ISYS90076 - IT infrastructure for ehealth

Lecture #6
Health Infrastructure Part 3
Data Centre, Processing, Storage, HA & DR

Frank Smolenaers

Wednesday 11/04/2018

This Weeks Agenda:

- Today's Lecture – "Data Centre, Processing, Storage, High Availability & Disaster Recovery"
- Today's Tutorial:
  - Minor Assignment 1 – debrief
  - Minor Assignment 2 – Q&A, class work time
  - SSLC* discussion – Led by Priyanka

* Staff Student Liaison Committee: 2018, Semester 1

DC, Processing, Storage, HA & DR

Introduction

- ICT hosting is NOT core business for Health
- HUGE expense to investment in:
  - data centres, hardware, operating systems
  - networks, apps, security
  - support teams and contract management
- The Cloud has opened up new Operational Expenditure (OPEX) models e.g. Pay as You Go (PAYG) and Pay for What You Use – c.f. Capital Expenditure models (CAPEX)
- Traditionally, Hospitals and health services still deliver many IT needs internally

A Hospital's Core Requirements

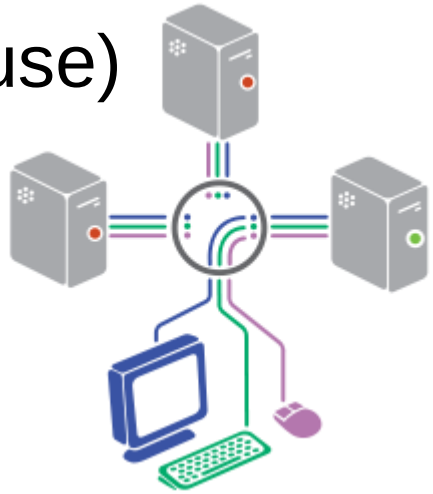
- Data Security – secured / vetted access of physical and electronic access (most sensitive data - Patient Privacy)
- Uptime - highly available / fault tolerant
- Environmentally controlled – temp, humidity, power, fire protection
- Monitoring & Support - Mx Systems to monitor, alert, rectify issues
- Enduring – scalable capacity, future proof?

DC = Data centre

Data Centre – the environment

- Primarily Contains Racks to host
  - Servers (processing)
  - Storage (data)
  - Tape libraries (backups)
  - Network/comms gear
  - KVM Switch (Keyboard Video Mouse)

headless systems



(Note: Std Racks are 19” wide)

DC Design / Security

- Physical Security
  - build DC deep inside the campus
  - obscure facility to help maintain low profile – no signs
  - limited access to authorised personnel ONLY
  - use ID badges and biometric scanning to challenge access
  - log all physical access
  - 24x7 onsite security, video surveillance, log retention
  - segregation of “others” equipment
    e.g. Telco, outsourced FM, etc.
    locked rack doors / locked cages

DC Design / Security

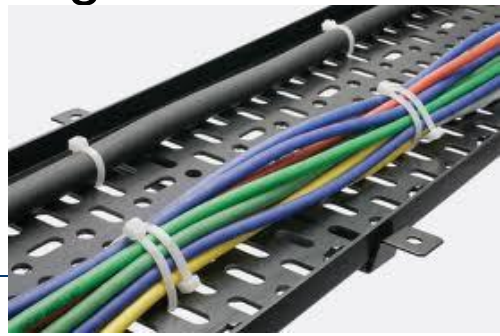
- Operational Security
  - create business processes and policies that follow security best practices
  - ISO 27001/2 based policies, reviewed annually (http://www.27000.org/)
  - limit access to confidential information and maintain tight security over time
  - documented infrastructure change management procedures
  - downtime & incident management process

DC Design / Security

- Cont...
  - secure document and media destruction
  - asset management and tracking (wipe data)
  - business continuity plan focused on high availability of infrastructure
  - independent reviews performed by third parties
  - continuous monitoring and improvement of security program

DC Design

- Network Infrastructure
  - no single points of failure throughout shared network infrastructure
  - cables properly laid (conduit/cable trays) and secured (cable tied)
  - proactive network monitoring & management > alerts
  - real-time topology and configuration adjustment to self heal (alternate paths)
  - network uptime backed by Service Level Agreements
  - network management ONLY performed by authorised personnel



Racks and Cable trays

DC Design / Security

- Environmental Controls
  - implemented to mitigate service interruption caused by fires, floods and other forms of natural disasters
  - dual power paths to devices & DC
  - uninterruptable power supplies – UPS (minimum N+1)
  - diesel generators (minimum N+1)

DC Design / Security

- Environmental Controls cont.
  - service agreements with fuel suppliers in place
  - HVAC = heating, ventilation, and air conditioning units (minimum N+1) – also HUMIDITY for datacentres
  - Smoke, heat, gas detectors & non aqueous fire suppression agents
    - e.g. FM-200 and HFC 125 remove heat from fire but these won't destroy your equipment
  - Water sprinklers as last resort

    stop fire spreading to other areas
  - Flood detection / raised floors
  - Continuous facility monitoring

DC Design / Security

- Human Resources / Governance
  - ensure authorised staff are vetted
    - understand their roles and responsibilities related to information security
    - e.g. non-disclosure of, or tampering with patient info
  - Police/reference checks taken for employees with access to patient info & systems
  - Security Officer oversight of Security Operations and Governance, Risk, and Compliance activities
  - Comprehensive Incident Management, Change Management, and Business Continuity policies
  - Log electronic access – audit trails back to user

Platforms / Processing

Servers host Health & other Apps

- Common Health Apps hosted by servers:
  - PAS – Patient Administration System
  - CIS – Clinical Information System
  - PACS – Picture Archiving and Communication System (Radiology Image repository & viewing)
  - RIS/RMS – Radiology Info/Mx system (reporting)
  - L(I)MS – Laboratory (Info) Mx System
  - Pharmacy – Meds Mx System
  - File and print services
  - +100?– Intranet, decision support, ED, ICU, Outpat, HITH, Risk Mx, paging, scheduling, staff & Pt. portals, HR, Payroll, Library, Finance, Supply, Pt. & staff education/LMS, IT helpdesk, etc…..

