Home Router/Firewall using OPNsense

My totally overkill home network

Shankar Viswanathan

Dec 2022

Outline

- Motivation for new home network
- SW & HW choices
- OPNsense basics
- Router & Network setup
- Power/performance
- Demo

What I had ...

- Typical consumer router running OpenWRT in the basement
- Coax between basement and first floor – MoCa adapter at each end
- First floor MoCa adapter had built-in Wifi AP
  - And Blinkenlights

It worked, but ...

- Wifi performance was poor in some rooms
  - Chicken wire in a few walls
- Latency was bad with multiple video calls in parallel
- Could never saturate 400/20 Mbps connection from ISP (over WiFi)

So …

- Cat6A cabling installed
- 10Gbps capable over distances < 100m

But what router?

1. Standard consumer router with OpenWRT

Or

2. DIY with a router-focused OS

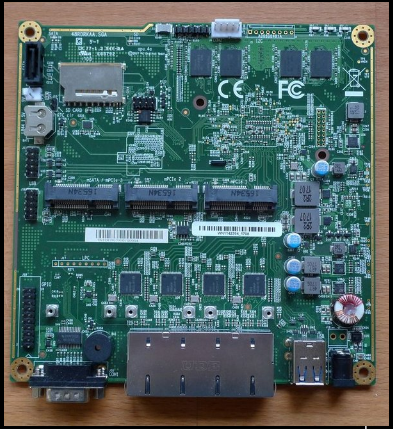


Image credit: asus.com, pcengines.ch

Winner – option #2

- Less hassle – don’t need to deal with vendor locking firmware
- No weirdness with flash size or revision number within router model
- More flexibility overall

Router OS Criteria

- Secure
- Stable
- Regular updates
- Flexible, ease of use
- FLOSS w/ reasonably active community

OS feature requirements

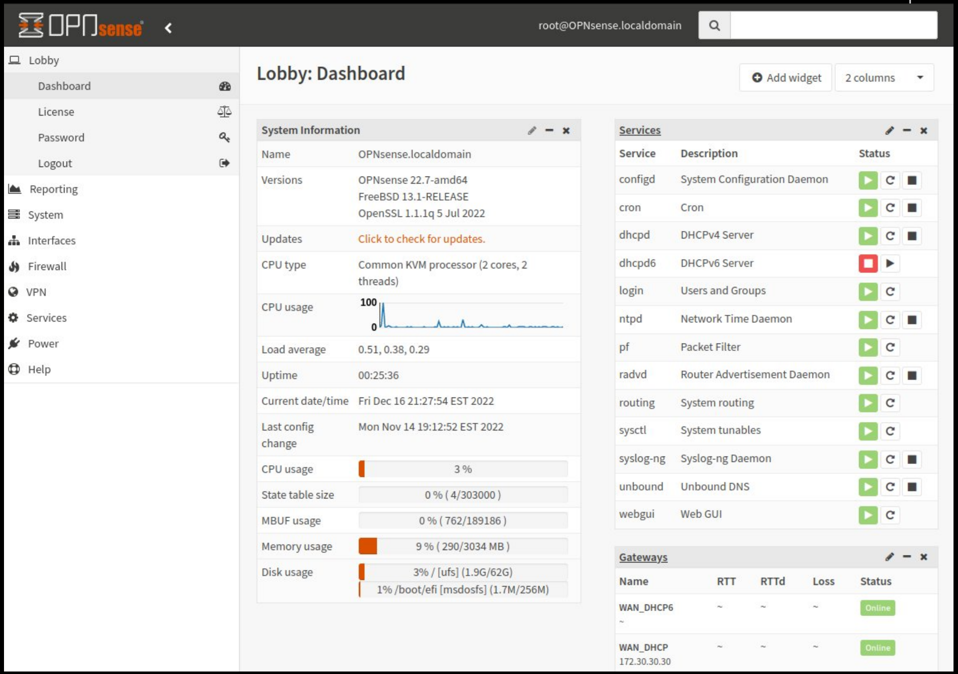
- Full featured stateful firewall
- DHCP server
- VLAN support
- Wireguard VPN support
- Optional: DNS filtering/blacklisting
- Optional: Traffic shaping / QoS

OS choices

- PFsense
- OPNsense
- OpenWRT
- IPFire
- Untangle

OPNsense

- Based on FreeBSD
- Fork of Pfsense
  - Itself a fork of m0n0wall
- Founded and since maintained by Deciso A.B.
- Continuously updated since its start in 2015 – 2 major updates each year
- Easy to use UI
- Fantastic documentation



Lobby: Dashboard

System Information

Name	OPNsense.localdomain
Versions	OPNsense 22.7-amd64 FreeBSD 13.1-RELEASE OpenSSL 1.1.1q 5 Jul 2022
Updates	Click to check for updates.
CPU type	Common KVM processor (2 cores, 2 threads)
CPU usage	100 0
Load average	0.51, 0.38, 0.29
Uptime	00:25:36
Current date/time	Fri Dec 16 21:27:54 EST 2022
Last config change	Mon Nov 14 19:12:52 EST 2022
CPU usage	3 %
State table size	0 % (4/303000)
MBUF usage	0 % (762/189186)
Memory usage	9 % (290/3034 MB)
Disk usage	3% / [ufs] (1.9G/62G) 1% /boot/efi [msdosfs] (1.7M/256M)

