WHEN UNIX MET AIR TRAFFIC CONTROL

Jim Reid
RTFM Ltd.

jim.reid@ukuug.org

```
#include <std_disclaimer.h>
```

EUROCONTROL

- the organisation
  - its role
- the systems and applications
  - change management
  - system admin procedures
  - system admin problems

THE INSTITUTION

- The European Organisation for the Safety of Air Navigation
- around 25 member states
- national aviation authorities
- premises in Benelux

HEADQUARTERS

- based in Brussels
  - Central Flow Management Unit - CFMU
  - Central Route Charges Office - CRCO
  - HQ: Admin, External Liaison and Integration
- Brettigny Experimental Centre
  - backup site for CFMU

OBJECTIVES

- standardisation and harmonisation
- ease congestion and reduce delays
    - smoothing ATC workload
    - lower airline operating costs

EUROPEAN ATC PROBLEMS

- protocol/systems Babel
  - autonomous national ATCs
  - EATCHIP initiative
- heavily congested routes
  - London, Paris, Amsterdam
- 30-60,000 flights/day
  - year on year growth

CMFU

- centralised flow management
  - regional & national FM
- no national bias
  - pan-European co-operation
- simplified administration
- assistance to national ATC
- in-house applications

CFMU OPERATIONAL SERVICE

- centralised handling of flight plans
  - submission and distribution
  - IFPS
  - only way to submit flight plans
- real-time slot allocation
  - TACT
    - — tactical system
- repeat flight plans:
  - RPL

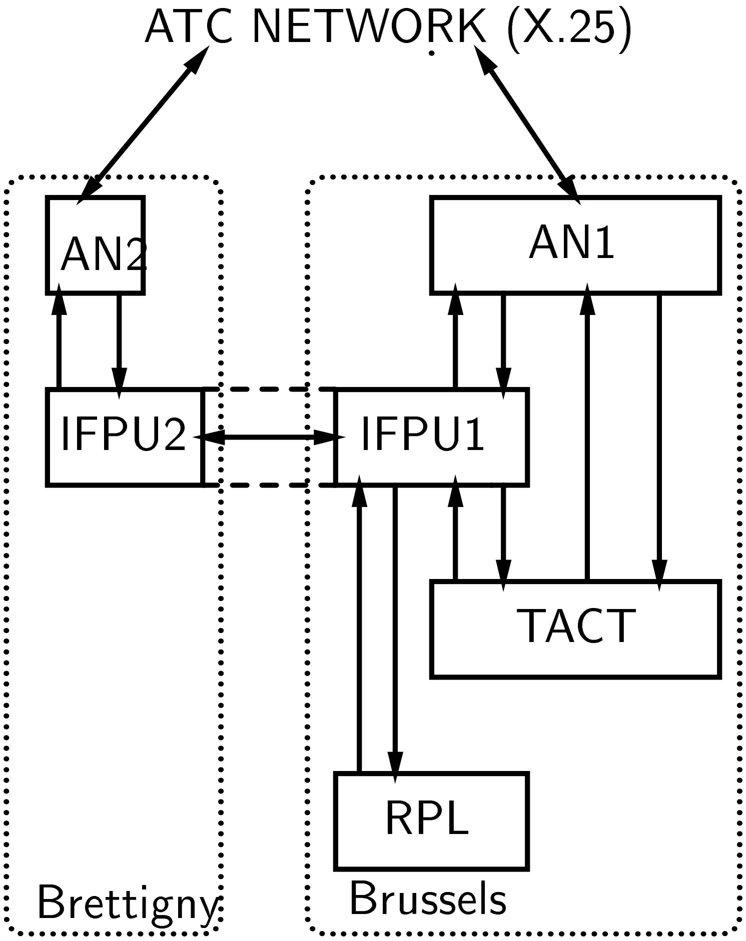
USER COMMUNITY

- air traffic controllers
  - scheduling tool
  - supplement to "life and death" ATC systems
- airlines & airports
  - better management of resources
    - — aircraft, fuel, gates, etc
    - — takeoff and landing slots

