



DIT SPAM Experience

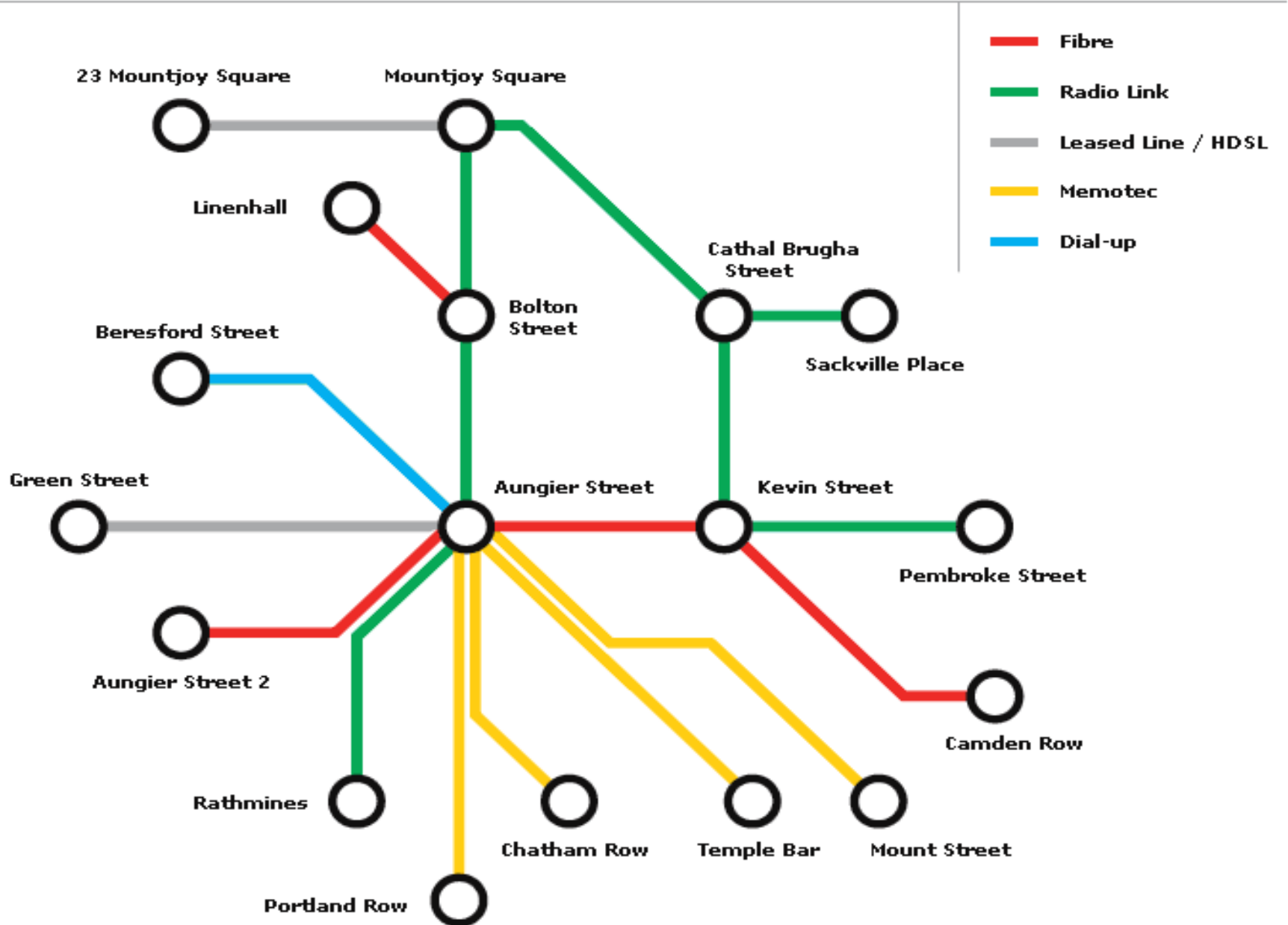
Patricia Keena

Systems Administrator

Information Services

Dublin Institute of Technology

DIT Metropolitan Area Network





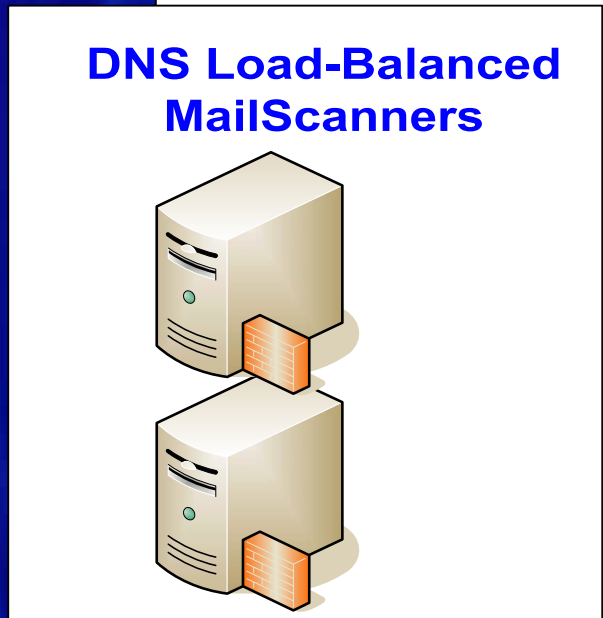
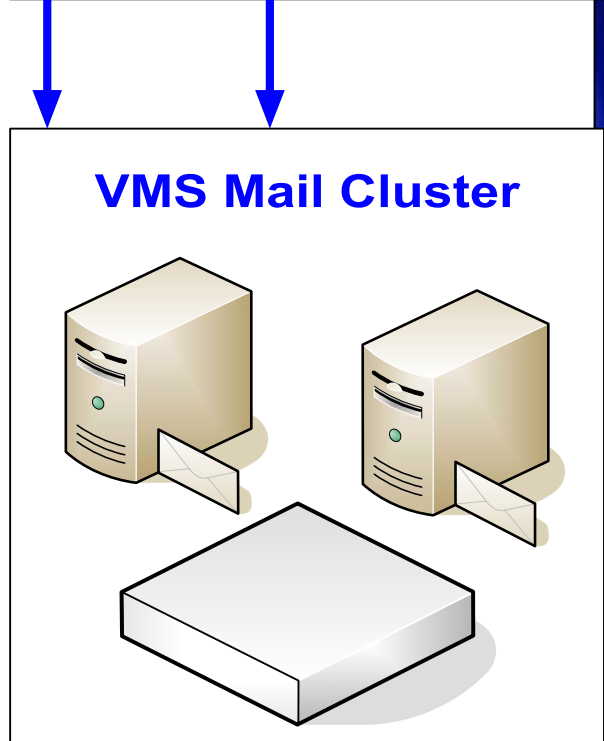
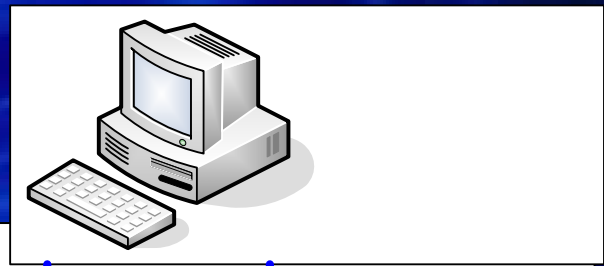
SPAM Challenges

- Excess of 20,000 active e-mail accounts.
- More than 140,000 messages daily.
- Excess of 56,000 messages detected as SPAM (40%).
- False-positive and false-negative messages.
- Filter SPAM whilst providing easy access to filtered content.



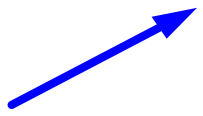
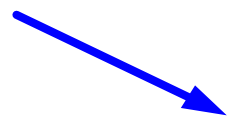
Current Infrastructure