Services

Service	Description	Status
configd	System Configuration Daemon	▶ ↻ ■
cron	Cron	▶ ↻ ■
dhcpd	DHCPv4 Server	▶ ↻ ■
dhcpd6	DHCPv6 Server	□ ▶
login	Users and Groups	▶ ↻
ntpd	Network Time Daemon	▶ ↻ ■
pf	Packet Filter	▶ ↻
radvd	Router Advertisement Daemon	▶ ↻ ■
routing	System routing	▶ ↻
sysctl	System tunables	▶ ↻
syslog-ng	Syslog-ng Daemon	▶ ↻ ■
unbound	Unbound DNS	▶ ↻ ■
webgui	Web GUI	▶ ↻

Gateways

Name	RTT	RTTd	Loss	Status
WAN_DHCP6 ~	~	~	~	Online
WAN_DHCP 172.30.30.30	~	~	~	Online

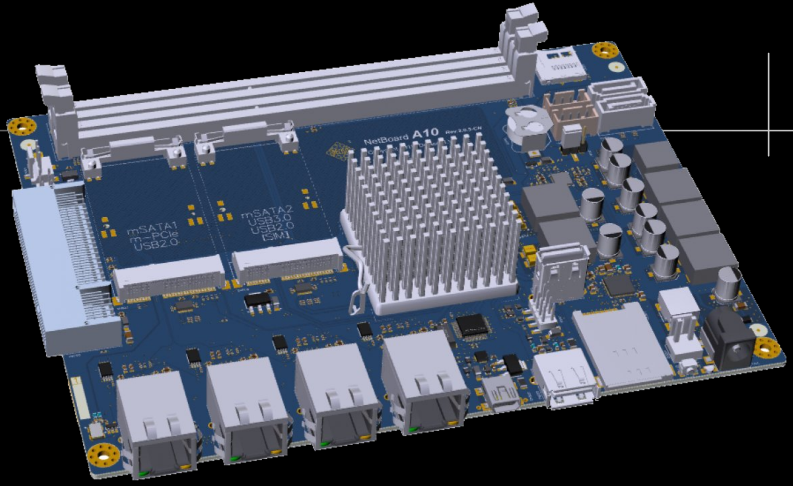
OPNsense: Major features

Feature	Support
Stateful Firewall	✔
DNS and DHCP servers, dynamic DNS	✔
Two-Factor Authentication	✔
802.1Q VLAN support	✔
Link Aggregation & Failover	✔
Traffic Shaping	✔
Built-in reporting and monitoring tools	✔
Intrusion Detection & Prevention	✔
Virus scanner	✔
VPN Services (IPsec, OpenVPN, WireGuard)	✔
Support for plugins	✔

OPNsense installation

- Install images available for amd64 architecture only
- Can be installed from USB or flash with a display or via serial
- As with FreeBSD, finding drivers can be tricky for certain devices – Intel NICs are generally the best supported
- A “nano” image is available for embedded devices: all writes go to ramdisk, logs do not persist upon reboots
- ZFS is the recommended filesystem for standard installs
- Can install on baremetal or in a VM (VMWare, Xen, KVM etc)
- After installation, configuration can be done via console, web GUI or via ssh (ssh disabled by default)

Recommended HW



- > 1.5GHz multi-core CPU
- 4GB RAM
- Serial console or video (VGA) for installation
- > 120GB storage for OS & logs
- >= 2 NIC ports
  - Single NIC workable with a VLAN capable switch, so called “Router on a stick”

Image credit: shop.opnsense.com

First idea

- Get a PC Engines APU2 board + enclosure kit
- Load OPNsense
- Estimated cost: ~$225
- Unobtanium :-(

Image credit: teklager.se

Another option

- Various low power router boxes from Amazon, Aliexpress
- Deciso, Netgate, Protectli, Qotom, etc.
- 4 to 6 GbE ports
- Some come with PFSense/OPNSense preloaded
- Power draw: 15 to 35W
- Price range: $300 to $700

Image credit: qotom.com

Go down r/OPNsense rabbit hole ...

- Used slim PC or thin client with open PCIe slot
- Add 4-port GbE NIC
- Add larger disk or use USB storage
- Power: ~30W
- Estimated cost: ~$200

