Network Architecture and Security Issues in Campus Networks

Mohammed Nadir Bin Ali
Department of Computer Science & Engineering
Daffodil International University
Dhaka, Bangladesh
it@daffodilvarsity.edu.bd

Prof. Dr. M. Lutfar Rahman
Department of Computer Science & Engineering
Daffodil International University
Dhaka, Bangladesh
vc@daffodilvarsity.edu.bd

Prof. Dr. Syed Akhter Hossain
Department of Computer Science & Engineering
Daffodil International University
Dhaka, Bangladesh
aktarhossain@daffodilvarsity.edu.bd

***Abstract*— Network architecture with its security is a growing concern in the present time. A campus network faces challenges to address core issues of security which are governed by network architecture. This paper is mainly targeted towards campus networks which deliver required security. This is essential because, it prevents the institution from suffering any significant attacks associated with network. A university network has a number of uses such as teaching, learning, research, management, e-library, and connections with the external uses. Therefore, network architecture and its security are vital issues for any university. In this work, a network infrastructure is proposed on the basis of the practical and experimental requirements. The proposed network infrastructure is realizable with adaptable infrastructure.**

Keywords- Campus network architecture, Hierarchical network architecture, Redundant network design, Network security, Network threats.

I. INTRODUCTION

Nowadays a campus network is essential and it plays important role for any organization. Network architecture and its security are almost as important as air, water, food, and shelter. Computer network security threat and network architecture are always serious issues and are important. A campus network is an autonomous network under the control of a university which is within a local geographical place and sometimes it may be a metropolitan area network.

Generally, IT manager in a Computer network faces plenty of challenges in the course of maintaining elevated availability, excellent performance, perfect infrastructure, and security. Securing a big network has been always an issue to an IT Manger. There are a lot of similarities between securing an outsized network and university network but each one has its own issues and challenges. Present educational institution pay more attention to IT to improve their students learning experience. Architects of Campus can achieve this if IT managers hold on to the fundamental principles addressed in this reference architecture, namely LAN or WAN connectivity design considerations, security, and centralized management [1].

The physical network infrastructure is required for a contemporary university network. University Management and IT manger may know exactly what kind of network they want to setup, upcoming plans, and expected growths are more complicated to understand. So far contingencies for future area, power, and other resource must be part of the physical plan of a university. Building a contemporary university network atmosphere also contains functional and safety elements that also go beyond the IT department's obligations and skills. Modern networks need to develop more concrete in many ways beyond the network topology and devices themselves to meet the needs of the present social media atmosphere. Failures due to air conditioner problems, random routine draws, and shortages of area and information all lead to stability issues that now impact an incredible number of customers globally.

II. BACKGROUND

We know, Computer networks are of many different types such as Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), Storage Area Network (SAN) and Wide Area Network (WAN). LANs are capable of higher data transfer within small geographical area. LAN usually operates high speed data transfer usage. CAN has larger network than LAN. CAN is usually established in university campus to connect among different buildings, computer labs, library, research labs, registration, and different academic units.

2.1 Network architecture in Campus Network

The campus network of our study is designed in a hierarchical manner which is a common practice of campus and enterprise networks [2]. It provides a modular topology of building blocks that allow the network to evolve easily. A hierarchical design avoids the need for a fully-meshed network in which all network nodes are interconnected [3].

2.2 *Network security*

Several key events contributed to the birth and evolution of co mputer and network security. The timeline can be started as the 1930s. Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II [4].

In the 1990s, internet became public and the security concerns increased tremendously. Approximately 950 million people use the Internet today worldwide [5]. On every day, there are approximately 225 major incidences of security breach [5]. These security breaches could also result in monetary losses of large degree. Investment in proper security should be a priority for large organizations as well as common users.

2.3 General Design guidelines

There should be redundancy in any network so that a single link or components failure does not separate any part of the network leading to those users dropping access to network sources. The quantity of redundancy required differs from network to network. Some network might need a backup link between two websites, and some network might need repetitive redundant links, routers, and switches. The quantity of redundancy is determined by how much money we want to invest on the extra devices and what level of risk we are willing to agree to by not having the redundancy.

When a less-than-optimal topology is used, long-existing but frequently misunderstood situations can occur as a result of the difference between ARP and CAM table aging timers. If VLANs span across multiple access layer switches, return path traffic can be flooded to all access layer switches and end points. This can be easily avoided by not spanning VLANs across access layer switches. If this cannot be avoided, then tune the ARP aging timer so that it is less than the CAM aging timer [1].

