OpenBlockS

or

{small, silent, cheap}

pick three!

Henri Servomaa

TLUG Jan 14, 2006

Presentation outline

OpenBlockS basic hw/sw overview
General usage discussion

Home, SOHO, DC use cases
Hobby uses

Sniffing demo


OpenBlocks
Plat'Home
SAFETY MATCH


openBlocks
Ether1
Ether2
RS-232C
DC IN
INIT

Wow? What is it ??

- small PPC server made by PlatHome (http://www.plathome.co.jp)

  size: 7 x 10 x 5 cm (1U)
- headless
- 24/7 operation
- runs Linux
- basically unrestricted in capab.

Some hardware specs

- CPU: IBM 405GP (PPC) @ 200MHz
  - MMU, Ethernet, serial, PCI, SRAM, SDRAM
- 8 MB ROM
- 64 MB RAM
- RS232 serial port
- 2 x RJ45 ethernet (100 BaseT)
- 2.5 “ IDE disk or CF

Electrical mumble

- CPU typical 1300 mW
- Peripherals (eth, bus) 1000 mW
- CF 25mW - 300 mW
- Hard disk 1-5 W

Total with CF: 2.4 - 2.6 W
Total with HD: 3.3 - 7.3 W

For comparison:

50 mm CPU fan ~ 1.0W
80 mm case fan ~ 2.0 W

Typical 8 port switch ~ 4 W

About manufacturer

Century Systems Inc:
http://www.centurysys.co.jp

Largest user/developer?
http://www.iij.ad.jp/en/pressrelease/2005/0222.pdf

OBS
Shipped software

- 2.4.10 kernel (2002)
- 2.4.26 kernel (2005)
- SSD linux (v0.1 , v0.2, v0.3-current)
- iptables, dhcpd, bind, sendmail, apache, snort, X11...
- http://plathome.co.jp/support/labo/obssr/

SSD linux

- Sotokanda Software Distribution

v0.3 is development tree. Latest release Jan 6 2006

Kernel 2.4.26
gcc 3.3 + devtools

Previous distributions have obsolete libs or lack many dev tools and libs

Boot configuration

Default

At boot, the kernel is read and executed from flash ROM and no use is made of storage devices

Utility “flashconfig” to:

1. Enable booting from CF
2. Enable booting from HD
3. Boot from ROM
4. Write config to ROM

Hmm.. what could I do with this ?

Full fledged Linux:!

64MB, HD, gcc, free software, source...

But...

CPU@200 MHz -> Not CPU bound tasks

SSL, 3DES etc

IPSec VPN ok for ~ 10 users (guesstimate)

Older distributions “obsolete”, difficult to compile apps.

Perspective:Ye olde days at HUT ...

- First student system at was SUN/3
- HP 700 series, CPU up to 66 MHz !!
- Best work done on:
  - SS10, 50MHz !!!
  - Ultra 1, 120 MHz -> OMG!!
- IO IO on to work we go..

Use cases for home & SOHO

- router: default gw to inet, PPPoE
- firewall: masq, one segment for DMZ
- DNS (Internal + forward)
- DHCP

Using CF for storage

Firewall

- ip routing is in kernel
- packet filtering in kernel
  - (http://www.netfilter.org/)
- userland utility: iptables
- many features (NAT, QoS, mangling..)
- stateful (IPV4)
- cf. http://www.packetfactory.net/Projects/firewalk/
- stable/mature (34 bugs)

Problem with iptables:

If NAT rules are required, scripting complexity grows.
-> weakened security
-> poor maintainability

- http://www.simonzone.com/software/guarddog (gui)
- http://www.shorewall.net/ (hll)
- http://www.fwbuilder.org/ (gui, multitargets)
- http://firehol.sourceforge.net/ (hhl)

Use nmap to verify your rules!

Local DNS

- Forward external lookups
- Resolve local lookups

Needs only reference to self in /etc/hosts

-> avoid maintenance of /etc/hosts
on multiple machines

named.conf

```
options {
    directory "/etc/namedb";
    listen-on { 127.0.0.1; 10.0.2.1/32; };
    forward only;
    forwarders { 202.232.2.38; };
    query-source port 53;
};
```

named.conf continued

```
zone "tin.local" {
    type master;
    notify no;
    file "zone.tin.local";
};
zone "2.0.10.in-addr.arpa" {
    type master;
    notify no;
    file "revp.tin.local";
};
```

Populate zones with standard entries

DHCP config

```
option domain-name "tin.local";
option domain-name-servers 10.0.2.1;
get-lease-hostnames true;

subnet 10.0.2.0 netmask 255.255.255.0 {
    range 10.0.2.128 10.0.2.254;
    option routers 10.0.2.1;
    option domain-name "tin.local";

    host kebab {
        hardware ethernet 00:0A:95:C5:E8:46;
        fixed-address 10.0.2.30;
    }
}
```

DC tasks

- netboot install server
  - RH using kickstart
  - Debian using FAI
  - Solaris using jumpstart
- dump/restore
- syslogger

Hobby/research

OpenBlockS has a RS232 serial connector!

