OpenWRT + cheap routers

= Cheap, customized security sensors & training devices

Ryan Wilson @SpotlightCybsec

Spotlight Cybersecurity

spotlightcybersecurity.com

My Plan for Today

Why Should You Care About OpenWRT?

Quick History

How to Install

Quick OpenWRT Tour

Use Cases for the current & aspiring Cybersecurity Professional

More Notes & Instructions under “Blog” at spotlightcybersecurity.com

Spotlight Cybersecurity

Why Should You Care About OpenWRT?

Spotlight Cybersecurity

In the Local News…

Sunday, September 23, 2018 THE SOUTH'S OLDEST NEWSPAPER - Est. 1785 @AUG_Chronicle facebook

Students work during an "ethical hacking" class at the Georgia Cyber Center. A 2017 Augusta University study found companies ranked experience over college degrees and certifications when it came to hiring for cyber-related and information technology jobs. [MICHAEL HOLAHAN/THE AUGUSTA CHRONICLE]

Experience vital in cyber job hunt

https://www.augustachronicle.com/news/20180922/experience-often-key-in-cybersecurity-job-market

Spotlight Cybersecurity

Need Enterprise Experience...

… on a beer budget

Enter SOHO Embedded System Routers

Linksys WRT54G:

- released in December 2002
- ran Linux
- firmware open-sourced
- built-in programmable Ethernet Switch
- flash memory

Spotlight Cybersecurity

no moving parts:
no fans, no hard drives

Linksys EA4500 - <$40; Ethernet Switch; Good Wifi

N900 Dual-Band Wireless-N Router with Gigabit and USB (Certified Refurbished)

by Linksys

378 customer reviews | 51 answered questions

Price: $39.77 & **FREE Shipping**.Details

Get $10 off instantly: Pay $29.77 upon approval for the Amazon Prime Store Card.

prime | Try Fast, Free Shipping

- This router has been fully tested and certified by Linksys to look and operate Like-New. Linksys provides a 90 day warranty
- Best-in-class Wireless-N speed and performance for the ultimate home entertainment experience
- Dual-band 3x3 wireless supports high bandwidth applications such as video streaming or file sharing with speed up to 450 450Mbps
- Wireless-N technology uses multiple radios to create a robust signal that travels farther and faster with reduced dead spots
- Storage Link transforms any USB storage device into a NAS (Network Storage Device)

Compare with similar items

Spotlight Cybersecurity

<$20!

TP-Link N300 Wireless Wi-Fi Router - 2 x 5dBi High Power Antennas, Up to 300Mbps (TL-WR841N)

by TP-Link

15,518 customer reviews | 625 answered questions

Price: $19.99 & **FREE Shipping** on orders over $25 shipped by Amazon. Details

Get $50 off instantly: Pay $0.00 upon approval for the Amazon Rewards Visa Card.

prime | Try Fast, Free Shipping

Model: **Wi-Fi Router**

Wi-Fi Extender	**Wi-Fi Router**
$29.08	**$19.99**

- Wireless N speed up to 300Mbps ideal applications for video streaming, online gaming VoIP, web browsing and multi-tasking
- Two 5dBi antennas greatly increase the wireless robustness and stability
- Easy Setup Assistant provides quick & hassle free installation
- Features parental control function managing the

No longer recommended, but my “goto” router for a while.

Spotlight Cybersecurity

Pi - Costs More; No Ethernet Switch; So-So Wifi

Roll over image to zoom in

CanaKit Raspberry Pi 3 B+ (B Plus) with Premium Clear Case and 2.5A Power Supply

by CanaKit

4.4 ★★★★☆ 181 customer reviews | 37 answered questions

Price: $54.99 & **FREE Shipping**.Details

Get $50 off instantly: Pay $4.99 upon approval for the Amazon Rewards Visa Card.

prime | Try Fast, Free Shipping

Service: **Get professional installation** Details

Without expert installation | Include installation +$84.23 per unit

See more

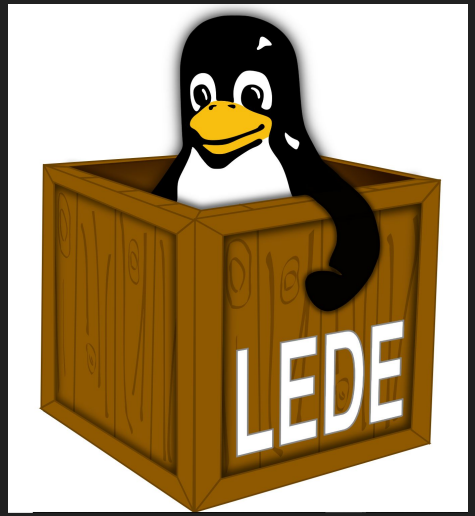
- Includes Raspberry Pi 3 B+ (B plus) with 1.4 GHz 64-bit Quad-Core Processor and 1 GB RAM
- CanaKit 2.5A USB Power Supply with Micro USB Cable and Noise Filter - Specially designed for the Raspberry Pi 3 B+ (UL Listed)
- Dual band 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Enhanced Ethernet Capability

Spotlight Cybersecurity

History of Custom Firmware

dd-wrt.com

Tomato
Version 1.00.0905



OpenWrt
Wireless Freedom

Spotlight Cybersecurity

OpenWRT & Me

I'm frugal.

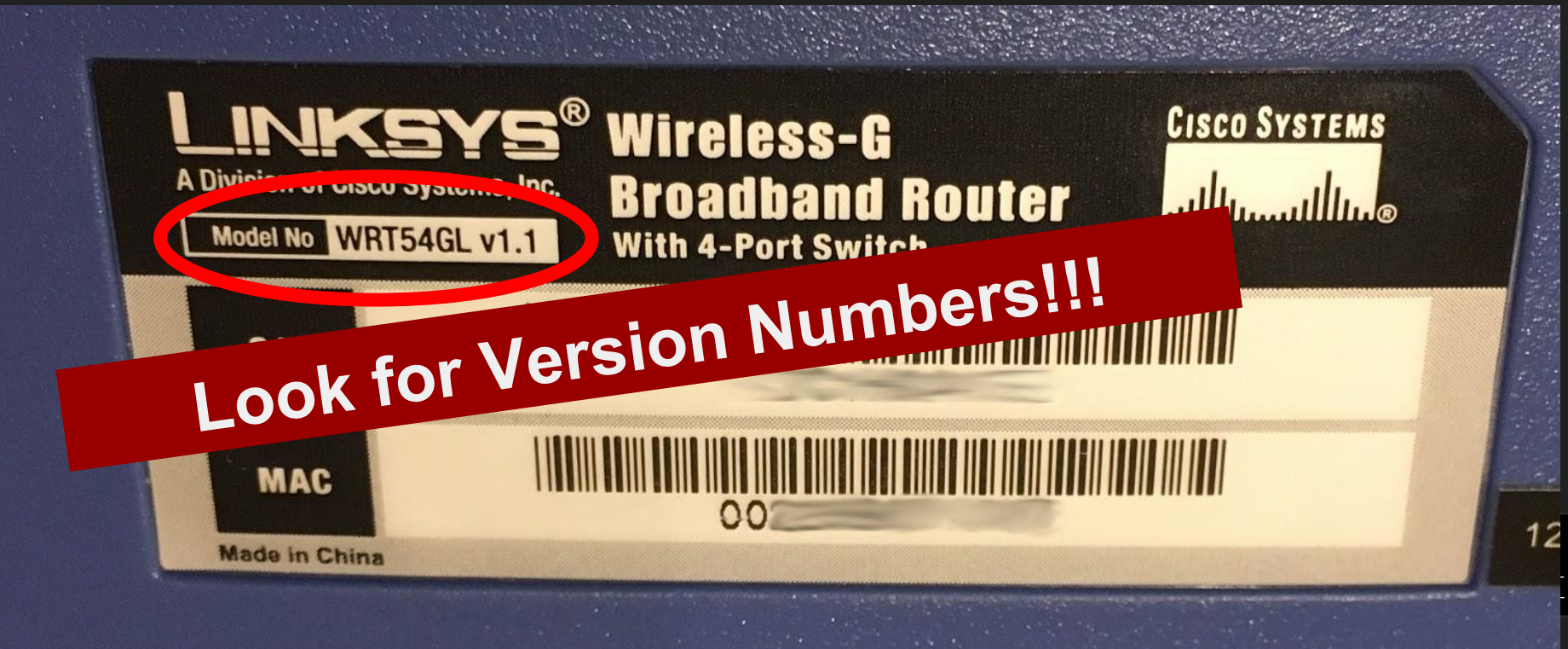
Still have my Linksys WRT54GL!

