IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 1, Ver. I (Jan. - Feb .2016), PP 72-77
www.iosrjournals.org

Design and Implementation of a Cost-effective and Secured "Private Area Network" for smooth as well as hassle-free Computing in the University Campus

Joysankar Bhattacharjee
Master of Technology, Electronics & Communication Engineering Visionary Entrepreneur; New Delhi, India

Abstract: *In recent days, the wide use of computer networks has been marked its sign to the modern civilization. Almost in all the organizations, various types of computer networks, namely, LAN, MAN, WAN, PAN, CAN, SAN etc. are used. While using a computer network, the main factors, which arise are, 1. Construction of the network, 2. Type of the network, 3. Good features of the network for smooth computing, and 4. Security of the network. In this theoretical paper, a different concept, „Private Area Network" is designed which should be implemented in the university or college campuses for cost effective, smooth and secured routing. This paper is basically a combinational implementation of „Cisco EIGRP", „ACL mechanism" and a different „CAN (Campus Area Network)" with Networking Security Concept. In this system, the higher authority can directly contact to the desired department with secured and hassle-free computing. The network should be implemented with the help of construction plans mentioned in this paper. Protocols must be maintained according to the guidelines and then the security concept will prevent the network from various attacks.*

Keywords: *ACL, Campus Network, EIGRP, Firewall, Network Security, Security Management, VLAN, VPN.*

I. Introduction

The old saying "a picture is worth a thousand words" is especially true when you are working with a network analysis report. Network analysis is a visual art form. The rapid development and wide applications of computer networked systems effectively thrive in today`s world. We always want a strong and secured network for our computing. Due to this, Network Security is indeed an important issue to every computer network. Vast use of computer networks also expose various types of networking threats, the prevention of which is always a challenge to the network professionals. Here comes the security concept. The Security process can be anything such as identification, authentication, authorization etc. and sometimes visual systems to protect authenticity, accountability, integrity of computer hardware and network equipment.

For any organization, Campus Area Network is essential. Network security and its construction is very much important issues here. The Campus Network is maintained by the university authority. The university will must have a proper location and sometimes it can be a part of a Wide Area Network or a Metropolitan Area Network. As we have used Cisco EIGRP here for smooth routing, therefore our network is a part of Cisco WAN. Access Control List is another mechanism used here to make the network a secured one.

The Network Design and Implementation has always been a critical part to many IT organizations. When the infrastructure is designed, both the Management and Technical parts are must be taken care of with great expertness. The Management Part and the Technical Part are described in the paper so that the implementation can be done easily.

Various Research papers and Articles have been consulted for Network Security Methods and Network Threats. The rest of the paper is a description of each and every step and the detailed explanation of implementing the said network.

II. Background

In this world, depending upon the need of computation we have various types of networks such as, Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Campus Area Network (CAN), Personal Area Network (PAN), Storage Area Network (SAN), Wireless Local Area Network (WLAN), System Area Network and Virtual Local Area Network (VLAN).

- **Local Area Network** – A LAN is a connection of computers and network devices where a common communication line is shared. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings.
- **Wide Area Network** - As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address.

- **Metropolitan Area Network** - A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned and operated by a single entity such as a government body or large corporation.
- **Campus Area Network** - A Campus Area Network (CAN) is a proprietary Local Area Network (LAN) or set of interconnected LANs serving a corporation, government agency, university, or similar organization.
- **Personal Area Network** – A PAN is a computer network organized with an individual person. Generally a PAN can be contained a mobile computer, a cell phone or any handheld computing device.
- **Storage Area Network** – A SAN connects servers to data storage devices through a technology like Fiber Channel.
- **System Area Network** – This network links high-performance computers with high-speed connections in a cluster configuration. Also known as Cluster Area Network.
- **Wireless Local Area Network** - A LAN based on Wi-Fi or wireless network technology is called a WLAN.
- **Virtual Local Area Network** – VLAN is a segment of a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability and security.

***Note**: Definitions are taken from different articles and research papers.

Here, in this paper, the network security of Campus Area Network has been discussed widely and Virtual Local Area Network is used for the secured network purpose. A different concept of campus network, in the name of „private area network" is designed.

III. Traditional Campus Network Design

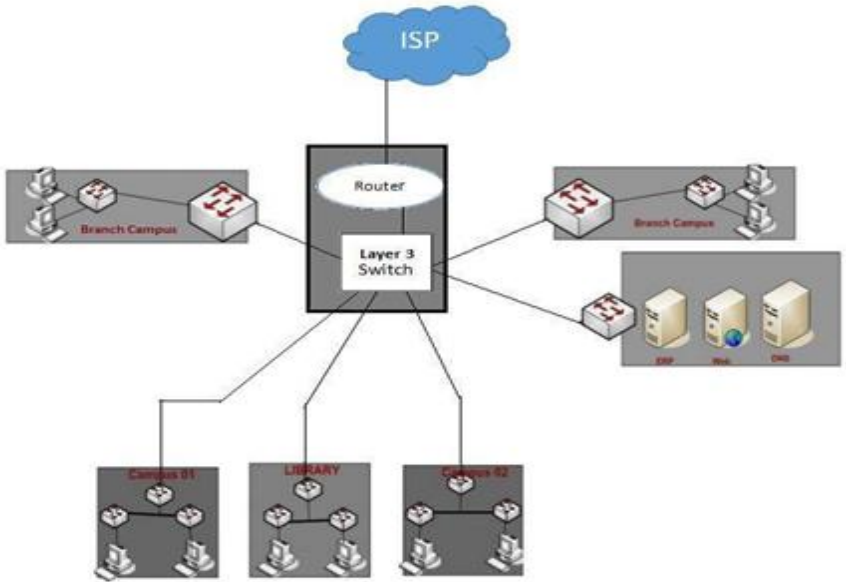

Fig.1 Traditional Campus Networks

IV. Overview Of The Proposed System

The proposed system is mainly a modified campus network where the higher authority can directly contact to any employee/staff/department. Though this action also makes us remember about individual e-mailing system, the e-mails can be done through different communicating network tools but the proposed system is fully maintained by the university authority itself. As a result of which, the university authority does not need to rely on those communicating networking tools for security, instead they design their secured network by their own. Various network attacks and threats must be prevented by themselves. This state of action increases the capability of the university authority as well as maintains their privacy.

