



# \$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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon<sup>®</sup>, CERT<sup>®</sup> and FloCon<sup>®</sup> are registered marks of Carnegie Mellon University.

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>

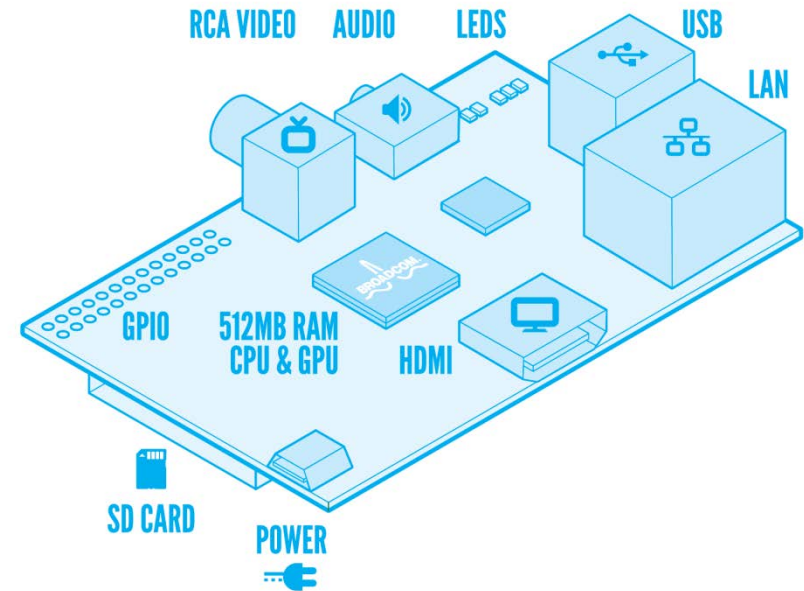
# Raspberry Pi

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



[http://en.wikipedia.org/wiki/Raspberry\\_Pi](http://en.wikipedia.org/wiki/Raspberry_Pi)

## RASPBERRY PI MODEL B



<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

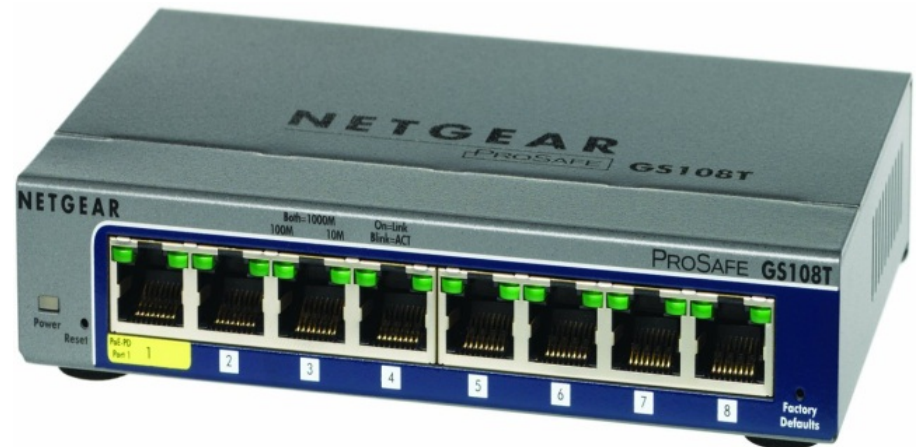
---

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)

# 2<sup>nd</sup> Ethernet Adapter

---

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



[http://www.tmart.com/Rj45-Ethernet-10-100-USB-Network-Adapter-Purple\\_p123164.html](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](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)

