OpenWRT Introduction

Enterprise Security on low cost hardware

Parth Shukla,
pparth@pparth.net

Hardware Specifications for WD N600

- RAM: ~128 MB (real available about 123 MB – why? Info in `dmesg`)
  - Can be checked by running command `free` or `cat /proc/meminfo`
- Flash: ~16 MB (real available about 11 MB due to core taking up rest)
  - Can be checked by looking at output of `df -h`.
  - This is actually plenty of storage to easily do everything we want and more.
- CPU: 560 Mhz (that's really good for an embedded system)
  - Can be checked by reading through the output of `dmesg` after boot
- 5 x 100 MB/s ports, 1 x 2.4 GHz Antenna, 1 x 5 Ghz Antenna, 1 x USB 2.0 port
- VLAN support (through AR934X built-in switch in eth0 only)

➢ Western Digital N600 costs ~$50 at umart.com.au: http://umart.com.au/pro/products_listnew.phtml?id=10&id2=20&&bid=2&sid=107092

Firmware Flash

Upgrading your route to the Internet

Introduction

Everything Has to start somewhere

What is OpenWrt?

- “OpenWrt is an operating system / embedded operating system based on the Linux kernel, and primarily used on embedded devices to route network traffic.” (Wikipedia)
- “OpenWrt provides a fully writable filesystem with package management. This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application.” (opnewrt.org)
- Mainly GPL – but other free licenses also included
- Due to use of Linux and Package Management, OpenWrt is extremely powerful in utilising low cost hardware to its maximal potential.
- If other Linux distros can do it, good chances OpenWrt can too.

Why OpenWrt?

- Customisation and full control
- Linux and Package Management
- GPL
- Huge Feature set (over 3400+ packages and growing)
- Still actively developed
- Extremely easy to deploy and manage
    - Can be scripted if you want to manage a fleet of them
- For people with Linux in their network already, this can be considered just another Linux box.
- Developed to be deployed on low cost hardware