Advances in routing protocols and campus hardware have made it viable to deploy a routing protocol in the access layer switches and use an L3 point-to-point routed link between the access and distribution layer switches. This design can provide improvement in several areas, most notably reliable convergence in the 60–200 ms range [1].

III. Hierarchical Network Design

Campus network design is proposed to follow hierarchical design because it is easy to measure, understand, and troubleshoot by promoting deterministic traffic patterns. In a hierarchical design, the potential features, and performance of a particular device are enhanced for its place in the network and the part that it performs. This encourages scalability and stability. The number of moves and their associated bandwidth specifications increase as they navigate factors of gathering or amassing and move up the structure from entry to submission to primary. Features are allocated at each layer. Hierarchical design prevents the need for a fully-meshed network in which all system nodes are connected.

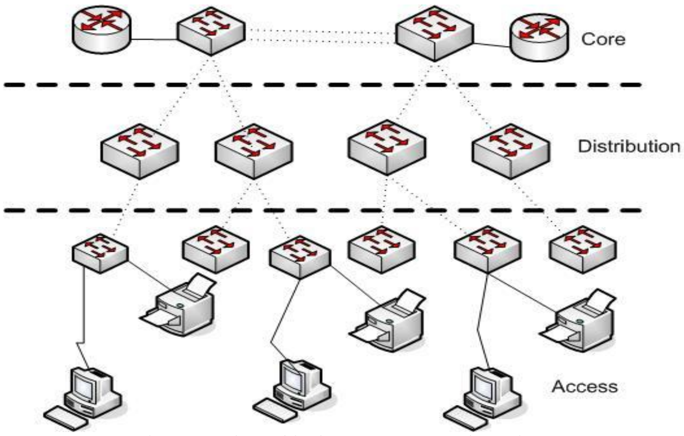

Figure 1. Hierarchical Campus Network Design

The building blocks of modular networks are easy to replicate, redesign, and expand. There should be no need to redesign the whole network each time a module is added or removed. Distinct building blocks can be put in-service and taken out-of-service without impacting the rest of the network. This capability facilitates troubleshooting, problem isolation, and network management.

Compared to other network designs, a hierarchical network is easier to manage and expand, and problems are solved more quickly. Hierarchical network design involves dividing the network into separate layers. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, the network design becomes modular, which facilitates scalability and performance. The typical hierarchical design model is broken up into three layers: Access Layer, Distribution Layer, and Core Layer [6] as described below:

3.1 Access Layer: The access layer relationships with end device, such as PCs, modems, and IP phones, to provide entry to the rest of the system. The accessibility part can include wired or wireless routers, switches, and wireless access points. Primary objective of the access layer is to provide a means of linking gadgets to the system and handling which gadgets are allowed to connect on the network.

3.2 Distribution Layer: The distribution layer combined the information obtained from the access layer switches before it is accepted on to the core layer for direction-finding to its last place. The distribution layer manages the movement of network traffic using suggestions and delineates passed on sites by doing direction-finding features between VLANs described at the access layer. VLANs allow you to area the traffic on a switch into individual sub-networks. Distribution layer changes are usually high-performance devices that have great accessibility and redundancy to make sure stability.

3.3 Core Layer: The core layer of the requested style is the high-speed main resource of the internetwork. The core layer is essential for interconnectivity between distribution layer gadgets, so it is important for the primary to be incredibly available and recurring. The core area can also get linked with Internet resources. The core aggregates the traffic from all the Distribution layer gadgets, so it must be able of delivering significant amounts of details quickly.

3.4 Advantages of using Hierarchical Network Architecture

There are many benefits associated with hierarchical network designs. Hierarchical networks scale very well. The modularity of the design allows anyone to duplicate elements of design as the network grows. Because each instance of the component is consistent, development is simple to plan and implement. As a network grows, availability becomes more important. We can dramatically increase availability through easy redundant implementations with hierarchical networks.

Communication performance is enhanced by avoiding the transmission of data through low-performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases. The distribution layer then uses its high performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination. Because the core and distribution layers perform their operations at very high speeds, there is no contention for network bandwidth. As a result, properly designed hierarchical networks can achieve near wire speed between all devices.

Security is improved and easier to manage. Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network. We also have the flexibility to use more advanced security policies at the distribution layer. We may apply access control policies that define which communication protocols are deployed on your network and where they are permitted to go. Some access layer switches support Layer 3 functionality, but it is usually the job of the distribution layer switches to process Layer 3 data, because they can process it much more efficiently.

Manageability is relatively simple on a hierarchical network. Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. Therefore, if you need to change the functionality of an access layer switch, you could repeat that change across all access layer switches in the network because they presumably perform the same functions at their layer. Deployment of new switches is also simplified because switch configurations can be copied between devices with very few modifications.

