CERT

$100 SiLK Network Flow Sensor

Ron Bandes
John Badertscher →
Dwight Beaver

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0000885

Agenda

- What are: SiLK? a Micro-server?
  Arch Linux ARM?
- Server choices (Raspberry Pi vs. PogoPlug)
- Network Infrastructure – (taps, adapters etc.)
- Design/Implementation choices
  (Network locations)
- Installation Procedures
- Server Configuration
- Server Management (updates, logs, memory)
- Problems – Things We Would
  Have Done Differently

What is SiLK?

Tools for the collection and analysis of network flow data

http://tools.netsa.cert.org

http://vimeo.com/67177328

What are Micro-Servers?

Characteristics: Small, Low Wattage, Silent

- Raspberry Pi
- PogoPlug
- Typically run Arch Linux [ARM] operating system

What is Arch Linux ARM?

Lightweight Linux OS; well supported by user community

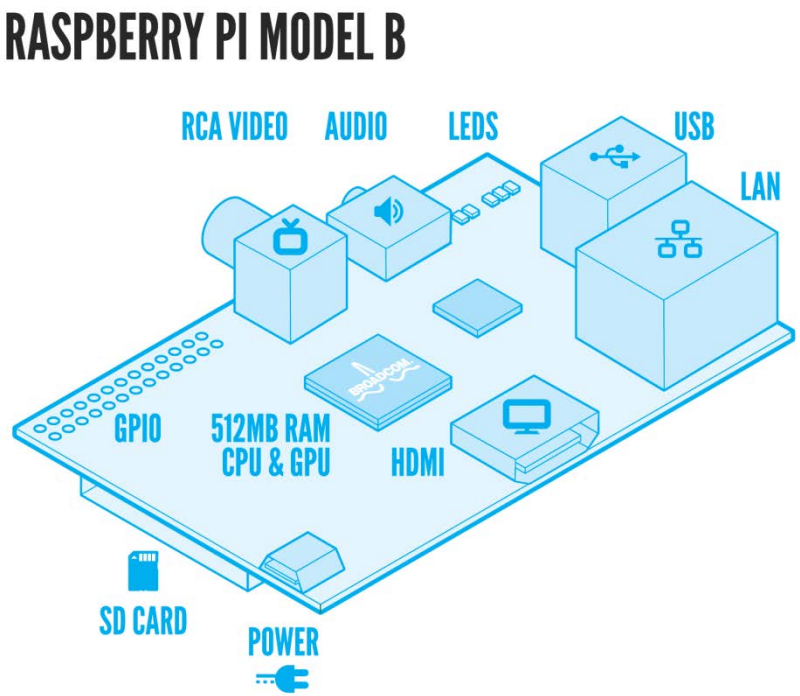
Minimalist – Simplicity - Full control by end-user, targeting competent Linux users

https://github.com/archlinuxarm

Raspberry Pi

- Linux server intended for hobbyists $40
- Includes a graphics adapter (HDMI)

http://en.wikipedia.org/wiki/Raspberry_Pi



http://www.raspberrypi.org/faqs

PogoPlug E02

- Intended as a Network Attached Storage (NAS) device $25 on eBay
- Not intended as an all-purpose server
- No console. SSH only

http://www.crunchbase.com/company/cloud-engines

http://mediastreamers.productwiki.com/pogoplug-video

Server Comparison

PogoPlug v2 (E02)

- No Console
- ARMv5te Marvell Kirkwood
- 1.2 GHz processor clock
- 256 MB RAM
- 128 MB NAND FLASH
- 4 USB 2.0 jacks
- Gigabit Ethernet
- No Real Time Clock
- Includes enclosure & power supply

Raspberry Pi model B

- Dual VideoCore IV (HDMI)
- ARMv6h ARM1176JZFS
- 700 MHz processor clock
- 512 MB SDRAM
- SD, MMC, SDIO slot
- 2 USB 2.0 jacks
- 10/100 Mbps Ethernet (USB)
- No Real Time Clock
- User provides enclosure & power supply

Alternative Platforms

- Raspberry Pi
- Old laptop/desktop
- Virtualization!

