



# The business case for network management

by Jason Peach

---

The business need for network management: the cost of downtime

page 2

Network management function: best practice

page 3

Network management function: people

page 4

Network management function: process

page 5

Network management function: systems

page 6

Appendix A: Defining the network management function

page 10

---

---

## The Business case for network management

*The term Network Management has many definitions and is often misunderstood, or very simply used to describe a PC that sits in a corner somewhere collecting dust. However, Network management is in reality a broad functional area of IT incorporating many disciplines to ensure IT is aligned to the business or organisation it aims to support.*

*Network Management does involve device monitoring and troubleshooting, but Network Management as a function, performed properly, should maximise the business benefit of IT by sustaining and optimising IT services – ideally coordinated by an experienced Network Manager or Administrator.*

*This paper discusses the term Network Management, providing broader operational context for people, process, and systems; describing the case for an effective network management function; a function that can directly affect an organisation's overall operational and financial performance.*

### ***The Business Need for Network Management: The Cost of Downtime***

An Infonetics study, "The Costs of Downtime", stated that SME companies experience an average of nearly 140 hours of downtime every year. The study concluded that the impact of an outage was 55% lost revenue and 45% lost productivity. ***This leads us to the question what is network downtime?***

Although downtime due to actual outages accounts for around 70% of availability problems, service degradation accounts for the remaining 30% of network problems, and is far more difficult to determine and resolve.

Degradation means there is some impairment to network performance that affects some, or all, IT applications.

Recent research from IDC concluded that even for SMB's "well-targeted technology upgrades, coupled with a rigorous program to standardise and improve IT practices can deliver substantial risk reduction and could reduce total annual outage risk by as much as 85%, in some cases".

IDC went on to state: "The amount of downtime reduction can deliver significant business savings, given that one group of SMB's in the study experienced an average loss of \$70,000 per downtime hour" (Boggs Raymond, p1).

The financial impact of downtime is easier to calculate when there is an outage, rather than a degraded service which is often harder to qualify. Tools like the one developed by the University of Warwick Business School, make calculating the cost of downtime for any business simple: <http://www.networksfirst.com/calculator/index.php>

Further analysis found other studies into the causes of downtime concluded that 40-45% of all network outages are caused by configuration error; sometimes referred to as soft issues; inevitably these problems cost hard cash, typically 55% lost revenue and 45% lost productivity as suggested earlier.

Given this, managing better network availability has to be a business critical function. In an economy now dominated by IP communications; from email to ecommerce, from data transactions to IP telephony; the IP infrastructure forms the foundation for business communications and is increasingly significant to bottom line performance.

### *The Network Management Function - Good Business Practice:*

In establishing the business need for an effective Network Management function, it is useful to understand what Network Management is, and the benefits it will provide.

In short, to ensure maximum return on investment (ROI) of a Network Management tool, it should be operated by skilled professionals. A good network management function requires a combination of people, process, and tools (systems) to ensure the delivery of an effective IT function.

In return, an effective Network Management function should provide the organisation a measured delivery, and governance, to ensure the ongoing success of the communications infrastructure in support of, and aligned to, organisational goals.

The Network Management function requires performance measures and statistical metrics (KPI's) to benchmark normal operational specifications of the network before abnormal events can be observed and acted upon.

However, for many organisations the Network Management function is not well defined. As an operational IT discipline, it is often neglected in favour of more

pressing 'customer facing' IT priorities. An operational culture may have evolved in some organisations where reactive or project based activity takes precedence in favour of the day to day focus necessary to monitor and perform preventative maintenance activities on the network infrastructure.

An effective Network Management function requires the following elements, driven by a culture promoting a life-cycle of preventative monitoring and maintenance measures; this in turn will drive high availability and an optimised network performance and ROI:

#### **The Network Management Function - People:**

The Network Management function requires more than NMS software; it requires skilled Network Professionals with the expertise and operational know-how, to regularly benchmark the compliance of the network infrastructure, to support the evolving needs of IT applications and of the organisation itself. Organisations are never static and the communications infrastructure supporting its function is therefore constantly evolving.