Because hierarchical networks are modular in nature and scale very easily, they are easy to maintain. With other network topology designs, manageability becomes increasingly complicated as the network grows. Also, in some network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier. Adding switches to one layer does not necessarily mean there will not be a bottleneck or other limitation at another layer [6].

IV. Security issues in Proposed Campus Network Infrastructure

Security threats are necessary when dealing with computers, networks, and hosts. There are two types of network threats:

a. Internal: Internal threats take place when someone has allowed entry to the network with either an account or physical accessibility.
b. External: These kinds of threats are brought on by from people operating outside of a company who do not have authorized entry to the network. They crack into campus network system mostly from the internet.

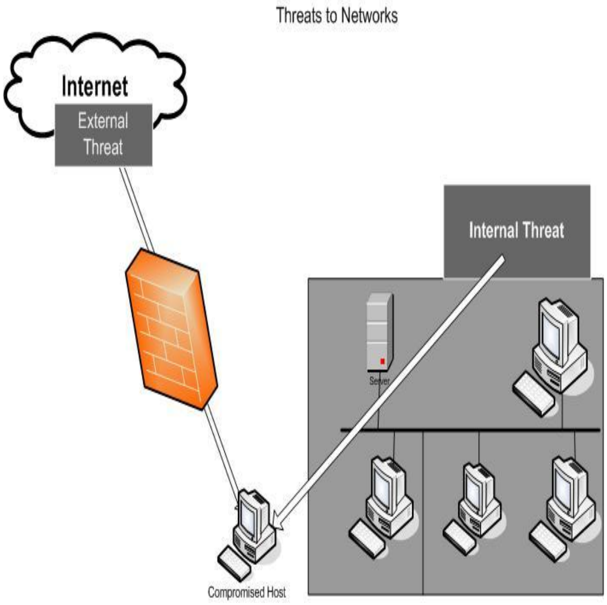

Figure 2. Security threats in Campus Network

4.1 The primary vulnerabilities for end-user computers are virus, worm, and Trojan horse attacks

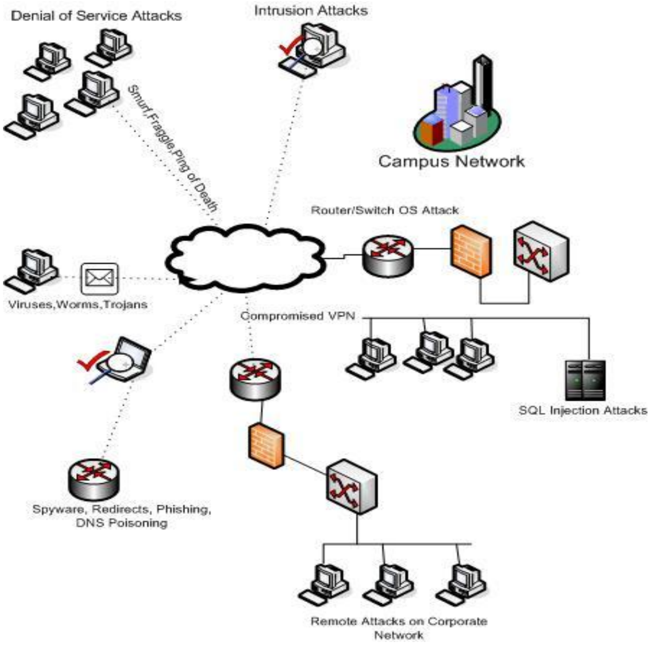
Denial of Service Attacks
Intrusion Attacks
Campus Network
Smurf,Fraggle,Ping of Death
Router/Switch OS Attack
Viruses,Worms,Trojans
Compromised VPN
SQL Injection Attacks
Spyware, Redirects, Phishing, DNS Poisoning
Remote Attacks on Corporate Network

Figure 3. Security threats in Campus Network [7]

4.2 Solution of Viruses, Worms, and Trojan Horses

A greater part of the application vulnerabilities that are exposed to connect with buffer overflows. A buffer overflow happens when a fixed-length buffer gets to its potential and process efforts to store data above and beyond that highest possible limit. Buffer flows over are usually the most important avenue through which viruses, worms, and Trojan Horses do their damage. In reality, there are reviews that recommend that one-third of the application vulnerabilities determined by CERT relate with buffer overflows. Viruses, worms, and Trojan horses can cause serious problems on networks and end systems. IT Managers have several means of mitigating these attacks.