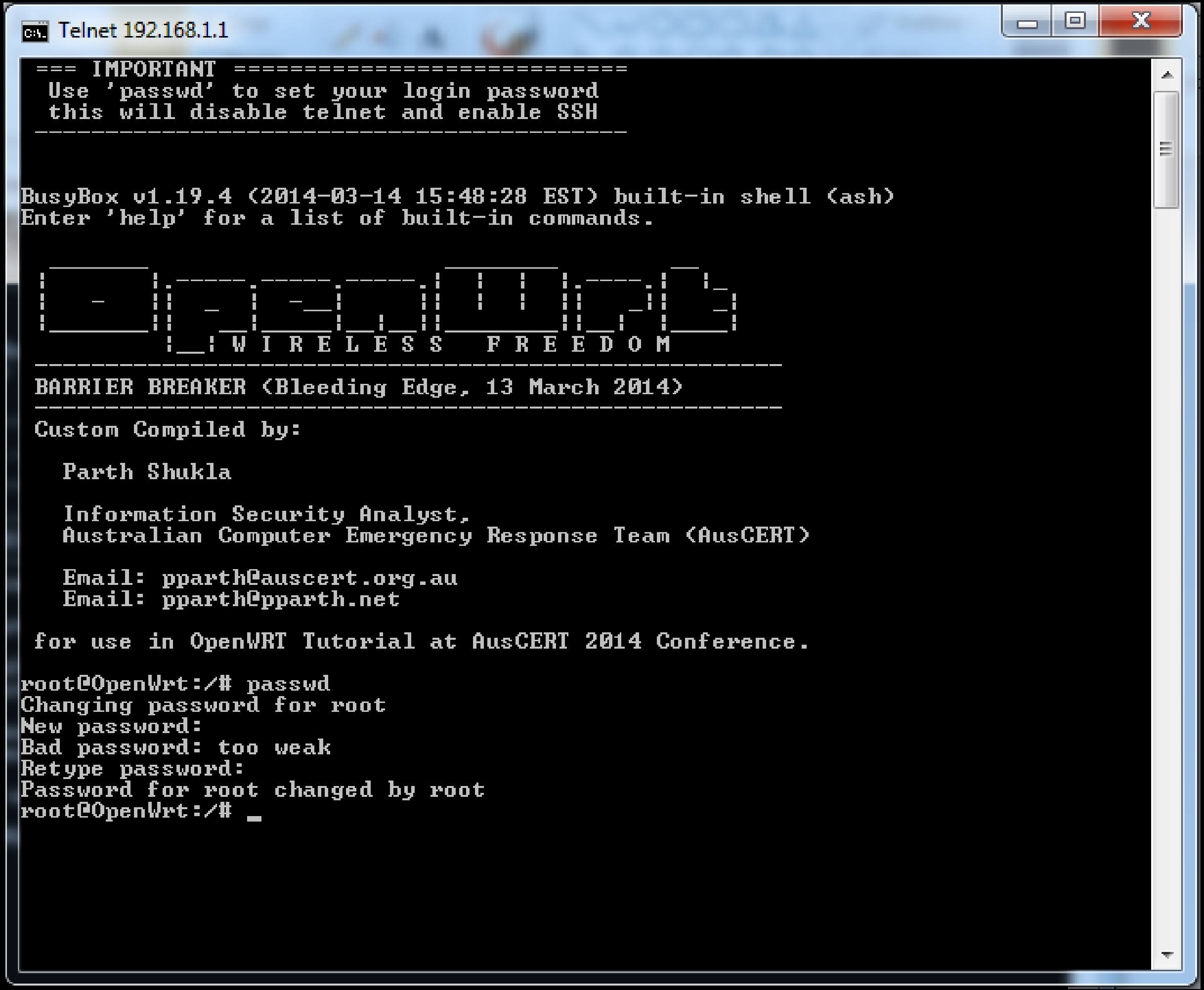
My personal reasons for loving it?

- All of the above and
- 99.99% of time, working on OpenWrt or applying changes has no effect on current network operations or traffic
- Most modern home/SOHO routers need to "reboot" after you have applied some fairly simply change (sometimes just for adding a new device in the 'allow' list.)
- With OpenWrt, almost anything you do, can be applied 'live' without interrupting current network connections.
- Restarting firewall? No worries. Restarting DHCP? No one will be the wiser!

Logging into OpenWrt

There’s a first for everything!

First Login – telnet (cont.)



```
 === IMPORTANT ============================
  Use 'passwd' to set your login password
  this will disable telnet and enable SSH
 ------------------------------------------


BusyBox v1.19.4 (2014-03-14 15:48:28 EST) 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 (Bleeding Edge, 13 March 2014)
 -----------------------------------------------------
 Custom Compiled by:

   Parth Shukla

   Information Security Analyst,
   Australian Computer Emergency Response Team (AusCERT)

   Email: pparth@auscert.org.au
   Email: pparth@pparth.net

 for use in OpenWRT Tutorial at AusCERT 2014 Conference.

root@OpenWrt:/# passwd
Changing password for root
New password:
Bad password: too weak
Retype password:
Password for root changed by root
root@OpenWrt:/# _
```

OpenWrt Basics

Everyone should start with BASIC and work their way up.

OpenWrt is built on BusyBox

Commands to find Hardware Info *

- Memory:
  - ❑ `free`
  - ❑ `cat /proc/meminfo`
- Disk Space:
  - ❑ `df -h`
  - ❑ `cat /proc/mtd`
  - ❑ `cat /proc/partitions`
- For CPU normally run:
  - ❑ `cat /proc/cpuinfo`
  - But this will not reveal Mhz in our case. We can get that from `dmesg` instead

Other Commands to find Info *

- Other info:
  - ❑ `dmesg` (kernel messages)
  - ❑ `logread` (system log messages)
    - Only a certain number of lines are buffered here, older lines are deleted as newer ones are added. `logread` is filled more often then `dmesg`
    - You can redirect these messages to your own log server
  - ❑ Read through the output of these command to see what we find

❑ps (process list)

❑Press “tab” twice at the command prompt

- You’ll see almost all commands available on OpenWrt
- Shell commands won’t be in that list!