Ran my WRT54G until the capacitors (literally) burst

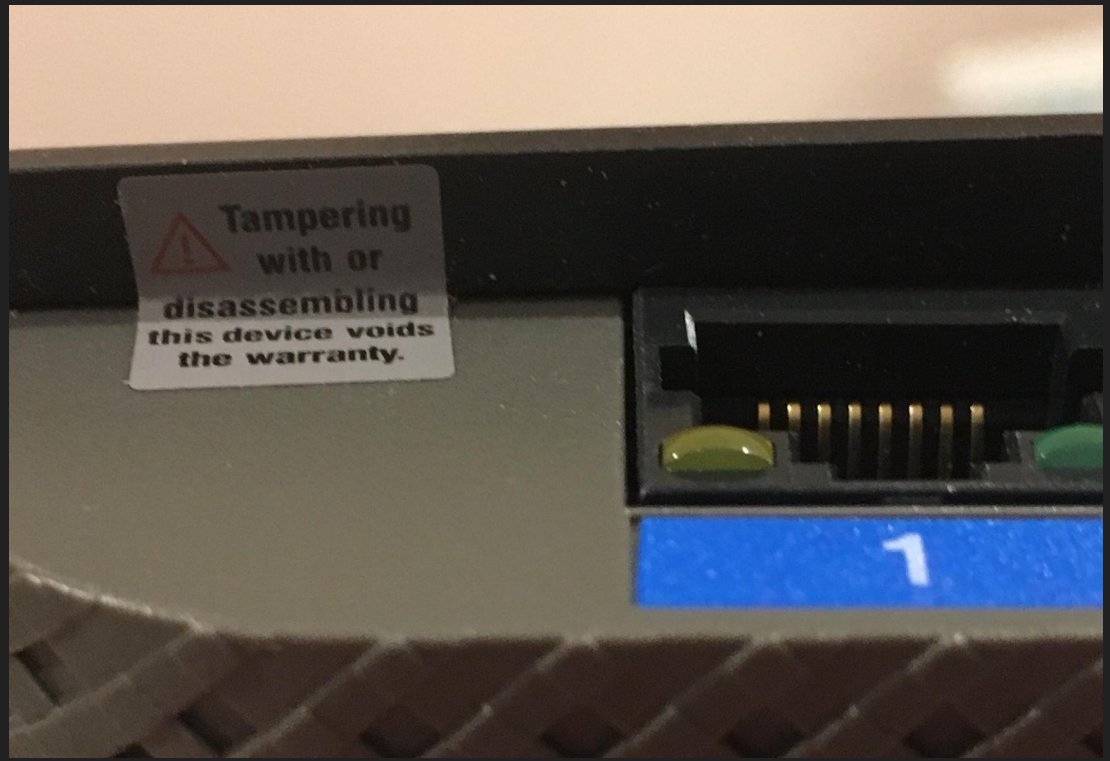
Spotlight Cybersecurity

Tradeoffs & Challenges

Inconsistent Manufacturer Model Numbers



Tradeoffs & Challenges



No Support! Void your warranty at your own risk!

“If it breaks, you get to keep both pieces.”

Spotlight Cybersecurity

Don’t Brick Your Device!

Spotlight Cybersecurity

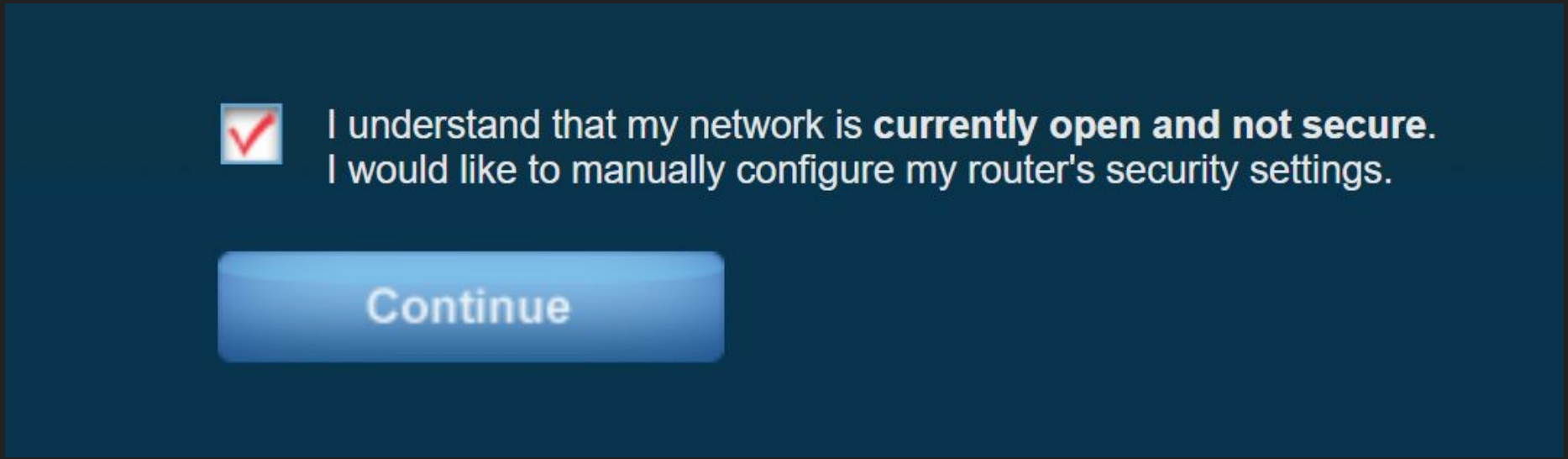
Hacking Your Router Takes Time!