Analysis from InfoTech Research in 2007 calculated that on average around 12% of an organisation's IT staff budget was aligned to a Network Management function. This implies that there are dedicate

network professionals specifically looking at network issues, and resolving underlying concerns. However, in these tough economic times, does this statistic apply today?

With the advent of convergence, where Voice, Video and Data applications all share the same IP infrastructure, networks have become even more business critical and complex. Network professionals now need a deep understanding of the advanced logical configuration of the IP network entity that supports contemporary IP line of business applications. Networking has been for some time more than just physical connectivity; it requires a policy based networking approach, providing secure and differentiated applications to IT Users, regardless of their location: in the office, on the move, or at home.

The challenge for network personnel is that they must now know and understand how to provision and support many technologies ranging from LANs, WANs, and ISP services to more recent developments requiring advanced Wireless and IP Telephony deployments. Keeping pace with the business demand and technology innovation is a tall order for many IT professionals; consequently, many organisations inevitably have skill gaps. This perhaps explains the resulting statistic that 40-45% of network

downtime is caused by configuration error (human error); evidence that appears to suggest that skills aren't keeping pace with IT innovation and business demands.

The question organisations should seriously consider is 'have we got the resource to sustain and manage change within the context of their network infrastructure, one which is increasingly complex to manage, but is ever more business critical'?

### **Network Management Function - Process:**

In operational terms, to achieve high availability of the network; maximising the ROI on the business applications and functions that rely upon it; requires constant vigilance and effort. However, building proactive preventative maintenance regime is time consuming and expensive.

Our own research from various sources concludes that on average companies spend around six IT man-days per month dealing with changes, and that between 40-60% of all network problems are caused by change related issues. Additionally estimates suggest that an out-of-compliance network is 90% more costly to operate according to research done by Infonetics. Having an effective operational process in place, therefore, is vital to ensure the efficient and effective operation of a network management function.

There are numerous NMS software solutions on the market but very few skilled Network Professionals that dedicate themselves to operate them effectively. IT Support functions have many competing demands so effectively very little resource is given to operate NMS systems effectively. An effective NMS operation requires the proactive benchmarking of the network service, to monitor the key metrics that allow proactive analysis of the performance of components, and the Network Management function as a whole, against the benchmark. Through benchmarking it is possible to capture sub-optimal performance or failing states before they impact the IT service.

Any component has basically four operational states, it is either:

- **Optimised** – Configured to deliver Optimum Performance
- **Working** – Functioning to an Operational Standard
- **Failing** – Providing Sub-Optimal or below Standard Performance
- **Failed** – Not Functioning

The goal of a proactive Network Management function is to plot metrics for optimum and standard performance through benchmarking, and isolate working and failing states so they can be restored or re-configured to an optimised operational state.

However, it is inevitable that because of the sub-second speed

of some component failures there will always be a need for a very reactive maintenance and support service to perform a responsive restoration activity to avoid prolonged and unexpected business downtime.

Never-the-less, since 30% of all downtime can be attributed to a degraded service, and between 40-60% of outages are configuration or change related issues; there is a considerable case for a dedicated skilled network management entity. This proactive focused approach to network operations will in turn optimise systems availability and an organisation's ROI derived from all its other investments in IT and people assets.

Therefore, to ensure a business network can sustain high availability, optimal performance, and remain secure in the long-term, a life-cycle approach must be employed to proactively managed, refined, and developed the network; ideally performed by an experienced and dedicated team of skilled network professionals; to derive most business benefit.

Research suggests only well organised, skilled network professionals can focus on interpreting network conditions, and can effect remedial actions in an appropriate manner. Please refer to Appendix A of this document for more information offering an appreciation of the

operational tasks required to be covered by an effective dedicated Network Management function.

