2007

Some problems in Network and Data Centre Management

David Veal
Edith Cowan University

Gurpreet Kohli
Edith Cowan University

Some Problems in Network and Data Centre Management

D. Veal and G. Kohli
School of Computer and Information Science (SCIS)
Edith Cowan University (ECU)
Perth
Western Australia
Australia
d.veal@ecu.edu.au

Abstract

Computer networks are vital to the running of modern organisations. Network managers are often concerned with the running of data centres. This paper provides an overview of some of the more important issues in managing modern computer networks and data centres and the problems faced in undertaking this task. It would be impossible to provide a complete list which, due to the fluid nature of this industry, would become outdated very quickly. It is important that network managers have an awareness of modern Occupational Health and Safety (OHS) requirements, training and skills. There is also a need for network managers to plan for backup of staff, equipment, premises and for disaster recover. Furthermore, network managers need to be aware of the need for effective network design and up-to-date documentation procedures and implementation.

Introduction

There are a large number of demands competing for the attention of network managers (Nelson, Ahmad, Martin, & Litecky, 2007). These include not only the day-to-day running of the network, and data centres but also providing internet services to applications and staff. Keeping such systems up and running is a vital component of enterprises in the information age. Network managers often experience problems in keeping up-to-date with rapid technological change in terms of new equipment needs, associated staff development and training requirements as well as changes in law, safety requirements and practices.

Modern Developments in Network Management

Modern computer networks exhibit a high degree of complexity both in their management and in their implementation (Olifer & Olifer, 2006). This includes very fast rates of change coupled with a high expectation from end-users. Furthermore, there has been significant convergence of many technologies such as Voice over IP (VoIP) whereby voice communication can be enabled over computer networks potentially resulting large cost savings and new additional value added services when compared to exclusively using the traditional telephone network (Nortel, 2007). There is also the need to allow wireless networks and to combat the many security risks involved (Ciampa, 2007). Furthermore, there is the problem of the shortage of staff with suitable experience combined with the problem of continual rapid change both in equipment and the associated technologies. Moreover, there are increases in security related incidents due to more readily available powerful network penetration tools (Ruffi, 2007).

Data Centres

A data centre is a facility where much of the communication and server infrastructure is centrally located. This avoids unnecessary duplication of power, cooling, security and specialised buildings with their associated fire and smoke alarm systems (EPA, 2007). According to US Environmental Protection Agency (EPA) data centres: "*… have become essential to the functioning of business, communications, academic and governmental systems*" (EPA, 2007). The planning of data centres requires that all key stake holders are consulted and discussions undertaken regularly during the planning, design and implementation stages as has been noted in many previous standard student courses and textbooks on systems analysis. However, in a white paper entitled *"Data Center Energy Efficiency and Productivity"* Brill notes that: *"The rate at which change is occurring exceeds the ability of most organizations to adapt and cope. The result is confusion, delay, increased downtime risk, and sub-optimal decisions"* (Brill, 2007). There are ongoing problems with network security that require urgent attention within the infrastructure design.

Security Problems

Security problems can include the physical security of the devices as well as the need for staff to be aware of such issues and the required procedures and policies to be followed. This can include all staff entering the premises including outside maintenance staff as well as cleaning staff. The demands of network security have also been increasing at a fast rate where new security protocols and devices need to be introduced to combat new threats. A lack of understanding of the operation of these protocols can lead to security holes in the network which can have disastrous consequences (Ingham & Forrest, 2002). Some protocols can, in certain circumstances, interact with other protocols to cause them not to operate correctly. New security devices and software may need to be understood, tested and installed (Roberts, 2005). New security patches to cover newly discovery security holes in installed software also need timely application. This can place a huge demand on staff to keep the entire infrastructure patched and to quarantine system sub-components should a security breach occur.

