Far away but still close

Dr. Dirk Wetter, Hamburg

mail@drwetter.org

Dr. Wetter
IT-Consulting

Overview

I. Intro

II. What's the benefit?

III. Remote Management Devices

IV. Operation

I. Intro

Out-of-Band end devices:

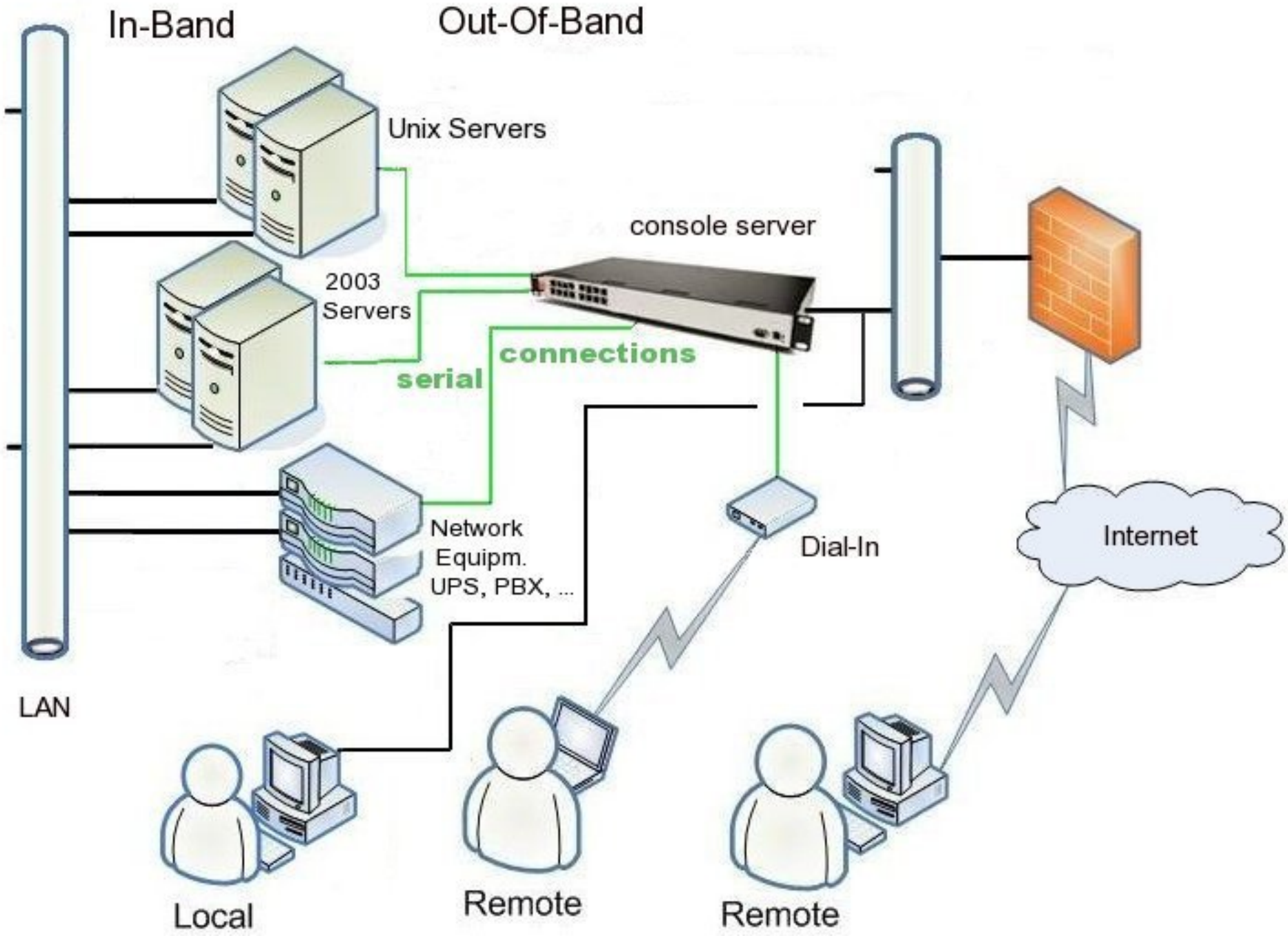
a) Serial-over-IP, vulgo console servers

b) KVM-over-IP

c) Remote-Power

d) Management processors (covering a+c)

I. Intro


In-Band
Out-Of-Band
Unix Servers
console server
2003
Servers
serial
connections
Network
Equipm.
UPS, PBX, ...
Dial-In
Internet
LAN
Local
Remote
Remote

I. Intro

	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
- Security reasons

II. Why?

Higher Availability:

- marketing speak: reduces downtime
- sysadmin speak: don't have to come in in the middle of the night (fast reaction)
- access ~ from all over the world (but: security)

II. Why?

Money:

- lost earnings
- penalties (SLA)
- costumers leaving, non-satisfaction

II. Why?

Productivity:

- data center is cold+uncomfortable
- maintenance/emergency operations better from comfortable “admin commander center/chair”
- flexibility

II. Why?

Space:

- data center space wasted
- it's precious

II. Why not...

... use it if not properly addressed:

Security:

- 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

III. Remote Management Devices
a) Unix

- Time of console servers with propriety OS is over
  (Cisco 2511, Xyplex Maxserver, Lantronix SCSxx00)