The most important means of mitigating virus and Trojan horse attacks is anti-virus software. Anti-virus application inhibits serves from getting contaminated and growing harmful value. It needs much more time to fresh up contaminated computer systems than it does to sustain up-to-date anti-virus application and anti-virus explanations on the same devices. Anti-virus application is the most commonly implemented protection product available. Several companies that make anti-virus application, such as Symantec, Computer Associates, McAfee, and Trend Micro, have been in the business of discovering and removing viruses for more than a several years. Many organizations and schools purchase amount licensing for their users. The users are able to log in to a website with their accounts and obtain the anti-virus application on their personal computer systems, notebooks, or hosts.

Anti-virus items have upgrade automated options so that new virus definitions and new software up-dates can be downloadable instantly or on need. This exercise is the most crucial need for keeping a system free of virus and should be formalized in a network security policy. Anti-virus items are host-based. These items are set up on computer systems and hosts to identify and remove viruses. On the other hand, worms are more network-based than viruses. Worm minimization needs persistence and synchronization on the part of network security experts.

The containment phase involves limiting the spread of a worm infection to areas of the network that are already affected. This requires compartmentalization and segmentation of the network to slow down or stop the worm and prevent currently infected hosts from targeting and infecting other systems. Containment requires using both outgoing and incoming ACLs on routers and firewalls at control points within the network [7].

V. PROPOSED REDUNDANT CAMPUS NETWORK ARCHITECTURE

Our main concentration is network design should be redundant. The hierarchical network model stresses redundancy at many levels to remove a single point of failure wherever the consequences of a failure are serious. At the very least, this model requires redundant core and distribution layer switches with redundant uplinks throughout the design.

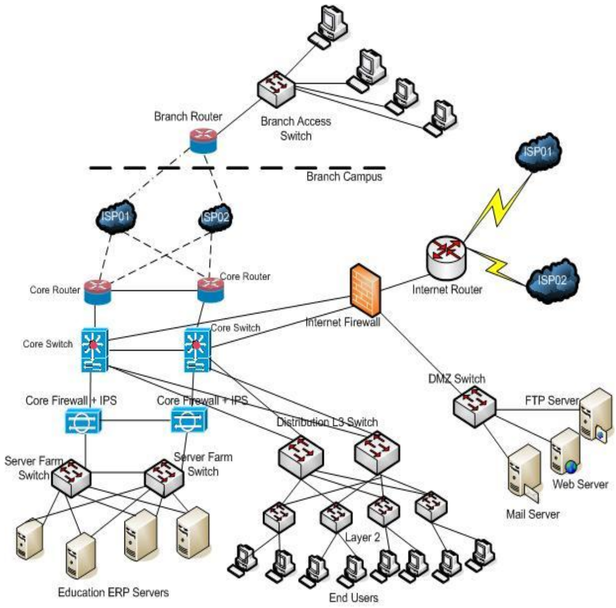

Figure 4. Hierarchical Campus Network Architecture

5.1 Requirement of the proposed Campus Network

The campus network infrastructure consists of an enormous range of equipment including email & web servers, network storage devices, directory servers, cabling systems, network switches, and routers, and more. Considering the fact we have to ensure the layer 3 devices and device selection matter should be careful.

In a common hierarchal campus network, distribution layer is regarded as the demarcation point between layer 2 and layer 3 areas where layer 3 uplinks get involved in the campus network core routing using an Interior Routing Protocol (IGP) which can help to interconnect several campus distribution layer together for end to end campus connection. Consequently the choice of the IGP is essential to a repetitive and efficient routing for campus network. Some of the aspects that can be regarded for selecting an IGP for a university network: Size of the network, convergence time e.g. OSPF and EIGRP can meet during a link failing faster than RIP, authentication support, support of VLSM, etc.

After completing the design of a campus topology and made some decisions regarding the placement and selection of the devices of switch, router, and firewall from various vendors. Product should be selected by analyzing the requirement. Based on requirement we have used the below products for Daffodil International University Campus network: Layer 2 Switch: Cisco 2960, Layer 3 switch: C3750, Firewall: ASA5520.

5.2 Proposed Design and Qualification

Now we would like to describe why we will use this diagram and what are the reasons for using these devices. This diagram shows an example of a fully redundant network diagram with two separate equipment accommodations, now would like to illustrate how we will get benefit from this architecture.

- Two separate equipment accommodations with redundant links.
- Two separate Routers and two separate core switches. Redundant routing using BGP is recommended.
- Redundant L3 design on campus may use IS-IS or OSPF
- Each distribution and access layer switch has connections to two separate switches, which demand comprehensive use of optical fiber.
- Servers are placed in a dedicated place with server farm switches. There is redundant access from each server to two separate server switches. Each server switch has two separate connections to each core switch.

