Functions of netowrk management, performance and fault management Report RESUB -- REVISED

P4 – M2 – D1 Tom Hutchings

UTC Reading

BTEC IT Unit 5 Assignment 1

P4 – Functions of Network Management

Network management encompasses a wide range of functions. While it includes tasks such as simply maintaining a network, adding nodes and reconfiguring settings when needed, it also includes larger and more complicated tasks like designing and creating new networks.

**Network Setup**

Setting up a network requires both planning and theory skills, and practical skills knowledge. When creating a network one must plan ahead and assess the needs of the network, the limits of the network and the optimal setup for its needs.

On the theory side of network setup a network engineer will analyze the functional requirements of a network and the environment it needs to work in. They will then choose an optimal topology and the best node configuration for the network. They will make part counts and price up estimated costs for the network.

When the network needs to be built practical skills come into play. Installing racks, cable trays and other networking requirements. Installing servers, switches, firewalls, and any rack mount network devices, running cables between the devices and ensuring all connections are working are among the tasks that are performed once the network is planned. The networks individual devices are then configured to function correctly.

**Adding to Networks**

As networks need to expand and adapt to changing requirements new nodes or devices need to be added to a network. Depending on the network topology this varies in complexity, for example adding to a star network is a simple case of a single cable to the hub, whereas adding a node to a ring requires not only two cables to be connected to a machine, but the network to be restructured. Once the new device is physically installed it is then configured to function correctly on the network.

**Network Troubleshooting**

An imperative part of managing networks is identifying faults. When networks malfunction they may do so in ways that may not immediately present themselves obviously. Diagnosis of networks requires logically breaking down larger errors into their possible causes, and investigating and testing each possible cause in order to track down the offending device, software, faulty hardware or other networking system. Once an issue is diagnosed and the cause is discovered and verified it is up to network engineers to act on this research and solve the issue. While some issues may be a simple case of replacing a broken cable, some are larger in scale and may require whole servers to be replaced.

**Network Repair**

Once an issue is diagnosed it needs repair. If the issue is correctly diagnosed then repair should be straightforward, though not always easy. Because of the varying severity of issues, network engineers are trained for many scenarios, and able to fix many issues. Due to the divide between hardware and software, solutions vary in their methods.

Software issues require an admin to either remotely connect to a device or use a serial cable and port to connect. They will then perform the tasks needed to resolve the issue. This can involve installing, removing, modifying, rebuilding or restarting software.

Hardware issues can be more in depth, sometimes requiring computers to be disassembled and components replaced. Sometimes cables need to be replaced, or simply the connectors on the ends changed.

**Network Security**

In a network security is imperative. Networks are by their very nature insecure and require encryption and physical security. Standard unencrypted network traffic is easy to intercept and read, so encryption is needed for any information that is secret or contains personal information. Businesses also need to secure their own servers to protect from incoming attacks, where an attacker can gain access to the servers and stored information of a business. Businesses also have a legal obligation to keep users information private, so using encryption for sent data is often a legal requirement for any service using personal information. Networks use firewalls, encryption, and intruder detection systems among other security systems to keep networks safe from attacks. Many datacentres also use biometric and key card security systems to keep unauthorized users from accessing the servers.

Fault Management and why it’s important – M2

Fault management is a key part of network management. Without proper fault management a network is more prone to failure, and when errors occur dealing with those errors becomes much more difficult, as no system detected the error and further investigation will be required, even if it is a simple error that could have been easily logged and resolved.

Fault management systems will detect and log errors, sometimes even taking steps to correct the errors. They will either wait passively for devices to send an alarm or error message, or actively ping devices and sound an alarm when one goes down. They also manage logs, sorting them and collecting from devices in the network.

When fault managements systems fail entire networks can go down. Without sufficient monitoring and quick intervention from admins a small fault can propagate into a very large issue. Smaller hacking attacks will not be detected and the attacker could steal valuable information, or even private user data. This then becomes a large scale crime.

Fault management systems are in place to prevent what no one wants to happen. If a network or system fails it is needs recovery, and a system to log and report why the error happened, and how to prevent it if it happens again. Fault management systems can repair trivial errors that previously would have required a person to repair. This is the aim of fault management, to maintain systems when they break, and to log why they broke.

Performance Management and why it matters – D1

Without performance management checks systems can become slow and inefficient. Bottlenecks can and will appear in systems, drastically slowing it down and decreasing efficiency, without admins noticing. Performance management software can aid in inefficiency and speed issues, at relatively little cost.

Keeping systems cost effective is important to a business, and networks are no exception. Users also become discontent and impatient when web interfaces are slow, causing user unhappiness, arguably a bad thing. Users become discontent when interfaces are below expected quality standards, and poor performance management drastically decreases quality.

While performance management may not seem to be very related to quality control, it actually plays a large part. Speed and responsiveness of a service is a part of its quality, and performance management systems manage speed of a service.

Say we have a web service which visualizes stored Data in a university research department. Experiments are carried out and the Data is recorded, and the web interface actively query’s this data. The web server application and the database run on different physical servers connected together via a network. The web application has to transfer large amounts of data from the Database server, which are then rendered into HTML pages and transferred to the client in this compact image hypertext and image format. Without performance management systems optimizing the network the transfer between the Data server and the Web Server is slowed, perhaps giving large increases to the transfer time.

This causes the web application to take more time rendering the data and generating the HTML files. As the users of this service are mostly researchers they require the system to be quick and responsive. If many users are simultaneously requesting pages from the web server, the link between the web and data servers is further strained. Users may perceive this as being an inadequate or poorly designed system, with bad quality control during development. In fact, it is a simple case of poor installation, and a network performance management system could optimize for the large data transfers and greatly increase the speed of the program, without requiring a full analysis of the software and network.

# References and Bibliography

* Wikipedia
* BTEC Book