- embedded Linux!
  - “8.5” vendors: Avocent/Cyclades, Digi, Raritan, Perle, Lantronix, MRV, Logical, Opengear
  - CPU Arch: PPC, Arm, MIPS, i386
    (48 MHz PPC to 1 GHz PIII)

III. Remote Management Devices
a) Unix / serial

User interfaces (administration / operation):

- Linux command shell
- Proprietary shells:

  from sophisticated (IOS-like, MRV) to relatively dumb
- Web browser
- Java applets, applications
- any combinations of the above

III. Remote Management Devices
a) Unix

Watch out for:

- Security (more below)
- Syslog forwarding:
  - kernel + authpriv messages +port connects of/to console servers
- NTP: more or less (restrictions of busybox NTP)

III. Remote Management Devices
a) Unix

Further considerations:

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

III. Remote Management Devices
a) Unix

Nice to have:

- Port status (wrong serial adapters/cables)
- no fans (can fail, thus can system)
- Factory reset

- cross development kit
- redundancy options: dual PSU, dual Ethernet
- PCMCIA-Slots, if needed

III. Remote Management Devices
a) Unix

Last years review for iX-magazine:

- GPL compliance
- Security shop of horrors (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) Unix

security, cont'd:

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

III. Remote Management Devices

b) Windows (et al)

- KVM-over-IP has been around since 2000
- “poor man's solution”: VNC/RDP over SSH
- Windows 2003

III. Remote Management Devices
b) Windows and others

KVM over IP:

- KVM signals electronically transformed in VNC
- K,M: (USB), PS/2, Sun
- V: VGA-UXGA (RGB), DVI?
- Access via:
  - Java-capable browser
  - VNC viewer
  - ActiveX needed sometimes (ups)

III. Remote Management Devices
b) Windows and others

KVM over IP:

- in theory w/o configuration from BIOS to OS GUI
- Price: is ~30% more than console server

  addt'l. cost (~ 100 Euros per node)

  for converter to VNC
- available as PCI card / appliance

III. Remote Management Devices
b) Windows and others

VNC over SSH:

- no OOB technology
  - → needs kernel + IF up & running
- VNC/RDP tunneled over PPP (eth. if s/w)
- integrated in
  - → Opengear's console server: *SDT*
  - → Digi: *virtual KVM*

III. Remote Management Devices
b) Windows and others

Windows 2003 (watch your neighbor):

- comes with **E**mergency **M**anagement **S**ervice
- text mode, also for recovery console
- serial redirection of BIOS is on during install:

  → EMS activated

  (`bootcfg /EMS on /PORT` *`port`* `/BAUD` *`baud`*)

III. Remote Management Devices
b) Windows and others

Windows 2003 (cont'd):

- if OS is up: **S**pecial **A**dministration **C**onsole
- prompt: limited command set
- `cmd` after authentication gives `cmd.exe`

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

III. Remote Management Devices

c) Remote Power

Simple type:

- 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/HTTP
- some: HTTPS/SSH, SNMP agent/traps
- 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”

How do I manage/operate my OOB equipment?

- Hardware
- Software

- both: C/S architecture
  - server: manages OOB end devices
  - client: UI

III. Remote Management Devices
d) “über management”

Hardware (from one vendor):

- 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 (original: Ohio State University L.)
  - only console servers

- C(-)LIM / MO:
  - commercial (Ki Networks)
  - 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 end 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: `--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:

- Windows + Unix platforms
- additional GUI for connect, config
- configures known console servers
- “backup-failover” (BFD) = CLIM cluster
- notification upon pattern (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, has really anyth. else changed?
- well: only emser tunnels
  - ➔ no support of “legacy” console servers

- CLIM+MO:
  - no ChangeLog
  - no clear release cycles
  - English only (not operators' mother tongue)

IV. Operation
a.) practical hints

quick'n dirty stuff:

- everybody knows (laptop / neighbor computer):

  `tip`, `minicom`, `hyperterm` + null modem cable

- terminal program old serial palm pilot: *ptelnet*
- multiport serial cards + Opengear CD = console server
- watch out for cables:
  - pinout of DB9/25 is standardized
  - serial RJ45 is not

IV. Operation
a.) practical hints

- Sun SPARC is smart
- PC config under Linux:
  - BIOS + bootloader + kernel + init (Remote Serial HOWTO)
  - some progress bars limited by serial throughput (9600bps)
  - syslog messages on console:
    - `kern.warning;*.err;authpriv.none`
    - logging issue: Linux-Firewall (`log-level`)
    - console on syslog server: NTsyslog is a hog

IV. Operation
b.) Security considerations

exchange: physical (computer room) w/ network security

- measures (network/OOB device):
  - keep track of firmware updates!
  - dedicated management LAN w/ tight access rules

    (hack/workaround: host firewall on OOB device)
  - avoid cleartext protocols
  - add user to OOB device, don't work as root/admin
  - force authentication to console server (pw, ssh-pub key)

IV. Operation
b.) Security considerations

- measures (network/devices), 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.) Security considerations

- measures (nodes):
  - log out (session hijacking)
  - boot password
  - maybe reconsider:
    - SysRq / STOP-A /...
    - direct root login console while initlevel=3,5

Thanks for your patience

Questions?

Dr. Dirk Wetter, Hamburg

mail@drwetter.org

Dr. Wetter
IT-Consulting