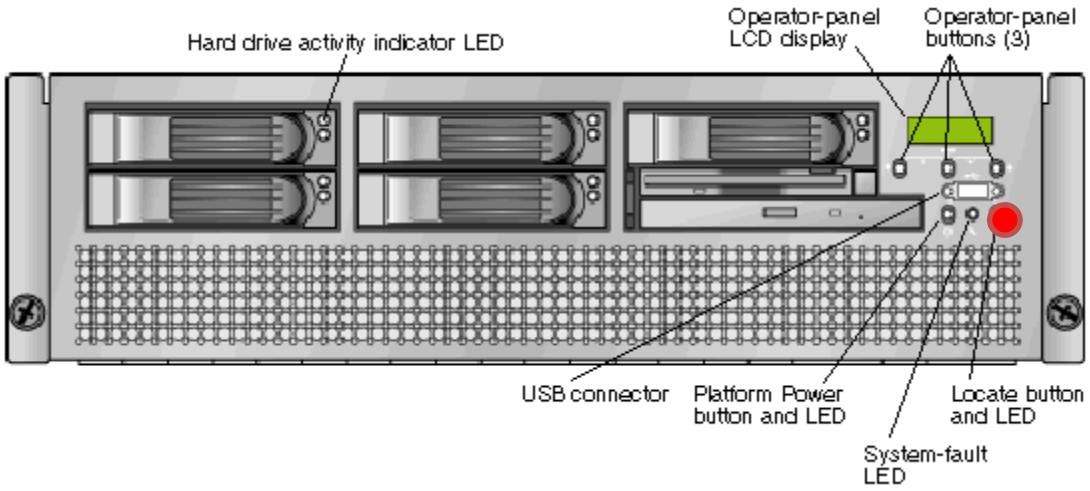
Servers

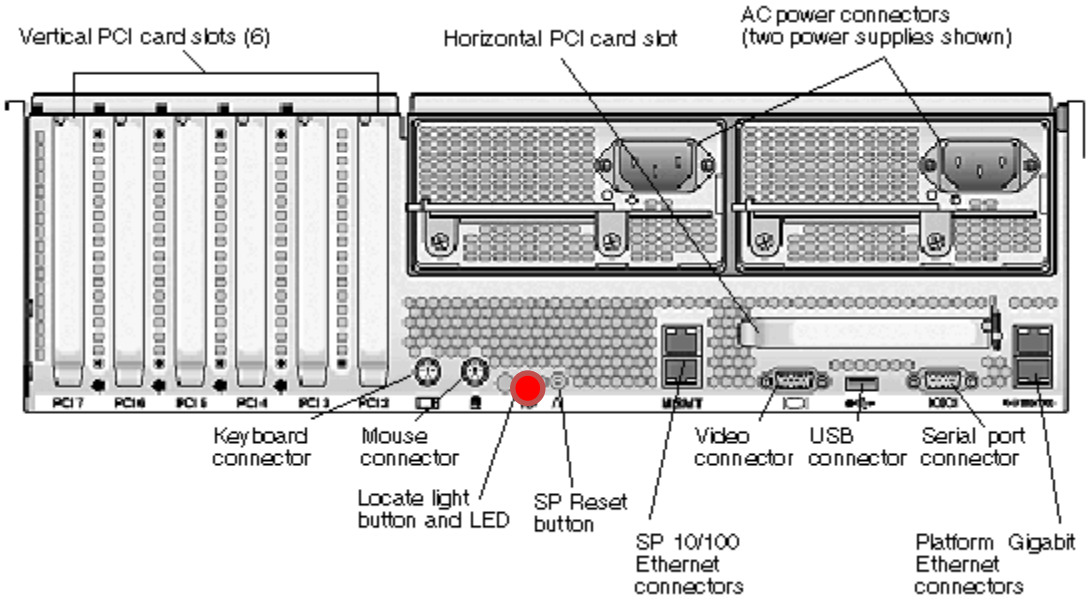
- Various server operating systems:
  - Microsoft Windows Server (Dominant)
    - Standard / Enterprise
    - Datacentre
    - Web Server
  - Linux flavours
    (e.g. Red Hat, SuSe, Debian)
  - Others:
    - Unix / HP-UX / Sun Solaris / Mac Server
    - IBM AIX
    - Novell

Server configurations

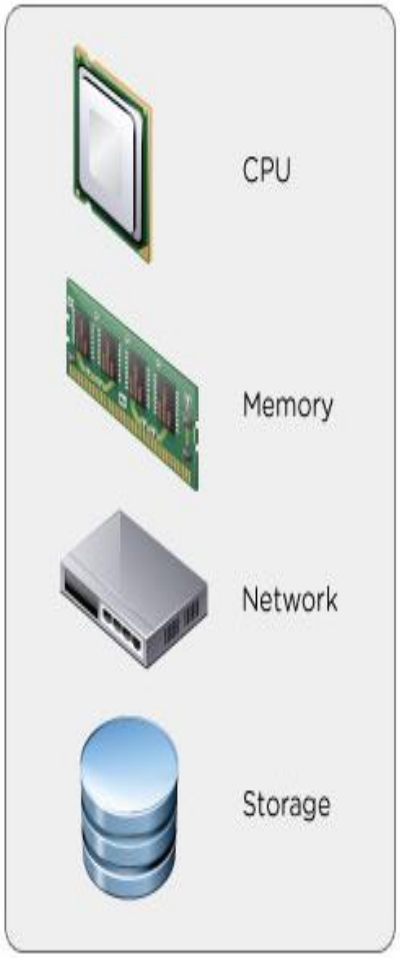
- 1 RU (Rack Units 1.75”) –
  small footprint, lower specs
- xRU – more CPU, internal disk, RAM and Host Bus Adapter cards (HBA) e.g. SCSI, SAS, Fibre Channel – connect to storage
- Blade Centre
  - common chassis, many blades
  - internal switch & HBA’s
  - variety of HW architectures and OS