### Network Management Function - Systems:

There are many Network Management Systems available, varied both in terms of price and features. Some are vendor specific, others offer comprehensive systems management capabilities. Never-the-less, the ITU Open Systems Interconnection (OSI) standards that define them is ISO 7498-4, this defines concepts and terminology for key NMS disciplines; linked with the ITU-T M.3400 recommendation; it specifies five network management functional areas for NMS software leading to the standards based FCAPS network management model:

<b>Fault management</b>	detect, isolate, notify status & correct network faults
<b>Configuration management</b>	configuration, backup, software management
<b>Accounting management</b>	usage information of network resources
<b>Performance management</b>	measure, monitor, optimise performance
<b>Security management</b>	secure access to network resources

Further to FCAPS, Gartner Inc. developed a Network Management Maturity model based upon research across a number of organisations of varying size and industry sector. The Networking Maturity Model is designed to allow network teams to identify shortcomings, to establish priorities, and to set goals for improvement. The model describes network maturity in terms of five phases: Chaotic, Reactive, Proactive, Managed, and Optimal (Chen Catherine, p4 & 5).

**Chaotic Phase I** - In the initial, Chaotic phase, the network is undocumented. There is no procedure in place to guide employees' actions when problems arise; only ad hoc approaches that are applied on an individual or case-by-case basis. The overall approach to management is disorganised.

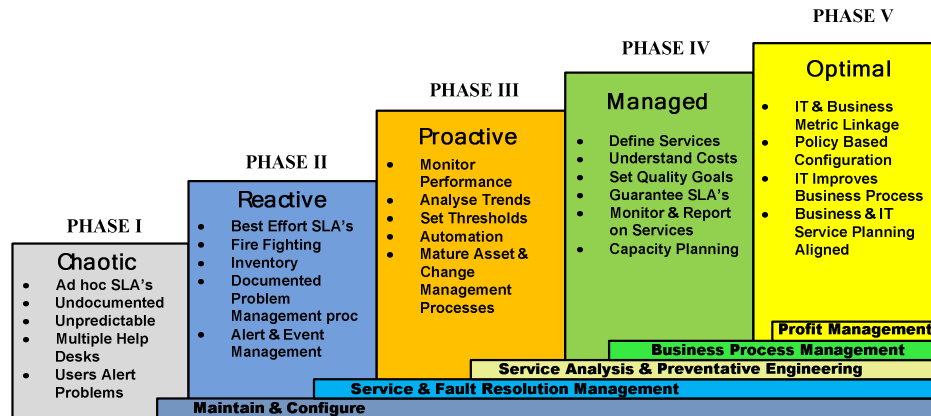
**Reactive Phase II** - In the Reactive phase, processes have been developed and followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. Network administrators deal with networking problems after they had occurred.

**Proactive Phase III** - In the Proactive phase, procedures have been standardised, documented, and communicated through

training. Network personnel set thresholds on various parameters for the network management tools to send warnings to alert the personnel before network problems arise. In addition, network administrators record trends of network usage and proactively management the utilisation.

**Managed Phase IV** - In the Managed phase, it is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Network administrators are able to forecast and plan the network capacity needed in the future.

**Optimal Phase V** - In the Optimized phase, processes have been refined to a level of best practice, based on the results of continuous improvement; for example via ITL, ISO 9000, and ISO 27001 standards. The NMS is used in an integrated way to automate change via workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt and to optimise the functional and financial benefit derived from the network assets that in affect become aligned closely with the business processes they support.



## Conclusion

Due to the increasing need for change and improvement in business process; perhaps using lean disciplines to ensure economic security and success; organisations are often turning to IT to drive productivity and change working practices. Now as never before, an effective Network Management function, whether completely in house or with elements out-tasked, has to be essential to supporting change and to enhance operational success.

Forrester Research Inc. found that 67% of their respondents reported that they were unaware of problems until end-users called the helpdesk, and 41% categorised their approach to network management as reactive to problems (Saran, 2004).

This research we have referenced may be old, but is it out of date?

Organisations should ask themselves what has changed significantly in their Network

Management practices since 2004, and indeed where do they sit now relative to the Networking Maturity Model?

It is worthy of note that only in the Proactive, Managed, and Optimal Phases of the Networking Maturity Model can an organisation start to realise a business benefit from their investment in Network Management; if indeed it exists as a dedicated IT function?

