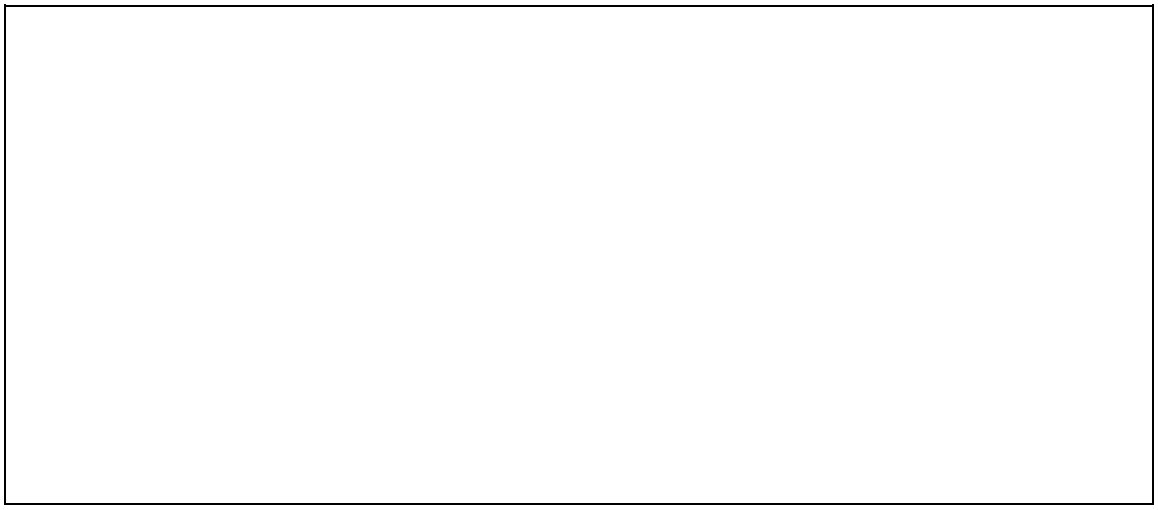
Contents

Introduction

Note this is an old and most likely out of date wiki page. The procedure below has not been verified.

This article describes how to set up dd-Wrt to provision a public CIDR routed over a dynamic WAN connection and a private IP space served by DHCP



Background

The reasons for developing this procedure was two-fold.

1. The way public IP space is delivered by my ISP as described above.
2. Having many TCP and UDP connections because of operations going on in the public CIDR space. The older dd-Wrt builds using the 2.4 kernel support 4096 maximum connections of which only 512 can be alive at any give time. The 512 live hashsize storage is a compile time parameter that can not be changed. The 2.6 kernel allows the number of connections to be set at run time and the size of the hashtable to store live connections to be modified in the /proc system table, hence my reqirement for a 2.6 kernel.

See this forum thread for more information on that subject
K2.6 Increase Maximum Connections ip_conntrack_max hashsize

Hardware, Firmware

The assumption for this HOWTO is that you know how to flash your router with dd-Wrt.

I developed this procedure on a WRT54G-TM Linksys/T-mobile router. The router is flashed with dd-wrt.v24_mega with a kernel 2.6 kernel, build 13972. This procedure should work with other 2.6 kernel builds however I have not verified this.

ISP public CIDR delivery

The network configuration has a either a static or dynamic IP address on the WAN side that is not in the same range as the routed subnet. This is a common way provision static sub-nets in the US for AT&T and Sonic.net (probably others as well). Other providers may use similar methods of delivering service using PPOE.