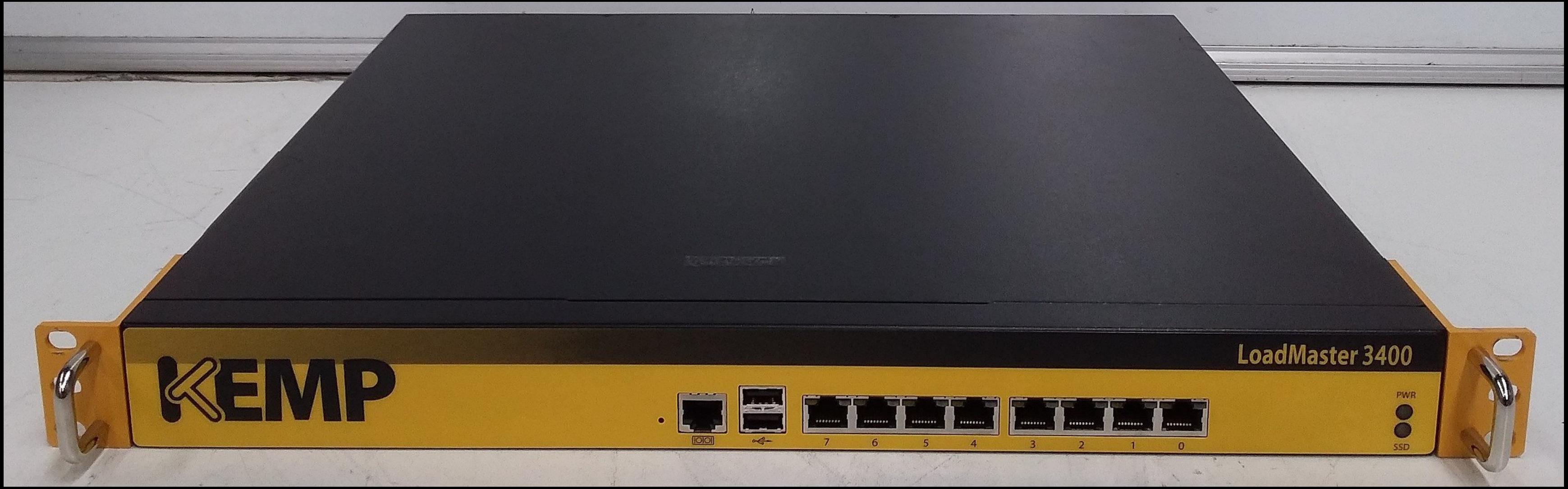
Image credit: servethehome.com

Get crazy deep into r/homelab

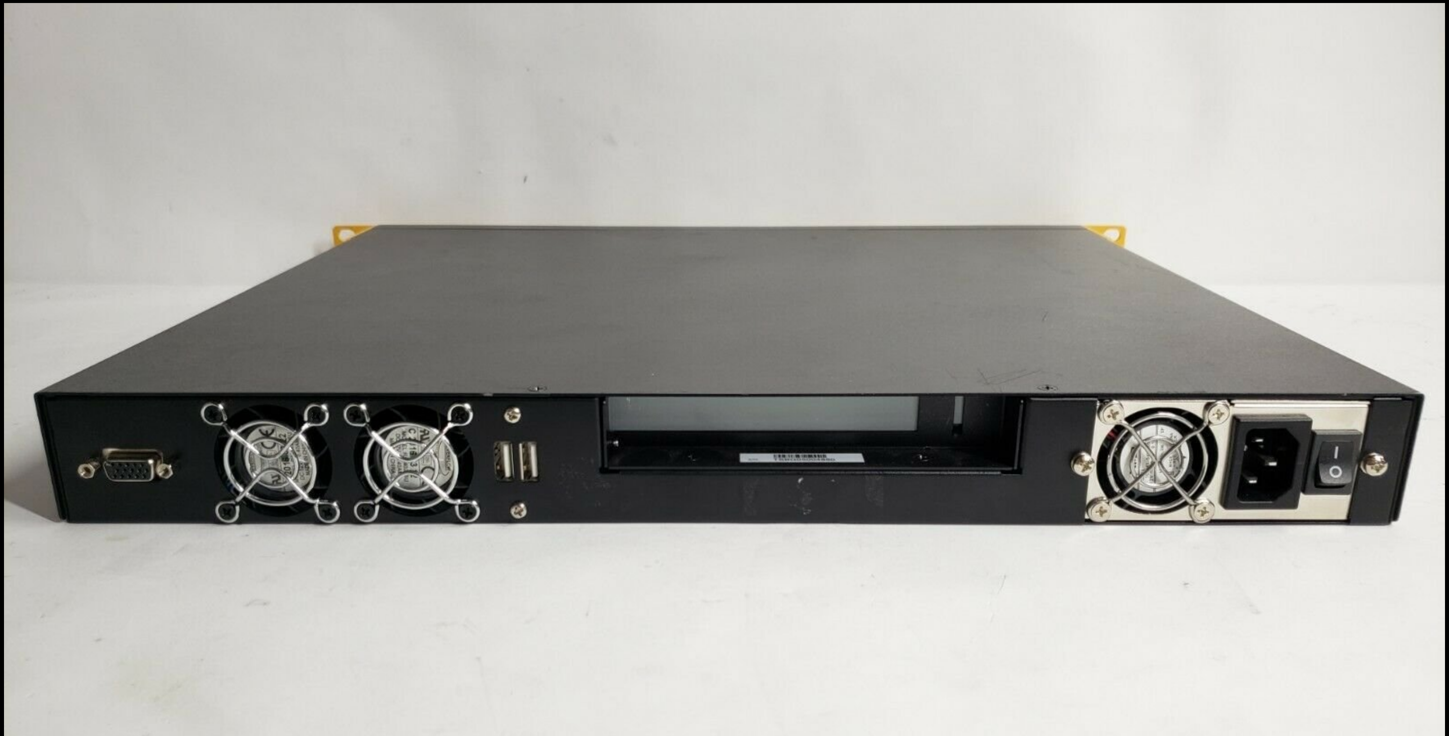
Why not get a rackmount server with a bunch of ethernet ports?

