Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 12, December-2016

Design and Implementation of a Campus Area Network

Prof. Manav Thakur[1], Swati Kumari[2], Khyati Pandey[3], Priyanka Prasad[4]

[1]*Training & Placement Officer, D Y Patil School of Engineering Academy, Ambi, Pune, Maharashtra, India*

[234] *Dept. of Computer Engineering, D Y Patil School of Engineering Academy Ambi, Pune, Maharashtra, India*

Abstract -— In today's world all the computers and networking systems is of great importance, the need for computer and network security becomes necessary and important. The increase in the computer network system has exposes many networks to many kinds of network threats. Campus network is important and it plays an essential role for any college. Computer network security threat and network design are always major concern. A campus network design is an self organized network under the control of a organization which is within a local geographical place and sometimes it may be a MAN (Metropolitan Area Network).

***Key Words*:** Campus Area Network, Security, Metropolitan Area Network, Firewall

1. INTRODUCTION

Mostly, Network Engineers in a computer network faces lots of challenges in maintaining availability, high performance, perfect infrastructure, and security. Securing a large network has always a concern to a Network Engineer. There are many similarities between securing a college campus network but sometimes many of them has its own issues and challenge. Present educational organization pay attention to IT to improve their students' learning experience. Design of campus can achieve this if IT managers hold on to the fundamental principles addressed in this reference architecture, namely LAN or MAN connectivity design, security, and centralized management. The network design has become a critical part for some organizations in present years. An important network design for today's networks is creating to support future expansion in a reliable, scalable and secure manner. This requires the designer to define the client's unique situation, particularly the current technology, application, and data design. The physical network infrastructure is required for a organization network. Organization Management and IT manager may know exactly what kind of network they want to set up, upcoming plans, and expected growths. Building an organization network atmosphere also contains functional and safety elements that also go beyond the IT department's constraint and skills.

1.1 BACKGROUND:

There are various types of network such as :

A Personal Area Network (PAN) is a computer network used for data transmission amongst devices such as computers and personal digital assistants. A Local Area Network (LAN) is a group of computers and associated devices that share a common communications line or wireless link. Connected devices can share the resources of a server within a small geographic area i.e. approx 1 m. A Metropolitan Area Network (MAN) is a computer network that interconnects users with computer resources in a geographic area or bigger than that cover by local area network (LAN) but smaller than the area covered by wide area network (WAN). A Campus Area Network (CAN) is a type of Local Area Network (LAN) or set of interconnected LANs serving a government office, university, or similar organization. A Storage Area Network (SAN) is a high-speed network of storage devices that also connects those storage devices with servers. It provides block wise storage that can be accessed by applications running on any networked servers. A Wide Area Network (WAN) is a telecommunication network that extends over a large geographical distance.

2. NETWORK ARCHITECTURE IN CAMPUS AREA

It consists of a North Building (NB), and South Building (SB), and a Data Center (DC), all connected through a frame relay switch. The Data Center is connected to the Internet service provider to get to the simulated Internet.

The Steps:

North Building

1 Switches: IP addresses: Configure IP address for the switches, their default gateway. Verify by *ping*.

2 Switches: VTP and VLANS: Configure the ports connected between the switches to trunk ports. Create VLANs 3 and 4 on one switch, name them DATA1 and DATA2 respectively. Configure the VTP domain "NB" on the switch (you'll have to configure the password on the other switches). Assign the ports that will have PCs attached to the VLANs. Verify that all VLANs have replicated by *show VLAN* on the other switches.

3 Switches: STP: The top switch will be the root switch. As practice, try to figure out which port (on the other switches of course) will become blocked. Configure the top switch to be the root switch for all VLANs (1, 3 and 4). **Optional:** Configure ports that are connected to PCs/routers. Verify by show spanning-tree on all switches that the top switch is the root.

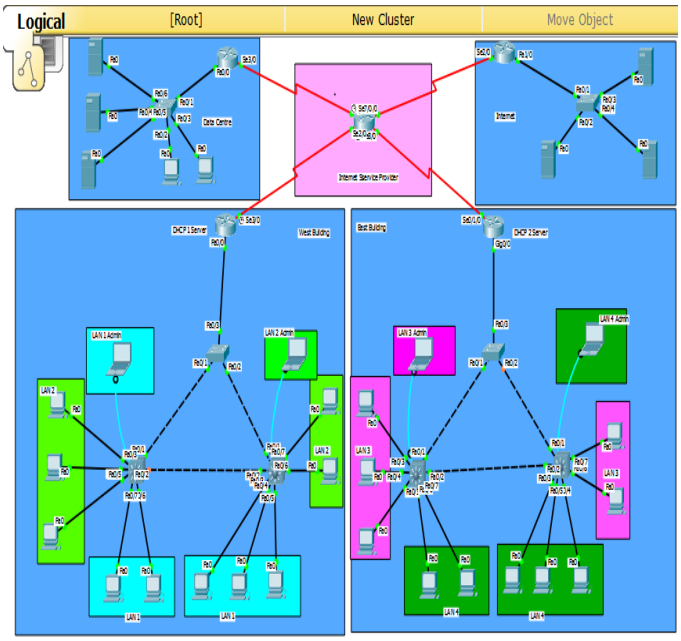

Fig: NETWORK ARCHITECTURE

4 Routers: Router-on-a-Stick: Configure the router's Fast-Ethernet port on VLAN 1 and two sub interfaces for each of VLANs 3 and 4; don't forget to tell them they'll be getting VLAN information from the specific VLANs.