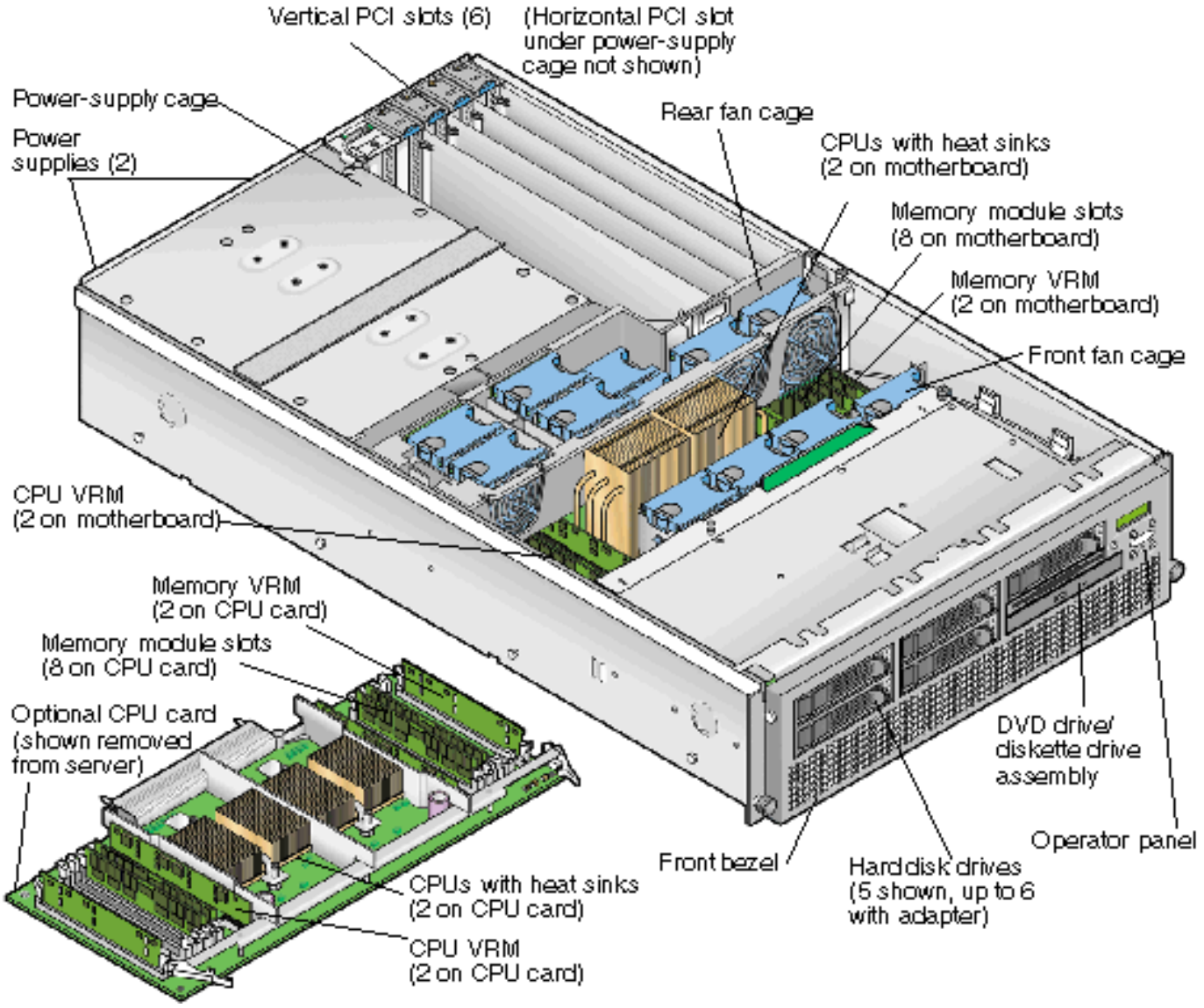
Front & Back of a 3RUServer





Inside a 3RU Server





Storage

Disk / Storage requirements

- Boot partition
  - First disk seen by server firmware (BIOS)
  - Holds and loads the operating system (kernel)
  - May hold application installations & swapfile
- Data partition
  - Holds the required data e.g.
    - Website root folder
    - Database files
    - User documents
- Why separate the 2 partitions? Wastage?

Storage Options

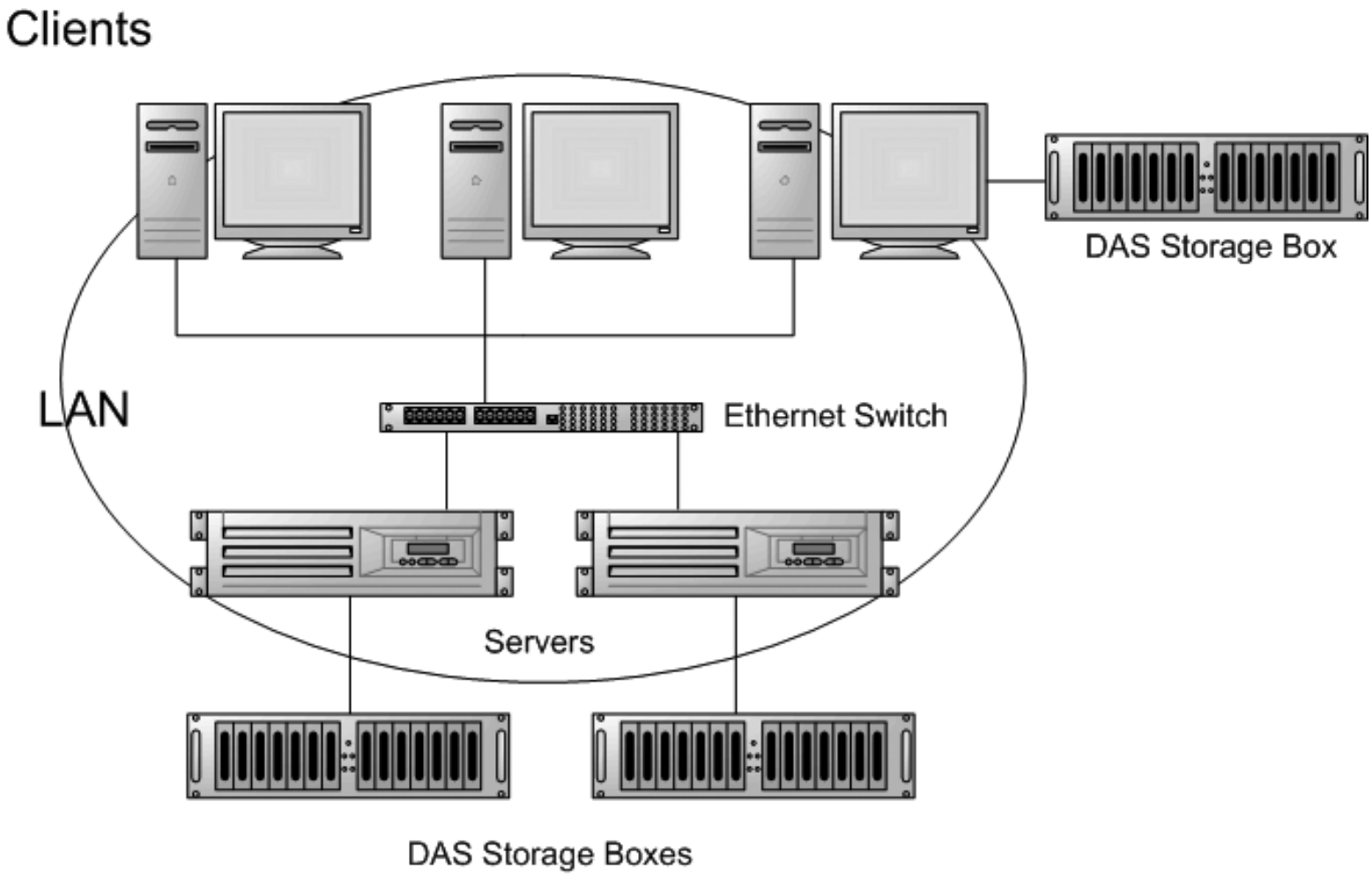
- Hard Disk Drives (HDD's)
  - 2.5" or 3.5" – platter size
  - Typically 73GB to 2TB capacity
  - Local Attached
  - Internal to server chassis
    - Hot swap caddy
    - SATA, SAS, SSD