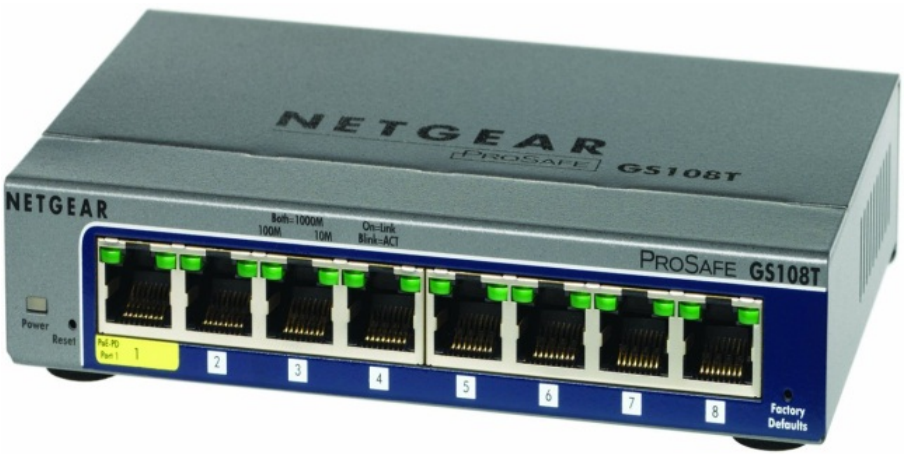
Network infrastructure choices

Taps, adapters etc.

- Cheap managed or “smart” switches

  Netgear GS108T-NAS

  - VLANs
  - LAGs
  - Port Mirroring
  - $80



- Iptables on a wireless access point (OpenWRT)
  - iptables -A PREROUTING -t mangle -j ROUTE --gw <sensor ip> –tee
  - iptables -A POSTROUTING -t mangle -j ROUTE --gw <sensor ip> --tee

Solution Components

$100 Solution

- PogoPlug server ($25)
- NoName Ethernet Adapter ($4)
- MikroTik switch as network tap ($40)
- 16 GB Flash Drive ($10)

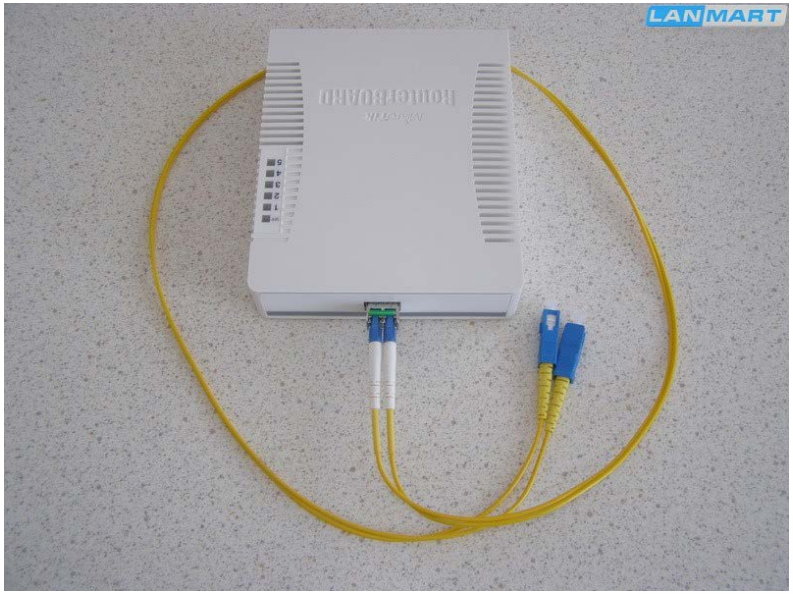
2nd Ethernet Adapter

- For network monitoring – 10/100 Mbps $3.75
- The 1st adapter is for server management

http://www.tmart.com/Rj45-Ethernet-10-100-USB-Network-Adapter-Purple_p123164.html

Network Tap

- MikroTik RB260 switch w/SPAN port $40



http://www.lanmart.ru/blogs/review-mikrotik-rb260gs

http://www.cisco.com/en/US/products/hw/modules/ps4999/products_tech_note09186a00807a30d6.shtml

Design & Implementation Choices

- Network monitoring locations
- Separate analysis server or combined node
- Implications of flash storage