Uptime Demands and Backup

There is a need for a high uptime and this requires additional equipment which leads to extra costs. It should be noted that a large fraction of an organisation's annual budget can be consumed in IT costs (Gutierrez, 2005). Redundancy may also need to be implemented by obtaining power from different substations, and the use of Uninterruptible Power Supplies (UPSs) using battery backup. UPSs can also provide a defence against high voltage power spikes possibly caused by nearby lightning strikes that could damage electronic equipment.

The US based Telecommunications Industry Association (TIA) 942 Data Center Standards Overview provides guidelines and benchmarks for data centre design. The TIA's highest rating for a data centre is 99.995% fault tolerance where planned activity does not disrupt the critical load and that the data centre can sustain at least one worst-case incident, multiple active power and cooling distribution paths along with an annual downtime of 0.4 hours (TIA, 2005). In order to achieve this level an organisation may need to spend many years of effort and planning. The cost of cooling can also be a concern. Brill notes that: *"The performance per dollar of IT equipment continues to increase dramatically. Less obvious is that the power consumed per computer rack or cabinet has also jumped dramatically"* (Brill, 2007). Furthermore, Kotadia has commented that: *"The problem is so bad that the analyst firm Gartner expects to see more money spent this year on power and cooling technologies than on the actual servers themselves"* (Kotadia & Morton, 2007).

An often overlooked redundancy is the need for trained experienced staff to provide backup. Staff training is vital but having actual working experience with the system in the data centre is of the upmost importance. Moreover, it should be noted that possessing the appropriate skills and understanding to engage in effective troubleshooting is also of vital importance. A solution that may have been effective previously in a given situation may not necessarily be a correct solution in another scenario, even though the observed symptoms may be similar, but have different causes due to differing implementations. This situation has its analogies in the sphere of medicine. Staff involved in the day-to-day operation of the data centre will have a great deal of experience and understanding of the various component systems used and the typical problems encountered.

Load sharing can also be used as a form of redundancy enabling the traffic and device workload to be distributed according to their demands and their respective capacities (Teare & Paquet, 2007). Care should be taken to ensure that links or equipment still operating after a failure can handle the required extra demands. Furthermore, it is not much use if an automatic alarm system provides a warning only in the effected area of operation e.g. if the device needing to receive the warning is itself dead due to the same fault that triggered the warning. This is the 'dead sentry' effect. The device relied upon to give the warning may itself be dead. Just because no alarm is received may not be an assurance that all is well. Redundancy can also be implemented via a whole redundant backup data centre, should this be required but incurring much higher implementation and running costs.

Network Scalability

All modern systems are designed to cater for scalability and service level agreements. Scalability is the ability of a network design to cater for changes in protocols and devices without the need to significantly change the whole network resulting in major increases in both cost and implementation time, and most likely, the introduction of new errors (Teare & Paquet, 2007). However, a rigorous methodology should be followed by people undertaking such a task and the most appropriate tools to be used. It is well known from previous research, that this information is either sourced from the vendor providing that particular equipment, or solutions, or it is based upon obtaining the fastest equipment available within the budget constraints. This may lead to either under utilisation (Maj, Veal, & Duley, 2001) or inefficiency in the actual running of the system (Kohli, Veal, & Maj, 2003).

Network Documentation and Design

Another factor, often overlooked, in reducing downtime is effective and readily available documentation (Lewis, 2005). This is frequently postponed due to the more immediate demands to keep equipment up and running with constant changes also taking place (OECD, 2006). Lack of effective documentation may also be used as a form of job protection insurance in an age of employment uncertainty. If a particular employee is the only person who knows the network layout then they become a key employee. Moreover, management may be pleased that there are not too many complaints about the computer network yet they may not be aware of the crucial importance of good documentation. Therefore staff efforts may not be directed towards developing or maintaining up to date documentation. In addition, to the need for documentation, there is also a need for meaningful labelling of devices, ports and cables to reduce the time required to troubleshoot and recover the system in cases of major downtimes and relocation of devices. Effective instructions on the procedures to adopt should a particular device malfunction, and the staff needed to be contacted about this situation, should be made readily available in case of an emergency. Such requirements and procedures need to be included under staff training. There are many network management monitoring applications to assist the day-to-day running of the network, its security, configuration, testing and reporting. Again this means that staff needs to be aware of what is on offer, what are the areas of application, and what are the strengths and weaknesses of these various offerings?