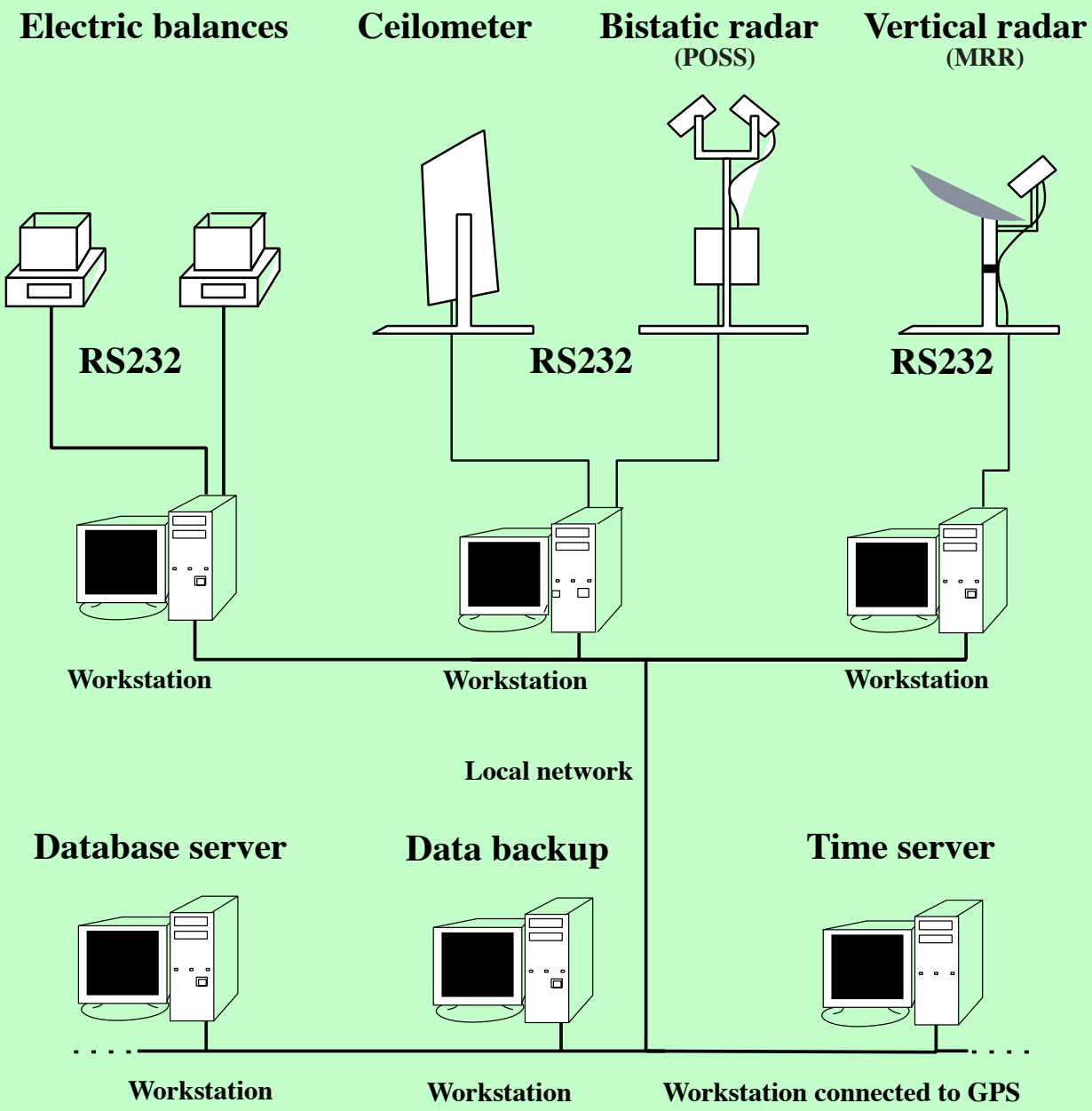
You can use it for data acquisition and distribution over the net!

Battery operation (5V)!

Application types:

- environment sensors
- gps logger
- industrial/scientific sensors

For example...


Electric balances
Ceilometer
Bistatic radar
(POSS)
Vertical radar
(MRR)
RS232
RS232
RS232
Workstation
Workstation
Workstation
Local network
Database server
Data backup
Time server
Workstation
Workstation
Workstation connected to GPS

Packet sniffing

- tcpdump, snort
- http://naughty.monkey.org/~dugsong/dsniff/
  - collection of tools:

    dsniff, mailsnarf, msgsnarf, urlsnarf, arpspoof
    dnsspoof, macof

Roundup

Nice tinkering platform

cf {Kurobox, Soekris, Mac mini}

Great for simple services

basic net infrastructure

log storage

Cheap? ..

Old distro sucks.

-> SSD any good ?

THANK YOU