- Direct Attached Storage (DAS)
  - Separate disk enclosure - JBOD
  - Connected by various cables & protocols: e.g. SATA, eSATA, SCSI, SAS, and Fibre Channel

SATA = Serial Advanced Technology Attachment
eSATA = external SATA
SCSI = Small Computer System Interface
SAS = Serial-attached SCSI
SSD = solid-state drives

DAS

Direct Attached Storage



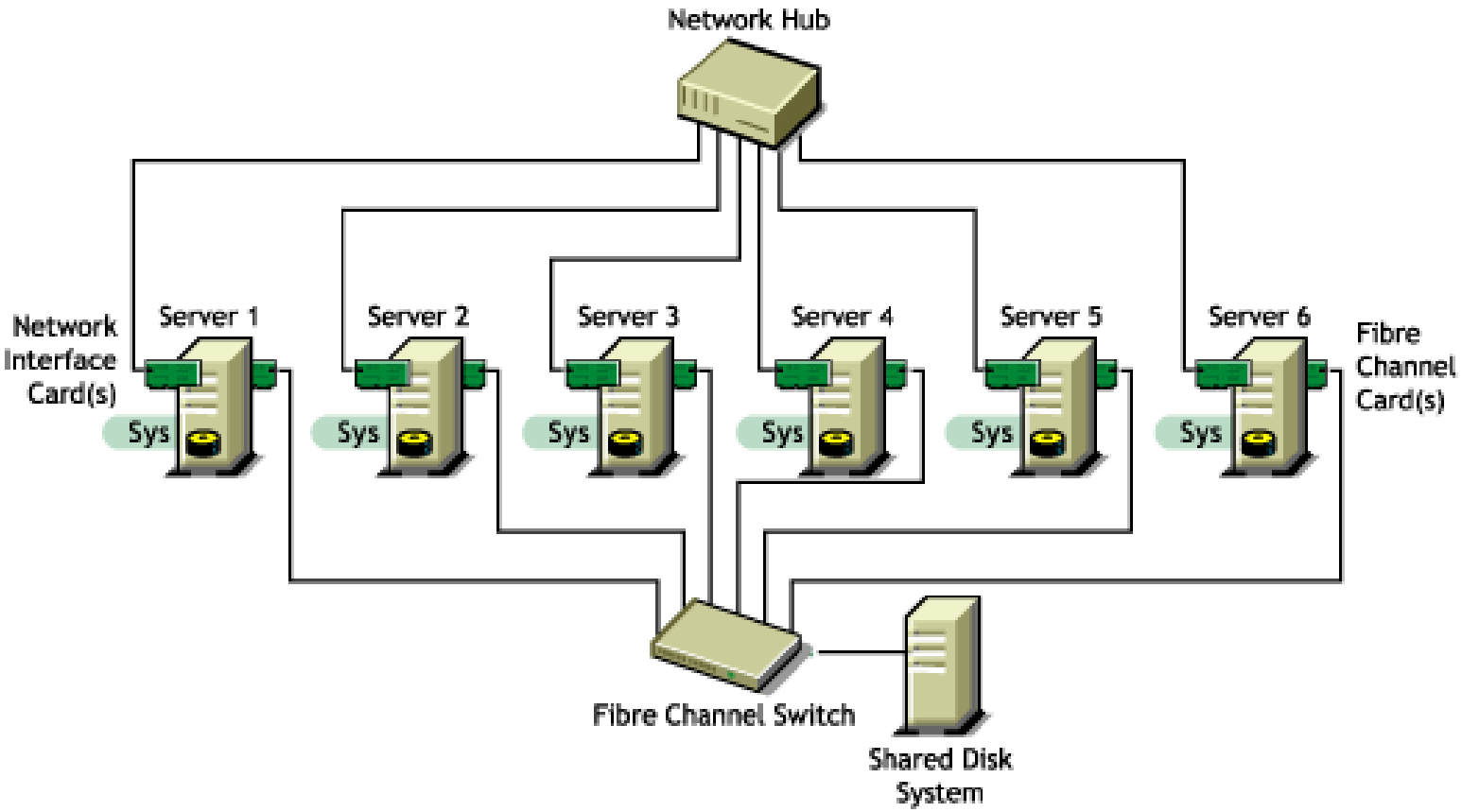
SAN – Storage Area NW

- Abstract storage from Tin (Host server)