Other Tradeoffs & Challenges

- High Temperature (I haven’t had this problem…)
- Hardware Weirdness (it’s not really enterprise grade)
- Limited CPU
- Limited Memory (Flash and RAM)

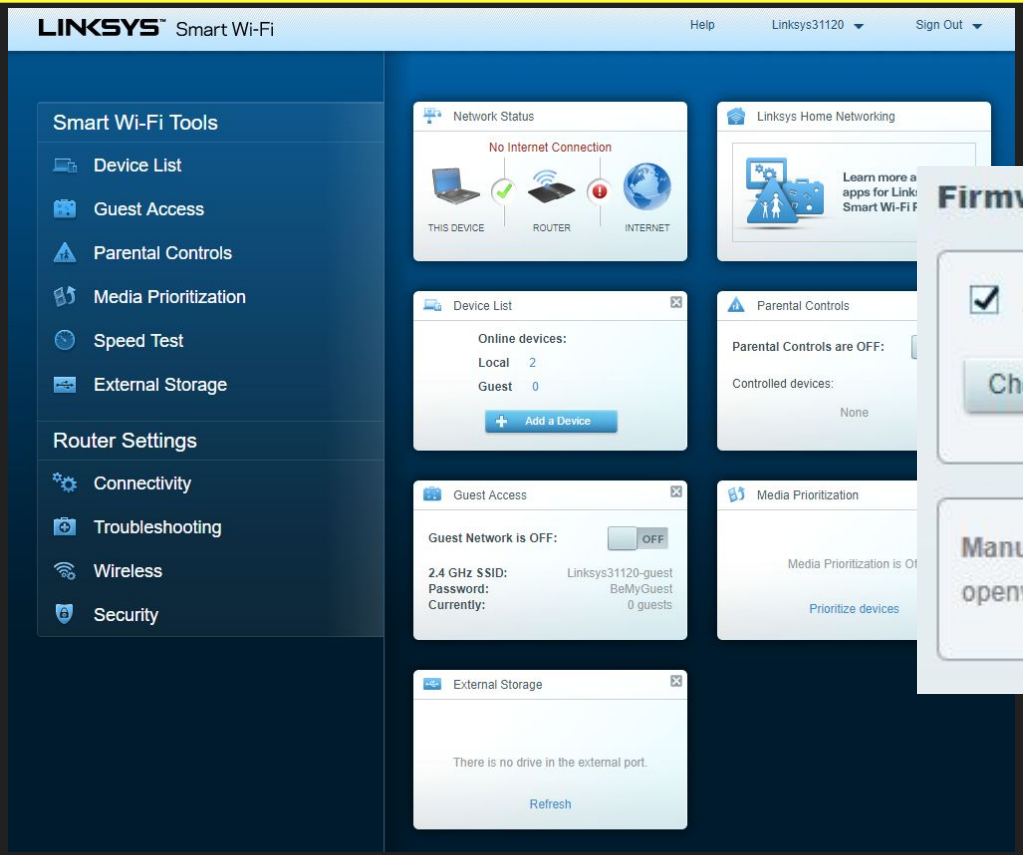
Installing on Linksys EA4500

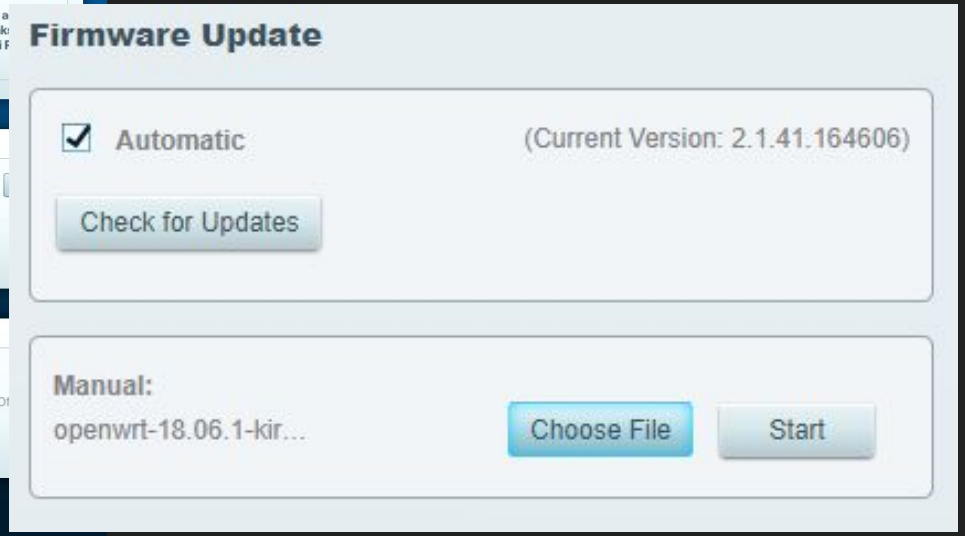
Thanks Cisco!



Spotlight Cybersecurity

Installing on Linksys EA4500 - Flashing





http://bit.ly/2CYhU1W

Spotlight Cybersecurity

Installing on Linksys EA4500 - OpenWRT Setup

root@OpenWrt: ~

```
login as: root


BusyBox v1.28.3 () built-in shell (ash)

 _______                     ________          __
|       |.-----.-----.-----.|  |  |  |.----.|  |_
|   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
|_______||   __|_____|__|__||________||__|  |____|
         |__| W I R E L E S S   F R E E D O M
-----------------------------------------------------
 OpenWrt 18.06.1, r7258-5eb055306f
-----------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
---------------------------------------------------
root@OpenWrt:~#
```

Not secure | 192.168.1.1/cgi-bin/luci

OpenWrt

No password set!

There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.

Go to password configuration...

Authorization Required

Please enter your username and password.

Username root

Password

Login Reset

Powered by LuCI openwrt-18.06 branch (git-18.228.31946-f64b152) / OpenWrt 18.06.1 r7258-

We’re In! Now What?

Spotlight Cybersecurity

Quick Tour - Package Management

Package management with opkg

`opkg update`
- download the latest package feeds (so you can search and install package)

`opkg install` *`PACKAGENAME`*
- install a package and all of its dependencies

Spotlight Cybersecurity

Quick Tour - Configuration

(Almost) All OpenWRT configuration done in `/etc/config/*`
Just edit the text files you find there and reboot. Or use the uci command:

`uci show`
- display the current configuration (loaded in-memory, may be different than the files)

`uci set 'network.lan.ipv6=off'`
- change a setting (in-memory)

`uci changes`
- see what changes are in-memory but not yet saved

`uci commit`
- save all in-memory changes to disk

Spotlight Cybersecurity

Protect My Network; Play With Real Traffic

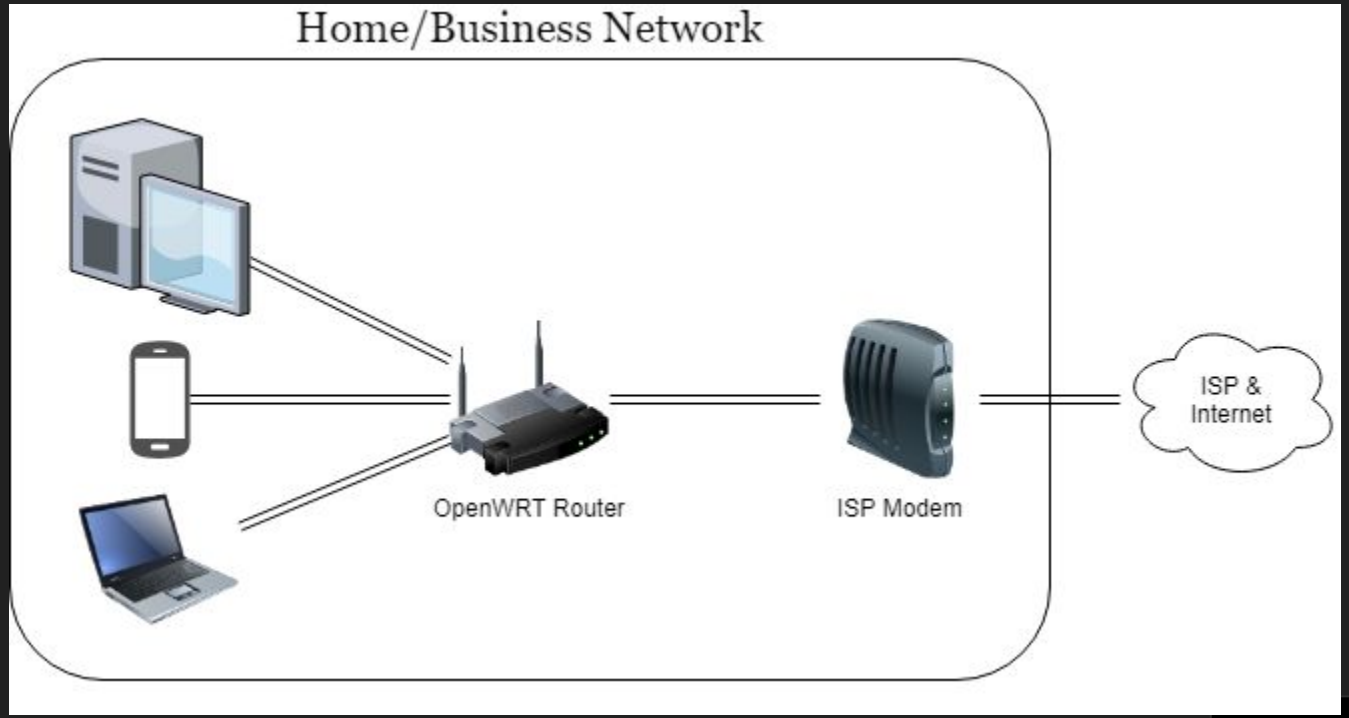
Want to Defend Your Home/Business Network?