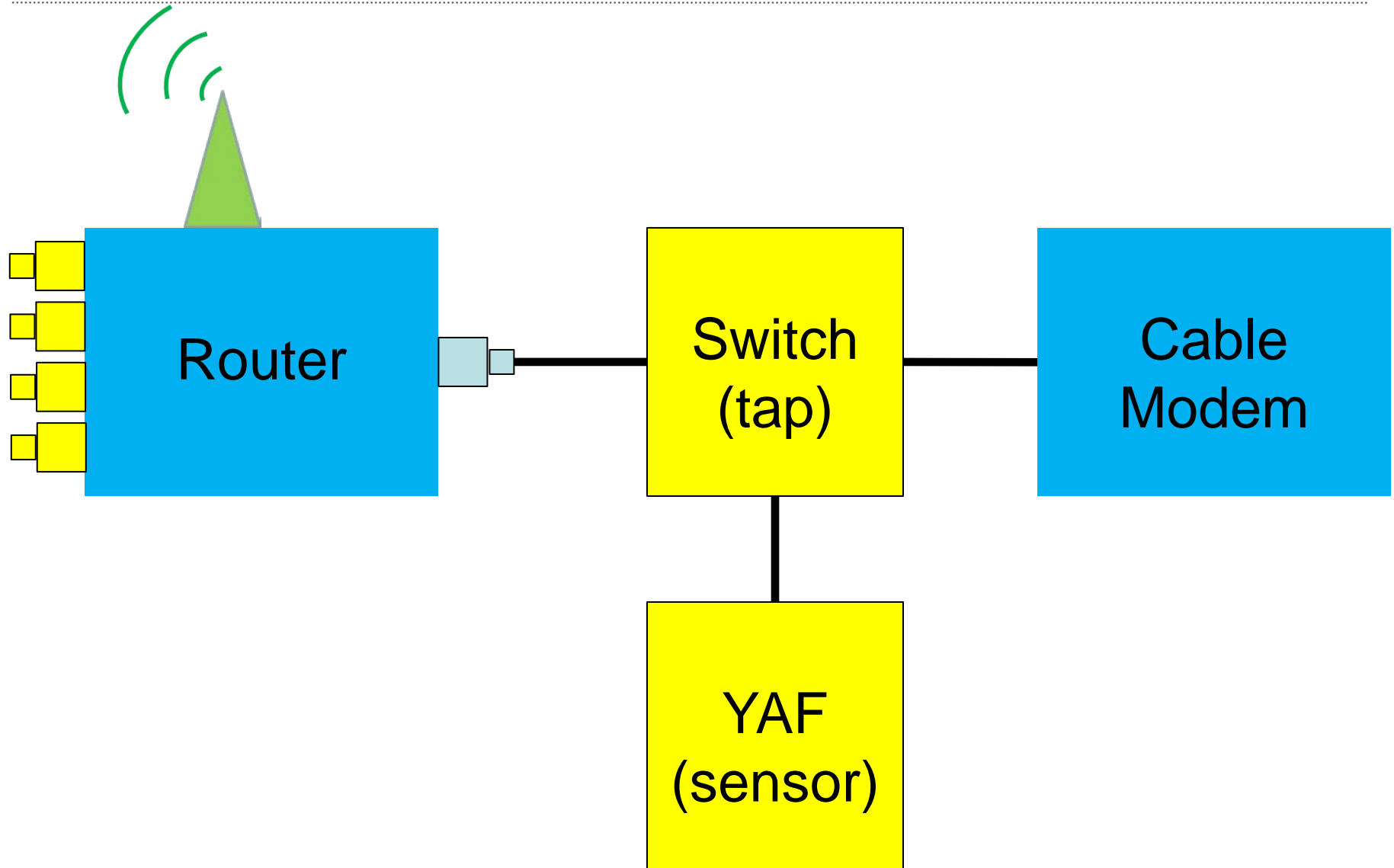
## On LAN

- 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

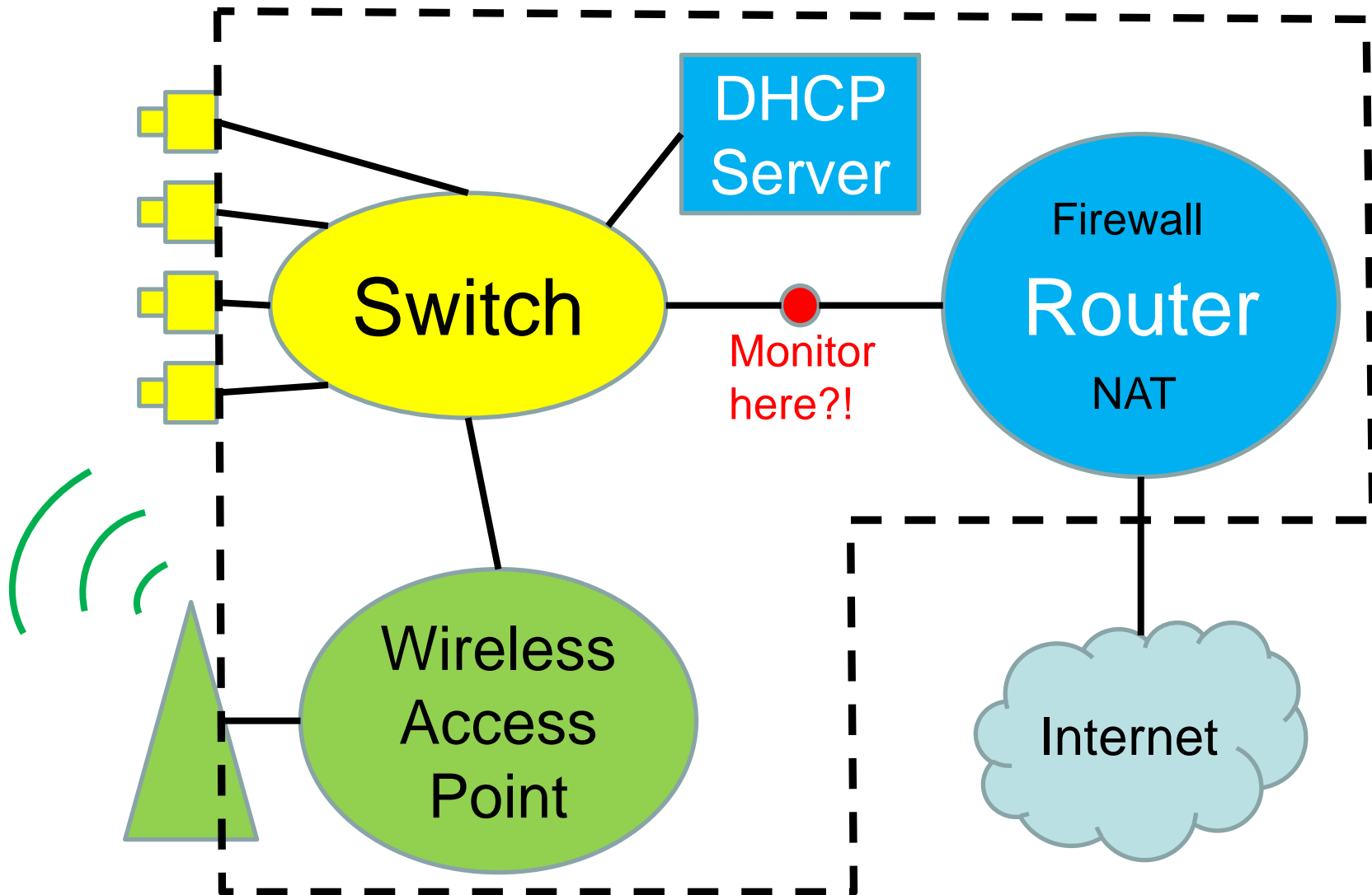


# Tap between Router and Cable Modem

---



# 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

## MikroTik SwOS

[Link](#)
[SFP](#)
[Forwarding](#)
[Statistics](#)
[VLAN](#)
[VLANs](#)
[Static Hosts](#)
[Hosts](#)
[SNMP](#)
[ACL](#)
[System](#)