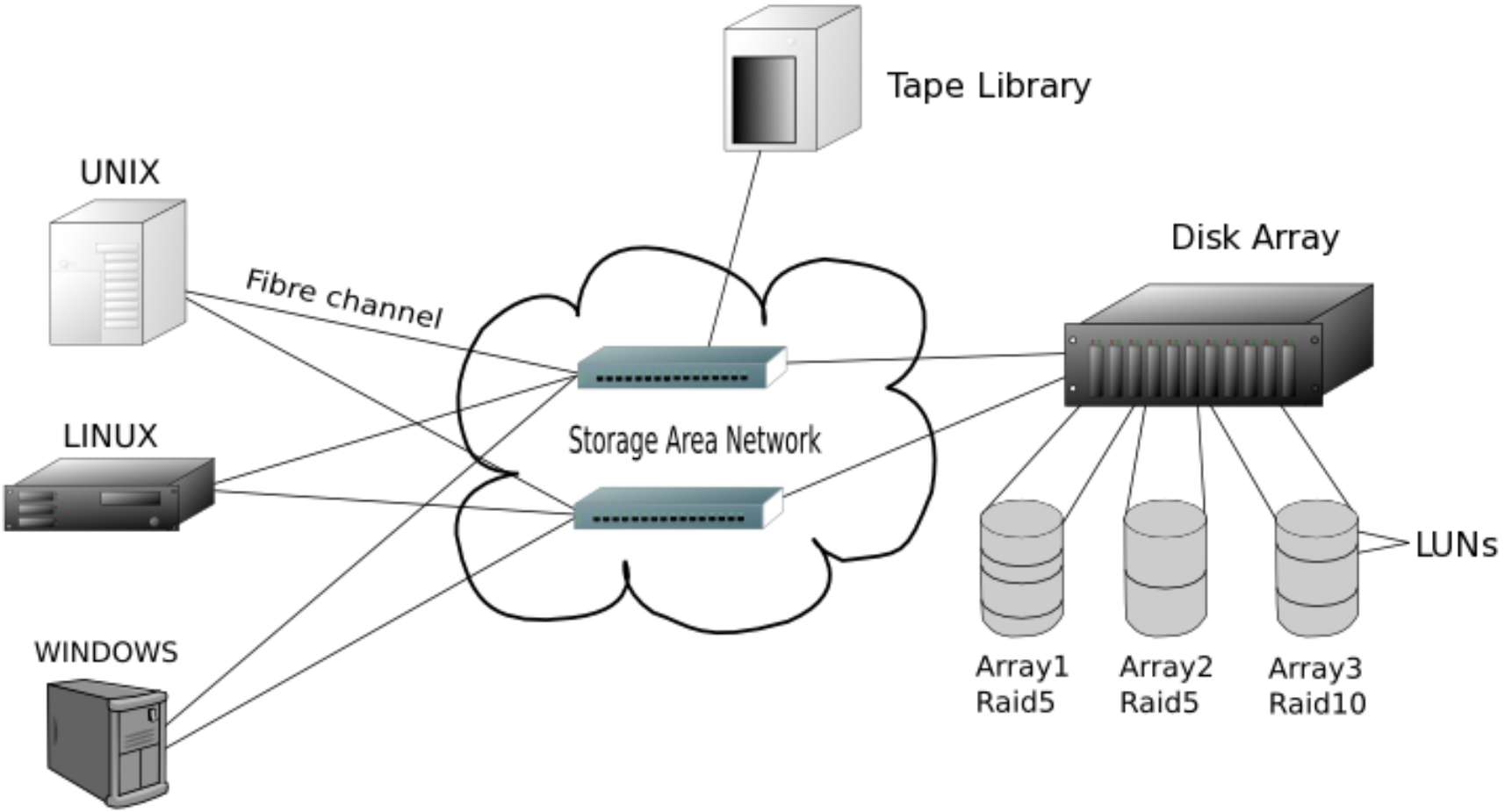
  e.g. Storage separation or virtualisation

- Adaption of DAS - *Network* attached storage at BLOCK Level
  - Acts like a remote Hard Drive – BUT the server sees the disk as local/DAS
  - Uses a network e.g. **Multiple** servers are connected via the network to a Disk Array
    - SCSI over Fibre Channel
    - Fibre Channel over Ethernet (FCoE)
    - iSCSI = SCSI over TCP/IP

SAN & IP NW


Network Hub
Network Interface Card(s)
Server 1
Server 2
Server 3
Server 4
Server 5
Server 6
Sys
Fibre Channel Card(s)
Fibre Channel Switch
Shared Disk System

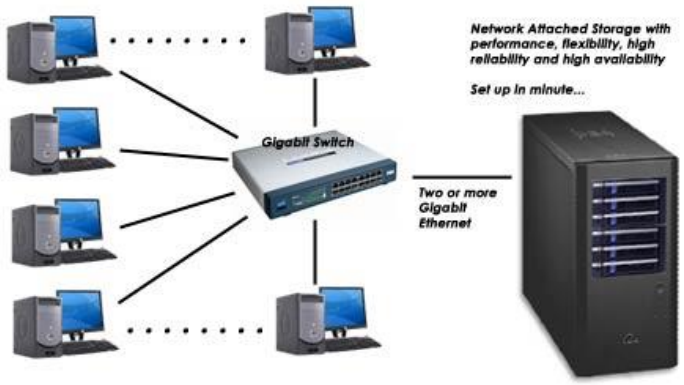
SAN Fabric and devices



NAS – Network Attached Storage

- NAS is a fileserver appliance with redundant disk and mini OS - uses CIFS or NFS to allow access to shared folders like H: G: or W: drives
- An intelligent device that allows users over the network to easily and safely share storage (AD Auth)
- Multiple users attach to the

file shares and read/write files



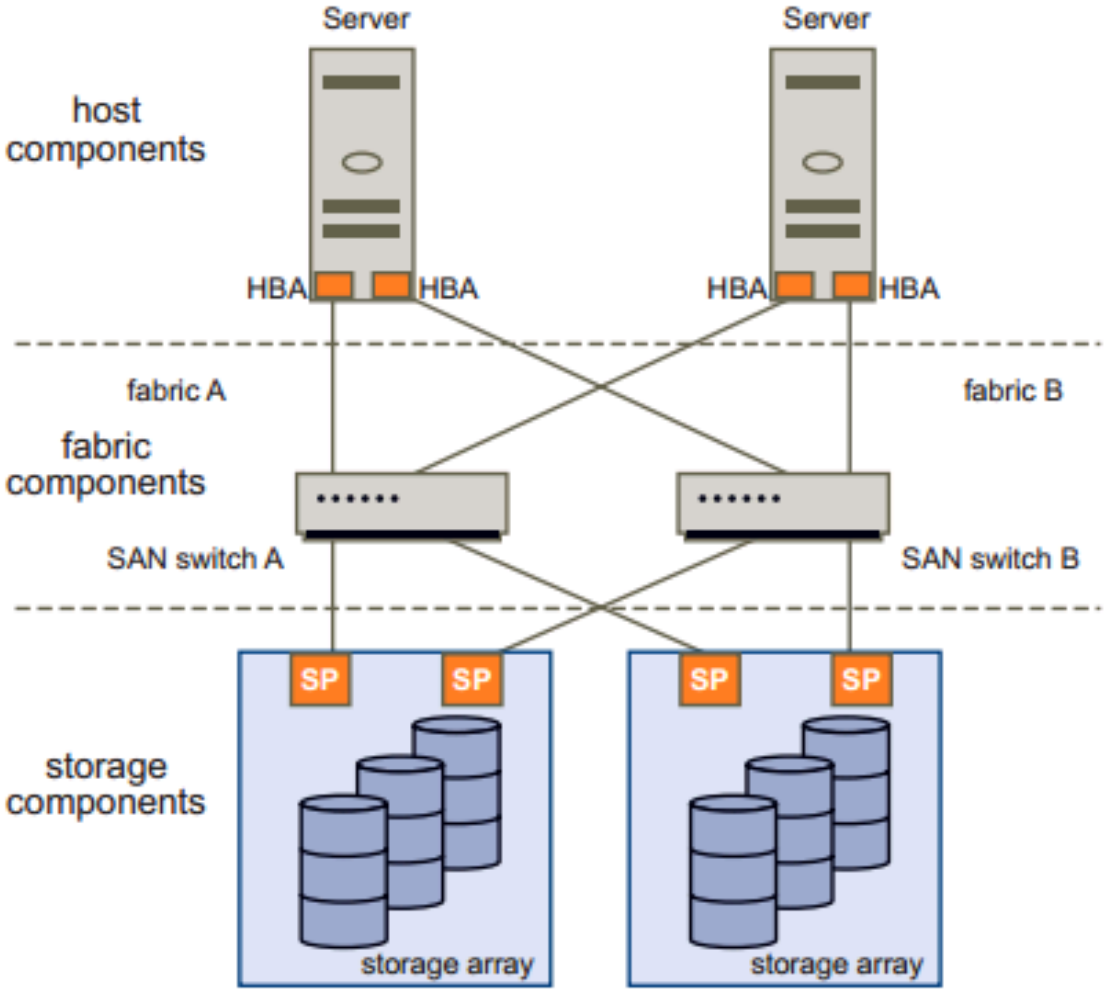
CIFS (Common Internet File System) is a proposed standard protocol that lets programs make requests for files and services on remote computers
NFS Network File System is a distributed file system protocol originally developed by Sun Microsystems in 1984

