Assignment 2:GEC Network Survey

Table of Contents

INTRODUCTION

A network survey was recently done at GEC, Farmagudi, Goa, wherein the entire network was studied thereafter which a much more reliable abd resilient solution was given to them with the primary motive of keeping them pace with the new trends in the network industry.

A number of important factors have been taken into considerations while designing this solution which is necessary in today's network industry. These requirements include points where a part of the architecture is already existing which includes the structured cabling while upgrading of new devices at the layer 2 and layer 3 level will be seen further on this document. Ultimately a good network has to be reliable and scalable.

DESIGN FACTORS

During the design of a network, a number of factors have to be taken into consideration. These include the following:

- Speed/Bandwidth:
  Considering a network like GEC, with the bandwidth demanding applications that students use, it is of utmost importance that that backbone is very strong to handle the very high data transmission that could take place at peak times or even on a regular basis. It has to also be ensured that the switching capacity at the backbone level is much higher to handle all the data flows smoothly.

- Scalability
  Changes take place rapidly and it has to be ensured that the network is designed in such a way that it is scalable for future requirements that might come up. This could be with regards to the number of nodes, upgrading of new devices or even the use of new applications that are bandwidth driven.

- Manageability
  Manageability is also a key criterion during the design of a network. It has to be ensured that manageability is not hampered in any way considering GEC has a huge network.

- Quality of Service
  QoS nowadays is of key importance. Prioritizing traffics, giving preference to certain types of traffic such as voice and data packets needs to be part of the network infrastructure to help the network to run smoothly as possible.

- Security
  Considering GEC as an education institution, security would be an important criterion as there would be a lot of confidential data being stored on servers and other data centers. It has to be taken into considerations that this information is isolated from the entire intranet and the extranet as well so as to ensure no leak of any type of confidential data takes place.

- Interoperability

Interoperability is important considering changes take place very fast. A network has to be interoperable as new devices are added to the network. Addition of new devices or changes to the network should not hamper the network in any way.

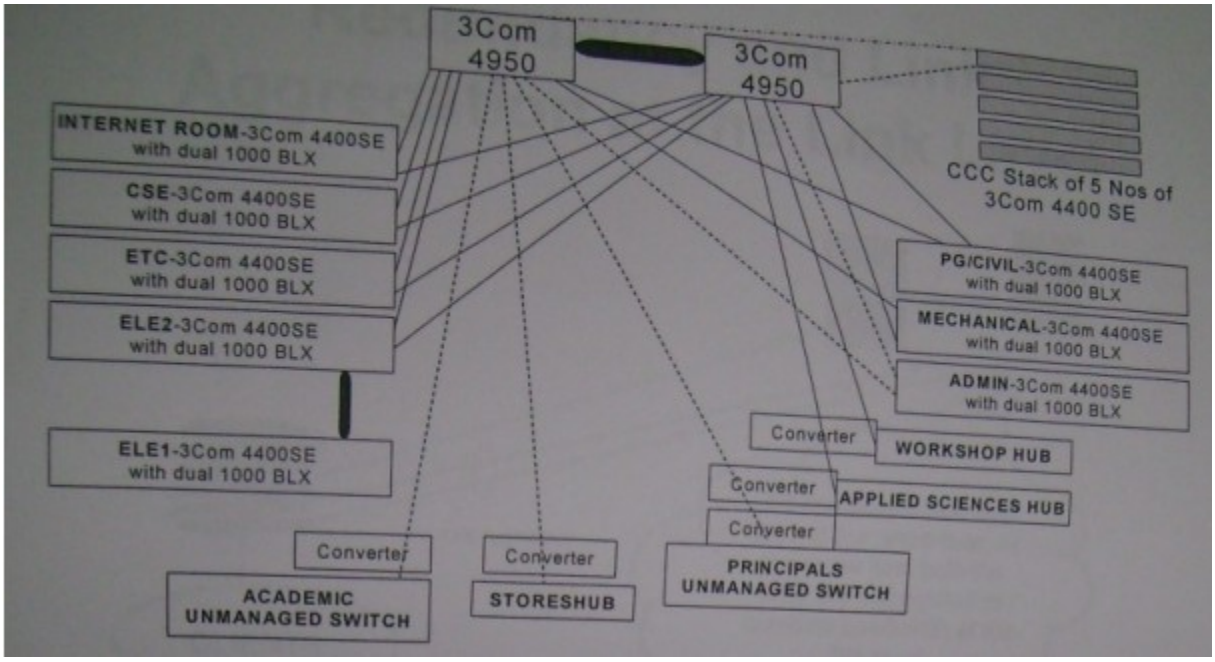
- Technical support
  Once a network is up and running, any problems should be automatically brought into notice of Network Administrator by way of e-mail notification and attended as soon as possible to avoid downtime.