Hierarchical network design prevents the needs of a fully-meshed network where all network nodes are interconnected. The components of the hierarchical networks are the access layer, the distribution layer, and the core layer as proven in Figure1. The hierarchical network design is easy to reproduce, redesign, and expand. There is no need to upgrade the whole network each time a component is included or eliminated. Unique foundations can be put in-service and taken out-of-service with little effect on the rest of the network. This ability helps problem solving, problem solitude, and network control. In an ordered design, the potential, features, and performance of a precise network are enhanced for its position in the network and the part that it performs. The number of streams and their associated information specifications increase as they navigate factors of gathering or amassing and move up the structure from access to distribution and to core layer.

The core layer works as a central source of the network. The core devices are enormous competence routers and expected to be very strong as most of foundations depend on it for connection. The distribution layer combined nodes from the access layer, defending the core from high-density peering. Moreover, the distribution layer makes a fault margin providing a sensible segregation factor in the event of a failing beginning in the access layer. Naturally there is one distribution node per building and it is implemented as a pair of L3 switches, the distribution layer uses L3 switching for its connection to the core of the network and L2 services for its connection to the access layer. The access layer is the 1st position of entry into the network for border devices and end nodes.

Redundancy is addressed in several ways. Core routers have redundant power supplies, and all devices connected to them are connected to both, providing redundant paths between core and distribution layers. In the distribution layer, stackable switches provide redundant power supplies and redundant supervisor engines where possible by connecting each device to more than one other switch in the stack. Access-layer uplinks are redundant as well, and some of the access switches have redundant power supplies. Connections to hosts are typically non-redundant, though there is provision in the data centers for servers to be connected with dual links, with the servers NIC drivers responsible for managing the connections [3].

VI. SECURITY PROBLEMS IN CAMPUS NETWORK AND ITS SOLUTIONS

There are a wide range of network attacks, network attack methodologies, and categorizations of network attacks. The query is, 'How do we minimize these network attacks? 'The type of attack, as specified by the categorization of reconnaissance, access, or DoS attack, determines the means of mitigating a network threat.

6.1 Reconnaissance attacks can be mitigated in several ways

Using powerful authentication is a first choice for protection against packet sniffers. Strong authentication is a technique of authenticating users that cannot quickly be evaded. A One-Time Security Password (OTP) is a way of powerful authentication. OTPs implement two-factor verification. Two-factor verification brings together something one has, such as a symbol card, with something one knows, such as a PIN. Computerized teller machine (ATMs) use two-factor verification. Security is also efficient for mitigating packet sniffer attacks. If traffic is secured, it is essentially unrelated if a packet sniffer is being used because the taken information is not understandable.

Anti-sniffer application and components resources identify changes in the reaction time of hosts to figure out whether the hosts are handling more traffic than their own traffic loads would point out. While this does not absolutely remove the threat, as aspect of an overall mitigation system, it can decrease the variety of instances of threat.

A switched infrastructure is the standard today, which makes it difficult to capture any data except that on your immediate collision domain, which probably contains only one host. A switched infrastructure does not remove the threat of packet sniffers, but can decrease the sniffer's effectiveness.

It is challenging to minimize port scanning. But using an IPS and firewall can restrict the information that can be found with a port scanner. Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers. However, when these services are turned off, network diagnostic data is mislaid. Furthermore, port scans can be run without full ping sweeps. The scans simply take more time because inactive IP addresses are also scanned.

Network-based IPS and host-based IPS can usually inform an IT Manager when a reconnaissance attack is under way. This caution allows the manager to better get ready for the arriving attacks or to inform the ISP from where the reconnaissance sensor is releasing from.

6.2 Several techniques for mitigating access attacks

An amazing number of access attacks are carried out through simple security password guessing or brute-force dictionary attacks against passwords. The use of encrypted or hashed authentication protocols, along with a powerful security password policy, greatly decreases the prospect of successful access attacks. There are specific methods that help to ensure a powerful security password policy. Disabling accounts after a particular number of failed logins. This exercise helps to avoid ongoing security password efforts. Not using plaintext security passwords. Use either a one-time security password (OTP) or encrypted password. Using powerful security passwords, Strong security passwords are at least eight figures and contain uppercase characters, lowercase characters, numbers, and special characters.

The principle of minimum trust should also be designed into the network structure. This means that systems should not use one another unnecessarily. For example, if an organization has a server that is used by entrusted devices, such as web servers, the trusted device (server) should not trust the entrusted devices (web servers) unconditionally.