Modifying files

- `vi` is the default editor on OpenWrt
  - However, it is **NOT** intuitive if you are not familiar with it
  - If you are familiar with `vi` then you can use it throughout the day
    - Who is familiar with `vi`?
  - It is not easy to quickly learn `vi`.
  - We cannot spend anytime today teaching or learning `vi`

- If you don’t know `vi` then WinSCP can be used to easily edit files on OpenWrt
  - This is already installed on your laptop today
  - It can be downloaded and installed from: http://winscp.net/eng/download.php

Package Management *

- The opkg command is used for managing packages on OpenWrt

❑ opkg

- What possible things can be done?

❑ opkg list-installed

- This will give you the bare minimum system that's currently installed

❑ okpg info ubusd

❑ opkg info firewall

❑ opkg files firewall

❑ okpg files ubusd

❑ opkg search /etc/firewall.user

❑ opkg print-architecture

Installing Web Management Interface

Why get your hands dirty on the keyboard if clicking through a pretty interface can get the job done

Everyone loves web management *

- The luci and luci-ssl packages provide web interface to OpenWrt
  - luci-ssl will install luci as well.
  - luci-ssl will obviously allow web management using SSL
- Find out what each package is about and what it contains:
  - ❑ `opkg info luci`
  - ❑ `opkg info luci-ssl`

❑ `opkg install luci-ssl –noaction`

  - Just to see what will be done

- When you’re happy and ready to install, go for it:
  - ❑ `opkg install luci-ssl`

Web Interface Notes

- WMI comes in handy in many ways.
- Web Management Interface is just an ‘interface’.
  - Everything we’ll do today using the Web Interface can be done using command line.
  - Most of the time, relying only on command line, results in a lot more work
- Consider removing LuCI, if you ever become pressed for space on the router.
  - LuCI takes up about ~1.2 MB of space
  - That’s 10% of space available to us!
- I find the web interface very important and useful
- After initial setup, I rely heavily on the web interface for day-to-day matters such as adding devices to DHCP.

Change to an already prepared router

To prevent the wrath of the demo god

Wireless info Commands *

- ❑`iw`
- ❑`iw list`
  - This gives you everything that the wireless adapter supports
- ❑`iw dev`

Network Setup

Everyone’s gotta do what everyone’s gotta do.

VLANs before other Network Setup

- Setup VLANs **FIRST** on your router.
- A mistake setting up VLANs can result in a bricked router.
  - So be careful and setup in small steps
- Once your network segments are well defined then it is easy to setup firewalls, openvpn etc.
- You should plan to ensure that network segments don’t change often

Making sense of the network hardware*

- **Most** router will have at least one managed switch built-in that will usually pan all the LAN (as opposed to WAN) Ethernet ports
  - As we saw in `dmesg` the N600 has only two interfaces eth0 and eth1.
    - Funny, don't we have 5 ports? 5 ports and two interfaces?
  - `dmesg` said that eth0 has a switch in it
  - We don't really know what eth1 is at this point (strongly suspect it is the WAN port)

❑ `swconfig list` – this will list all available switches on your router – usually 1