Only in the Managed and Optimal phases of the model can the Network Management function be a positive business asset; contributing to financial planning and success of the organisation; providing visibility and availability of its mission and associated critical IT applications, which in turn allows the possibility to optimise employee and business productivity.

Given the earlier question "What is Network Management?" the answer, in simple terms is that it just makes good business sense, and should be business best practice.

### Research Notes & References:

In doing the research for this paper it became apparent that many of the sources of empirical information are less than current; this is surprising since it is widely recognised that in particular with the adoption of IP Telephony, that IP networks undoubtedly form the foundations for all business communication.

Networks First is dedicated to invest in People, Process, and Systems so we can guarantee business communications through our advanced network services. Our **swift** Network Management Service for example is designed to augment internal IT resources to provide a proactive preventative maintenance regime on behalf of our customers. The **swift** service offered by Networks First combines the expertise of our engineers, with ITIL compliant operational best practises, with FCAPS compliant NMS systems to predict and resolve operational problems on behalf of organisations who's network and IT systems is mission critical, needing high availability guarantees, and the best ROI from investment in IT.

### References

1. IDC White Paper sponsored by HP, Reducing the Downtime and Business Loss: Addressing Business Risk with Effective Technology, Doc # 219697, August 2009
2. Chen Catherine, (2009), Computer Network Management: Best Practices, Gartner, Page 4 and 5
3. Infonetics: "The Cost of Downtime: North America 2006" [www.infonetics.com](http://www.infonetics.com)
4. Management and Staffing- Info Tech Advisor Premium, How to Right Size Your Network Team, June 2007, p3.

*When delving deeper into the process of Network Management there is no definitive guide that says what a network professional should do, how often they should do it, and how this is important to IT operations and in business terms. Hence Networks First has encapsulated below some of the most common, or fundamental tasks that a network management function should perform to successfully manage the IT network asset to best business advantage. Why should a business commit time and money to perform these tasks and how often should they be performed if a network is to remain compliant to business, industry sector, or even government directives?*

**Periodic Operational Tasks performed by a Network Manager or Administrator:**

Network Management as a function is often referred to as a “black art”. This is possibly since it has never been well defined. A Network Manager is somewhat isolated in that they are afforded specialist status but often work independently of others, out of hours, or within a small IT support team.

A lot of a Network Managers work can be under the covers of the IT system itself and out of view of their peers in IT or wider business stakeholders. Often when the network is performing well this is when network personnel are doing their best proactive work. When the network is down somehow this is when they are ‘appreciated’ most by their fellow workers but only

because their reactive work is brought sharper into focus; and only will they be appreciated if issues are resolved swiftly within SLA and outages are infrequent and clearly outside of their control to prevent.

Network Managers generally have a wide remit and this is extending all the time with directives around security, hardware, software, and configuration compliance; additionally the green agenda also adds to the complexity of the function; but consider the typical job description for a Network Manager below. Given these activities it seems reasonable that organisations may need the assistance of out-tasked services from a dedicated and trusted network partner, if only to provide holiday or 24x7 cover even if an optimal network management function already resides in-house.

**Periodic Tasks include: Reporting, Planning, Design & Policy Administration**

- *Budget Management & Cost Control*
- *Carrier & Supplier Management*
- *Disaster Recovery & Business Continuity Planning*
- *Network Design & Topology Development*
- *IP Address Space & DHCP Scope Management*
- *ISP & DNS Registration Management*
- *Network Security & Policy Management*
- *Configuration Policy & Interoperability*
- *Network Design & Provisioning New Services*

- *Application Performance  
Trend Analysis*
- *Network Standards  
Compliance*

### Daily Tasks include: IIMAC's, Software Bug Fixes, Monitoring & Troubleshooting

*Network professionals should ideally adopt ITIL best practice to help ensure they effectively manage service operations to a high standard. An ITIL based Service Desk can use its knowledgebase to ascertain if the incident is a known error. In all cases the Service Desk will manage the incident through to a resolution. Although ITIL is a personal qualification not a business level accreditation; it involves certification for Service Level Management, Service Desk Management, Problem Management, and Change Control, all of which are of high value to the IT function and to business operations overall. Preventative maintenance tasks, such as ensuring software compliance, along with IMACs performed formally under Change Control can provide significant benefits to network availability but require a skilled Network Professional to derive this benefit day to day, particularly in an SME networks comprising of more than 500 Users. The Network Manager's job specification is widely available, and again helps to provide some appreciation of the activities requiring the attention of a dedicated network management function within an SME or Enterprise level organisation.*