Want to See Real Network Traffic?

- Setup a Firewall?
- Learn Wireshark?
- Monitor Traffic or Detect Intrusions with Snort or Bro?
- Setup Security Onion?
- Do Content Filtering?

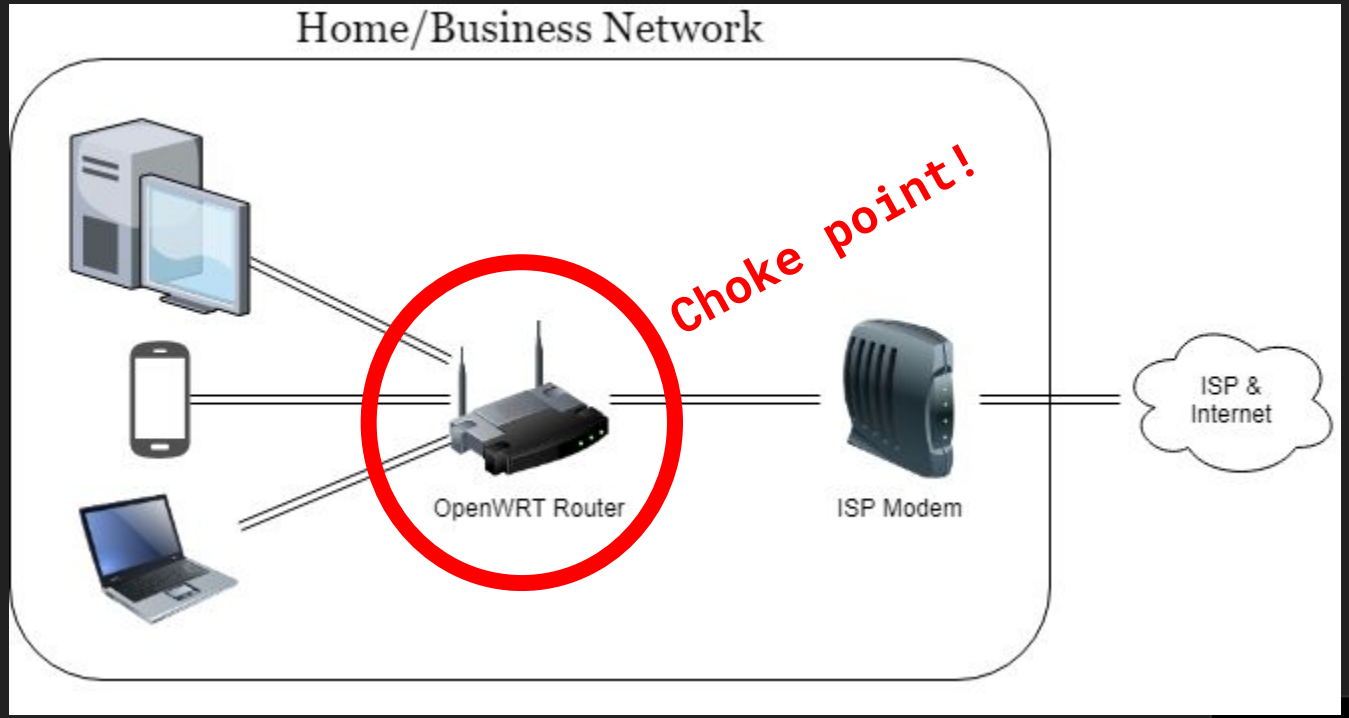
Spotlight Cybersecurity

Common Home/Small Business Network Setup



Spotlight Cybersecurity

Common Home/Small Business Network Setup



Spotlight Cybersecurity

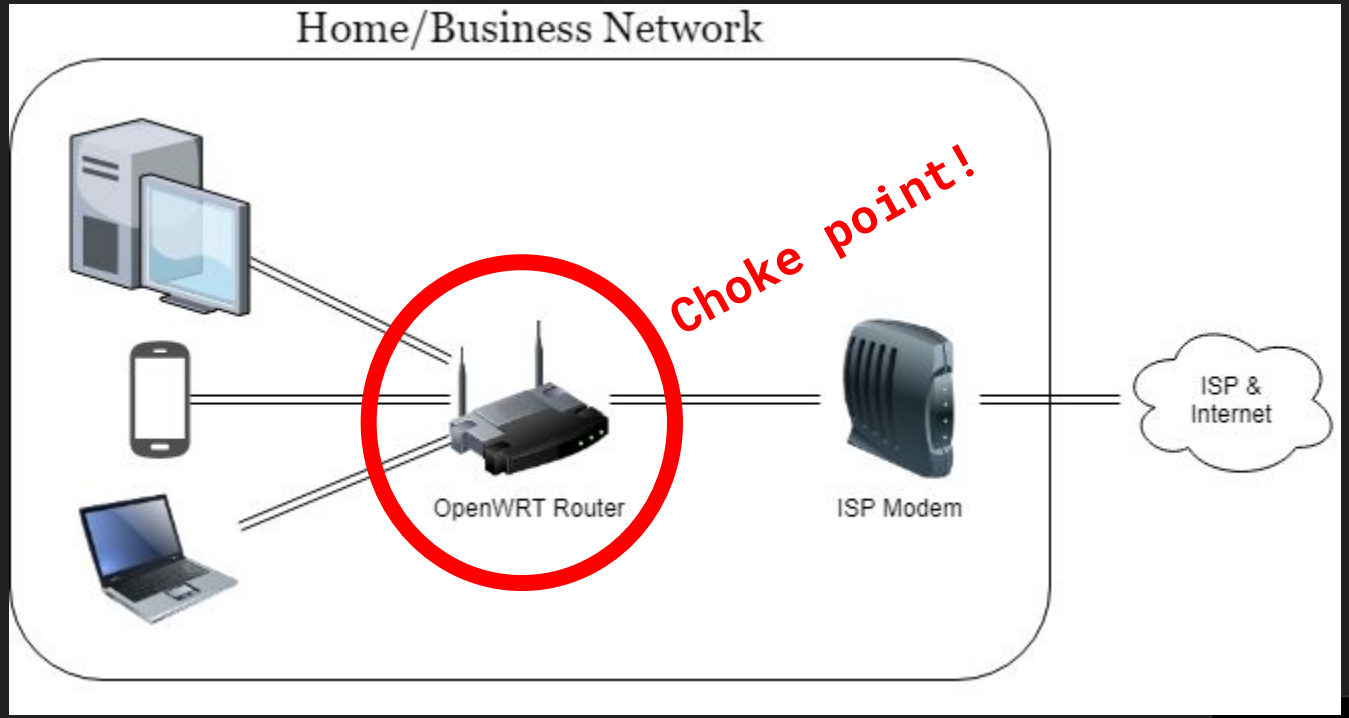
Full iptables Firewall

Custom OpenWRT firewall setup -
https://openwrt.org/docs/guide-user/firewall/start

Or just write your own iptables commands in `/etc/firewall.user`
To play nicely with the custom stuff,
use `input_rule`, `output_rule`, `forwarding_rule`
instead of the usual `INPUT`, `OUTPUT`, `FORWARD` chains.