Storage Redundancy

- RAID – Redundant Array of Independent* Disks
  - combines multiple disk drives into a logical unit (LUN)
  - provides disk/data redundancy and improved performance
  - Levels 0 (striping), 1 (mirror), 5 (striping with Parity), 10 (mirrored RAID 5 – used in health)
- Global Hot Spare – spare disk at the ready
- SAN – MUST have redundant connections
  - Multiple HBA's, paths, SAN switches, Controllers

* &/or inexpensive disks

Redundant SAN Architecture



Break - Hernia Repair Surgery anyone?

HA = High Availability

High Availability (HA)

- No single point of failure ➡ Redundancy:
  - Servers
    - RAID internal Disk & MEMORY
    - Redundant power supplies, fans, HBA's, NIC's
    - Multi-homed to NW and SAN fabric
  - Storage
    - RAID disks, Global hot spare disk
    - Redundant controllers and SAN fabric connections
  - Networks
    - Duplicate HW & paths, internet connections
  - Data Centres
    - Mirror data and processing (MAN/WAN Links)

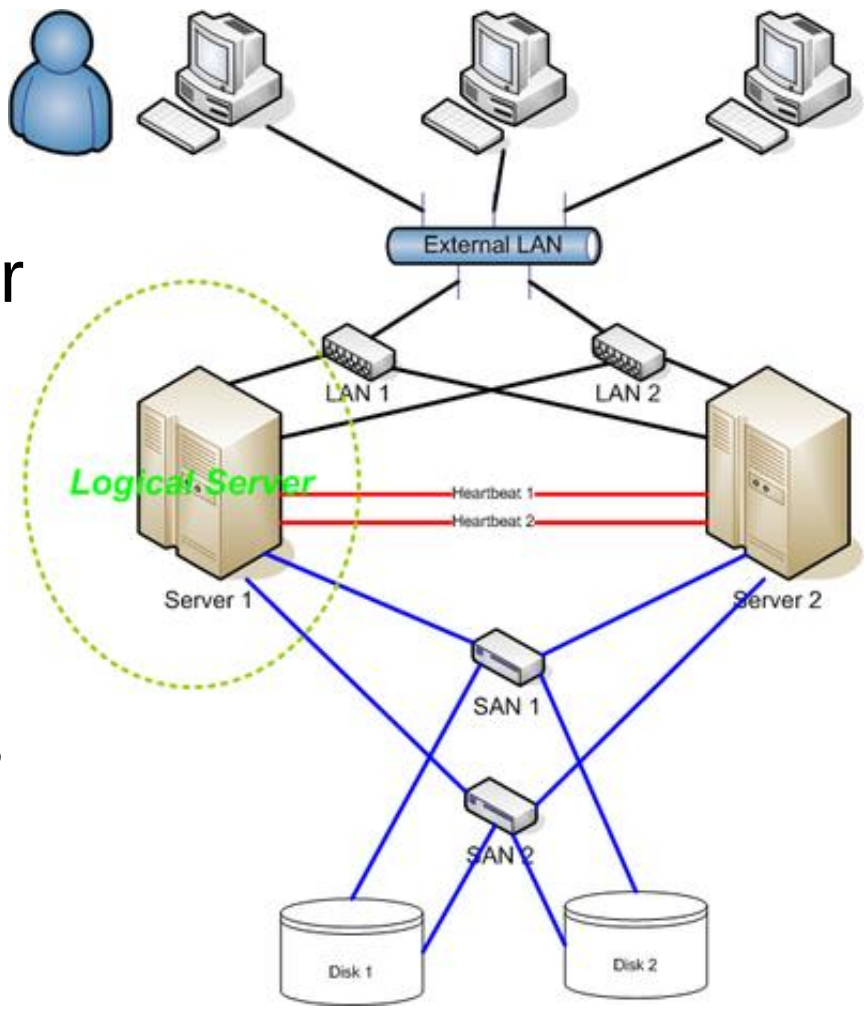
High Availability (HA)

- Fail-over / Self rectify:

N+1 — Provides an extra node (server) that is brought online to take over the role of the node that has failed.

The extra node must be capable of assuming the roles of the primary nodes it is responsible for.

Active/Active vs Active/Passive



DR = Disaster Recovery

Disaster Recovery (DR)

1. Data Recovery = Backups
   - Near-line then Offline copy of data on tape (~320GB) or offsite disk e.g. Cloud
   - GFS* tape rotation – Daily, Weekly, Monthly = granularity of restore
   - Full vs Incremental = speed of restore
   - Data de-duplication – save much space

DLT Tape & Drive

*Grandfather-father-son backup refers to a common rotation scheme for backup media

Disaster Recovery (DR)

2. Cold/warm standby site (data centre)
   - Invoke network links
   - Bring up spare servers/spare data centre
   - Restore data from last backup
   - Reconfigure DNS – point all clients to the IP addresses of new servers
   - Set live to users