Found this on Ebay: Kemp LM3400

8GbE ports, 2 USB2, Cisco-style serial

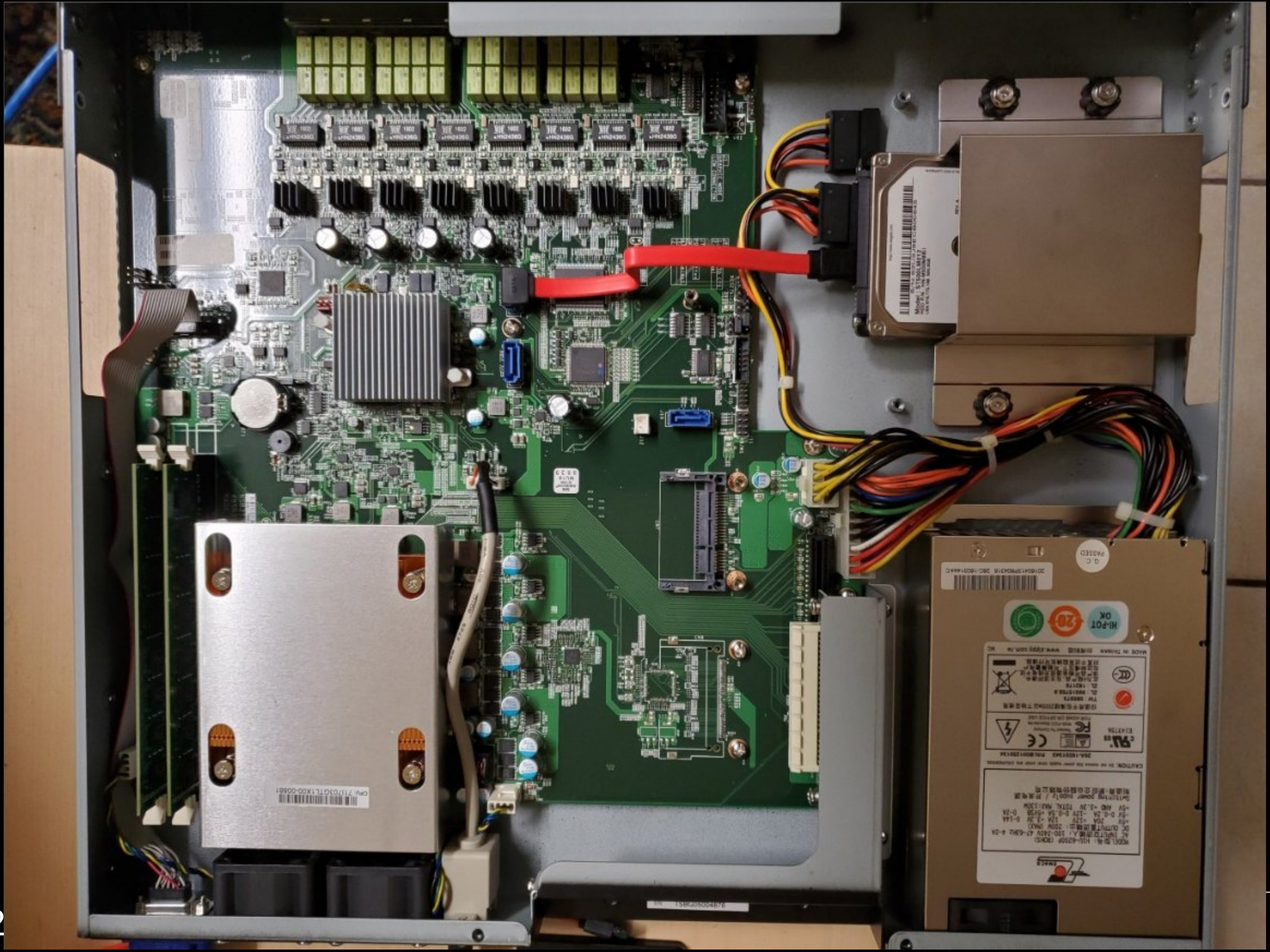


VGA, 2 more USB2s, power

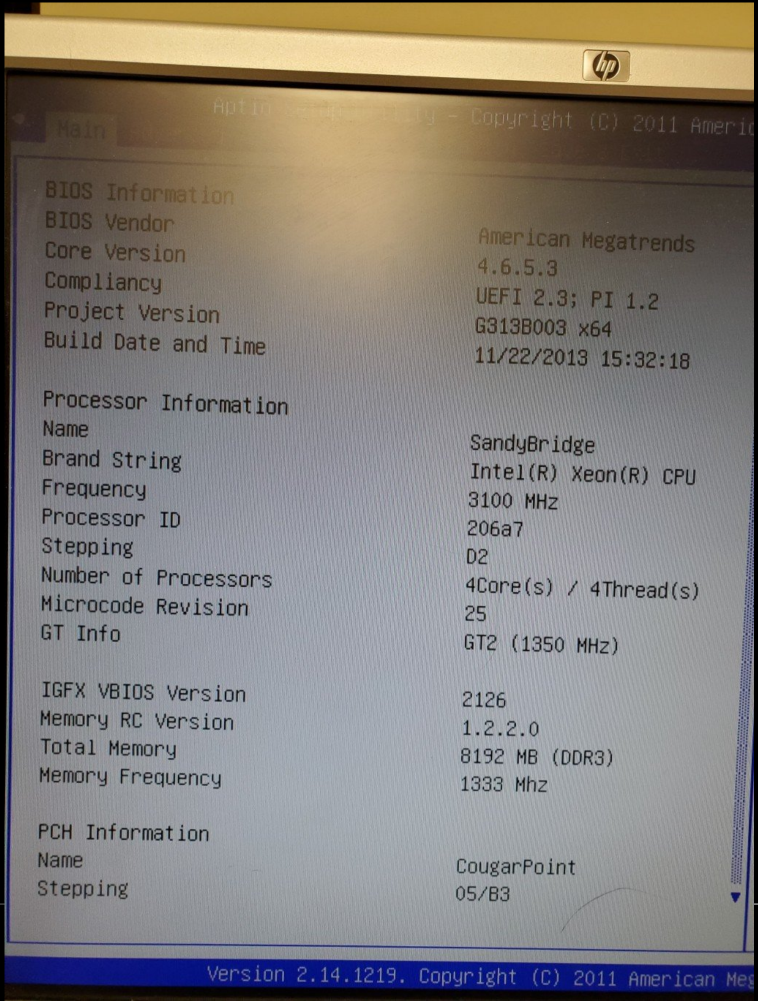


BLU, Dec 2022

A look inside



4-core SandyBridge Xeon, 8GB DDR3



```
Aptio Setup Utility - Copyright (C) 2011 Americ
Main

BIOS Information
BIOS Vendor                     American Megatrends
Core Version                    4.6.5.3
Compliancy                      UEFI 2.3; PI 1.2
Project Version                 G313B003 x64
Build Date and Time             11/22/2013 15:32:18

Processor Information
Name                            SandyBridge
Brand String                    Intel(R) Xeon(R) CPU