Network Monitoring Locations

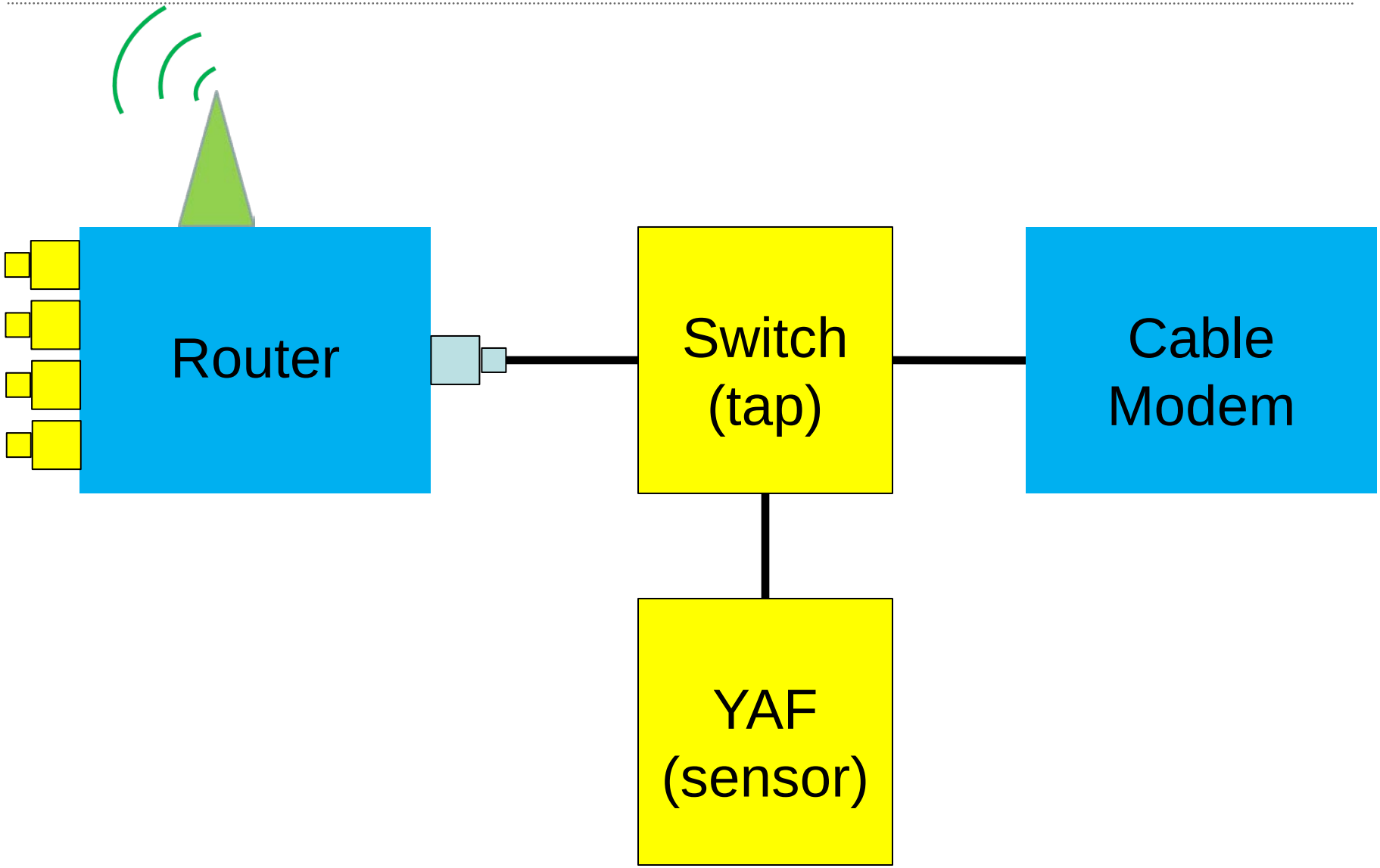
Between edge router and cable modem

- Easy constriction point for monitoring
- Outside the Network Address Translation (NAT)