Integrating a new and upgraded technology taking into consideration all the network design parameters is the main motive of this project.

The following points have been identified which have been integrated with the existing technology in our solution. These have been taken into consideration during the design of the GEC network:

- Redundancy at the core and link level
- Load sharing at the core level
- Link aggregation at both the link and core level
- Use of gigabit switches with module slots for single mode and multi mode modules
- Centralized control of wireless access points
- Security for servers
- Stacking of switches to increase bandwidth
- Higher backbone capacity

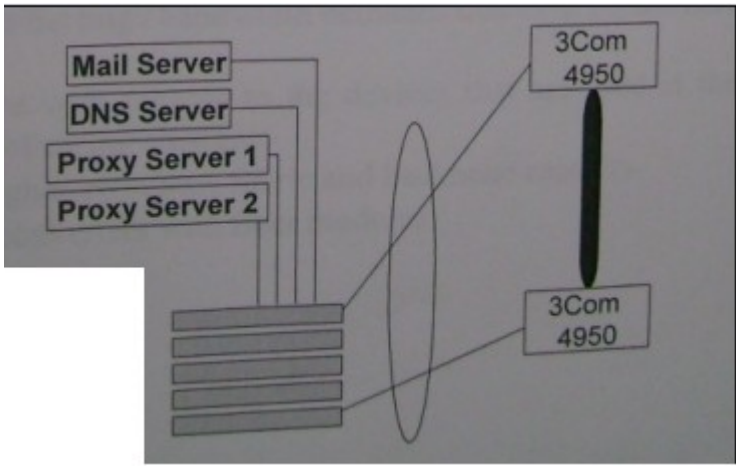
GEC EXISTING NETWORK



The above figure shows the existing network of GEC as of today. In the above network, it can be seen that redundancy is available at the core level but having just one link per core switch isn’t the ideal network

scenario. If the link which connects the edge switch to the core switch fails, there would be no redundancy available for this link causing tremendous overload for the other redundancy switch that is available. Although load sharing is enabled in the present scenario, it would not be of any use considering one link has failed. This can better be seen in the below diagram:

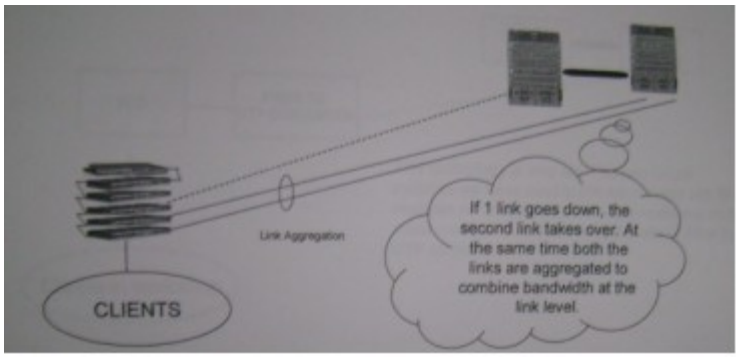
EXISTING GEC NETWORK HAS NO REDUNDANCY AT LINK LEVEL



In the existing network setup, the switches at the edge level have no link redundancy. If the link goes down to a particular switch, the only pass-through is through the redundant core switch which is available.