### A Typical Description – Network Manager or Network Management Function

**Job Description:** The Network Manager's role is to plan, direct, and coordinate the design, installation, and connectivity of computer and network systems to ensure the stable operation of the organisation's IT assets. This includes developing, configuring, maintaining, supporting, and optimising all new and existing network hardware, software, and communication links. The Network Manager may also schedule and direct the activities of a small team of network specialists to resolve end user hardware and software problems in a timely and accurate fashion.

#### Responsibilities:

#### Strategy & Planning

- Design and implement short- and long-term strategic plans to make certain network capacity meets existing and future requirements.
- Develop, implement, and maintain policies, procedures, and associated training plans for network resource administration and appropriate use.
- Develop and deploy methodologies for testing network performance and providing network performance statistics and reports.
- Establish best practices and policies for installing, configuring, maintaining, and troubleshooting end user workstation hardware,

software, and peripheral devices.

- Practice network asset management, including maintenance of network component inventory and related documentation.
- Establish service level agreements with end users.

### Acquisition & Deployment

- Plan, acquire, and coordinate installation of in-house and remote hardware and software across the organization's network.
- Conduct research and make recommendations on network products, services, protocols, and standards in support of network procurement and development efforts.
- Negotiate with vendors, outsourcers, and contractors to secure network products and services.
- Assess, approve, and administer all equipment, hardware, and software upgrades.

### Operational Management

- Manage and ensure effectiveness of servers, including e-mail, print, and backup servers, and their associated operating systems and software.
- Manage and ensure optimal operation of all network hardware and equipment, including routers, switches, firewalls, IDS/IPS, VOIP, wireless and so on.
- Manage and ensure effectiveness of security

solutions, including firewalls, anti-virus solutions, and intrusion detection systems.

- Establish and maintain regular written and in-person communications with the organization's executives, decision-makers, stakeholders, department heads, and end users regarding pertinent network activities.
- Approve and administer user accounts, permissions, and access rights.
- Direct and administrate a contingent of network analysts and technicians, and where necessary, conduct performance reviews and corrective action.
- Provide guidance to junior members of the team.

### Formal Education & Certification

- Four-year university degree or college diploma in the field of computer science and/or [...] years equivalent work experience.
- Certifications in [...].

### Knowledge & Experience

- 5 years experience managing and configuring enterprise-wide LANs, WANs, WLANs, VPNs, etc.
- Exceptional technical knowledge of network and PC operating systems, including [...].
- Hands-on experience troubleshooting hardware such as servers, routers, bridges, switches, hubs,

- modems, network interface cards, and so on.
- Excellent knowledge of current protocols and standards, including [...].
- Experience with programming languages such as [...].
- Extensive application support experience with [...].
- Knowledge and understanding of system flow charts, data processing concepts, and telecommunications principles.
- Experience installing network cabling and patching telephony systems.
- Knowledge of applicable data privacy practices and laws.

### Personal Attributes

- Demonstrated leadership and personnel management skills.
- Good understanding of the organisation's goals and objectives.
- Strong interpersonal, written, and oral communication skills.
- Ability to perform general mathematical calculations for the purpose of creating needs assessments, budgets, and so on.
- Able to conduct research into networking issues and products as required.
- Ability to prioritize and execute tasks in a high-pressure environment and make sound decisions in emergency situations.
- Ability to present ideas in a user-friendly language.

- Highly self-motivated and directed.
- Keen attention to detail.
- Proven analytical and problem-solving abilities.
- Strong customer service orientation.
- Experience working in a team-oriented, collaborative environment.

### Working Conditions

- On-call availability for [...] days per month.