	Port1	Port2	Port3	Port4	Port5	SFP
<b>Forwarding</b>						
From Port 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
From Port 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
From Port 4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
From Port 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
From SFP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Port Lock</b>						
Port Lock	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock On First	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Port Mirroring</b>						
Mirror Ingress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mirror Egress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mirror To	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

# Repurposing Non-Hobbyist HW

---

- PogoPlug requires you to register on [pogoplug.com](http://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 2<sup>nd</sup> 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

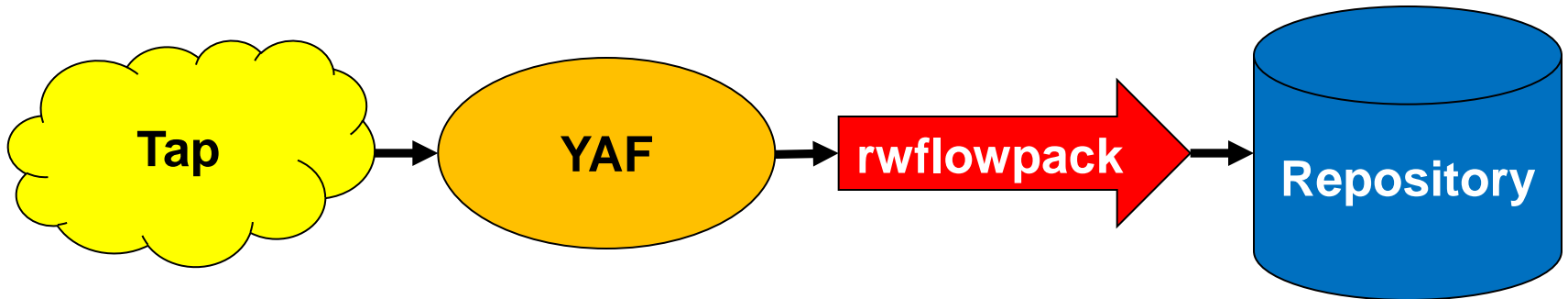


[http://wwiimodeller.co.nz/wp-content/uploads/1355087242\\_s\\_010\\_basic\\_boxes\\_small.jpg](http://wwiimodeller.co.nz/wp-content/uploads/1355087242_s_010_basic_boxes_small.jpg)

# Server Configuration

---

1. Create “service” to bring up 2<sup>nd</sup> Ethernet adapter
2. Create service for rflowpack
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

```
rwflowpack-19691231.log.gz  rwflowpack-20131218.log.gz
rwflowpack-20131110.log    rwflowpack-20131219.log.gz
rwflowpack-20131114.log    rwflowpack-20131220.log.gz
rwflowpack-20131116.log    rwflowpack-20131221.log.gz
rwflowpack-20131118.log.gz rwflowpack-20131222.log.gz
rwflowpack-20131119.log.gz rwflowpack-20131223.log.gz
rwflowpack-20131120.log.gz rwflowpack-20131224.log.gz
rwflowpack-20131121.log.gz rwflowpack-20131225.log.gz
rwflowpack-20131122.log.gz rwflowpack-20131226.log.gz
rwflowpack-20131123.log.gz rwflowpack-20131227.log.gz
rwflowpack-20131124.log    rwflowpack-20131228.log.gz
rwflowpack-20131126.log    rwflowpack-20131229.log.gz
rwflowpack-20131203.log.gz rwflowpack-20131230.log.gz
rwflowpack-20131204.log    rwflowpack-20131231.log.gz
rwflowpack-20131208.log.gz rwflowpack-20140101.log.gz
rwflowpack-20131209.log.gz rwflowpack-20140102.log.gz
rwflowpack-20131210.log.gz rwflowpack-20140103.log.gz
rwflowpack-20131211.log.gz rwflowpack-20140104.log.gz
rwflowpack-20131212.log.gz rwflowpack-20140105.log.gz
rwflowpack-20131213.log.gz rwflowpack-20140106.log.gz
rwflowpack-20131214.log.gz rwflowpack-20140107.log
rwflowpack-20131215.log.gz rwflowpack-20140108.log
rwflowpack-20131216.log.gz rwflowpack-20140109.log
rwflowpack-20131217.log.gz rwflowpack-20140111.log
```