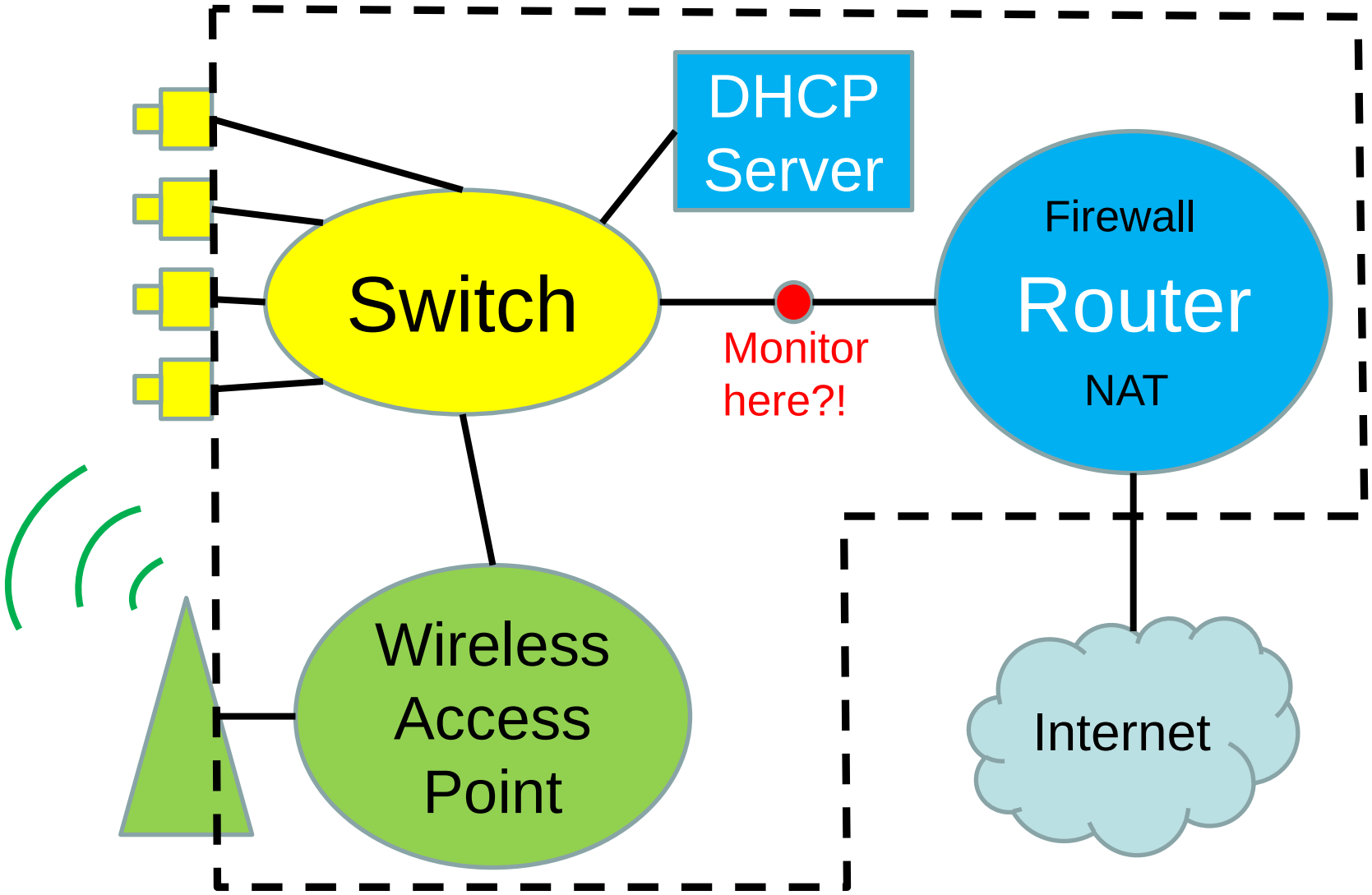
On LAN

- Inside the NAT
- Hard to place when a residential router is used
  - Need to interpose tap between the LAN switch and the router component, which is NOT exposed in residential router