Spotlight Cybersecurity

Common Home/Small Business Network Setup



Spotlight Cybersecurity

tcpdump on OpenWRT

opkg update

opkg install tcpdump-mini

tcpdump on OpenWRT

```
root@OpenWrt:~# tcpdump -i br-lan -n not tcp port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br-lan, link-type EN10MB (Ethernet), capture size 262144 bytes
16:44:50.000884 IP 64.233.177.189.443 > 192.168.1.140.49671: UDP, length 40
16:44:50.009128 IP 192.168.1.140.49671 > 64.233.177.189.443: UDP, length 29
16:44:52.320940 IP 192.168.1.140.50235 > 64.233.177.189.443: UDP, length 23
16:44:52.349656 IP 64.233.177.189.443 > 192.168.1.140.50235: UDP, length 20
16:44:55.933978 IP 192.168.1.140.54945 > 52.55.159.78.443: Flags [.], seq 678267589:678267590, ack 3914959977
, win 251, length 1
16:44:55.959748 IP 52.55.159.78.443 > 192.168.1.140.54945: Flags [.], ack 1, win 1821, options [nop,nop,sack
1 {0:1}], length 0
16:44:59.010009 IP 23.73.162.72.443 > 192.168.1.140.55289: Flags [P.], seq 690921223:690921254, ack 130210933
5, win 328, length 31
16:44:59.011215 IP 192.168.1.140.55289 > 23.73.162.72.443: Flags [P.], seq 1:36, ack 31, win 254, length 35
16:44:59.030269 IP 23.73.162.72.443 > 192.168.1.140.55289: Flags [.], ack 36, win 328, length 0
16:44:59.804057 IP 64.233.177.189.443 > 192.168.1.140.49671: UDP, length 47
16:44:59.812105 IP 192.168.1.140.49671 > 64.233.177.189.443: UDP, length 29
16:45:01.175700 IP 64.233.177.189.443 > 192.168.1.140.49671: UDP, length 40
16:45:01.183342 IP 192.168.1.140.49671 > 64.233.177.189.443: UDP, length 29
16:45:02.566466 IP 64.233.177.189.443 > 192.168.1.140.49671: UDP, length 47
16:45:02.575440 IP 192.168.1.140.49671 > 64.233.177.189.443: UDP, length 29
```

Spotlight Cybersecurity

tcpdump -> USB Storage

Spotlight Cybersecurity

tcpdump -> USB Storage

Prepare USB as ext4 filesystem; Attach to Router

```
opkg install block-mount kmod-usb-storage kmod-fs-ext4
```

```
mount /dev/sda1 /mnt
```

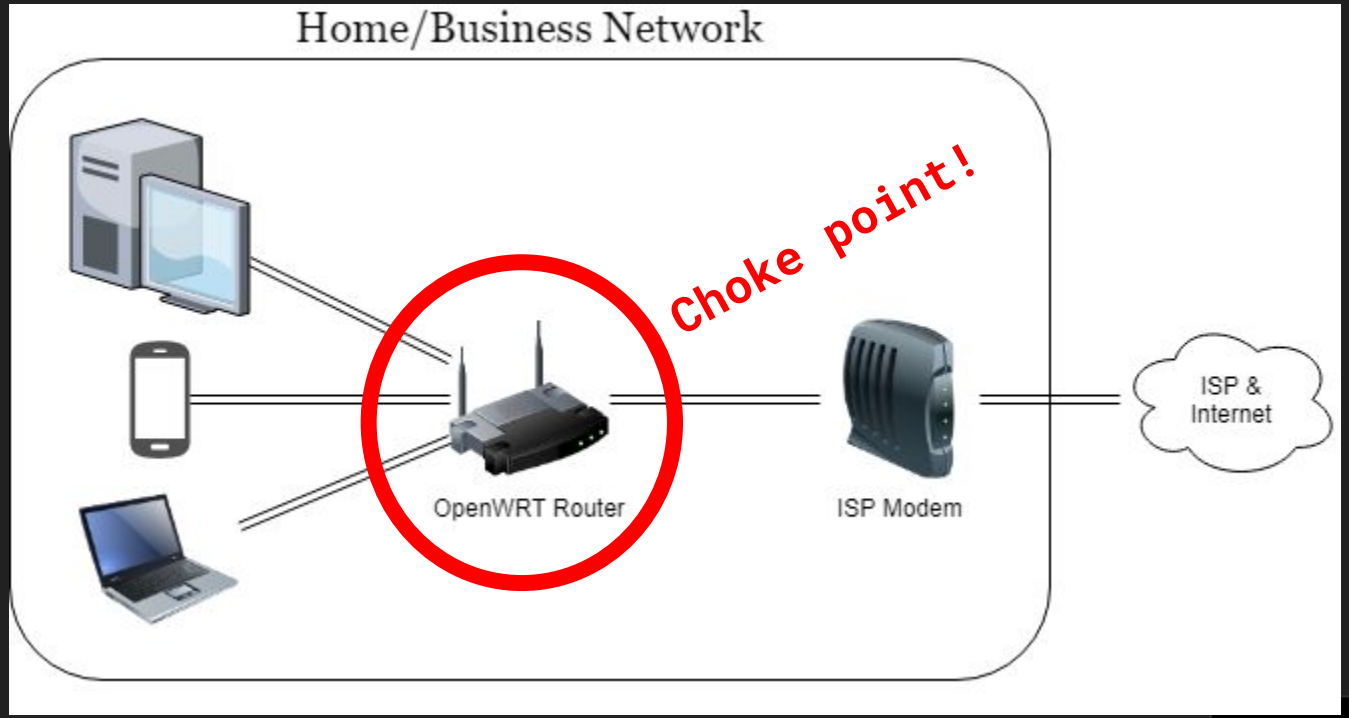
```
tcpdump -i br-lan -n -w /mnt/mynetwork.pcap
```

Then scp the file to your desktop for analysis (Wireshark?)

More Info:

Spotlight Cybersecurity

Network Tap?



Spotlight Cybersecurity

Active Taps are Expensive

ETAP-2003

Dualcomm 10/100/1000Base-T Gigabit Ethernet Network TAP

by Dualcomm

★★★★★ 18 customer reviews

| 15 answered questions

Amazon's Choice for "ethernet network tap"

Price: $219.95 & **FREE Shipping**.Details

Get $50 off instantly: Pay $169.95 upon approval for the Amazon Rewards Visa Card.