Frequency                       3100 MHz
Processor ID                    206a7
Stepping                        D2
Number of Processors            4Core(s) / 4Thread(s)
Microcode Revision              25
GT Info                         GT2 (1350 MHz)

IGFX VBIOS Version              2126
Memory RC Version               1.2.2.0
Total Memory                    8192 MB (DDR3)
Memory Frequency                1333 Mhz

PCH Information
Name                            CougarPoint
Stepping                        05/B3

Version 2.14.1219. Copyright (C) 2011 American Meg
```

And I paid ...

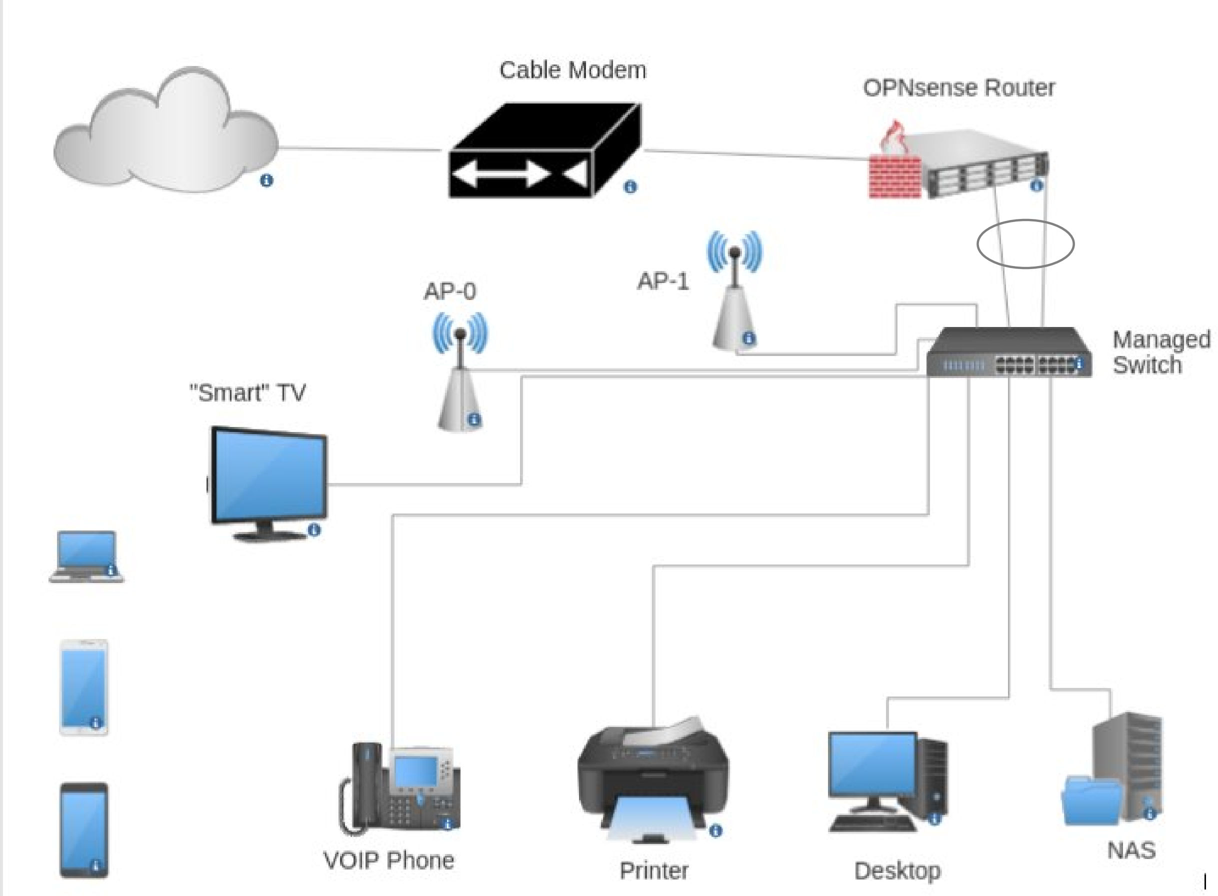
$53.11

(incl. tax & shipping, sans disk)