Tap between Router and Cable Modem



Residential Routers

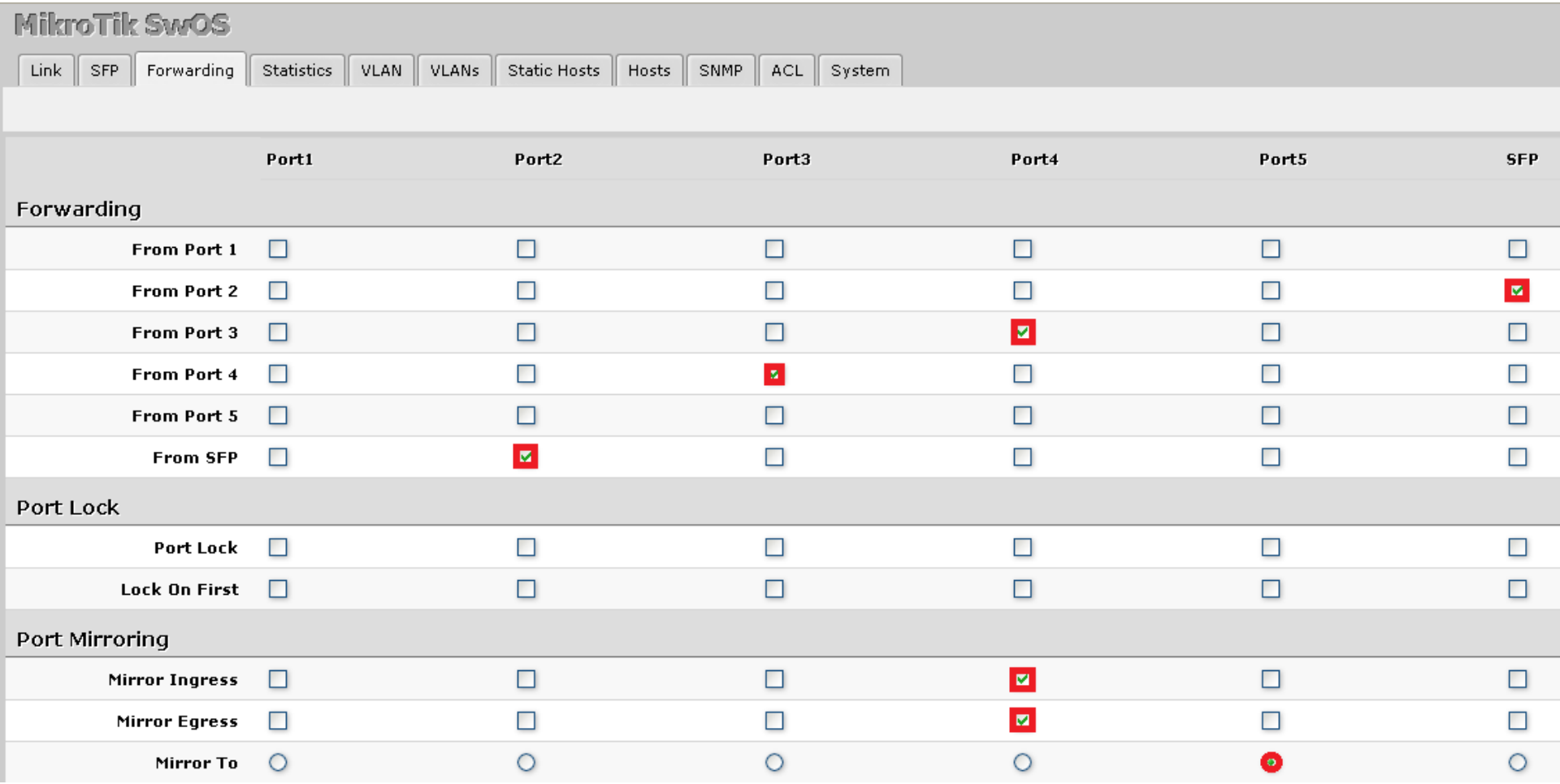


Configuring the Tap

- Port 1 – Switch management
- Ports 2&6 – Unused
- Ports 3&4 – Link to be tapped (rtr & cable mdm)
- Port 5 – Monitoring port 4

http://www.tapmytrees.com/

Switch (tap) Configuration



Repurposing Non-Hobbyist HW

- PogoPlug requires you to register on pogoplug.com before you can SSH into your device
- This could be a problem if you bought the PogoPlug on eBay and the original owner registered it
- PogoPlug can be repurposed for a variety of applications (e.g, Tor Relay, NAS, Streaming Server etc.)