Basic Setup

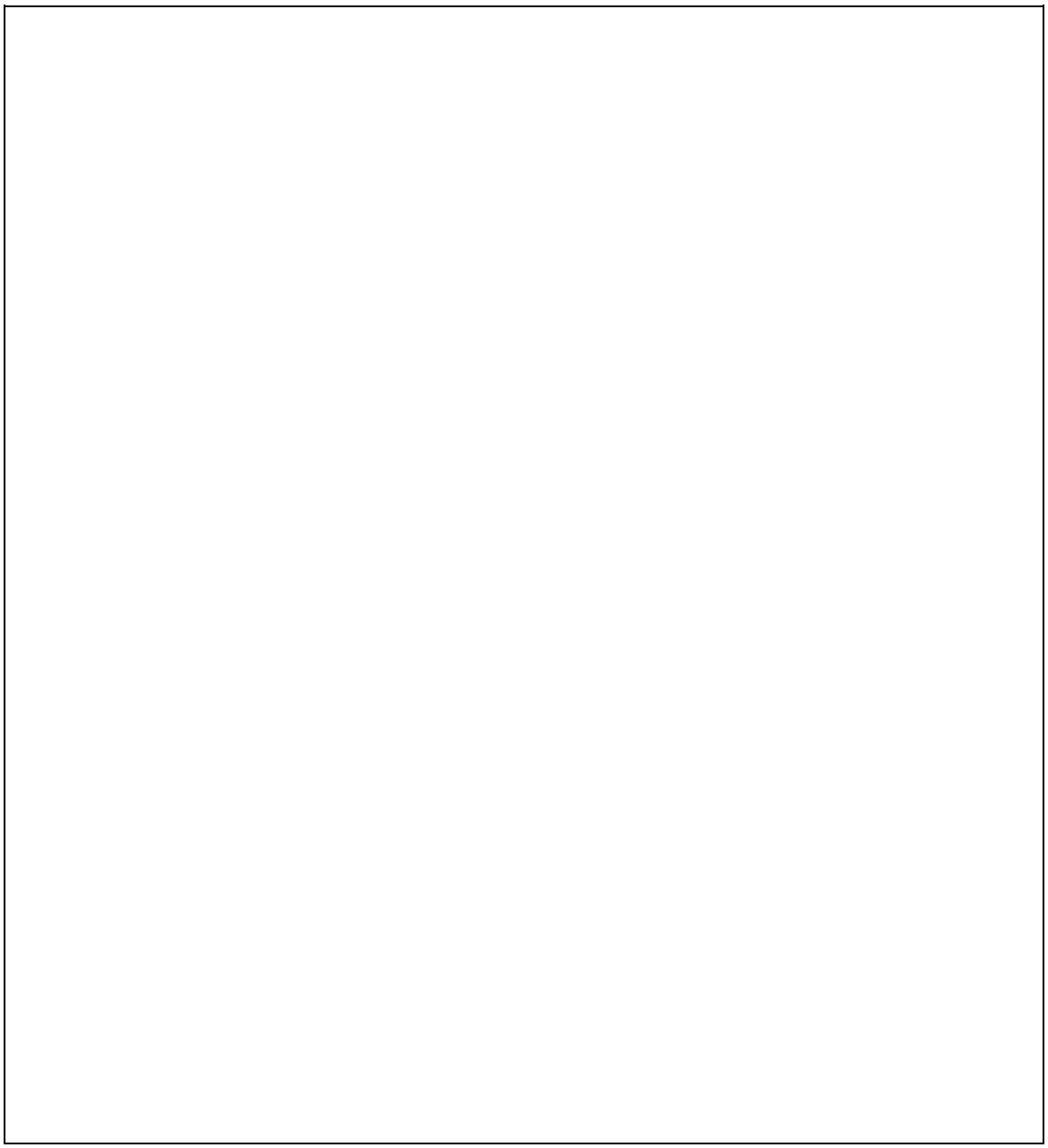
Hard resetting the router to its initial state is recommended before configuring using this procedure. See your hardware's instructions on how to properly hard reset it.

Set up the connection for the WAN and LAN as you would if there were not a routed public CIDR block. The WAN connection should be set up per the ISP's directions for static, dynamic, or PPPoE connection. The LAN should be set with a private IP for your NAT'd segment.

The WAN port is commonly in **vlan1** while the LAN and WIFI are connected to the internal bridge **br0**. We will create a new VLAN by splitting off two of the LAN ports for our routed public CIDR block.

