# Central issues in network management

Sarah Lowman

April 2010

## Introduction

Network management is a set of activities, procedures and tools that concern the *operation*, *administration*, *maintenance* and *provisioning* of a computer network (Javvin Technologies, 2010). Operations is concerned with keeping the network and its services running efficiently, usually by monitoring the network and solving any problems before they affect users. Administration is about keeping the network under control, involving tasks such as monitoring the network resources and their assignment. Maintenance deals with repairs, upgrades and measures to improve the network such as configuration tweaks. Finally, provisioning deals with changing the network to handle new requirements or services.

There are many important subcategories in network management, including configuration management, accounting management, fault management, performance management, security management, bandwidth management, cryptographic key distribution and route analytics. FCAPS is a memorable acronym for the most important management areas - Fault, Configuration, Accounting/Administration, Performance and Security. FCAPS was first introduced in the OSI Systems Management Overview ISO in the 1980s. The intention was to create 5 separate protocols, one for each FCAPS management area. However, due to the similarity between the protocols, instead of five separate protocols, one overarching protocol was created named the Common Management Information Protocol (ISO/IEC 10040, 1998). FCAPS was also used in the ITU-T Telecommunications Management Network (TMN) protocol in the 1990s, and has become a standard way of thinking about network management.

There are many 3rd party network management solutions, such as WebNMS[1] and Zabbix[2], which exist for enterprises and other organisations with large networks. These utilise pre-existing network management protocols and can collect data using numerous methods including logging, packet sniffing, and installing intelligent agents (Bieszczad, Pagurek, & White, 1998) on the infrastructure to provide complete FCAPS management. The emergence of cloud computing and on-demand virtual resources has resulted in an ever-increasing reliance on networks. Businesses therefore have to constantly re-evaluate and upgrade their network management solutions (Goyal, Mikkilineni, & Ganti, 2009).

[1] http://www.webnms.com/solutions/nevs_fcaps.html

[2] http://www.openwatersolutions.com/zabbix.htm

This essay will describe each of the management areas of FCAPS in more detail, describing some of the problems that arise in network management and their solutions.

## Fault Management

Fault management is the detection and correction of malfunctions on the network. Network faults can be divided into hardware and software faults. Hardware faults can be caused by wear and tear, accidental or malicious damage or incorrect installation. Software faults can be caused by bugs, incorrect design, the use of unsuitable software, or incorrect information – for example incorrect routing tables can result in a slow or faulty service (Gürer, Khan, Ogier, & Keffer, 1996).

The detection of faults is through real-time alarms or analysis of error log files. When a fault occurs, the device may send a notification (an alarm) to the network administrator via the Simple Network Management Protocol (SNMP). An alarm is a persistent indication of a fault, which will only clear when the fault has been fixed (Cisco, 2002). Alarms can be caused by either physical problems (e.g. a link being down) or logical problems (e.g. statistical measurements going over a threshold, such as link congestion). These alarms are often kept on an Active Alarm List (as defined in RFC 3877[3]). Alarm filters may be in place to correlate alarms and eliminate multiple occurrences of the same alarm. Filters also assign the alarms to different severity levels. RFC 3164[4] (syslog) uses the severities: *debug, informational, notice, warning, error, critical, alert* and *emergency*, whilst ITU X.733 (Alarm Reporting Function) uses severities of *cleared, indeterminate, critical, major, minor* and *warning.*

This type of fault management is called *passive* – the fault management system only knows of a fault when it receives an SNMP alarm. A problem with this is that the device not only has to be intelligent enough to send the message, but also must be in a suitable state to do so. The fault may render the device unable to send the alarm, thereby allowing the fault to go undetected. *Active* fault management involves the system sending out periodic requests (such as Ping or Traceroute) to devices to check they are active (Nadi, 2009). If no response is received, an alarm is raised.