Cryptography is a critical component of any modern secure network. Using encryption for remote access to a network is recommended. Also, routing protocol traffic should be encrypted as well. The more that traffic is encrypted, the less opportunity hackers have for intercepting data with man-in-the-middle attacks [7].

6.3 Mitigating DoS attacks

Companies with a high-profile Internet existence should prepare how to reply to potential DoS attacks. Traditionally, many DoS attacks were procured from spoofed source addresses. These types of attacks can be beaten down using anti spoofing technology on edge routers and fire walls. Many DoS attacks today are distributed DoS attacks carried out by affected serves on several networks. Mitigating DDoS attacks requires cautious diagnostics, planning, and collaboration from ISPs. The most important components for mitigating DoS attacks are firewalls and IPSs. Both host-based and network-based IPSs are highly suggested. 'Cisco' routers and switches support a number of anti spoofing technology, such as port security, DHCP snooping, IP Source Guard, Dynamic ARP Inspection, and ACLs.

Lastly, although Quality of Service (QoS) is not designed as a security technology, one of its applications, traffic policing, can be used to limit ingress traffic from any given customer on an edge router. This limits the impact a single source can have on ingress bandwidth utilization [7]

VII. EXPERIMENTAL DESCRIPTION

According to the previous section proposed Campus Area Network (CAN) is implemented in the following scenario. Here we used OPNET IT Guru Academic Edition for our simulation purpose. The three red color subnets represent the Branch Campus, Education ERP server, and End users. In the application configuration three major applications such as File Transfer Protocol (FTP), HTTP and Mail is defined. For HTTP it is defined two situations. One is HTTP heavy web browsing and other is HTTP light web browsing. For FTP, it is also created three profiles in the profile configuration. One is for Bulk data transfer, other is for medium data transfer and last one is for small data transfer. After Successful configuration of the campus network topology the simulation is run for 5 minutes. After running the simulation, from the global statistics some parameters are selected such as HTTP traffic load, HTTP response time, and FTP traffic load and the results have been captured which are given in the result and simulation section.