Installation Procedures

1. Install Arch Linux ARM
2. Update Arch Linux ARM*
3. Install 2nd Ethernet adapter
4. Install YAF
5. Install SiLK

*Run Update FREQUENTLY

*When in doubt…update ***again!***

http://www.aquacityplumbing.com/images/pages/Plumbing-Installation.jpg

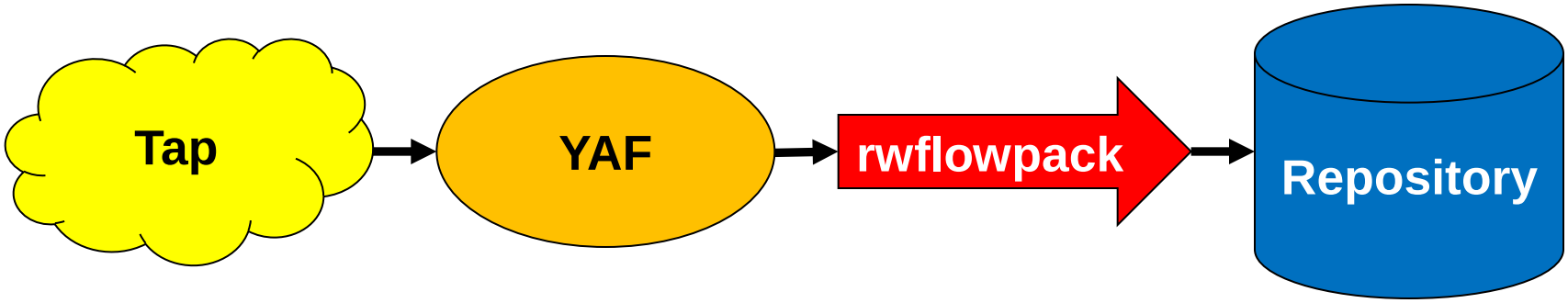
Installation Challenges

- Arch Build System: *buildpkg* & *pacman*
- *Systemd* vs. *init*
- *vi* vs. *vim*
- *U-Boot* boot-loader
  - Installed on internal Flash, not mass storage
  - Arch Linux requires newer *U-Boot* than what comes on the PogoPlug

http://wwiimodeller.co.nz/wp-content/uploads/1355087242_s_010_basic_boxes_small.jpg