Faults can be identified by requesting diagnostic tests and status updates from resources that raise alarms. Before the problem can be fixed, network administrators may want to reroute traffic away from that resource to ensure there is minimal loss of service. Once the fault has been identified and analysed, remedial actions can take place. These may involve the administrator replacing damaged hardware or debugging software. Some fault correction can be automated, with the fault management software autonomously launching scripts when particular problems occur.

[3] http://tools.ietf.org/pdf/rfc3877.pdf
[4] http://tools.ietf.org/pdf/rfc3164.pdf

## Configuration Management

Network Change and Configuration Management (NCCM) has become essential for IT organizations in enterprise, government and service provider environments (EMA, 2008). Configuration management focuses on the organisation, maintenance and updating of configurations for all the components on the computer network (both hardware and software). Usually configuration information is collected and kept in a database so that changes can be easily tracked. This allows identification and traceability of device configurations (BS ISO 10007, 2003). Configuration management is often named *change control* or *change management*.

Configuration management tools allow any changes made to be documented and easily rolled-back if they were not successful. When a fault has occurred, having an audit trail of any configuration changes means the source of the problem can be easily identified. For example, when multiple system administrators are working on the same network and step on each others' toes, this makes it is easier to see where things went wrong or to roll back to a known-working state. Configuration management is also useful in making large changes: manual updates to multiple devices would be time consuming, but by using intelligent configuration management the same changes can be rolled out automatically – saving time and reducing errors (Hughes, 2009).

Other requirements of any NCCM solution include providing multi-vendor support, easy deployment, easy use and scalability (EMA, 2008). A lot of networks have many different devices from different vendors, so having a common interface to configure them all is important.

## Accounting Management

Accounting management, also known as *billing management*, involves gathering network usage statistics so that users can be billed for usage or so that usage quotas can be enforced. For non-billed networks, 'accounting' is replaced by *administration*. Accounting/Administration management also involves the management of users and passwords, permissions and software backups and synchronisation.

Organisations do not have common accounting requirements, so there is not a single accounting protocol that meets all needs. Consequently, the goals of accounting management are to provide tools that can be used to meet the requirements of many different accounting applications (Aboba, Arkko, & Harrington, 2000). RADIUS, TACACS and Diameter are some of the protocols commonly used.

RADIUS (Remote Authentication Dial In User Service) is an Authentication, Authorization and Accounting (AAA) protocol, developed in 1991. RADIUS has broad support and is often used by Internet Service Providers and enterprises to manage access to the internet or internal networks (Posey, 2006). It is an application layer client/server protocol, which uses UDP as transport. RADIUS has three functions: to authenticate users/devices so they can access the network; to authorize those users/devices for any network services; and finally to account for the usage of those services (CISCO, 2006). Diameter is a successor to RADIUS.

The architecture of a network accounting system generally involves an accounting server, a billing server and the interactions between these and the devices on the network. The network devices collect accounting metric data, which is sent to the accounting server, normally using an accounting protocol. This data is processed by the accounting server and sent to the billing sever which handles the invoice generation. The billing server may also carry out auditing, cost allocation and trend analysis (Aboba, Arkko, & Harrington, 2000). Trend analysis involves forecasting future usage. This can be achieved through statistical sampling techniques.

Billing can either be usage sensitive, or non-usage sensitive. If the billing is non-usage sensitive, the accounting metric data is not needed by the billing server, unless it is carrying out any secondary functions like trend analysis. Usage sensitive billing may be required to conform to financial reporting and legal requirements, since any packet loss between the network devices and the servers may turn into revenue loss for the organisation (Aboba, Arkko, & Harrington, 2000). Auditing is likely to be required for usage sensitive billing. Auditing tasks include verifying the correctness of the accounting and billing procedures and verifying the invoices created.