OPERATING CRITERIA

- “no downtime”
  - 1 hour maintenance window per month
    - — systematic switchover & system updates
- no data loss
  - lost data means no flights!
- timeliness of TACT database
  - if it’s >1 hour old, it’s useless
  - => hot backups and standbys

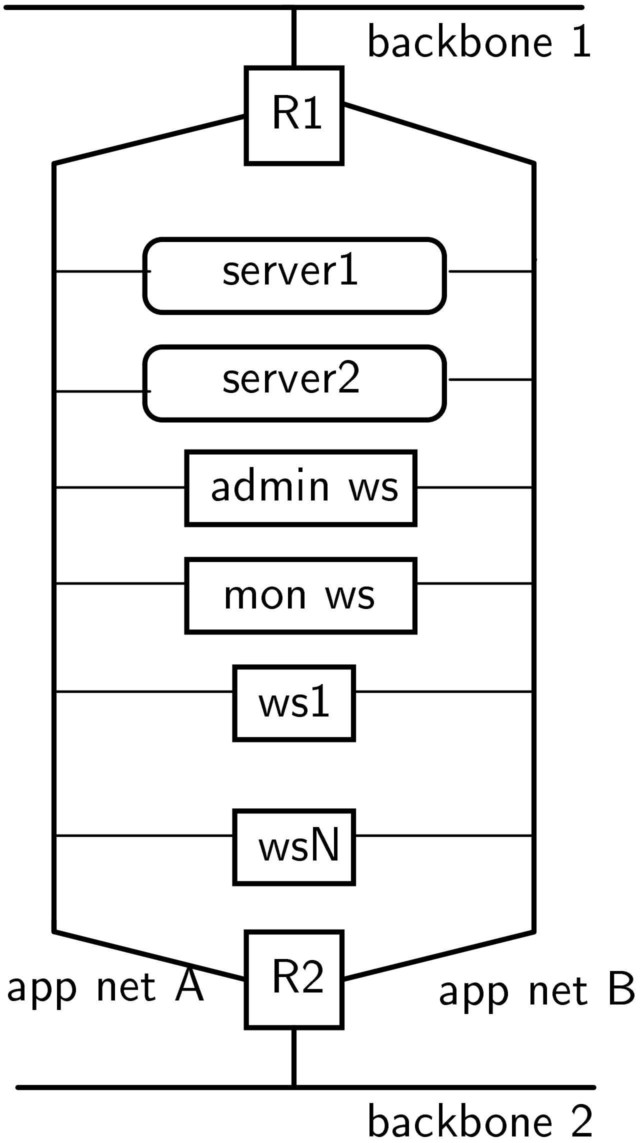
THE BIG PICTURE



MULTIPLE REDUNDANCY

- defence in depth
- no single point of failure
  - 2 computer rooms 400km apart:
    - — Brussels and Brettigny
    - — 2 independent network links
    - — UPS and diesel generators
- typical application cluster:
  - 2 servers, 2 networks
  - number of workstations