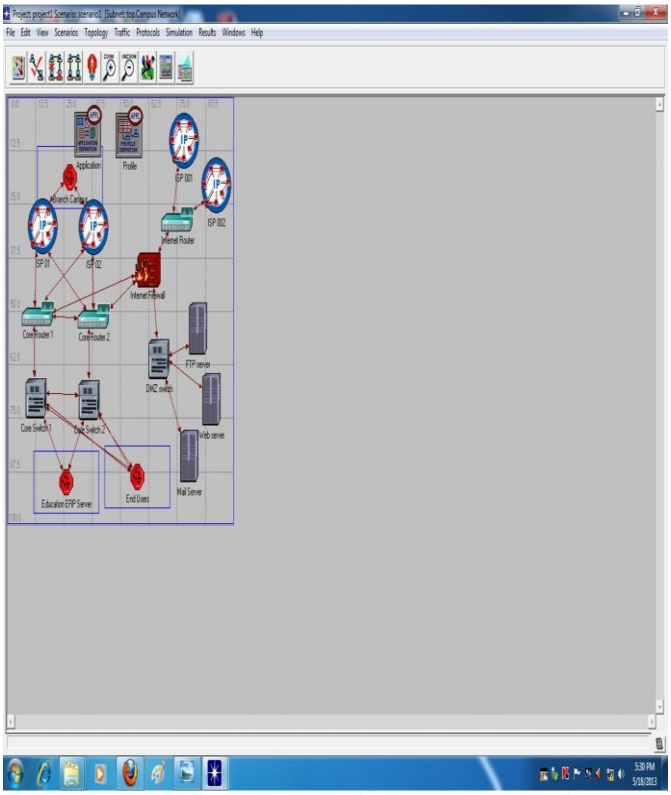

Figure 5. Simulation on Hierarchical Campus Network Architecture

A. Simulation result

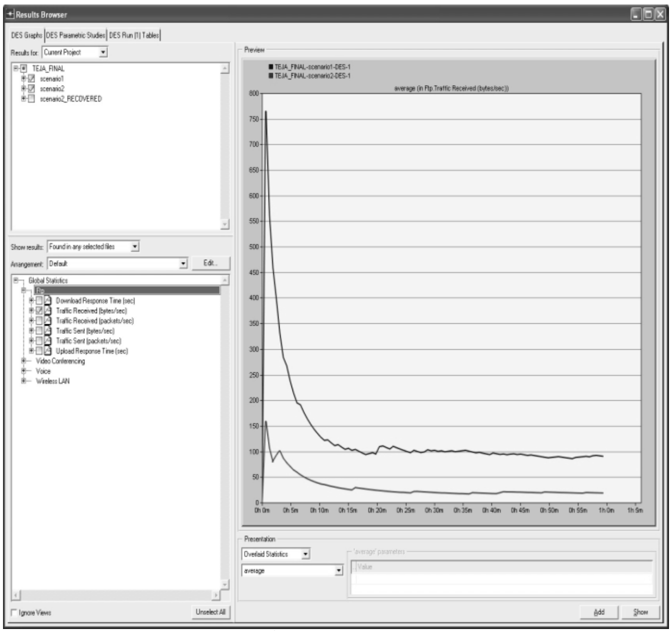

Figure 6. FTP response time (1st line without redundancy and second line with redundancy)

This graph shows that when background traffic is injected into the redundant network, the response time of ftp traffic goes up but at the same time the response time becomes down of the non-redundant link. When the redundant topology is used generally load is shared between the gateway nodes. For this the FTP traffic load for the redundant route is 150+ Bps, when no redundant is used that time the FTP traffic load is much higher and it comes 750+ Bps.

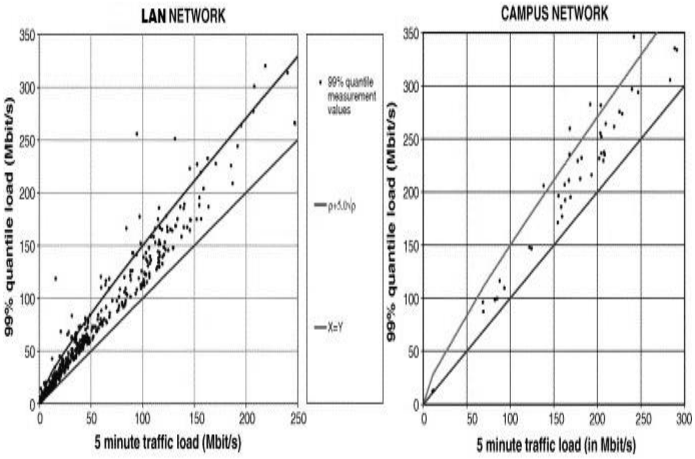

Figure 7. Traffic Load

This is the comparison scenario between LAN and Campus Network based on HTTP traffic load. Here we add two parameters for HTTP traffic. One is for high load which is expressed using upper line of graph and another is low load which is expressed using lower line of the graph. The dotted portion expressed the number of user connected. Thus, the

Campus Network is secured with Firewall, the anonymous users are blocked and limited users can access the internet.

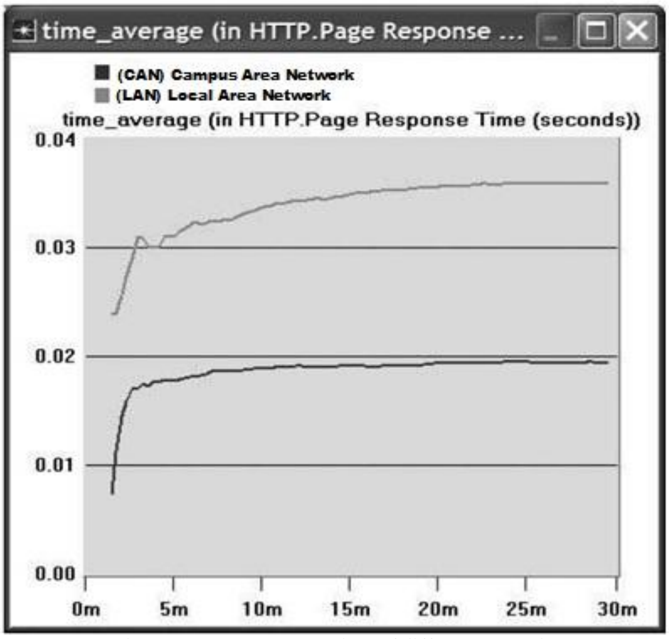

Figure 8. HTTP response time of different networks

The graph reveals that the response time of http between Campus Network and Local Area Network. As the HTTP traffic is low in Campus network, the HTTP response time is much lower. But in the Local Area Network the HTTP traffic is high so that the HTTP response time is much higher than Campus network.