## Performance Management

Network performance management is the measuring, planning and optimisation of networks to balance the performance needs of the organisation (in terms of capacity, reliability and speed) with the cost constraints. Different end-user applications require different performance needs: for example streaming video can be unreliable but needs to be fast to avoid lag (therefore UDP is often used instead of TCP). Some applications require a specific *Quality of Service*. Quality of Service is the ability to provide different applications a guaranteed level of performance, especially if the network capacity is insufficient to provide a good enough quality to all the services using it (Xiao, 2008). This is mostly used for real-time streaming services such as Voice-Over IP and online gaming which require a minimum bit-rate and are latency sensitive. Whilst Quality of Service guarantees for audio and video are important, it is also important these do not compromise connectivity, robustness, and performance for traditional best-effort traffic (Keshav & Sharma, 1998).

Several factors affect the delivery of data across a network, including latency, packet loss, retransmission delays and throughput. A network performance manager aims to ensure a network has high bandwidth with little latency and packet loss.

*Latency* is the time taken for a sent packet to be received at the destination, including the encoding and decoding times at either end. Latency can be improved by having fewer intermediary nodes for a packet to travel through, or reducing the amount of processing (such as filtering or accounting) that nodes perform. *Packet loss* can occur for a number of reasons, which include overloading of intermediary networks, rejected packets due to corruption or errors, faulty networking hardware or drivers, signal degradation or intentional discarding of packets to enforce a particular level of service. *Retransmission delays* are caused by packet loss in a reliable network (such as TCP). The delay is twofold: there is the delay from retransmitting the data, and there is a delay whilst the receiver waits until packets can be recombined in the correct order before being promoted up the protocol stack. *Throughput* is the amount of traffic a network can carry, measured in bits per second. The throughput may be lowered due to many users sharing the same network resources. Throughput can also be lowered by the use of specific protocols on the network. For example, in the transport layer, TCP uses flow control and congestion avoidance, and in the datalink layer CSMA/CD and CSMA/CA use 'backoff' waiting times and retransmissions after detecting collisions (Tanenbaum, 2003).

To measure the performance of a network, several utilities can be used. Examples are Ping – which measures Round Trip Time (RTT) and packet loss; Traceroute – which measures RTT and path taken (Barford, 2008); and Multi Router Traffic Grapher (MRTG). MRTG can used to collect and collate information from SNMP-enabled devices. It can then produce graphs for things like network throughput over time.

## Security Management

Network security management includes protecting the network and resources from unauthorised access, detecting and mitigating security breaches, managing security services, controlling and distributing cryptographic keys and managing user rights and privileges. Specialised risk assessment and risk analysis tools are often used to identify assets, threats and to rate network system vulnerabilities so that appropriate action can be taken to mitigate potential security problems. In a networked system, many devices, such as routers, firewalls, virtual private network gateways, and individual host operating systems, must cooperate to achieve security goals (Guttman & Herzog, 2004). Security management is difficult and error-prone as these devices may require different configurations depending on their location and purpose. The difficulty of security management is illustrated by the following truism: an attacker only needs to find *one* successful attack vector, whilst security management must be aware of and defend against *all* attack vectors.

Encryption key management involves key generation, exchange, storage and usage of encryption keys, with many different cryptographic mechanisms to choose from. Inappropriate choices may result in an illusion of security, but little or no real security for protocols or applications (Barker, Barker, Burr, Polk, & Smid, 2007). Successful management of the keys is critical to the security of a cryptosystem. It can be difficult to coordinate this with user training, system policy and organisational interactions.

# Conclusion

'Network management' is a term encompassing all factors of a network. FCAPS is a framework that allows administrators to divide up network management into five different areas: Fault management, which deals with detecting and correcting malfunctions on the network; Configuration management, which tracks and documents network configuration changes; Accounting management, which deals with the billing or usage allowances of network users; Performance management, which aims to optimise the performance of the network; and Security management, which deals with the control and management of security policies and encryption keys.

All of these areas need to be carefully managed to keep a network in good working order. Poor network management can result in costly problems for an organisation. For example, lax security standards can result in loss of private data, network congestion can result in poor employee productivity, ineffective billing can result in revenue loss and expensive network outages can occur due to poorly configured routers or faulty hardware. These problems can be avoided through use of effective network management tools and protocols.