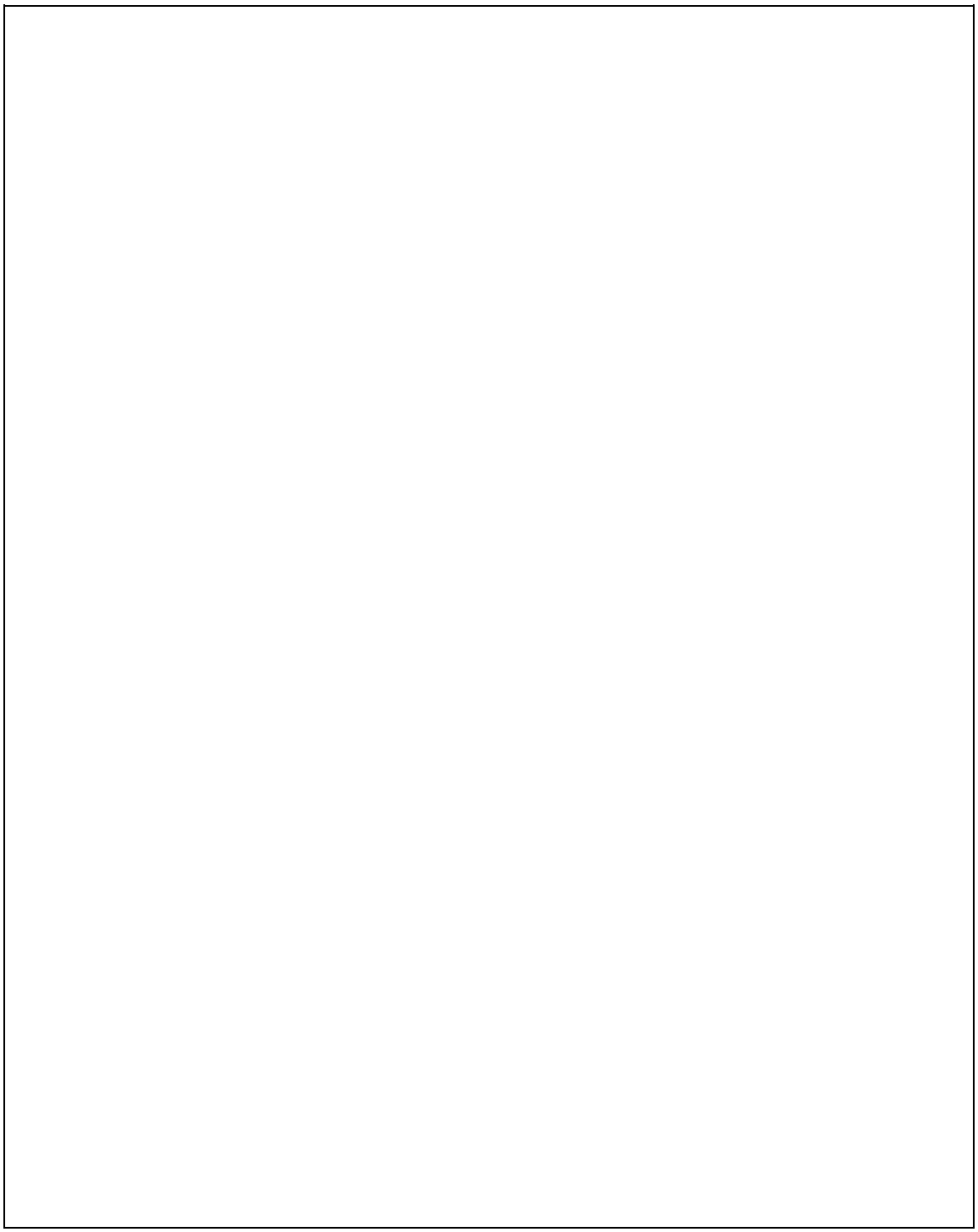
To create a new VLAN (**vlan2** in this case), open the web interface to the router.

- Go to SETUP -> VLANs
- In VLAN 0 uncheck ports 3 and 4
- In VLAN 2 check ports 3 and 4
- Leave VLAN 2's bridge assignment set to None
- Press Apply Settings and then reboot the router



The next step is to set up the IP space for the new VLAN **vlan2**

- Go to Setup -> Networking
- In the Port Setup section set Network Configuration vlan2 to Unbridged
- Set Masquerade / NAT to Disable
- Assign a usable IP address from your public block of addresses
- Assign the correct subnet mask for your public block of addresses



To finish the configuration we must add iptables rules for **vlan2**.

- Go to Setup -> Advanced Routing and verify that the router is in Gateway mode to NAT the private LAN.
- Go to Administration -> Commands and enter this script in the command box after editing it *with your IP addresses*

```
PUBLIC="66.55.44.0/28"
# optional BASTION host
```

```
BASTION="66.55.44.2"
WANIP=`nvram get wan_ipaddr`

# disable NAT for PUBLIC => WAN
iptables -t nat -I POSTROUTING -s $PUBLIC -j ACCEPT

# allow traffic to routed PUBLIC net
iptables -I FORWARD -o vlan2 -j ACCEPT

# block PUBLIC -> LAN, allow LAN -> PUBLIC
iptables -I FORWARD -i vlan2 -o br0 -m state --state NEW -j DROP

# block access to the router GUI/telnet/DNS/etc. from PUBLIC net, allow from BASTION host
iptables -I INPUT -i vlan2 -j DROP
iptables -I INPUT -s $BASTION -j ACCEPT

# block access to WAN IP from PUBLIC net
iptables -I INPUT -i vlan2 -d $WANIP -j DROP
```

- Press Save Firewall
- Reboot the router

Acknowledgements

The original idea for this came from a procedure written by Odel Arbel at:

setting-up-dmz-with-multiple-static-ips-on-an-office-lan-using-dd-wrt

The procedure I developed worked on 2.4 kernels but was awkward to say the least. When the requirement for a larger hash table size came up I posted to the dd-wrt forum in this thread:

ddwrt locks up with high active connection count

and with the help of "phuzi0n, DD-WRT Guru" the procedure in this HOWTO was generated.

enjoy, Miker Michael Robinton, michael(at)bizsystems.com