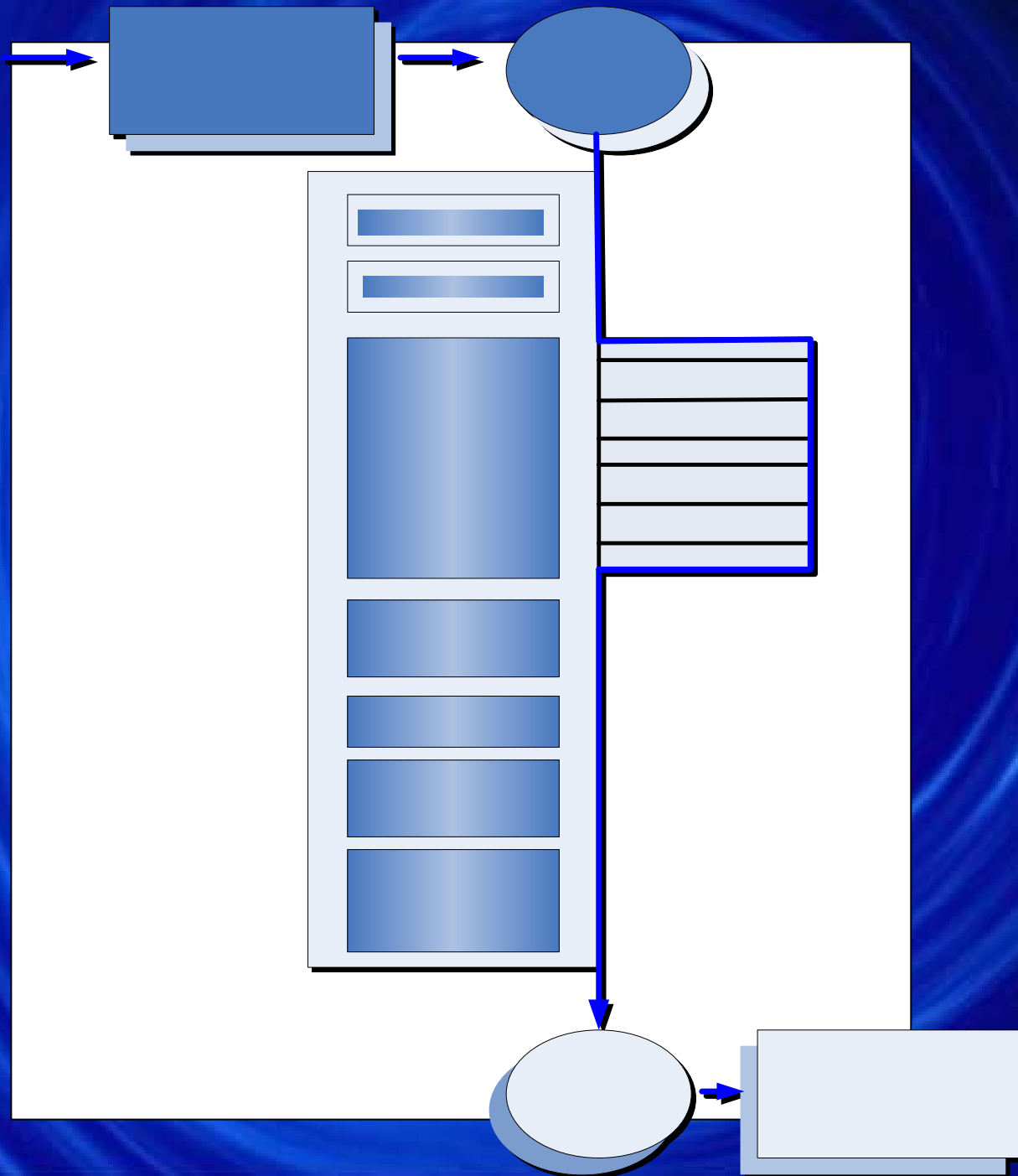
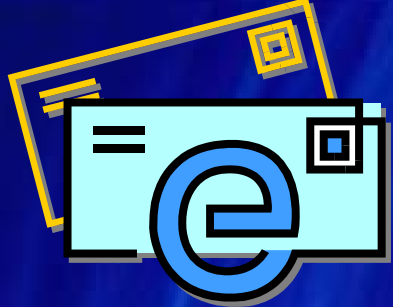
- Mail cluster - OpenVMS 7.3, PMDF 6.2.
- Two load balanced MailScanner Servers.
- Debian Woody 3.0r2 with MailScanner 4.30.
- SpamAssassin 2.63 with Bayes and RBL Checks.
- Additional SpamAssassin Rules i.e. rules du jour etc. www.rulesemporium.com
- Virus Scanning i.e. F-Secure and ClamAV.
- Email Clients i.e. Outlook, Netscape, SquirrelMail, WebMail etc.



← Un-Scanned Messages

→ Internal Addresses







Processing Messages

- SpamAssassin threshold 5.0.
- Messages exceeding 5.0 - subject line is tagged ??SPAM??.
- Virus messages - subject line tagged {Virus?} and attachment quarantined.
- SPAM tagged messages - filtered to users IMAP SPAM folder.
- SPAM is accessible to users via IMAP clients.



Our Experience

- Initial system deployment - summer 2002.
- Positive user reaction and acceptance.
- Early 2004, increased false-negatives.
- Mid 2004, new hardware and additional software e.g. SpamAssassin, Bayes, RBL, additional rules e.g. SURBL.
- Positive user reaction e.g. “makes coming to work almost a joy”



What we have learned

- Users will report false-positive messages.
- Blacklist account - difficult to maintain.
- User Education to prevent false positives.
- Investigate false-negative messages.
- Add additional SpamAssassin rules regularly.
- Follow the listserv for updates e.g. SURBL.



Plans for the Future

- European Coalition Against Unsolicited Commercial E-mail (EuroCAUCE).
- E-Mail Authentication.
- Black-list and white-list - client v server.
- Monitor the IT industry - new developments in SPAM control.
- Experiences of other organisations along with our own experiences.



Thank you!