Education and Training

There are various approaches that organisation can take to staff training. One such approach is to use vendor based training such as that provided by commercial training providers. These are often intensive short courses of about a one week duration based upon a particular technology. Additionally, the Cisco Networking Academy Program (CNAP) provides network curricula for schools, universities and TAFEs but do not offer the same range of vendor based training as commercial providers.

The need for hands-on skills has been flagged as an important requirement both in network technology education (Veal, Maj, & Duley, 2001) and for network managers (Gramignoli, Ravarini, & Tagliavini, 1999). The traditional Computer Science or Information Systems (IS) management courses, many of which are university based, often follow studies similar to those endorsed by the American Computing Machinery (ACM/IEEE, 2001) or Management Information Systems curricula (Gorgone, Gray, Stohr, Valacich, & Wigand, 2006). An OECD report on *"Information on Communication Technologies"* (ICTs) has noted that "*Full-time education is not currently the main source of ICT skills…*" (OECD, 2004). Most organisations expect staff to be well trained and in some cases also certified for the equipment they are supporting. Hence there is continuous need for updated vendor based certification and training as new technologies become available.

Health and Safety of Staff and Devices

Policies and activities related to the operational management of data centres need to comply with current local and national Occupational Health and Safety

(OHS) requirements (Ogletree, 2004; Verity, 2003). If this is not the case then the organisation and management may find that they incur hefty penalties and associated legal costs (Veal, Kohli, & Maj, 2004). Emphasis is often placed on OSH procedures related to fire and responding to, and the avoidance of, accidents. Should staff lack appropriate training in handling devices within the data centre then, in some cases, the mishandling of equipment could not only result in accidents, but possibly large unnecessary extra costs to an organisation both in compensation, fines and damage to expensive equipment.

Conclusions

Running and managing an organisation's network and data centre is a demanding task. There are a large number of problems that network managers may be called upon to solve such as OSH, IT training and recruitment as well as just keeping systems running effectively. There is continuous change taking place, where problems of security, new devices, and protocols present an ever present challenge to effective network management. There is also a need for good up to date accessible network documentation, disaster recovery procedures and effective staff backup. Furthermore, there is a need to understand the warning systems of devices under their control and any circumstances where these systems could fail to give appropriate warnings.

References

ACM/IEEE. (2001). *Computing curricula 2001 ACM/IEEE Joint Task Force Computer Science Final Report*: ACM.

Brill, K. G. (2007, March 4-7). *Data center energy efficiency and productivity.* Paper presented at the Invisible Crisis in the Data Center, Orlando.

Ciampa, M. (2007). *CWSP Guide to wireless communication*. Boston MA: Thomson.

EPA. (2007). *EPA report to congress on server and data centre energy efficiency: Executive summary*. Washington DC: Environmental Protection Agency.

Gorgone, J. T., Gray, P., Stohr, E. A., Valacich, J. S., & Wigand, R. T. (2006). MSIS 2006: Model curriculum and guidelines for graduate degree programs in information systems. *SICCSE Bulletin, 38*(2), 121-196.

Gramignoli, S., Ravarini, A., & Tagliavini, M. (1999). *A profile for the IT manager within SMEs.* Paper presented at the 1999 ACM SIGCPR 99 Conference on Special Interest Group Computer Personnel Research, New Orleans, LA.

Gutierrez, C. M. (2005). *Information and communication technology: 2003*. Washington DC: US Census Bureau.

Ingham, K., & Forrest, S. (2002). *A History and survey of network firewalls*. Retrieved 14 February, 2006, from http://www.cs.unm.edu/research/search_technical_reports_by_researcher/?string=ingham

Kohli, G., Veal, D., & Maj, S. P. (2003, 18th-20th November). *Modelling website infrastructure using B-Node theory.* Paper presented at the 9th ANZSYS Conference: Systems in Action, Melbourne, Vic, Australia.