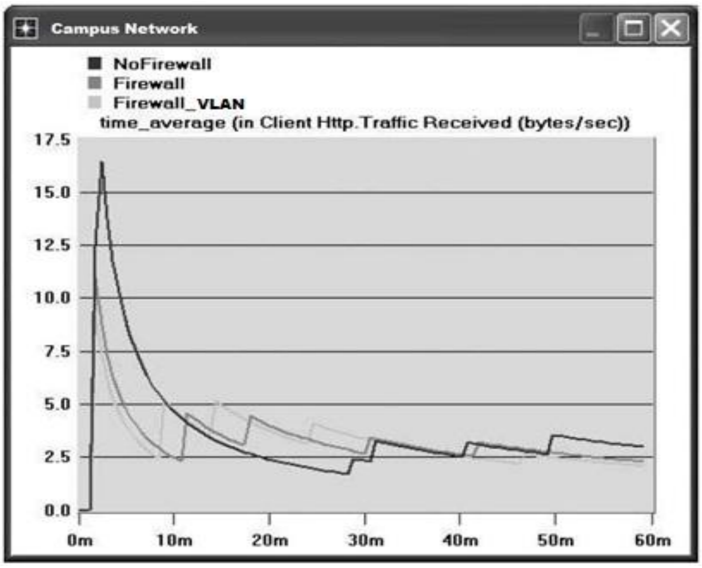

Figure 9. Traffic response Using Firewall in Campus Network

This graph shows the comparison scenario between the network using no firewall, network is using only Firewall and using Firewall-VLAN. When a network users no firewall, the http traffic will be higher because of anonymous attack. For this the HTTP traffic initially is 17.0 and after the network converges the traffic is 2.5+. When a network uses Firewall initially 11.0 and after convergences it is below 2.5. Finally Campus Network Firewall is used and as well as VLAN is also used. When Firewall and VLAN are used jointly in the Campus Network initial HTTP traffic is reduced up-to 7.5+ and after convergences the traffic become less than 2.0.

VIII. MITIGATING NETWORK ATTACKS

Defending your network against attack requires constant vigilance and education. There are 10 best practices that represent the best insurance for your network.

1. Keep patches up to date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.
2. Shut down unnecessary services and ports.
3. Use strong passwords and change them often.
4. Control physical access to systems.
5. Avoid unnecessary web page inputs. Some websites allow users to enter usernames and passwords. A hacker can enter more than just a username.
6. Perform backups and test the backed up files on a regular basis.
7. Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
8. Encrypt and password-protect sensitive data.
9. Implement security hardware and software such as firewalls, IPSs, virtual private network (VPN) devices, anti-virus software, and content filtering.
10. Develop a written security policy for the company.

These methods are only a starting point for sound security management. Organizations must remain vigilant at all times to defend against continually evolving threats [7].

CONCLUSION

Network architecture and its security are almost as important as air, water, food, and shelter. If we follow the hierarchical network design, network will be scalable, performance and security will be increased, and the network will be easy to maintain. In this work, we proposed a compact network infrastructure based on the work environment and required scalability, security and other aspects of the design; and the design was implemented for a real campus. This work may be extended in the area of network design with cloud and heterogeneity. A hierarchical architecture of campus network is configured with different types of traffic loads and security issues for ensuring the quality of service. The simulations were analyzed in order to understand how the networks react with different scenarios of the campus network. From simulation results, we found that with redundant ftp traffic load, it is over 150Bps, but without redundant traffic load it is higher and it becomes over 750Bps. On the other hand, based on http traffic load we also found that http traffic load and http response time are lower than those for regular LANs. We have used firewall in the campus network and found that without firewall http traffic initially is 17.0Bps and after the convergences the traffic was over 2.5Bps. But when the firewall is used initially http traffic was 11.0Bps and after convergences it was below 2.5Bps. At the same time when firewall and VLAN are used jointly in the campus network initial http traffic is reduced over 7.5Bps and after convergences the traffic becomes less than 2.0Bps. The results proved that response time and security are improved by using proposed network architecture in campus network.

REFERENCES

[1] Security Problems in Campus Network and Its Solutions, 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam1,2Department of Computer Science, NIT Agartala, India, 3National Informatics Centre, India

[2] Cisco White Paper, “Designing a Campus Network for High Availability,”http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/cdccont 0900aecd801a8a2d.pdf.

[3] Outage Analysis of a University Campus Network, Baek-Young Choi 1, Sejun Song2, George Koffler1, Deep Medhi1

[4] [4]Network Security: History, Importance, and Future “University of Florida Department of Electrical and Computer Engineering Bhavya Daya ”.

[5] “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[6] CCNA Exploration 4.0 LAN Switching and Wireless, Cisco Networking Academy, Cisco Systems, Inc 2007

[7] CCNA Security 1.0, Implementing Network Security, Cisco Systems, Inc 2009.