The growing business dependency on networked communication means that services and uses for networks are continuously being invented and evolved. Network management must evolve to keep pace, becoming more sophisticated and intelligent in the process (Grigonis, 2007). In the past, network management was only influenced by the skill of the staff. However, as networks have become more dynamic and complex, the use of good network management software has become just as important. This has given rise to software that uses artificial intelligence to solve some management problems (Gürer, Khan, Ogier, & Keffer, 1996), such as using mobile agents for fault management (Bieszczad, Pagurek, & White, 1998) and systems that can make security decisions automatically without the need for a network administrator (Guttman & Herzog, 2004).

Even with the help of autonomous and intelligent agents and network management software, the job of a network administrator is important and complicated. They must balance the different network management areas to make sure their system is properly configured and maintained.

## Bibliography

Aboba, B., Arkko, J., & Harrington, D. (2000). Introduction to Accounting Management. *Network Working Group* .

Barford, P. (2008, September 11th). *Network Performance Measurement and Analysis*. Retrieved from University of Wisconsin-Madison: http://pages.cs.wisc.edu/~pb/640/perform.ppt

Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2007, March). *Recommendation for Key Management - Part 1: General*. Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

Bieszczad, A., Pagurek, B., & White, T. (1998). Mobile Agents for Network Management. *IEEE Communications Surveys* .

BS ISO 10007. (2003). *Quality management systems — Guidelines for configuration management*. Retrieved from http://bjgyzy.com/pdf/4.pdf

Cisco. (2002). *Cisco Active Network Abstraction Fault Management User's Guide, 3.5.1*. Retrieved from http://www.ciscointernethome.net/en/US/docs/net_mgmt/active_network_abstraction/3.5.1/fault_management/user/guide/1fltmn.pdf

CISCO. (2006). *How Does RADIUS Work?* Retrieved April 16th, 2010, from http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml

EMA. (2008). Network Change and Configuration Management: Optimize Reliability, Minimize Risk and Reduce Costs.

Goyal, P., Mikkilineni, R., & Ganti, M. (2009). FCAPS in the Business Services Fabric Model. *18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises* , pp. 45-51.

Gürer, D. W., Khan, I., Ogier, R., & Keffer, R. (1996). An Artificial Intelligence Approach to Network Fault Management. *SRI International* , pp. 1-10.

Guttman, J. D., & Herzog, A. L. (2004). Rigorous automated network security management. *International Journal of Information Security. Volume 4, Numbers 1-2* , pp. 29-48.

Hughes, J. (2009, February 20th). *Network Configuration Management Introduction*. Retrieved April 16th, 2010, from openxtra: http://www.openxtra.co.uk/articles/network-configuration-management

ISO/IEC 10040. (1998). *Information technology - Open Systems Interconnection - Systems management overview.*

Javvin Technologies. (n.d.). *Tele-Communication (Telecom) Terms Glossary and Dictionary*. Retrieved April 5th, 2010, from Javvin Network Management & Security: http://www.javvin.com/telecomglossary/OAM.html

Keshav, S., & Sharma, R. (1998). Achieving Quality of Service through Network Performance Management. *Cornell Network Research Group* .

Nadi, F. (2009, November 17th). *Network Management & Monitoring Overview*. Retrieved from http://www.pacnog.org/pacnog6/presentations/linux-network/network-management.pdf

Posey, B. (2006). *SolutionBase: RADIUS deployment scenarios*. Retrieved April 16th, 2010, from Tech Republic: http://i.techrepublic.com.com/downloads/PDF/SolutionBase_RADIUS_deployment_scenarios.pdf

Tanenbaum, A. S. (2003). *Computer Networks.* Upper Saddle River, NJ: Prentice Hall.

Xiao, X. (2008). *Technical, Commercial and Regulatory Challenges of QoS: An Internet Service Model Perspective.* Morgan Kaufmann.