5 Routers: Gateway Router/DHCP: Configure it's Fast-Ethernet port on the VLAN 4 subnet; don't forget to configure the port on the switch on VLAN 4. Configure DHCP pools for VLANs 3 and 4.

6 Routers: Routing protocol: I used EIGRP. After configuring routing protocols on both routers, verify by *show ip route* on the Gateway router. You can verify by *ping*. Also, ping from a PC on one VLAN to another PC on the other VLAN.

South Building: Same thing as North Building. I chose the VTP domain "EB", VLANs 5 and 6 instead, different IP subnets; refer topology image. Use the same routing protocol.

Data Center: There is no VTP here, no STP, and you don't even have to have DHCP. Configure static IPs. Refer image. Use the same routing protocol. Configure the serial interface that will connect to the ISP with the IP address in the image.

ISP: Configure both serial ports with IPs. Configure a static route to network pointing to the next router (which will be our network on the Internet).

Internet: Configure static IPs to the servers and all that again, do NOT configure a routing protocol on the router. Instead, just configure a static route to the network going through the ISP router.

Frame Relay: Use point-to-point routing protocol. Subnets are indicated in the image. For the frame relay switch/cloud itself, just check out the configuration from the finished configuration, it's straight forward. At this point, most of the configuration is done. Verify connectivity between both buildings and Data Center by *ping* (and Web Browser on the PCs if you still have that HTTP server in the Data Center).

2.1 Implementation of Cost Effective Secure Campus Network:

Several challenges are there for the implementation of a secure network on a college campus, but most important challenge to his project is security. Hence, we have detailed possible solutions in maintaining and designing of our network in order to facing such solutions.

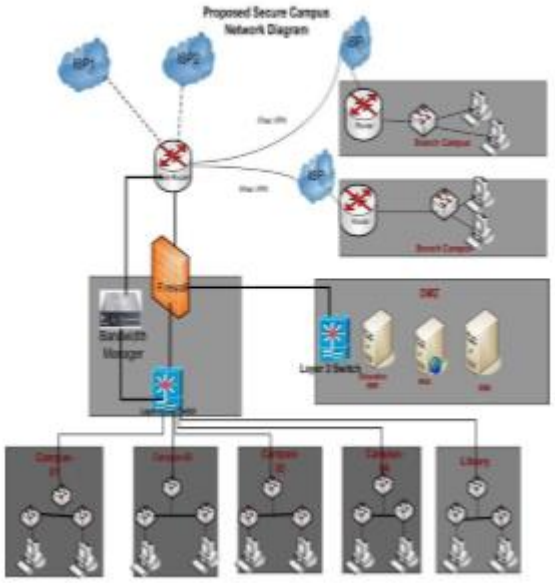

Fig: Secure Campus Network Design

A. Implementing Firewall for Security: A firewall works to monitor and block or allow network traffic, both incoming and outgoing, on a private network. While there is a hardware firewall to help protect the campus network security, this firewall affects certain outbound traffic and prevents unauthorized inbound traffic. NetBIOS, SMTP and other miscellaneous ports determined to pose a security risk are blocked in the outgoing direction. This does not impact the majority of academic work related programs used on the campus.

3. CONCLUSIONS

Network architecture and its security are important any organization. In this work, we proposed a compact cost effective secure campus network design based on the work environment and required scalability, security and other aspects. Henceforth, All the branches are communicating with each other and accessing the internet via ISP using internet and network protocols with security.

4. ACKNOWLEDGEMENT

We are also thankful to [SAURABH] for assistance with [a Network Technology], and [Prof: MANAV.A.THAKUR] who moderated and improved the manuscript significantly. We appreciate to the [Prof: LAXMIKANT] for sharing their pearls of knowledge with us during the course of this project.

5. REFERENCES

[1] Mohammed Nadir Bin Ali1, Mohamed Emran Hossain2, Md. Masud Parvez "Design and Implementation of a Secure Campus Network " Daffodil International University.

[2] Network Security, Sulaimon Adeniji Adebayo, Bachlor's Thesis (UAS) Degree Program in Information Technology Specialization: Internet Technology.

[3] "Network Architecture and Security Issues in Campus Networks" Mohammed Nadir Bin Ali, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) 2013.

[4] "Security Problems in Campus Network and Its Solutions" 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.

[5]"Network Security: History, Importance, and Future""University of Florida Department of Electrical a Computer Engineering Bhavya Daya"

[6]"Security Analysis of a Computer Network", Jan Vykopal, MASARYK UNIVERSITY FACULTY OF INFORMATICS .

[7]"Security and Vulnerability Issues in University Networks" Sanad Al Maskari, Dinesh Kumar Saini, Swati Y Raut and Lingraj A Hadimani--Proceedings of the World Congress on Engineering 2011 Vol I WCE 2011, July 6 - 8, 2011, London, U.K.

[8]"Campus Network Design and Implementation Using Top down Approach by Bagus Mulyawan", Proceedings of the 1st International Conference on Information Systems for Business Competitiveness (ICISBC) 2011.