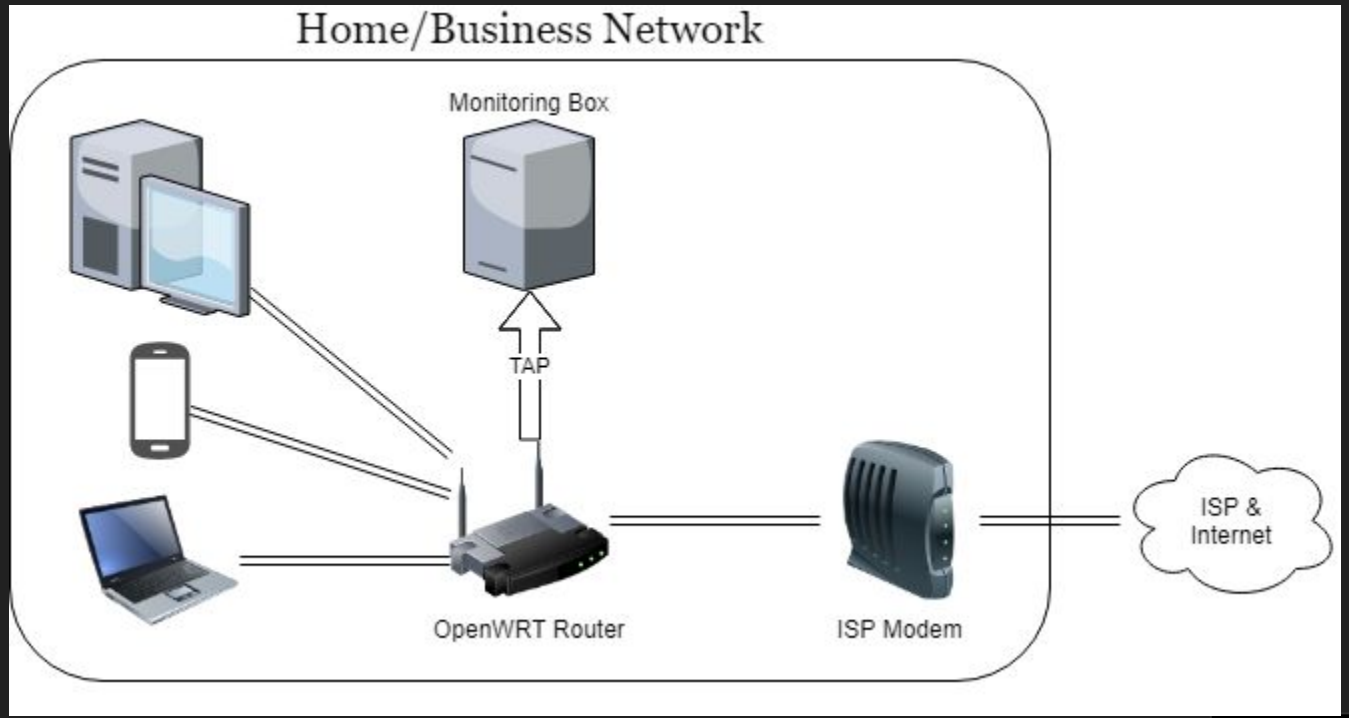
✓prime | Try Fast, Free Shipping

- Network Tap for Use with 10/100/1000Base-T Link
- Single Monitor Port
- USB Powered
- Compatible with Power over Ethernet (PoE)
- Portable

New (1) from $219.95 & FREE shipping. Details

Report incorrect product information.

Network Tap



Spotlight Cybersecurity

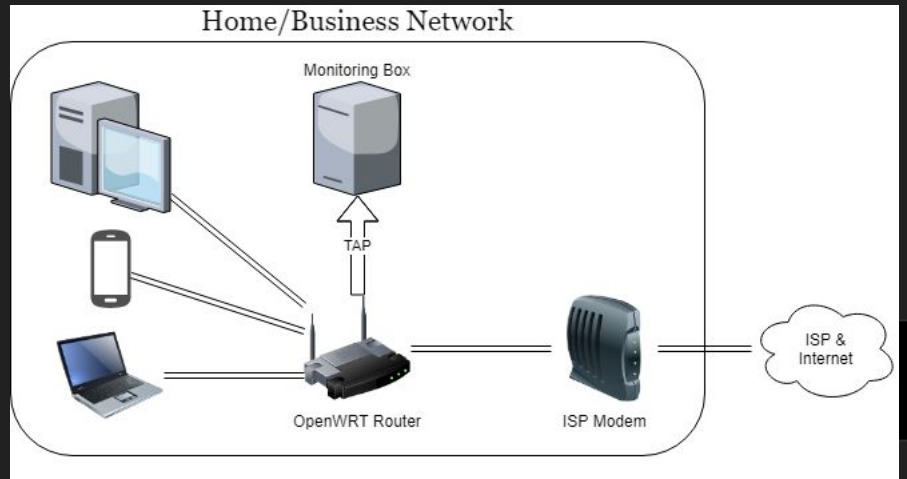
Network Tap

Option 1:
iptables TEE module (done in software, only IP packets)

Option 2:
hardware mirroring (only certain chipsets support this: TP-Link WDR-3600)

Option 3:
daemonlogger
(destination must not be a switched port)

http://bit.ly/2Cug4oC



Network Security Monitoring

Full Packet Capture

Netflow Session Data

Firewall/DNS Logs

Full Packet Capture

daemonlogger - utility to capture packets and rotate PCAP files by time/size

```
opkg install daemonlogger
```

```
daemonlogger -i br-lan -n lan -l /data/pcap -t 600 -d
```

- Collect on interface br-lan, save to /data/pcap, roll file every 600 seconds

Spotlight Cybersecurity

Netflow

```
opkg install softflowd daemonlogger
```

Configure `/etc/config/softflowd` to send to your netflow collector

Don’t have a Netflow Collector?

Send softflowd to 127.0.0.1:9995

```
daemonlogger -i lo -n softflowd -l /data/pcap -t 600 -d "udp dst port 9995"
```

Use nfcapd, nfdump, nfreplay to parse the PCAP later and replay it

Send to ELK Stack

Spotlight Cybersecurity

DNS log Capture

```
uci set dhcp.@dnsmasq[0].logqueries='1'
uci commit
/etc/init.d/dnsmasq stop; /etc/init.d/dnsmasq start
```

Example syslog output:

```
dnsmasq[4277]: 92239 10.1.0.238/15967 query[A] play.google.com from 10.1.0.238
dnsmasq[4277]: 92239 10.1.0.238/15967 forwarded play.google.com to 75.76.84.102
dnsmasq[4277]: 92239 10.1.0.238/15967 reply play.google.com is 74.125.21.138
dnsmasq[4277]: 92239 10.1.0.238/15967 reply play.google.com is 74.125.21.113
dnsmasq[4277]: 92239 10.1.0.238/15967 reply play.google.com is 74.125.21.139
dnsmasq[4277]: 92239 10.1.0.238/15967 reply play.google.com is 74.125.21.100
dnsmasq[4277]: 92239 10.1.0.238/15967 reply play.google.com is 74.125.21.101
```

Firewall Log Capture

Edit /etc/config/firewall, enable ‘log’ option on each zone, /etc/init.d/firewall restart

```
config zone
        option name 'wan'
        ...
        option log '1'
        option log_limit '100/second'
```

Example syslog Output:

```
Fri Oct 19 18:20:05 2018 kern.warn kernel: [689095.915261] REJECT(src wan)IN=eth0.2 OUT=
MAC=c4:e9:11:e8:fe:ff:0e:62:99:f3:07:26:08:00:95:70:00:fe SRC=185.255.31.78 DST=80.1.10.204
LEN=40 TOS=0x00 PREC=0x20 TTL=238 ID=11691 PROTO=TCP SPT=50293 DPT=20396 WINDOW=1024
RES=0x00 SYN URGP=0
Fri Oct 19 18:20:05 2018 kern.warn kernel: [689096.085186] REJECT(src wan)IN=eth0.2 OUT=
MAC=c4:e9:11:e8:fe:ff:0e:62:99:f3:07:26:08:00:95:70:00:fe SRC=185.255.31.78 DST=80.1.10.204
LEN=40 TOS=0x00 PREC=0x20 TTL=238 ID=11690 PROTO=TCP SPT=50293 DPT=20396 WINDOW=1200
RES=0x00 RST URGP=0
```

Syslog Capture

Logread - utility to view logs locally

Send logs remotely - https://wiki.openwrt.org/doc/uci/system

Or capture them locally (on USB): http://bit.ly/2ylBZeT

Content Filtering

Spotlight Cybersecurity

There is no technology silver bullet for protecting your kids online!