Kotadia, M., & Morton, E. (2007, April 26). *Moore's law can't stand the heat*, from http://www.zdnet.com.au/news/hardware/soa/Datacentre-energy-crisis-looms/0,130061702,339271875,00.htm

Lewis, W. (2005). *CCNP 4:Network troubleshooting guide*. Indianapolis IN: Cisco Press.

Maj, S. P., Veal, D., & Duley, R. (2001). *A proposed new high level abstraction for computer technology.* Paper presented at the SIGCSE ACM 2nd Technical Symposium in Computer Science Education, Charlotte, NC.

Nelson, J. H., Ahmad, A., Martin, N. L., & Litecky, C. R. (2007, April 19-21). *A comparative study of IT/IS job skills and job definitions.* Paper presented at the SIGMIS-CPR'07, St Louis MI.

Nortel. (2007). *Nortel technical solutions academy*. Retrieved September 11, 2007, from www2.nortel.com/go/news_detail.jsp?cat_id=-9721&oid=100217166&locale=en-US

OECD. (2004). *OECD information technology outlook: Highlights*. Paris France: OECD.

OECD. (2006). *Information technology 2006 highlights*. Paris France: OECD.

Ogletree, T. W. (2004). *Scott Mueller's Upgrading and Repairing Networks* (4 ed.). Indianapolis, IN: QUE.

Olifer, N., & Olifer, V. (2006). *Computer Networks*. Chichester, UK.: Wiley.

Roberts, C. (2005). *Voice over IP security*. Retrieved April 16, 2006, from www.ccip.govt.nz

Ruffi, A. W. (2007). *Network Security 1 and 2 companion guide*

Teare, D., & Paquet, C. (2007). *Building Scalable Cisco Internetworks (BSCI). Authorized Self-Study Guide* (3rd edition ed.). Indianapolis IN: Cisco Press.

TIA. (2005). *TIA-942 data center standards overview*. Retrieved August 18, 2007, from www.tiaonline.org/standards

Veal, D., Kohli, G., & Maj, S. P. (2004). *Safety on a hands-on computing science unit: Not merely an accidental extra.* Paper presented at the American Society for Engineering Education (ASEE), 2004 Annual Conference,, Salt Lake City, UT, USA.

Veal, D., Maj, S. P., & Duley, R. (2001, Feb 21st - 25th). *Assessing Hands-On Skills on CS1 Computer and Network Technology Units.* Paper presented at the ACM SIGCSE 32nd Technical Symposium on Computer Science Education, Charlotte, NC.

Verity, B. (2003). *Guide to network cabling fundamentals*

Biography

David Veal has a BA Degree in Physics from the University of York and a general Degree from the Open University UK. David has a Post Graduate Certificate in Education (PGCE) from the University of Keele UK where his subject specialist areas were Physics, Mathematics and Computing. David taught Physics for 10 yeas at South Devon College in the UK before migrating to Australia. He has a has a Graduate Diploma in Computing Science from Curtin University in Perth and a PhD in Computer Science from ECU where his research areas were competency-based assessment and models of computers and computer networks. David is a lecturer, tutor, and unit coordinator on the Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP) based units in Computer Science at ECU.

Gurpreet Kohli has a B.E. in Electronic Engineering from Nagpur University, India and an MSc Information Technology from ECU, where his research topics were the design of computer networks for multimedia applications. Gurpreet also has a PhD in Computer Science from ECU where his research area was state model diagrams of computer networks. He has presented numerous research papers at international conferences in Sweden, USA and Canada and within Australia and has lectured and tutored on computer networking units at ECU. As an invited speaker Grupreet has given many talks to university computer networking students on the problems of managing computer networks. Gurpreet has worked in the Perth as a software developer and is presently employed as a network engineer at Curtin University of Technology in Perth Western Australia.