The main aim is to provide a reliable and stable solution to the customer. This can be seen with the help of the below diagram and the explanation.

REDUNDANCY AND LINK AGGREGATION AT THE LINK LEVEL



In the above figure, redundancy is available at both the link level and core level. If a core switch fails, the other switch automatically takes over using a protocol technology called VRRP (Virtual Router Redundancy Protocol).

So, when clients are in the process of passing data through core switch 1, if core switch 1 fails, data is automatically routed through core switch 2 which is the redundant link. At the same time the links connected to the core switch are aggregated to make complete use of the bandwidth available and

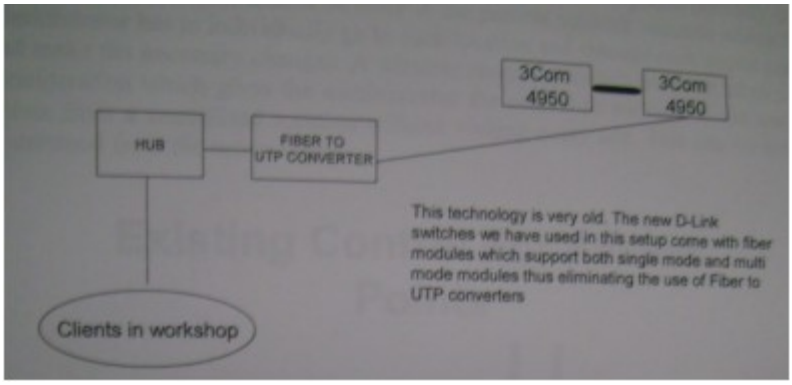
providing high speeds for bandwidth hungry applications. Here, if a link goes down, the second link automatically takes the load of the failed link thus preventing any disturbance in network traffic. Load sharing would also be enabled in this case to share the load of network traffic between both the core switches. Thus none of the switches would be overloaded with the huge bandwidth demands that exist on the network.

Another change would be with regards to the devices that are used at the edge level. These include the following changes:

- Switches with a higher switching fabric and backbone capacity
- Replacing media converters with fiber modules

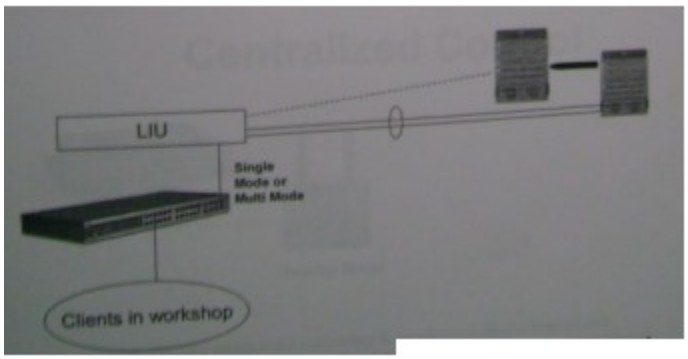
This can be better understood with the help of the below figure:

WORKSHOP EXAMPLE IN EXISTING NETWORK



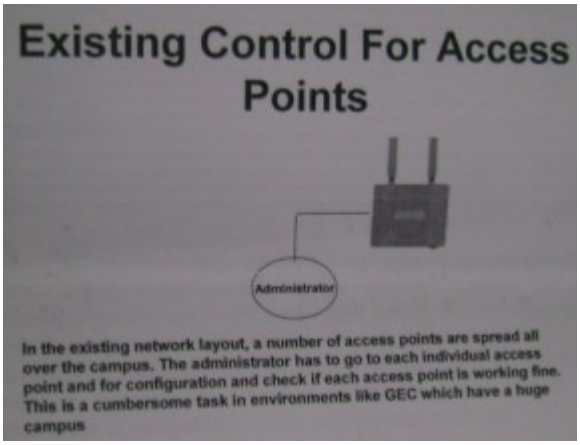
In the present network scenario, all the clients connect to a switch or a hub using UTP cable which is then converted to a fiber using a converter in some places which then directly goes to the core switches. This is an old technology and the new advances can be seen in the below diagram which are much more reliable and bandwidth efficient:

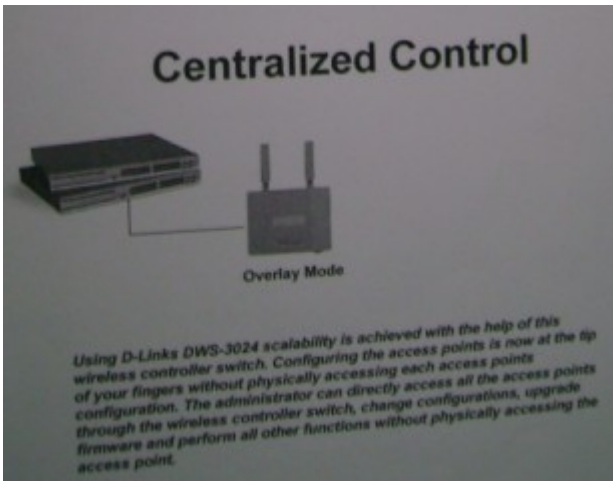
NEW SWITCH TECHNOLOGY IN SWITCH ENVIRONMENT



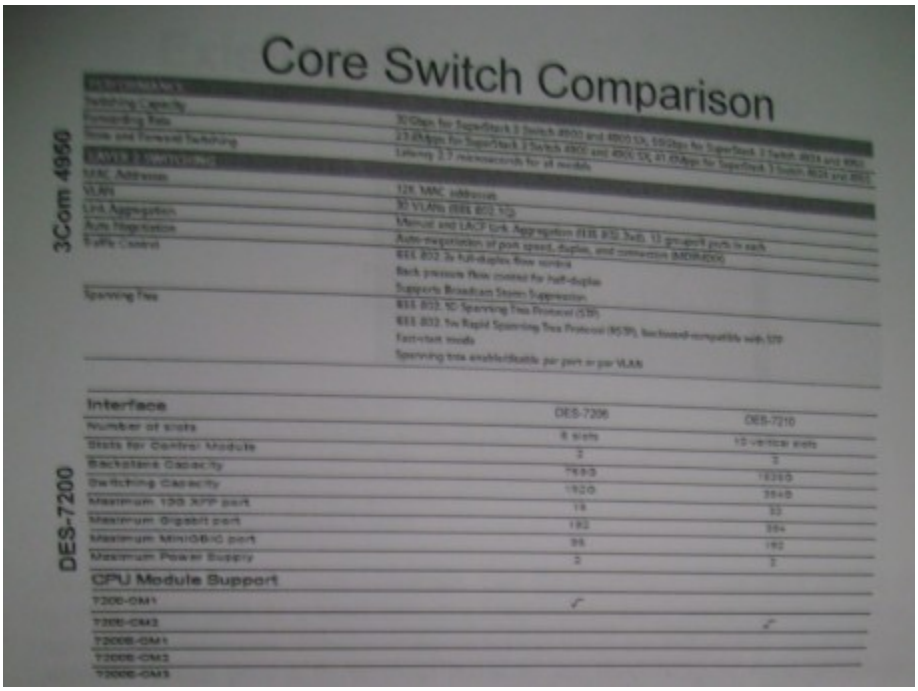
Unlike the existing network which make use of traditional switches and hubs alongside media converters, all the switches at the edge level will have an option for a fiber module which can be populated and this can be either single mode or multi mode. These Layer 3 switches support switching and routing and come with 8 combo SFP slots and have optional 10 Gb uplink modules.