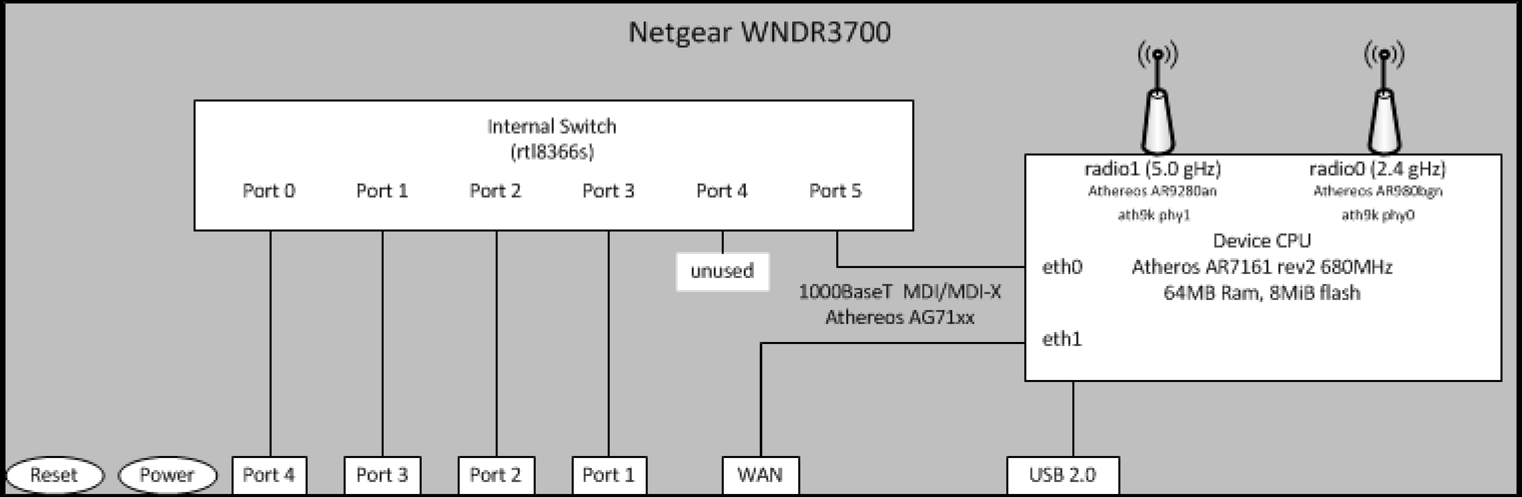
  - In our case we will see the familiar eth0 listed as the interface for `switch0`.

- You can get more Information on a particular switch (`switch0` in our case):
  - ❑ `swconfig dev switch0 help` – tells us the capabilities of the switch
  - ❑ `swconfig dev switch0 show` – tell us what's currently active

Switch Capabilities

- `swconfig dev switch0 help`
  - Tells you switch0 is provided by eth (which is AR934X)
  - The switch has 5 ports
  - The CPU is at Port `0`
  - Supports 16 VLANs
- The switch itself supports/contains three attributes:
  - “enable_vlan”, “apply” and “reset”
- Each VLAN supports/contains following attributs:
  - “vid” (VLAN ID) and “ports” (what ports belong to this VLAN)
- Each Port supports/contains following attributes:
  - “pvid” (Primary VLAN ID) and “link” (link information)