# It works!

---

```
[root@pogotor system]# rfilter --type=in,inweb --all=-  
| rwuniq --fields=dip
```

dIP	Records
192.0.2.212	55

```
[root@pogotor system]# rfilter --type=out,outweb --  
all=- | rwuniq --fields=sip
```

sIP	Records
192.0.2.212	49

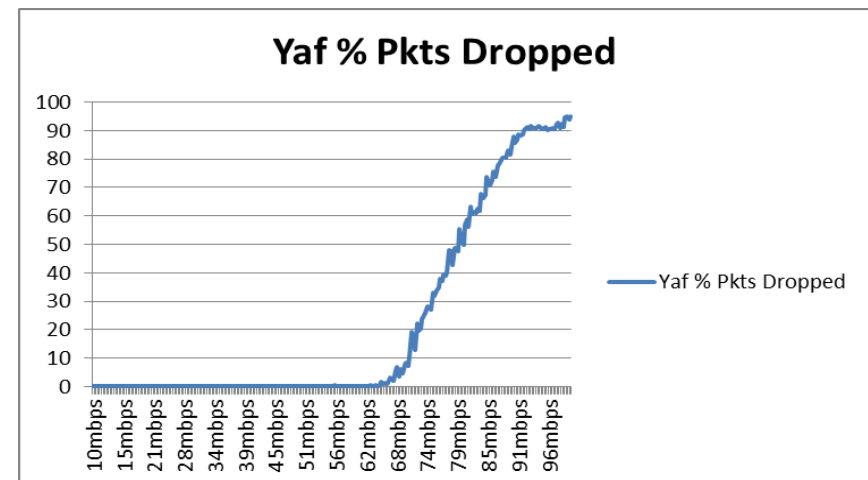
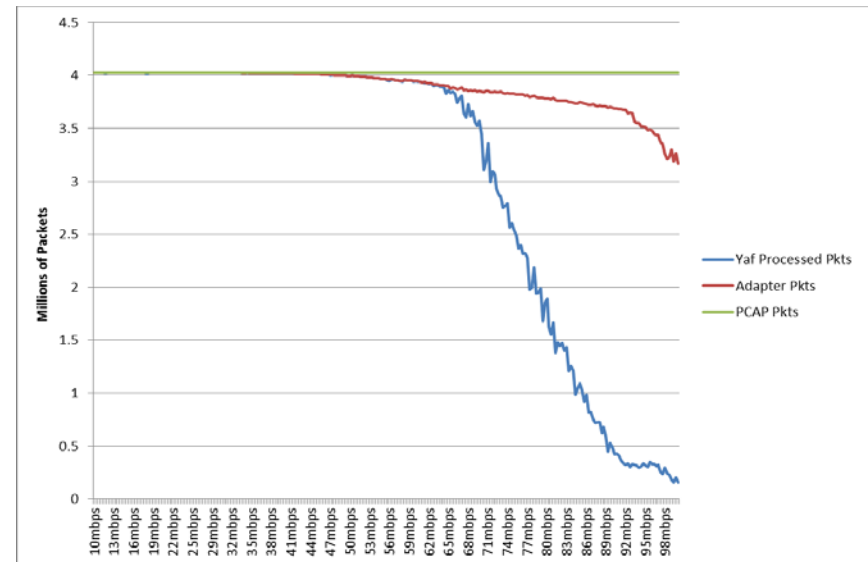
```
[root@pogotor system]# rfilter --type=all --all=- |  
rwuniq --fields=type
```

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