Example of pictorial description of the fcaps model essay

[Business](#), [Management](#)

Description of FCAPS model

FCAPS, an acronym for fault, configuration, accounting, performance and security is an International Organization Standardization (ISO) Telecommunications network management framework and model for network management. This is a management category in which network management tasks are defined by the ISO model. Accounting is always replaced with administration in most non-billing organisations. The term FCAPS was first introduced in the early 1980s. The main objective at this time was to define clearly five separate protocols for every functional area. Currently, this model places these working categories of the network system management into five distinct levels. These levels of management are the fault management (F), the configuration management (C), the accounting management (A), the performance management (P) and the security management(S).

A fault can be described as an issue that has negative significance. The main objective of fault management is to identify, separate, log and correct system faults that arise within the network system. Fault's management uses trend analysis in the prediction of errors to maintain the availability of network. It monitors different things within the system for abnormal behaviours. In case a faulty vent arises, a notification is sent the network operator by the network component. This is achieved by using an open protocol or a proprietary like the SNMP, to send a visible message to its console in order for the console server to capture and page. Configurations can be made to the management station to keep the network administrator posted of problems. Therefore, appropriate action can be taken on time to

control the fault. Faulty errors mainly occur in areas of configuration management and fault management within the communication system. Configuration's management is the second level of the FCAPS model management system. Its roles are to collect and store specific configurations from other network devices by employing both the remote or local methods, to make the configuration device simple, to identify and track specific changes and alterations on the configuration, to plan and organise for future scaling and expansion and to put configurations to circuits. Configuration's management monitors the configuration information and any abrupt changes that occur within the system. This is an important area because several network problems come up due to changes made to the configuration files, system hardware or updated software versions. A good configuration management system tracks all alterations made to the network software and hardware. Such changes include updating the operating system version of a switch, adding new modular interface card and changing running configuration of a given device. In order to gather and track all these information and changes, this system uses configuration management software like the Cisco Works 2000.

The third level of management is the accounting management. This systems main concern is to track information on network utilization. This is done for billing purposes of departments, individual users or business units. Accounting is replaced by administration for non-billed networks. The roles of administration are to administer and control set of authorised users. This is done by establishing passwords, users and permissions. It administers operations of the system by carrying out synchronization and software

backup. Generally accounting is the billing management. From the statistics obtained from the system, users are comfortably billed, and enforcement of usage quotas is easily achieved. These include the link utilization, CPU time and disk usage.

Performance's management is meant to ensure network performance is maintained at the required standards. This makes it easy for the manager to prepare and plan the network future. It helps determine efficiency of current network system in line with investments that take place to help set it up. This system is meant to manage the overall performance of the whole network. It addresses link utilization, throughput, percentage utilization, error rates, packet loss rates and network response times. The information is collected by implementation of SNMP system of management. It were configured and monitored to alert network administrators the fluctuation of network, in case it moves below or above the required threshold. Monitoring network performance is a critical step in identifying faults before they cause complications.

The security management system plays the role of controlling access to the assets within the network system. At this level, the network is protected from unauthorised users, hackers and electronic or physical sabotage. Datum's security is achieved through encryption and authentication. The security management also ensures that security-related information from the network system is regularly analyzed. The main functions of the security management are to manage network authorization, auditing and authentication to ensure that both external and internal users access only the required network resources. The security management was put in place

to ensure that hackers are controlled from accessing information that is not meant for them.

The ISO made this creation in order for people to easily operate network systems at high speed and efficiently. Customers and employers depend on IT services hence performance and availability are mandated. Coming up with this model boosted the IT sector and has made network operation smooth and efficient.

References

Kwiecien, A. (2012). Computer networks 19th International Conference, CN 2012, Poland, June 19-23, 2012. Proceedings. Berlin: springer.

Surhone, L. M. (2010). FCAPS: telecommunications management network, network management, alerts standard form. Mauritius: beta script:.