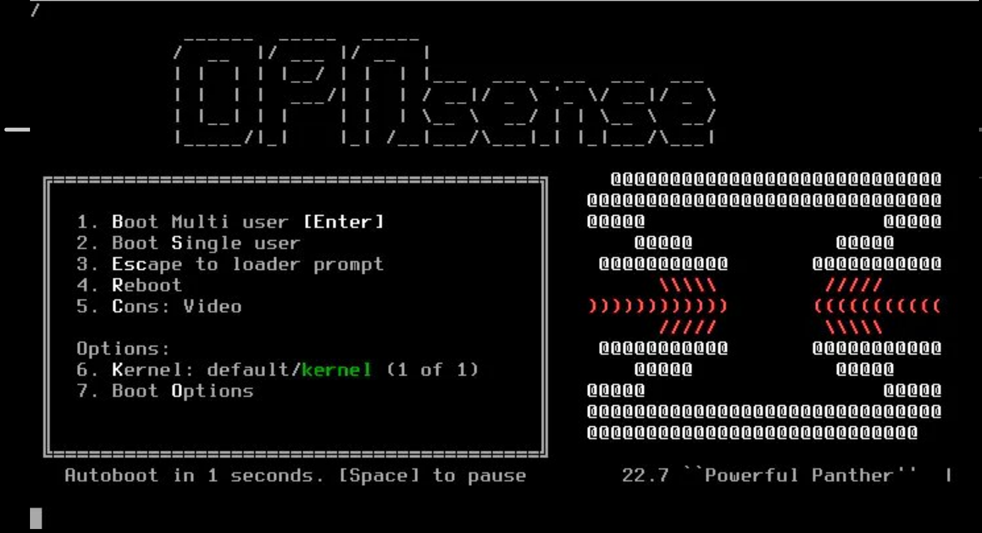
Setup

- OPNsense installed without a hitch
- All 8 GbE ports got recognized (em0 – em7)
- Configured WAN, link aggregrated 2 ports to main switch for LAN
- Setup VLANs and mapped to Wifi SSIDs:
  - Internal (NAS, desktop)
  - Devices (phones, printer, streaming devices)
  - Guest
- Configured Wireguard for remote access

Network topology



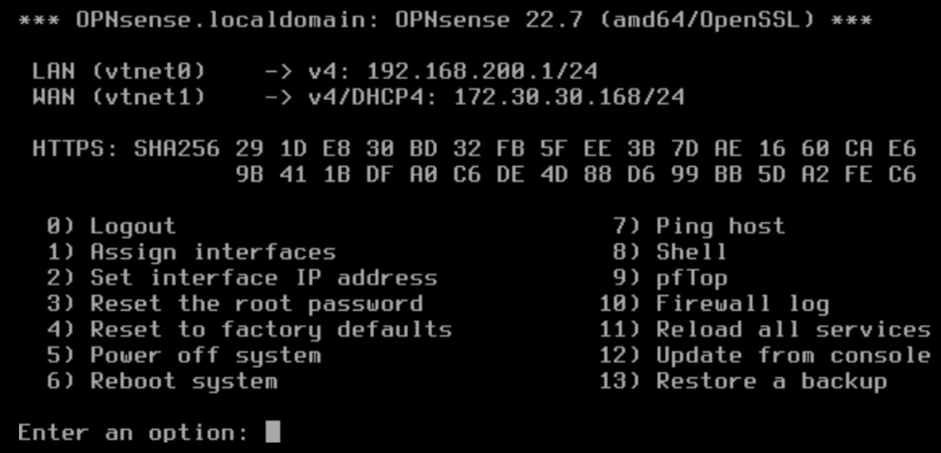
- Two links between router and switch form a LAN LAG
- VLANs go over the LAG
- Managed switch has PoE+ ports to power WiFi APs
- One ceiling-mounted AP in each floor, staggered placement



```
 1. Boot Multi user [Enter]
 2. Boot Single user
 3. Escape to loader prompt
 4. Reboot
 5. Cons: Video

 Options:
 6. Kernel: default/kernel (1 of 1)
 7. Boot Options

  Autoboot in 1 seconds. [Space] to pause        22.7 ``Powerful Panther''
```



```
*** OPNsense.localdomain: OPNsense 22.7 (amd64/OpenSSL) ***

 LAN (vtnet0)    -> v4: 192.168.200.1/24
 WAN (vtnet1)    -> v4/DHCP4: 172.30.30.168/24

 HTTPS: SHA256 29 1D E8 30 BD 32 FB 5F EE 3B 7D AE 16 60 CA E6
               9B 41 1B DF A0 C6 DE 4D 88 D6 99 BB 5D A2 FE C6

  0) Logout                              7) Ping host
  1) Assign interfaces                   8) Shell
  2) Set interface IP address            9) pfTop
  3) Reset the root password            10) Firewall log
  4) Reset to factory defaults          11) Reload all services
  5) Power off system                   12) Update from console
  6) Reboot system                      13) Restore a backup

Enter an option:
```