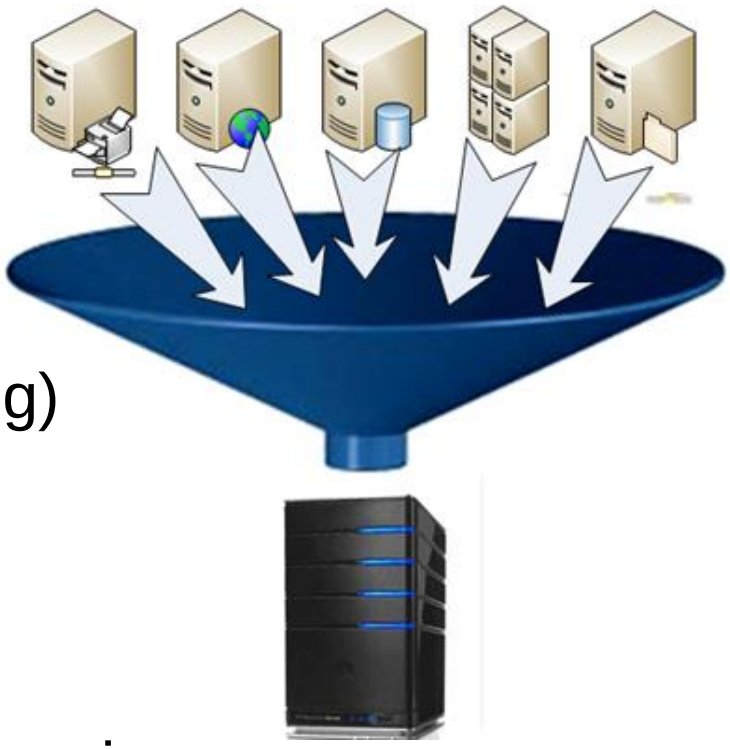
   NB: Servers need to be turned on periodically to test/patch etc.

DC Virtualisation – game changer

Virtualisation's contribution

Server/storage Virtualization has enabled:

- increased utilisation of high-density platforms
  - = reduced tin / bare metal server footprint
  - = much smaller physical locations
  - = lower power costs
  - = reduced storage (thin provisioning)
- health to move from on-premise data centres to co-located environments and to the cloud i.e. portability to a PaaS Hosted service



The Benefits of Server Virtualization

Dramatic savings

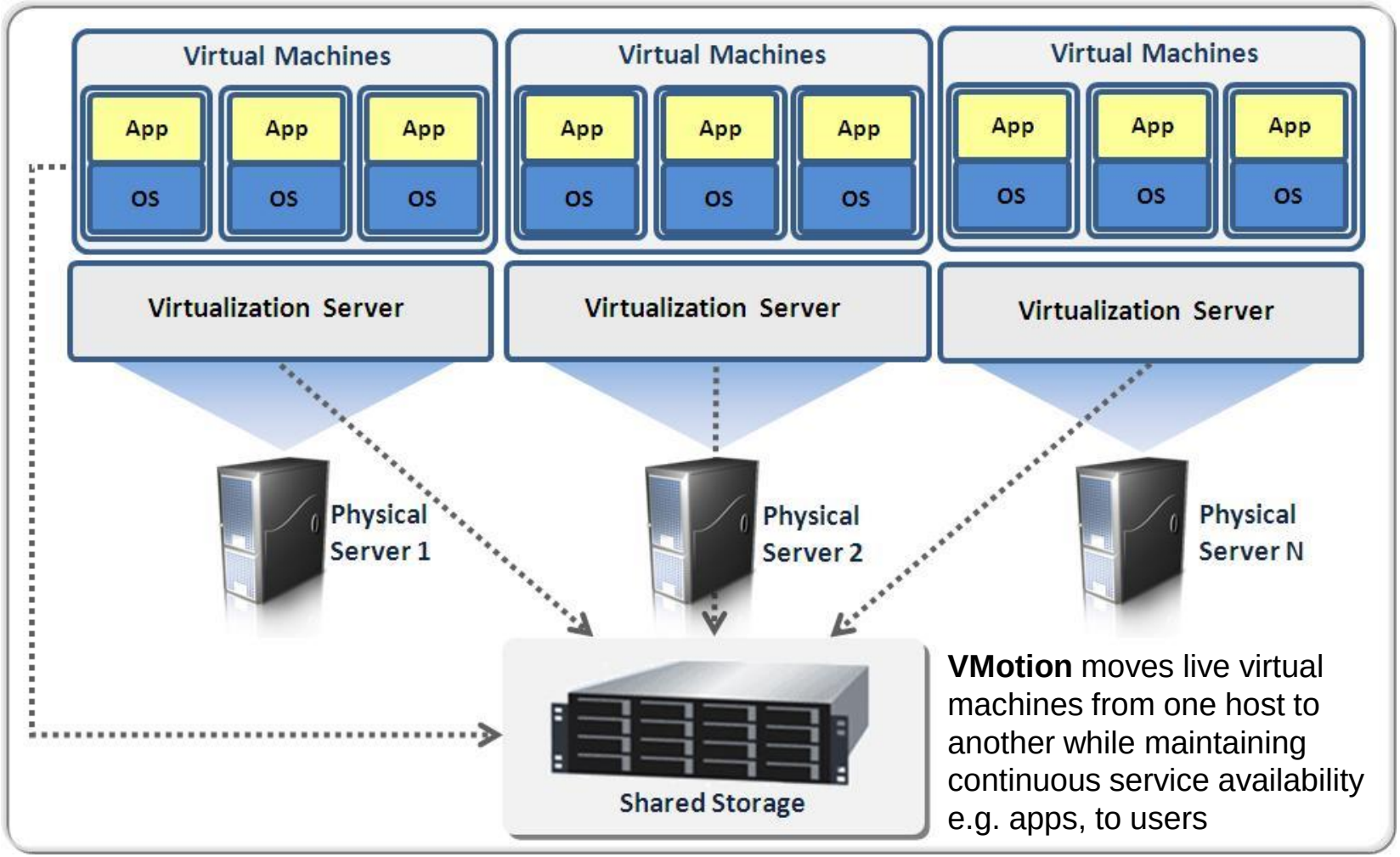
- Up to 80 percent greater utilisation of every host server
- Reductions in hardware requirements by a ratio of 10:1 or better
- Capital and operations expenses cut by half, with annual savings of more than $1,500 for each server virtualized
- Robust, affordable high availability.
- See more at: https://www.vmware.com/virtualization/virtualization-basics/what-is-virtualization#sthash.Yrg7u19U.dpuf

Efficiency

- Server templates – fast, standardised new server builds
- Cloning & snapshots for dev, upgrade testing etc.