SLIDE OF APPLICATION CLUSTER



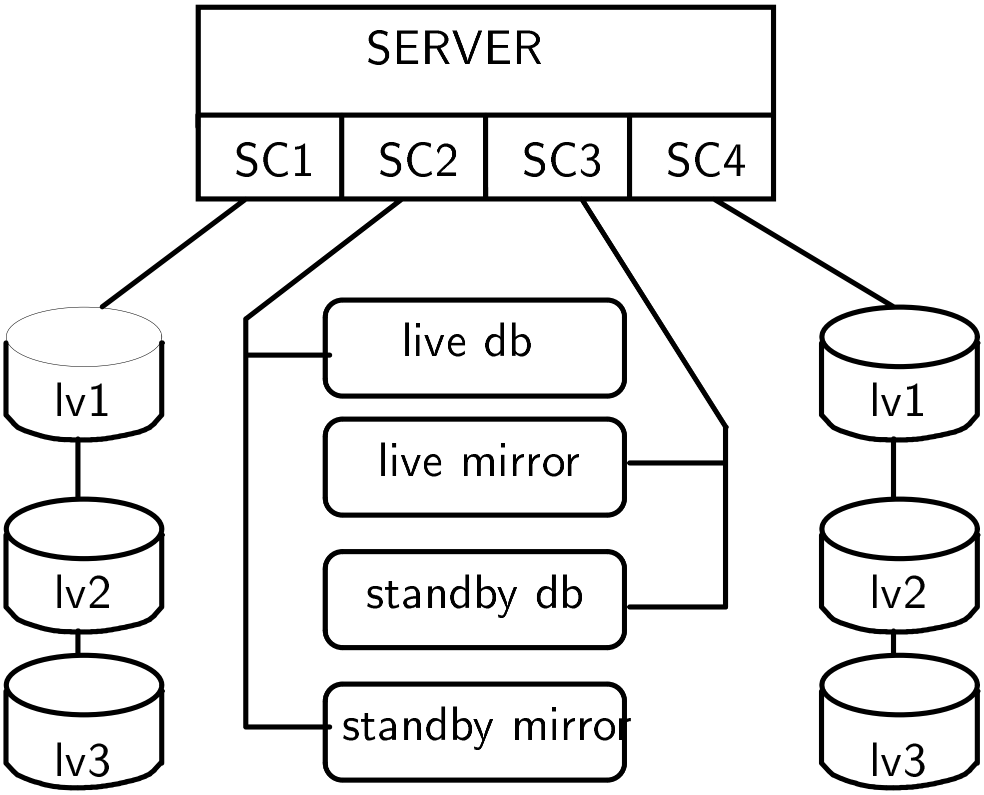
SWITCHOVER

- swap of operational and backup server
  - performed during maintenance window
  - also after system failure
- introduction of changes
  - software upgrades
  - patches
  - new configuration data

HARDWARE CONFIGURATION

- multiprocessor HP T90's
- 1GB+ of RAM
- Logical Volume Manager (LVM)
  - disk mirroring
  - no single point of failure
  - 4 shared hot-swappable disk arrays for database(s)
    - — mirrorred live and standby databases
  - approx 50 Gb/disk per server

SERVER CONFIGURATION



SOFTWARE CONFIGURATION

- **HP-UX 9**
  - **difficult migration to HP-UX 10**
- **Oracle databases**
- **minimal environment**
  - **KISS principle**
  - **no “dangerous” network services**
    - — **NFS, NIS, DNS, rdist**
  - **clumsy password file handling**

SUPPORT STAFF

- 4 UNIX system administrators
- 4 Oracle database administrators
- 4-5 networking/comms engineers
- 30 applications programmers
- 6 operators per shift - TMT
- army of management

UNIX ENVIRONMENT

- development environment
  - anything goes
- pre-operational environment
  - testing and training
  - considered "operational"
    - — fed live data
- operational environment
  - strict controls
  - rigorous CM

UNIX ENVIRONMENT - contd.

- **development environment copies OPS and Pre-OPS server setups**
  - **obvious testing benefits**
- **minor hardware differences**
- **irritating differences in UNIX configuration**
  - **username and UID divergence**
  - **pathname changes**
  - **environment variables**

CHANGE MANAGEMENT

- exhaustive CM procedures
- very conservative approach
  - all changes must be:
    - tested
    - documented
    - logged
- extensive audit trails
  - rarely examined

CHANGE METHODOLOGY

- programmers (where relevant)
- independent testing
  - quality assurance
- pre-ops installation
- ops installation
- no changes on live systems
  - use standby server
  - activate after a switchover

INCIDENTS AND CHANGE REQUESTS

- use Remedy
    - problem reporting and tracking
- 3 categories:
    - Type 1 incidents - I1's
        - operational failures
    - Type 2 incidents - I2's
        - operational errors
    - Change requests - CRs
        - alterations eg new systems