Server Configuration

1. Create “service” to bring up 2nd Ethernet adapter
2. Create service for rwflowpack
3. Create service for YAF

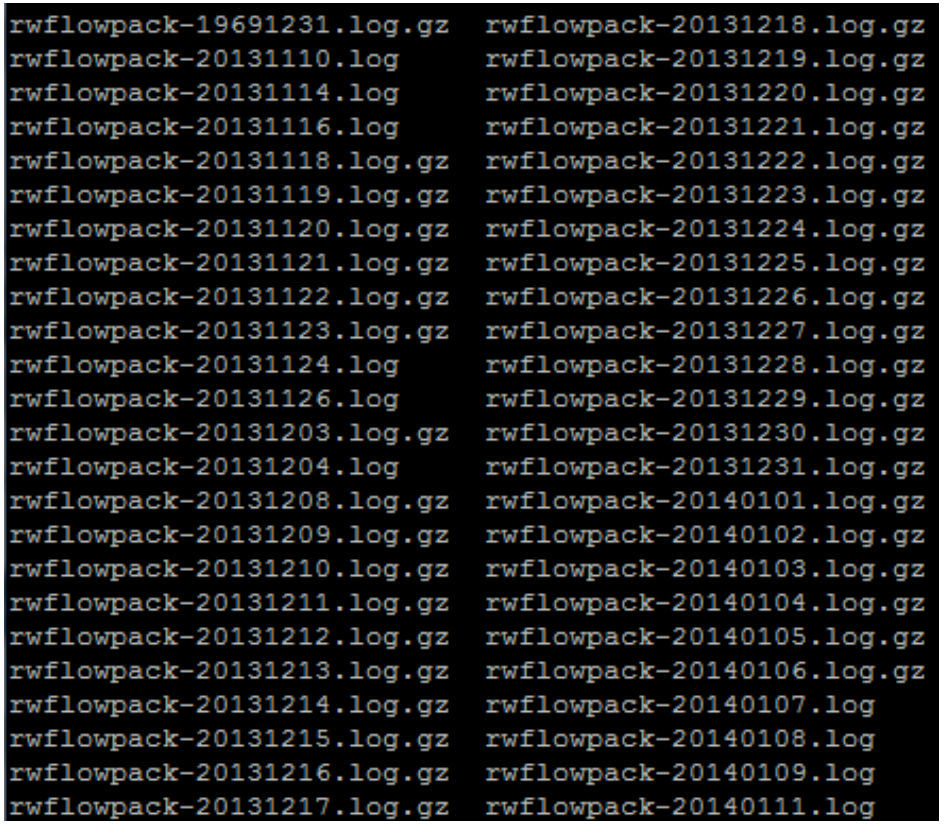


Management procedures

Arch Linux ARM updates

Logging

- Logs will eventually fill storage if you don't rotate them
- FLASH memory has a limited number of writes
  - Minimize writing by minimizing logging



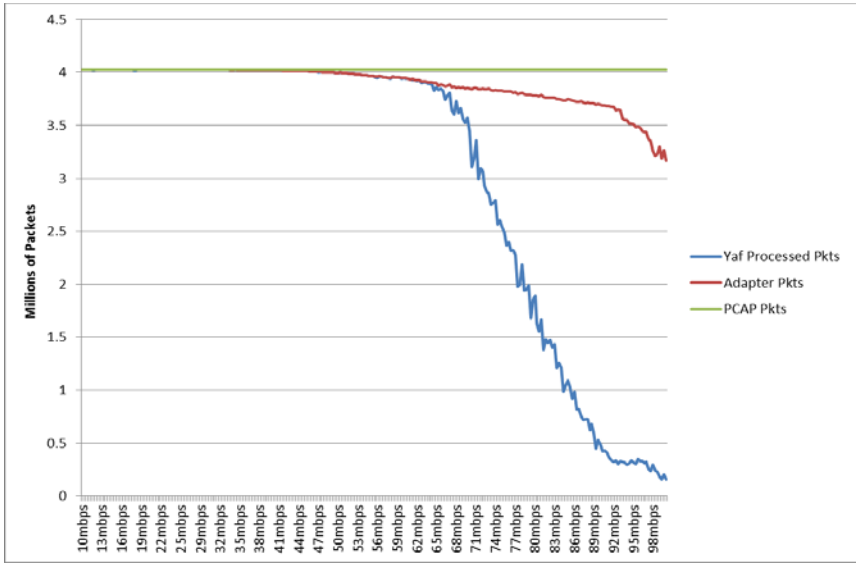
It works!

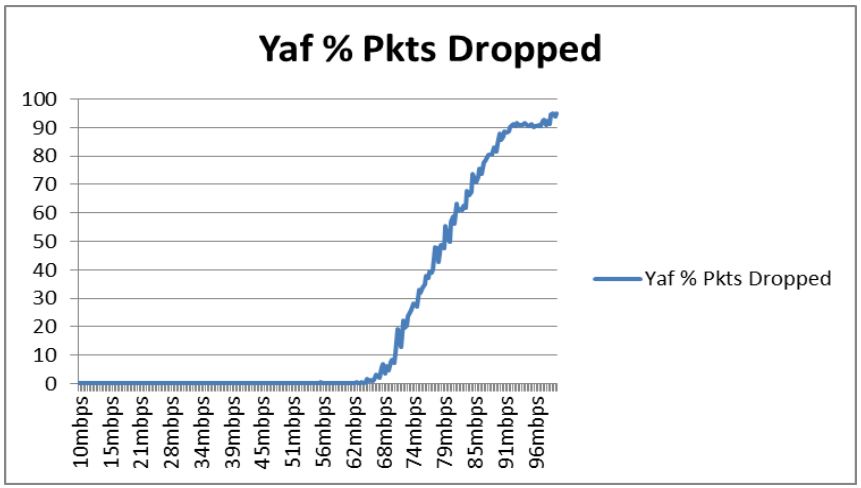
```
[root@pogotor system]# rwfilter --type=in,inweb --all=-
| rwuniq --fields=dip
                                        dIP|   Records|
                                192.0.2.212|        55|
[root@pogotor system]# rwfilter --type=out,outweb --
all=- | rwuniq --fields=sip
                                        sIP|   Records|
                                192.0.2.212|        49|
[root@pogotor system]# rwfilter --type=all --all=- |
rwuniq --fields=type
   type|   Records|
 outweb|        33|
     in|        18|
    out|        16|
  inweb|        37|
ext2ext|        30|
```

