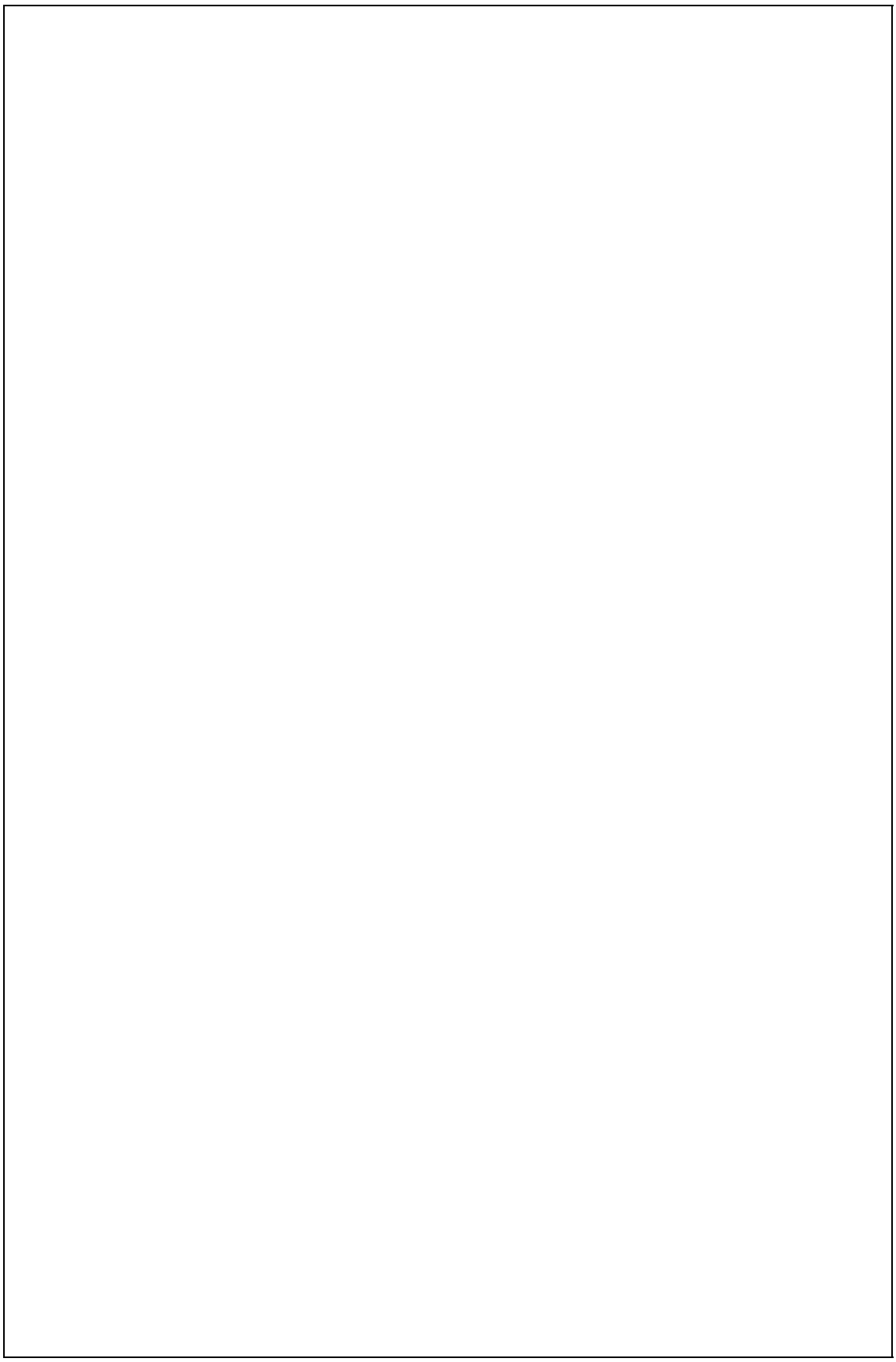
- seperate LAN port 2 from LAN port 1,3,4
- all clients are configured to use DHCP
- internet access for all clients

Procedure

Step 1: Settings in Setup > VLANs



Step 2: Settings in Setup > Networking



After these steps all clients are able to retrieve an IP via DHCP, can access the internet and each other. To deny the access each other go to Step 3.

Step 3: Firewall Settings in Administration > Commands

Type in ?Commands?:

```
iptables -I FORWARD -i br0 -o vlan2 -j DROP
```

and click ?Save Firewall?