INCIDENT DISPATCHING

- Type 1 incidents
  - TMT page on-call support staff
  - UNIX sysadmin inevitably gets paged
- I2's and CRs:
  - first sent to manager
  - sent to change control board
  - put under work
  - assigned to member of staff
  - originator closes I2 or CR on completion

CHANGE CONTROL BOARDS

- lots of them:
    - operations (OCCB)
    - software (SCCB)
    - TCCB - development systems
    - documentation
    - mainframe

THE OCCB

- meets weekly
  - focus for all operational activity
  - discusses I2's and CR's
    - reject or approve new ones
    - close completed ones
  - analyses intervention requests
  - clearing house for information

THE OCCB - contd.

- representatives from every group:
  - UNIX sysadmins
  - Oracle sysadmins
  - network/comms group
  - air traffic controllers
  - programming teams
  - maintenance department
  - TMT management

INTERVENTION REQUESTS - IR's

- must be tied to an I2 or CR
- declarations of intent
  - do something to operational system
  - when it will be done
  - impact
- line manager approves
- then goes to OCCB for acceptance
- usually 1 request per system

A TYPICAL I2

- **wrong permissions on `/tmp`**
  - **programmer raises I2**
  - **OCCB assigns to UNIX group**
  - **sysadmin allocated to I2**
  - **submits intervention requests**
  - **OCCB approves interventions**
  - **sysadmin does the task**
  - **I2 marked completed**
  - **finally closed by OCCB**

EXTRA FACTORS

- ISO9000 certification
- missed IRs must be resubmitted
  - rules get bent
- intervention log
  - based on Remedy
  - filled in after each intervention
  - informs management of changes
- I2s and CRs can create further I2s and CRs

SYSADMIN PROCEDURES

- **driven from CM procedures**
  - **must be an I1, I2 or CR**
  - **otherwise nothing gets done**
- **no editing of UNIX config files**
  - **files must always be present**
  - **create new one**
  - **copy old one, rename new one**
- **use management workstation**

A FEW WORDS ABOUT LVM

- **it's horrid!**
  - **too many similar commands**
  - **far from bulletproof:**
    - **— use `lvsync` or `vgsync`?**
  - **LVM disk labels unreadable**
    - **— can't readily check VGRAs and PVRAs**
    - **— disk verification impossible**
    - **— a major headache**

MORE WORDS ON LVM

- **commands are counter-intuitive:**
  - **args to `lvmerge` are wrong way round!**
  - **`vgscan` is destructive!**
- **command line typos can be disastrous**
  - **real worry at 3 am**
  - **solution: pass the buck**
    - **— take advice of HP support**

PUBLIC DOMAIN SOFTWARE

- officially banned
  - sneaked in
    - TACT includes `tcl/tk`
    - `gzip` widespread
    - HP support for `xntpd`
  - unnecessary duplication
- issue is support, not cost
- should be common set of PD tools

SYSADMIN PROBLEMS

- **switchover**
  - **influenced by HP product**
  - **simple yet over-elaborate task**
    - **— politically hard to fix**
  - **tight time constraints**
    - **— little room for manoeuvre**
    - **— full TACT start-up takes over 45 minutes**

MORE SYSADMIN PROBLEMS

- reactive rather than proactive
- conservative culture
  - don't fix what already "works"
  - keep operational service going
- management attitudes
  - solve short-term problems
  - avoid "radical" change
  - continuity of service

MORE SYSADMIN PROBLEMS

- **lack of communication**
  - **don't know what other groups are doing**
    - — **and** *vice versa*
- **vague interface between applications and UNIX**
- **vague interface between UNIX staff and DBA's procedures and actions**
  - **never sure what can go wrong**
  - **never sure of change's impact**