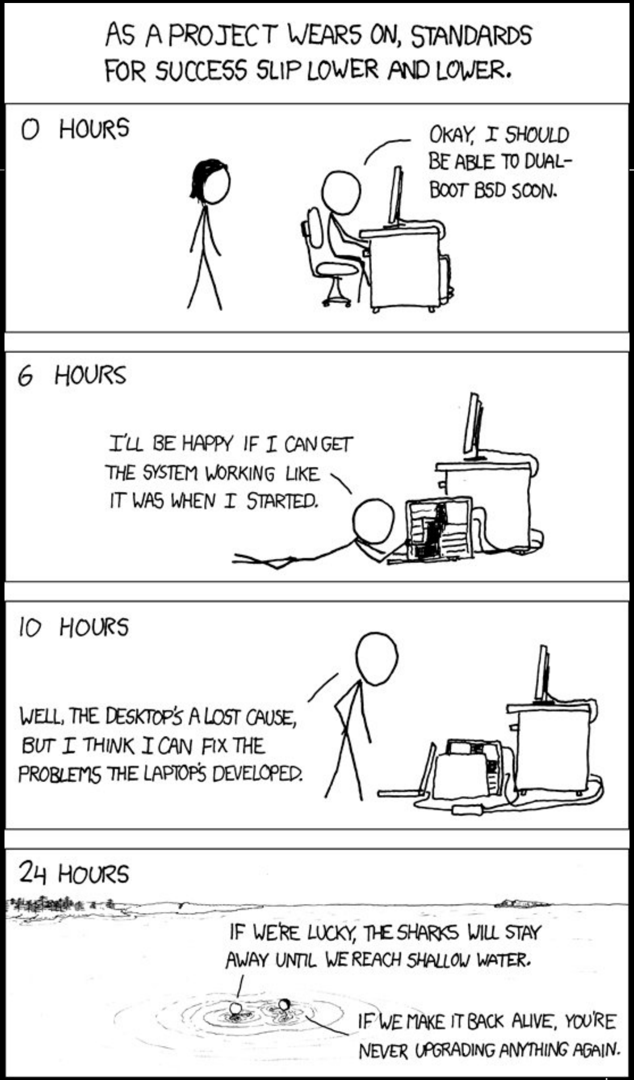

AS A PROJECT WEARS ON, STANDARDS FOR SUCCESS SLIP LOWER AND LOWER.
0 HOURS
OKAY, I SHOULD BE ABLE TO DUAL-BOOT BSD SOON.
6 HOURS
I'LL BE HAPPY IF I CAN GET THE SYSTEM WORKING LIKE IT WAS WHEN I STARTED.
10 HOURS
WELL, THE DESKTOP'S A LOST CAUSE, BUT I THINK I CAN FIX THE PROBLEMS THE LAPTOP'S DEVELOPED.
24 HOURS
IF WE'RE LUCKY, THE SHARKS WILL STAY AWAY UNTIL WE REACH SHALLOW WATER.
IF WE MAKE IT BACK ALIVE, YOU'RE NEVER UPGRADING ANYTHING AGAIN.