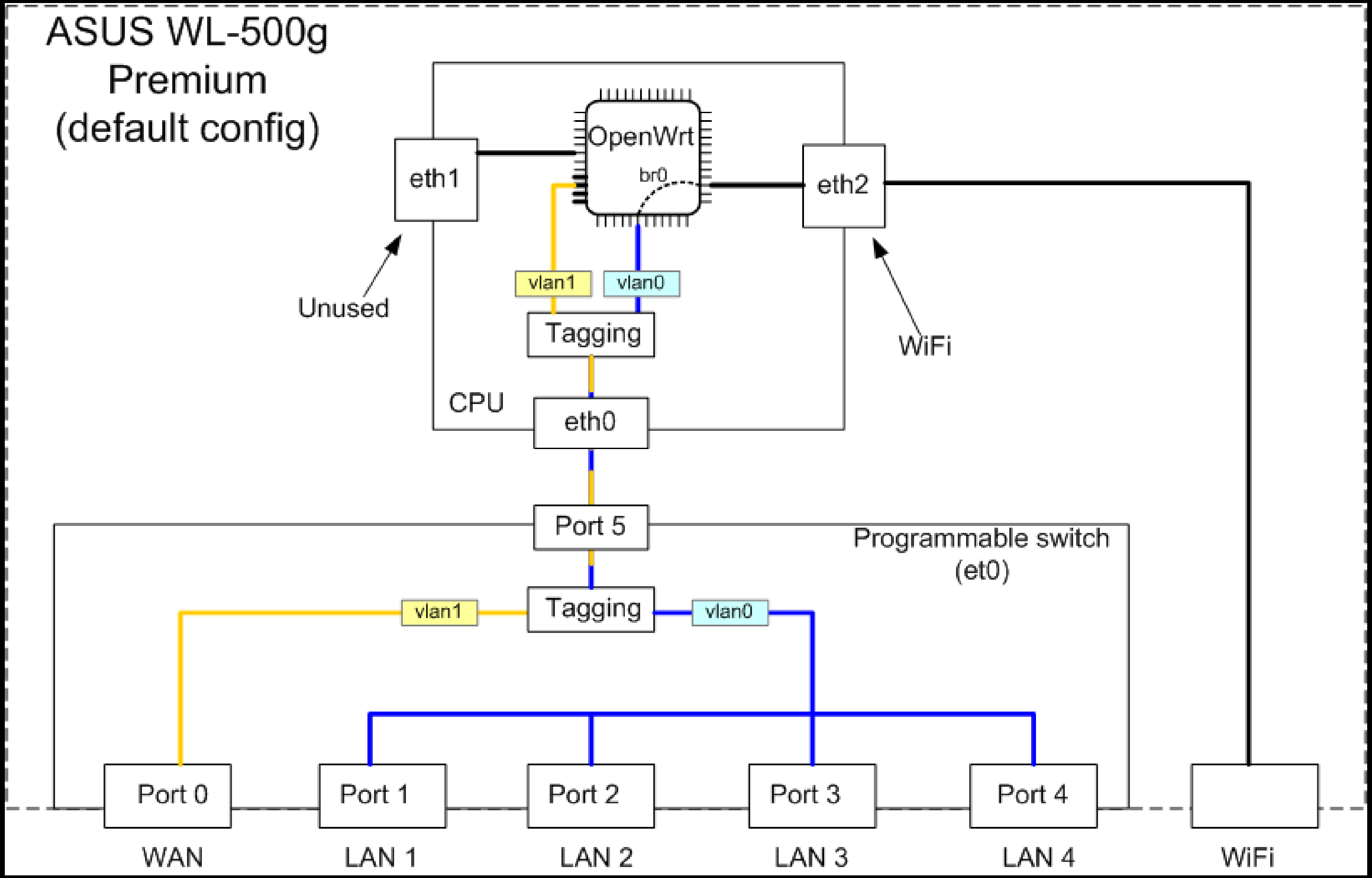
Router Internal – Example Figure



Physical port numbering does not equal logical port numbering

- This is **NOT** the actual internal layout for WD N600
  - We don't really know the exact internal layout of N600. We can only guess
- In this case Port 5 is the "CPU". The one that connects to eth0.
- eth0 is what's physically connected to the "network backbone"
  - "network backbone" = eth0, eth1, radio0 and radio1
- This hopefully gives you an idea of how to interpret output of `swconfig`.
- Next let's have a look at what it might look like if the switch was over ALL physical ports and not just the LAN ports.

Router Example 2 – All port Switch



Current VLAN configuration *

- ❑swconfig dev switch0 show
- ❑cat /etc/config/network – this is where switch configuration is stored
  - Look at “config switch” and “config switch_vlan”

Firewall

Everybody else only have normal walls

Understanding the Firewall Chains

- INPUT
  - describe what happens to traffic trying to reach the router itself through that interface.
- OUTPUT
  - describes what happens to traffic originating from the router itself.
- FORWARD
  - describes what happens to traffic coming from that zone and passing to another zone.