AUTOMATIC ADMINISTRATION

- **deployment of in-house tool**
  - **bad design**
    - **solved wrong problem**
  - **poorly documented**
  - **huge learning curve**
  - **myriad of config files and scripts**
  - **gratuitous changes to systems**
  - **all or nothing approach**
  - **encouraged diversity**
  - **cancerous impact**

SIMPLE SYSTEM ADMINISTRATION

- return to maintenance by hand
- gradual elimination of differences
  - removal of tool files and scripts
  - long process
- simple version control
  - central repository of config files
  - checkin change after updating the system file
  - SCCS, `diff` and email

MANAGEMENT PROBLEMS

- staff compartmentalisation
  - poor group interaction
  - DBAs write shell scripts
  - configuration data compiled into applications
    - IP addresses
    - TCP port numbers
    - system names
    - printer locations

SYSADMIN ARCHITECTURE

- only now being done
  - UNIX system admin. team
- needless diversity
  - no global UID & user name space
  - historical and human reasons
  - platforms managed separately
  - extra unnecessary work

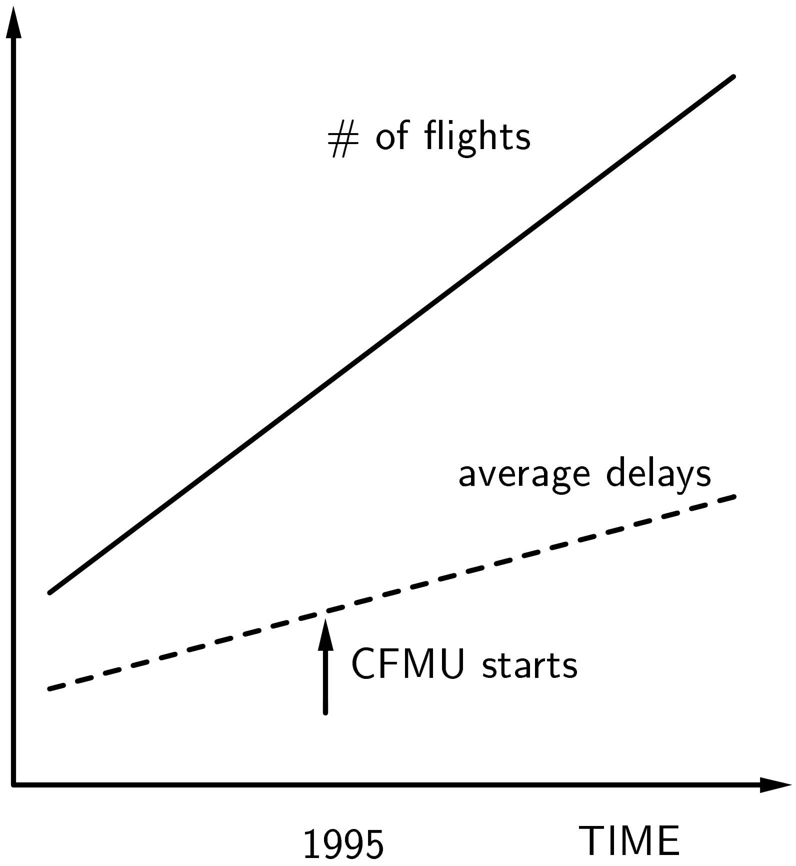
CONTINGENCY PLANS

- IFPS: no problem
  - used in anger
- TACT: none
  - service in Brettigny?
- disaster recovery is a worry
  - complex configurations
  - poor documentation
  - setup details dispersed
- a hard problem

CONCLUSIONS

- **it works! (sort of)**
  - **no downtime to end users**
- **redundant hardware is vital**
  - **“fault tolerant” vanilla UNIX?**
- **CM is painful and slow**
  - **but brings discipline to work procedures**
  - **expensive in time and resources**
- **the customers and users seem happy**

GRAPH



FUTURE DIRECTIONS

- new disk farms
- HP-UX10 migration
- 2-site TACT
- ATC developments
- statistical analysis
  - traffic patterns
  - AI techniques
  - predicting bottlenecks