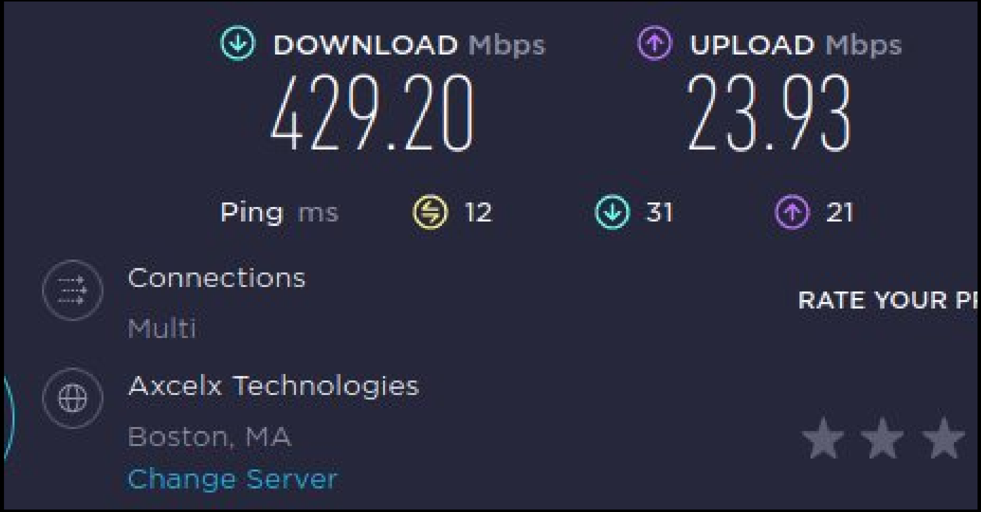
Image credit: xkcd.com/349

Performance: iperf3 simultaeneous

```
Connecting to host 172.16.2.25, port 52201
[  5] local 172.16.3.18 port 47572 connected to 172.16.2.25 port 52201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   112 MBytes   940 Mbits/sec    0    744 KBytes
[  5]   1.00-2.00   sec   110 MBytes   923 Mbits/sec    0    782 KBytes
[  5]   2.00-3.00   sec   111 MBytes   933 Mbits/sec    0    822 KBytes
[  5]   3.00-4.00   sec   111 MBytes   933 Mbits/sec    0    822 KBytes
[  5]   4.00-5.00   sec   110 MBytes   923 Mbits/sec    2    605 KBytes
[  5]   5.00-6.00   sec   111 MBytes   933 Mbits/sec    0    723 KBytes
[  5]   6.00-7.00   sec   111 MBytes   933 Mbits/sec    0    758 KBytes
[  5]   7.00-8.00   sec   111 MBytes   933 Mbits/sec    0    758 KBytes
[  5]   8.00-9.00   sec   110 MBytes   923 Mbits/sec    0    819 KBytes
[  5]   9.00-10.00  sec   112 MBytes   944 Mbits/sec    0    834 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  1.08 GBytes   932 Mbits/sec    2             sender
[  5]   0.00-10.01  sec  1.08 GBytes   929 Mbits/sec                  receiver
```

```
Connecting to host 172.16.3.18, port 5201
[  5] local 172.16.2.25 port 54792 connected to 172.16.3.18 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec   113 MBytes   949 Mbits/sec    0    430 KBytes
[  5]   1.00-2.00   sec   112 MBytes   940 Mbits/sec    0    648 KBytes
[  5]   2.00-3.00   sec   111 MBytes   933 Mbits/sec    0    717 KBytes
[  5]   3.00-4.00   sec   111 MBytes   933 Mbits/sec    0    717 KBytes
[  5]   4.00-5.00   sec   111 MBytes   932 Mbits/sec    0    749 KBytes
[  5]   5.00-6.00   sec   110 MBytes   924 Mbits/sec    0    785 KBytes
[  5]   6.00-7.00   sec   111 MBytes   933 Mbits/sec    0    830 KBytes
[  5]   7.00-8.00   sec   111 MBytes   933 Mbits/sec    0    830 KBytes
[  5]   8.00-9.00   sec   111 MBytes   933 Mbits/sec    0    830 KBytes
[  5]   9.00-10.00  sec   110 MBytes   923 Mbits/sec    0    830 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  1.09 GBytes   933 Mbits/sec    0             sender
[  5]   0.00-10.00  sec  1.08 GBytes   931 Mbits/sec                  receiver
```

Speedtest: Wired & WiFi



DOWNLOAD Mbps
429.20

UPLOAD Mbps
23.93

Ping ms 12 31 21

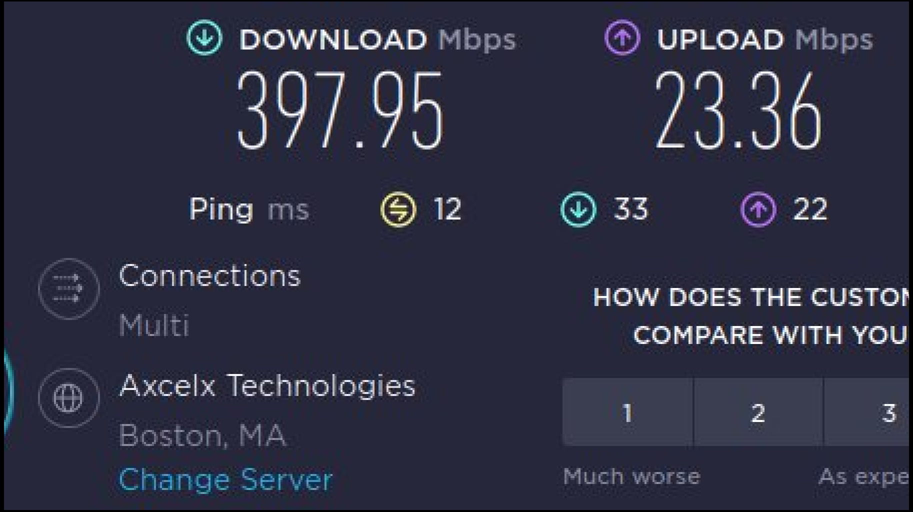
Connections
Multi

Axcelx Technologies
Boston, MA
Change Server

RATE YOUR PI

★ ★ ★

Wired



DOWNLOAD Mbps
397.95

UPLOAD Mbps
23.36

Ping ms 12 33 22

Connections
Multi

Axcelx Technologies
Boston, MA
Change Server

HOW DOES THE CUSTON
COMPARE WITH YOU

1	2	3

Much worse As expe

WiFi

WiFi test done in same room as AP

Power

- Measurements using Kill-a-Watt showed modem+router+switch consuming 89W on average over a 48 hour period
  - Includes PoE supplied to the 2 APs
- Router alone averaged ~65W
- With some tweaks to CPU power management settings in OPNsense, total average power came down to 77W
  - Fixed CPU frequency to 1600MHz (was adaptive earlier)
  - Enabled CPUs to go down to ACPI C3 state

```
dev.cpu.0.freq_levels: 3101/95000 3100/95000 3000/90163 2900/86347 2800/82600 2700/78924
2600/74419 2500/70905 2300/64048 2200/59864 2100/56612 2000/53437 1900/50315 1800/47257
1700/43458 1600/40536

dev.cpu.0.freq: 1600

dev.cpu.0.cx_supported: C1/1/1 C2/2/80 C3/3/104

dev.cpu.0.cx_lowest: C3
```

Demo time