Indp, part 2

[Technology](), [Information Technology]()

NETWORK DESIGN Within a network of computers in which exchange of information takes place, it is important to underline the concept of order. The computers are engaged in communication and rules need to be set to regulate data exchange and these rules constitute protocol. Communication protocol plays a significant role in controlling the speed and mode of communication among computer systems through a well-designed software package (Garduno & Diaz, 2011). This protocol aspect limits chaos and enhances efficiency.

In this design, it is important to note the underlying rationale. The design is TCP/IP protocol and Distributed network protocol. TCP/IP protocol is supported by many software applications and has universally accepted terms. In TCP, data is divided into manageable bits and the protocol ensures that secure and appropriate routines are in place to oversee data correctly arrives to its destination. Then IP enforces logical addressing and routing of data which brings in the reliability factor (Garduno & Diaz, 2011). TCP/IP supports ASCII standards that help in formatting information transmitted into a range of supported formats such as JPEG, text and MP3 standards among others. Distributed network protocol on the other hand supports communication in process automation systems and supports peer-to-peer and master-to-slave communications. Above all, this protocol is reliable in terms of security; it contains secure authentication features and does not require heavy infrastructure. Cost wise, both protocols are fairly affordable to implement due to fair infrastructural costs (Garduno & Diaz, 2011). Other features that make these protocols appropriate include both are open protocols, they support interoperability between different platforms and they

can be optimized

According to this design, the adopted network architecture defines secure, interpretable infrastructure that provides reliable and open-standard based communication for distribution of information. The architecture also defines technologies required to support communications between various client machines and servers on the network (Garduno & Diaz, 2011). There are established network standards that coordinate secure implementation of network architecture as well as supporting traditional data such as voice and video. The architecture is based on open standards

In explaining the usefulness of a traffic analysis, When some work has been done for ISPs net flow can be used to determine PPS (Packets per second) to detect instances of DOS (Denial of Service) attacks. It also can help one figure out if there is need to upgrade network because of running out of capacity and also when somebody asks if connection is running slow and it manages to work its way up to the top level escalation engineers, one can tell that it is fine from the amount of traffic hitting the CPE (Customer Premise Equipment). It is important to give a clear definition of some common terminologies and these include; Latency which refers to delays incurred in processing of network data. In networks, latency is measured using network tolls such as ping tests that determine the time it takes a network packet to travel from source to destination node and back. A low latency defines a system that experiences short delay times while high latency defines systems that experience long delays. Systems suffering from high latency are said to be unreliable and slow thus are inefficient. Response time also refers to time taken to establish communication on a networked

computer system. This is the time between and end of an inquiry and the beginning of a response. Low response times indicate efficient network performance while long response time indicates unreliable network performances. Jitter is another concept that refers to variation in packet transit delay arising from queuing and serialization effects along the path of transmission. Mostly, these delays are propagated by traffic congestion due to the size of bandwidth used and speed of transmission paths in place. In congested links, higher levels of jitters are likely to occur. Therefore, higher levels of jitters cause data transmission to be slow hence lowering the network performance.

It is worth to note that there are various effects of data rates on each part of the network. To begin with Network cabling in which Speed of information transmission on cables greatly impacts on the overall network performance. It signals the amount of time data is expected to travel from sender node to receiver node. High data speeds are preferable since they help avert congestion on the network as well as make performance efficient. Therefore, in our design, we shall use high speed network cables such as the fiber optic for optimal network performance. In Wireless network communication there is a wireless environment in which data speeds are higher than in wired networks. This implies that traffic within wireless resource is quite manageable and the overall network performance reliable. In Network adapter cards, data speed in network adapters affect the time in which the adapters prepare data from computer for the network cable. This also influences time incurred in sending data to another computer and the flow of data between the computer and cabling system. High data speeds therefore

contribute to faster network adapter card functionality in terms of sending and receiving information.

In describing strategies to ensure the availability of network access in switched and routed networks, the following are found;

i. Identifying all the network requirements

ii. Designing a hierarchical network

iii. Using routers and multilayer switches that combine routing and switching in the same device

iv. Employing the use of high-speed links

v. Use open short path first protocol which scales well in networked resources

vi. Employing load balancing technique

Reference

Garduno, B. D., & Diaz, M. (2011). Communicating systems with UML 2: Modeling and analysis of network protocols. London: ISTE.