- Each of the above chains exist in the firewall for each network segment
- The default action for each chain of each network could allow or disallow traffic
- Explicit rules can override the default chain rule

Current Config *

- ❑ On WMI, Network -> Firewall will show current configuration
  - It can look fairly confusing if you don't know what you're reading.
- On SSH, have a look at the firewall config:
  - ❑ `vi /etc/config/firewall`
- ➢ The config above is converted to iptables rules by /etc/init.d/firewall
- ❑ `fw3 print`
- ❑ `iptables –S`
- ❑ `iptables -L`
  - This is confusing because it doesn't tell you interfaces used
- ❑ What can you deduce from the current configurations observed above?

Manual over WMI *

- You could have easily have done all of this manually by entering it all in /etc/config/firewall.
- Biggest benefit of WMI: No Typos!

Sending Emails

Why check for problems when you can be notified

Install a Mailing Agent *

- `okpg install msmtp`
- `opkg files msmtp`
- `vi /etc/msmtprc`
  - Change “`host mailhub.oursite.example`” to “`host 10.100.0.115`”
    - This can be a DNS entry or an IP.
    - For today’s testing you’ll use a mail server I’ve setup
  - Add line “from root@[FQDN]”

Other Options to Explore

There is always more to know

Other Possibilities

- Creating non-root users
- Static IPs and MAC Filtering
- IPv6
- WAN Port can be another LAN port
- Wireless Repeater Bridge:
- Wired Port Extender
- PeerGuardian setup
- Setting up USB and sharing with Samba or NFS over network
- Packet Sniffer

Other Possibilities (cont.)

- Setting up a web camera on the router - can be used to monitor the office 24/7!
- Setting up a 3G dongle to use as a "backup" Internet connection
- Tethering your Smartphone Internet connection to the router using USB to allow it to connect to the Internet
- Setting up a printer on the router
- BGP, OSPF & MPLS

Other Packages of Interest

- `opkg info luci-app-qos`
  - For Quality of Service configuration
- A lot of applications have a ‘luci’ modules that allows you to manage it from WMI
  - opkg list | egrep “luci-app”

Thank You

Hardest Step with OpenWrt

- Software (OpenWrt) is very flexible and relatively easy to work with.
- Finding and buying hardware (a router), with the hardware specs that will allow you to do what you need it to do, can be very difficult.
- Difficult because, these type of home routers are not marketed for people like us.
  - No router will tell you that its hardware supports VLANs.
  - Most chips in modern routers have this functionality by default.
  - But you can’t be sure unless you do lots of research before buying; or buy and find out.
- The ‘Table of Hardware’ on OpenWrt’s website makes this step easier
  - It lists hardware and its capabilities along with which version of OpenWrt supports it
  - ➢ http://wiki.openwrt.org/toh/start
  - ➢ Let’s look at our own WD N600 model in this list

Choosing Hardware for OpenWrt

- When it comes to choosing hardware, for me, this is how it usually works:
  - Look through a store and see what's currently at a decent price for the specs – usually look for USB port(s), Gigabit vs 100 MB port(s), Wireless antenna(s)
    - No other hardware features are usually marketed
  - Find something I like for the price/features and then take a look at the 'Table of Hardware' to see if OpenWrt support already exists
    - If it doesn't, even though it's possible to add support, it's too much trouble so look for another model
      - If you are dedicated enough, there is lots of info out there to add extra hardware support
  - If support exists, see what its actual hardware features are – i.e. CPU, RAM, VLAN support and which version of OpenWrt supports it
    - Almost all past supported routers are also supported in latest 'trunk'
    - Search to find blogs of other people who may have put OpenWrt on that hardware
  - If happy with actual hardware features and price reasonable then buy it

Contact

- Parth Shukla
  - pparth@pparth.net