Performance & Metrics

Raspberry Pi

- No PCI BUS
- NIC lives on USB bus
- 700 MHz processor main bottle neck
- YAF starts dropping packets around 55 Mbps
- No application labeling





Problems: Things We Would Have Done Differently…

- You don’t get what you don’t pay for…
  - Effort (Opportunity Cost)
  - Bandwidth
- Update management
- *U-Boot*
- PogoPlug becomes a brick

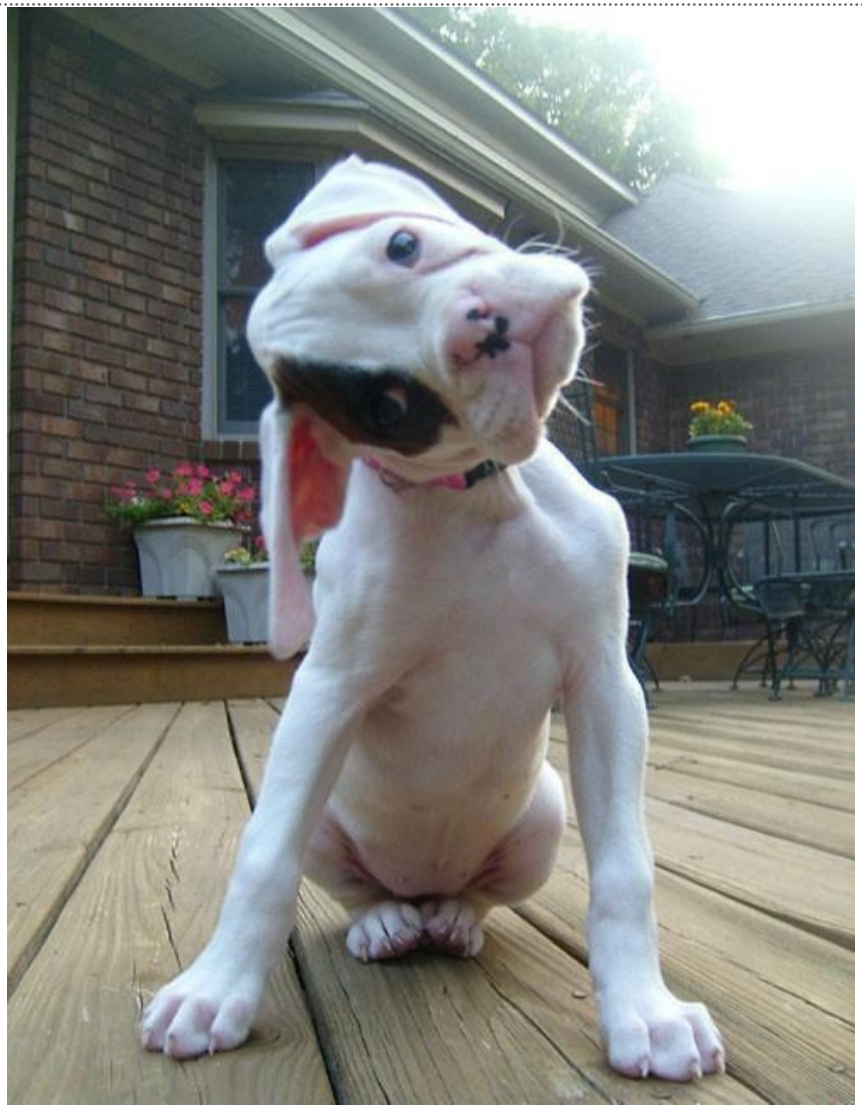
http://marketingforhippies.com/wp-content/uploads/2012/09/gravestone.jpg

Software Problem with ARMv5

Unaligned memory word accesses on ARMv5 processors have results that are “implementation defined.” Some Memory Management Units may handle this improperly.

It also helped (a lot) having CERT developers, Emily Sarneso and Dan Ruef, available to help.

Questions?



http://cuteoverload.files.wordpress.com/2012/10/8024316149_438e648edf_b1.jpg%3Fw%3D560