Managing access points is also of key importance and since GEC has a huge campus, managing these wireless access points centrally is a key requirement which cannot be done in the present network where the administrator has to individually go to each location and manage each access point and make the necessary changes. A wireless controller switch has been taken into consideration which gives the administrator the control to manage all the access points from a centralized location without visiting every site. This can be better understood from the below figure:





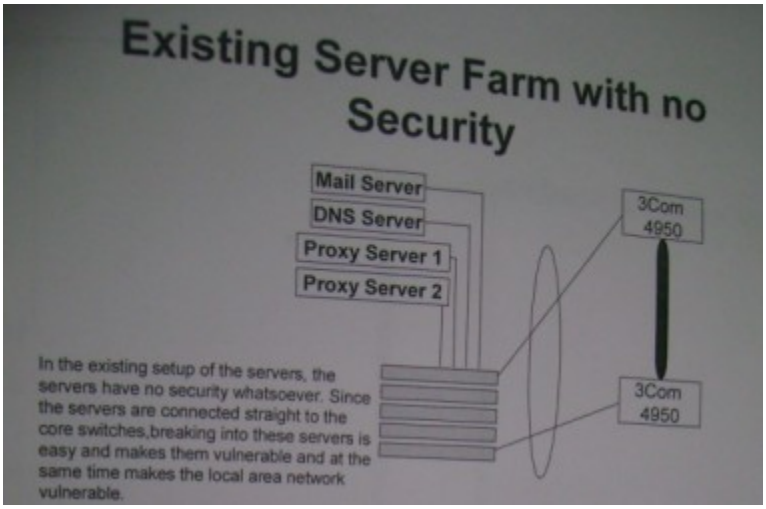
CORE SWITCH COMPARISON



In the current GEC setup, the switching capacity per core switch is on 56 Gbps which is not enough for the number of nodes that exist. The switching capacity has to be always high mainly in the core so as to handle tremendous amounts of data traffic.

The upgraded solution designed has a switching capacity of 192 Gbps and a backplane capacity of 786 Gbps which is comparatively higher in performance in comparison to the existing core switches.

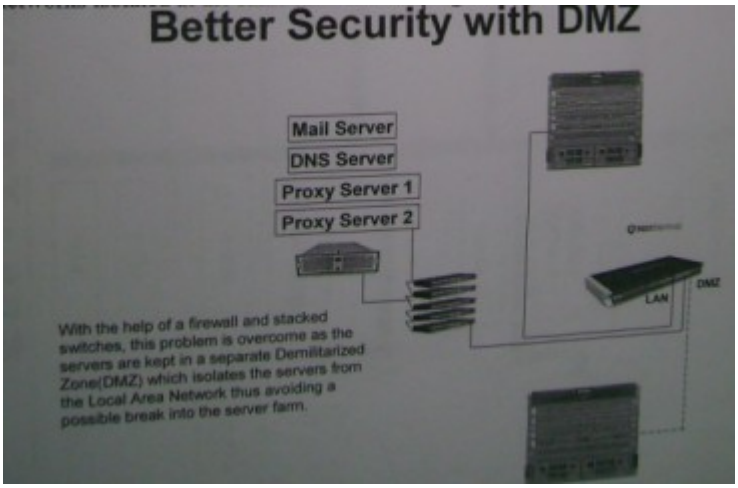
EXISTING SERVER FARM WITH NO SECURITY



As can be seen in the above diagram, GEC has a number of servers which include a Mail server, a DNS server and 2 proxy servers. All these servers are connected directly to the core switch and are available to the local area network which pose a tremendous threat to the functioning of these servers as anyone could hack into these devices thereby causing downtime and pose a threat to the local area network as well as anyone fro the internet trying to access these servers could get into the local area network.

This can be avoided with the help of a DMZ Zone which is created with the help of a firewall and a switch. All the servers are put in an isolated network in the DMZ Zone thus isolating the local area network from the server farm. This prevents any attack from taking place on the local area network and keeps both the networks isolated at the same time thus keeping security as its best priority.

BETTER SECURITY WITH DMZ



GEC LAN PHYSICAL LAYOUT