Spotlight Cybersecurity

But… some technology coupled with active parenting (rules & education) is an effective defense-in-depth strategy

Content Filtering - OpenDNS Family Shield

Malicious, Phishing Sites Blacklisted

Adult Content Domains Blocked

FREE!

Easy Configuration: Point dnsmasq at OpenDNS instead of your ISP’s DNS

http://bit.ly/2q2gL17

Spotlight Cybersecurity

Content Filtering - Google, YouTube, Bing Filtering

DNS Tricks to Enforce Google, YouTube,
and Bing Safe Searching Modes

Edit /etc/dnsmasq.conf

http://bit.ly/2yOfNt5

```
# force google safesearch
host-record=forcesafesearch.google.com,216.239.38.120
cname=www.google.com,forcesafesearch.google.com
```

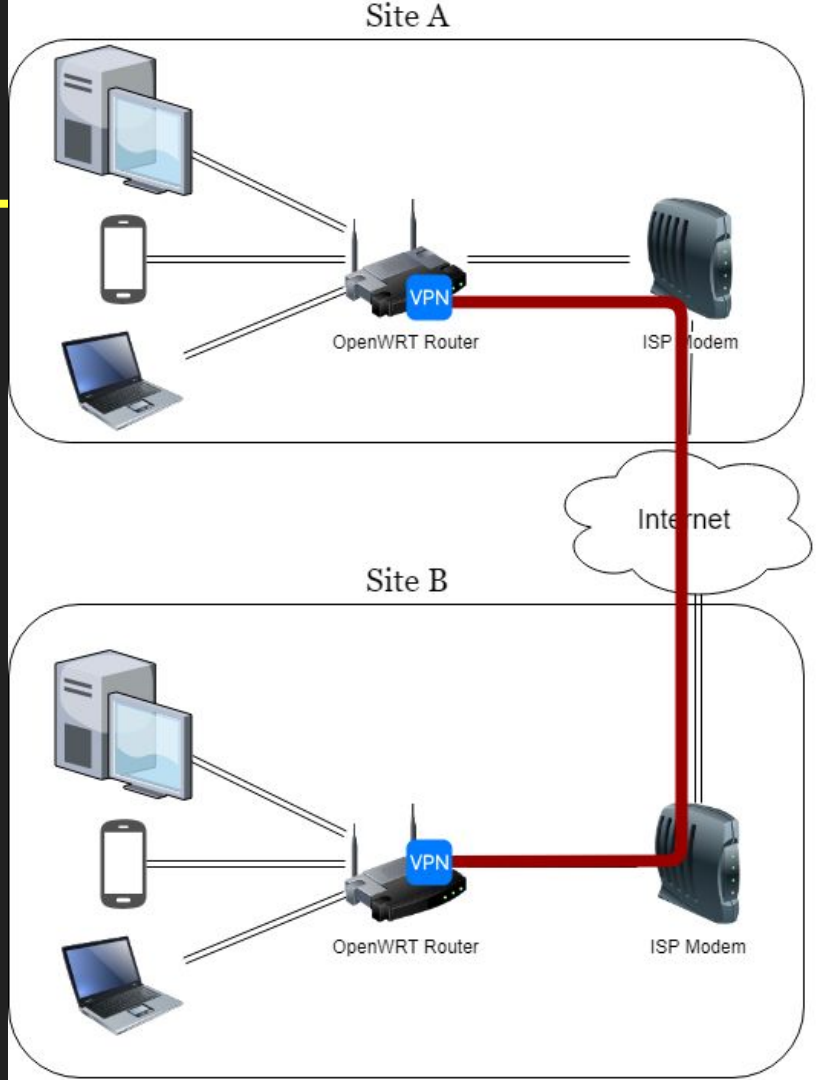
Spotlight Cybersecurity

VPNs with OpenVPN on OpenWRT

Spotlight Cybersecurity

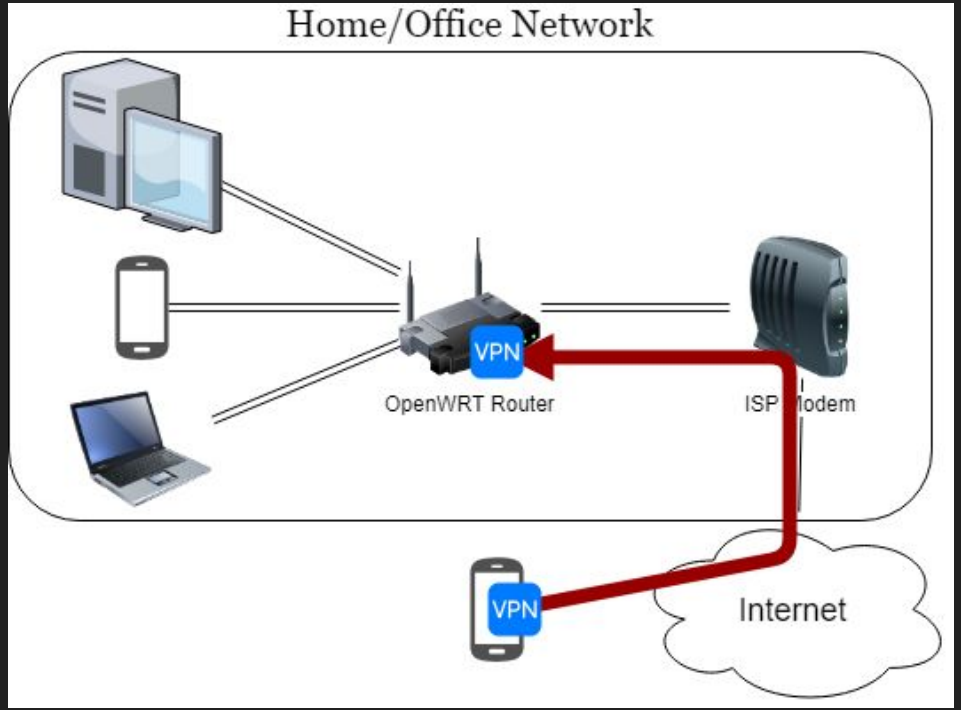
Typical VPN - Site-to-Site

Two networks, connected together virtually over the Internet.



Typical VPN - Remote Access

Remote clients “calling home” to join the home network.