Virtualisation LOAD SHARING AND FAILOVER

Shared Storage enables HA via Virtualisation (even across DC's)



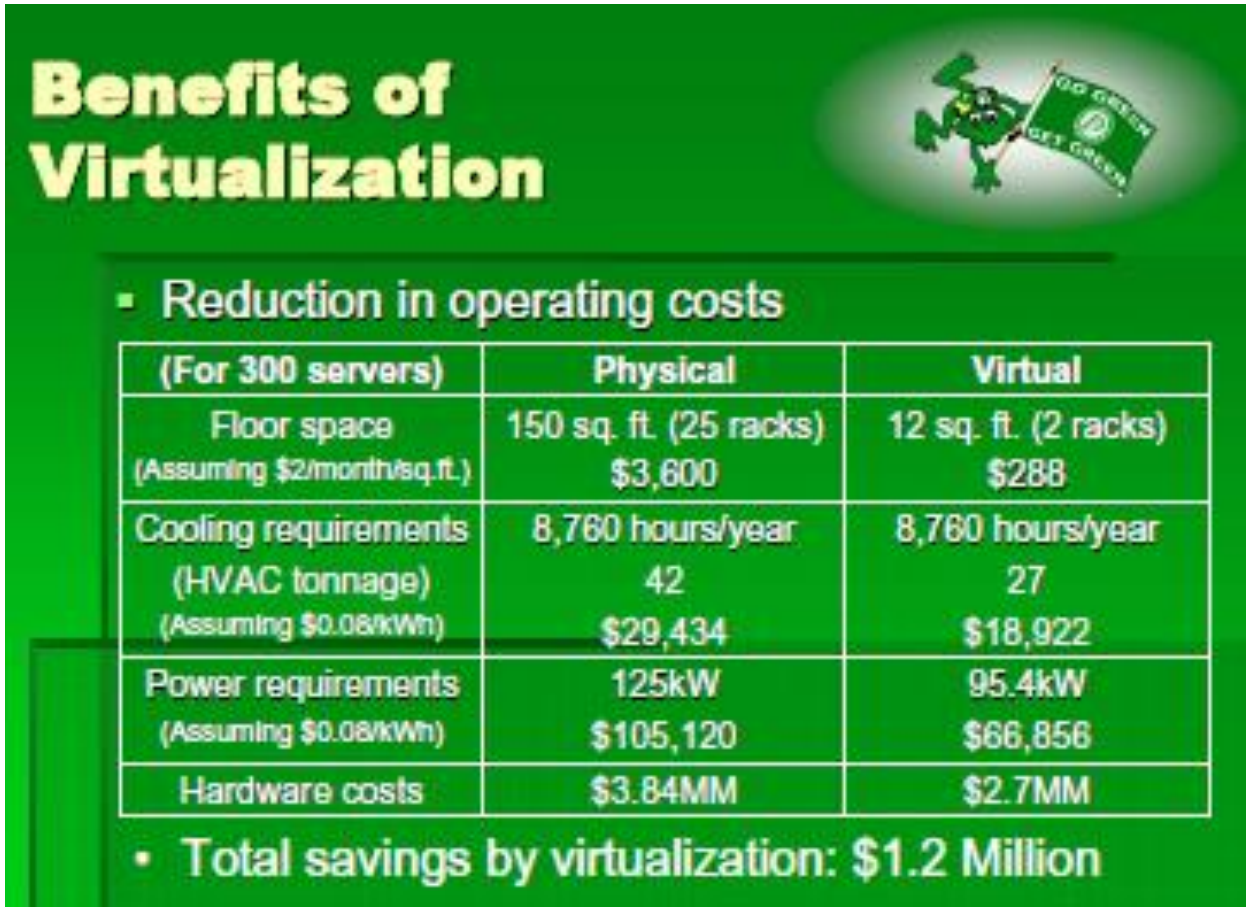
VMotion moves live virtual machines from one host to another while maintaining continuous service availability e.g. apps, to users

Virtualisation – sample savings

US State IT Dept

For 300 servers, the reduction in operating costs would be $1.2 Million.

Applications will continue to work as designed, despite being moved from physical to virtual servers



Benefits of Virtualisation

1. Save Energy
2. Reduce Data Centre footprint – space & cost
3. Faster server provisioning
4. Reduce HW vendor lock-in
5. Increase uptime
6. Cloning / Lab Environments
7. Improved DR
8. Application Isolation – Own OS
9. Extend life of old/legacy apps
10. Ease of moving to the cloud

Summary

Summary

- Health has high demands on the availability of critical systems
  - Hospitals require at least 2 DC's (one offsite)
- Computing infrastructure can be hosted in-house, in the cloud, or a hybrid of both
  - e.g. DR or Backups in the cloud
- Costs escalate with duplication
- Converged and co-located services can provide economies - e.g. shared email, VoIP

Tut – Assignment 1 (RRAA) debrief

Written Report Tips - revisited

Report Tips

- Proof read, proof read, proof read!!!!!!
  - Get someone else to proof read also
  - Beware spelling, grammar and punctuation
  - Reports need to be easy to read – font size and line spacing
- Ensure reports have date, student Name and number, subject and page numbers on each page
- Provide a total word count for body of the report (less Bibliography, top references, appendices etc.)
- Beware plagiarism – it will not be tolerated
- Use Headings akin to assessment criteria – A MUST
- No need to repeat the project brief – I know it!

Report Tips

- Report must have a focus on the use of solutions for Healthcare workers, and deployment within a hospital setting.
  - Pure tech answers are not enough
  - Consider the “end to end solution” and “End User Perspective” in every section of the report
- Brainstorm key elements of the report before you start.
- Be brief and on topic. Do NOT repeat yourself.
- Do NOT cut and Paste – think, and write in your own words.

Report Tips

- List assumptions in an appendix
- Provide several sources of info in Bibliography
  - Include some recent resources
  - Vendor web sites / info is ok – up to a point
  - list top references with a sentence under each for why is it was more valuable than others
- Be concise, yet address the specific requirements as per the task/criteria

Tips for good reports

- Take note of the whiteboard/tutorials – they provide immense guidance on what should be covered in the report.
- Ask for help if anything is unclear – It is OK to ask!
- Plan ahead, write ahead of time – *avoid requesting extensions – be ORGANISED!*
- Submit via TurnItIn well before DUE to cater for system down, system slow etc.
- Review “Similarity” before finalising submission

Tutorial – vMDT's - Web Collaboration Basics

Web Collaboration – The Basics

- Create a meeting – schedule, email calendar invite
- Attend - ? Video Breakout Rooms for each Pt group
- Voice options – Integrated or teleconference dial in
- Share Video
- Share desktop/app
- Handover to another presenter
- Co Collaborate
- Educate – Record session
- Etc.

http://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software

Assignment 2 (vMDT's) – Q&A

Staff Student Liaison Committee

SSLC* discussion – Led by Priyanka

*Staff Student Liaison Committee: 2018, Semester 1