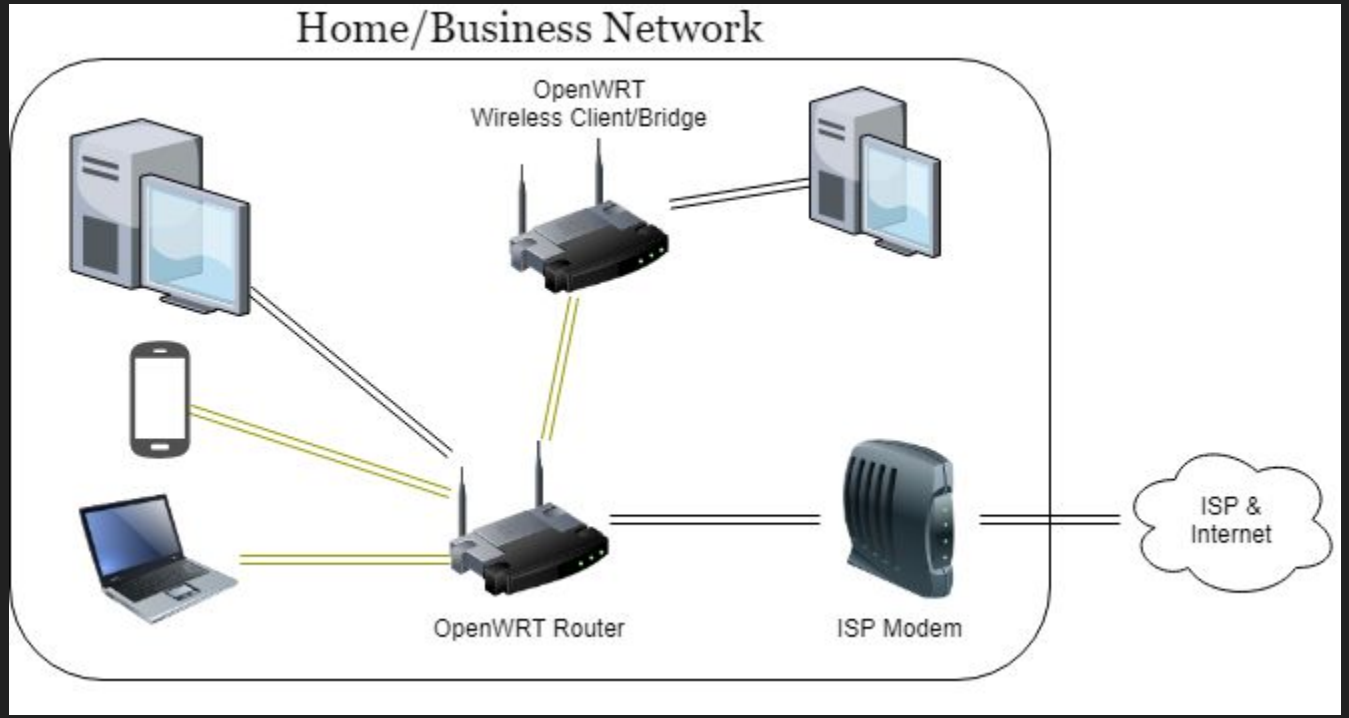


Spotlight Cybersecurity

Fun with Wireless

Spotlight Cybersecurity

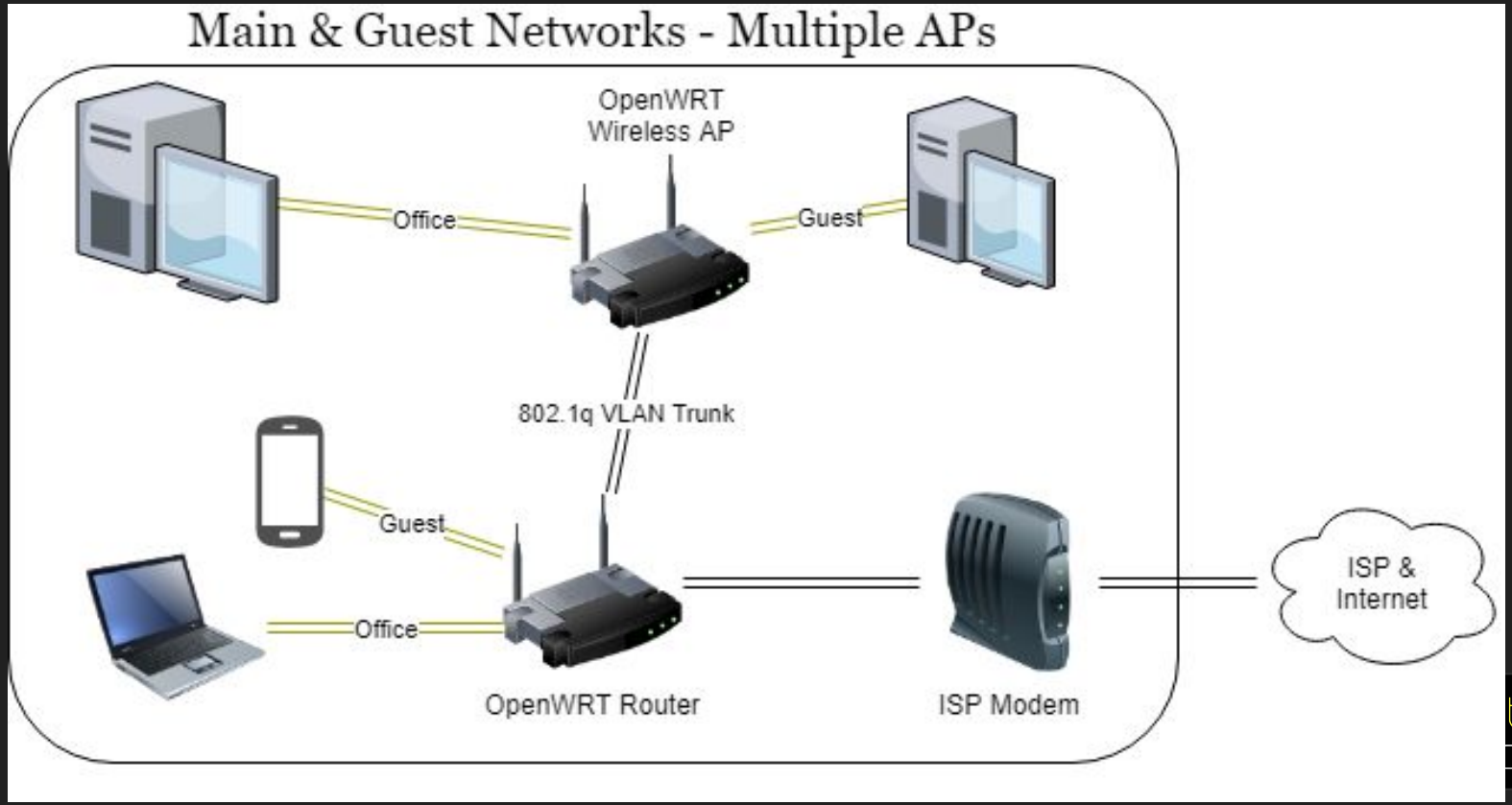
Wireless Bridge



http://bit.ly/2CtYDV8

Spotlight
Cybersecurity

Guest Network, Multiple APs -> 802.1q VLANs



Wireless Training - WEP & WPA2 Cracking; Surveys

Small, deterministic setup

WEP Cracking Lab for AU

DM @SpotlightCybsec to be notified when instructions posted

Remote Wireless Collection

Some router chipsets support monitor mode! (Atheros chipsets have historically worked better for me; avoid most Broadcom)

Not yet used operationally; tested only in lab

Other Use Cases

- PXE Boot - push boot images over the network from OpenWRT flash/USB
- Travel Router - take a secure wireless AP (with VPN to home?) with you
- Captive Portals - get your wireless users to register first
- Hardware Hacking
  - GPIO Ports
  - Audio
  - ...

OpenWRT
=
Versatile Security & Training Platform

Spotlight Cybersecurity

Get Started?

Instructions at our Blog:
http://bit.ly/2Ey9Tm7

@SpotlightCybsec

Spotlight Cybersecurity