V. Implementation Of The Network In The Campus

To implement a network in a university/college campus, we must follow two parts. These are 1. Management part of the system and 2. Technical part of the system.

The Management Part:

For the proposed network, in the Management part, first of all, we must construct a governing body for the network security management. Different department heads, expert faculties, IT professionals can be the members of the body. The governing body should not be limited with the university leaders only, expert technicians, group members can also be a part of it. This body takes care of daily maintenance routine of the network, public demands, solving and reporting problems etc. After the governing body, the next important thing is to form a strong technical team. Experienced faculties, expert IT professionals can be a part of the team. The university authority will choose skilled personnel for this technical team. This team designs and implement the network, maintain it every day and implement new ideas to make network more and more efficient. For the Management part, a well strategy of implementing technology is very much important. Without a strategy, the technology cannot be implemented properly. Accurate planning for the development of the campus network, proper arrangement for specific tasks, unified actions to complete the tasks etc. come under the strategy to implement the technology. After the strategy making part, next is to prepare a set of rules. Establishing a set of rules is important because without any rule or proper guideline, our main work won`t be done appropriately. For example, virus management, computer room management, system data management etc. are some effective rules. The rules must be scientific as well as operative. And last but not the least, the constructions of internal and external environment are also very important for the management. The computer labs, server rooms must be well constructed. Maintaining a good relationship with the ISP leaders provides a very favorable external environment.

The Technical Part:

In this paper, the technical part is divided into some steps. These steps are, A) Ensuring Physical Security, B) Implementation of Cisco EIGRP, C) Access Control List, D) Network Attacks, E) Network Threats, F) Firewalls, G) Implementing VLAN and H) VPN.

A) Ensuring Physical Security:

We must confirm the physical security of the central labs, departmental labs and their devices. Facilities of anti-theft, water and fire proof, anti-magnet etc. will be more effective to assure the said security. Campus network security is incomplete without physical security.

B) Cisco EIGRP:

To give all the flexibility of routing protocols, Enhanced Interior Gateway Routing Protocol (EIGRP) is designed by Cisco. EIGRP has Protocol Dependent Modules that can deal with AppleTalk and IPX as well as IP. The advantage with this is that only one routing process needs to be run instead of a routing process for each of the protocols. EIGRP provides loop- free operation and almost instant simultaneous synchronization of all routers. Whereas other routing protocols use a variant of the Bellman Ford algorithm and calculate routes individually, EIGRP uses the Diffusing Update Algorithm (DUAL) (SRI International) where routers share the route calculations (hence ' diffuse"). A router only sends routing updates as distance vectors of directly connected routes, rather than every route that is in the network. Also, the router only sends an update of a particular if a topology change has occurred to that specific route.

EIGRP Packet Format:

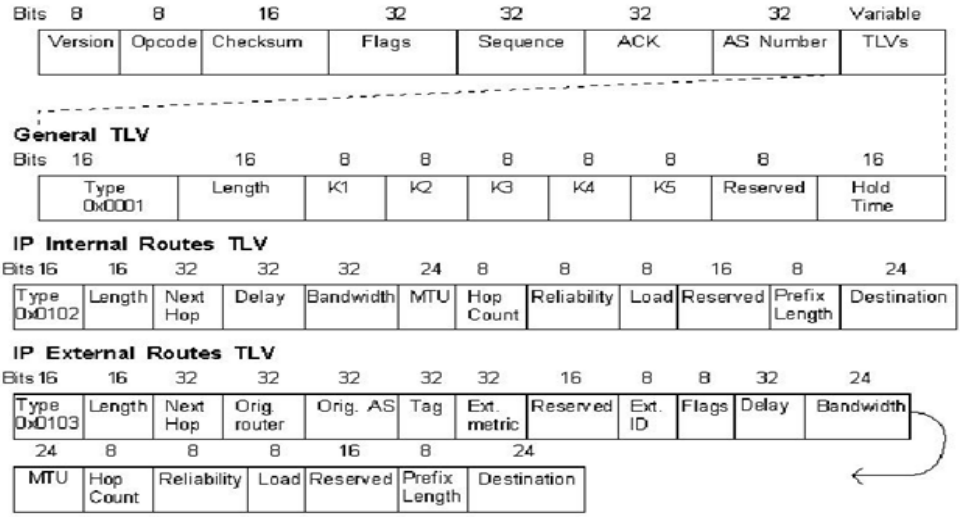

Fig 2: EIGRP Packet format

Enabling EIGRP:
We can enable one EIGRP routing process on the ASA. The following steps should be performed to enable the EIGRP.

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# router eigrp 2	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	**network** *ip-addr* [*mask*] **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0	This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command. Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process. If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces in EIGRP.

Fig 3: Enabling EIGRP

Example: EIGRP Neighbor Database:

```
Router# show ip eigrp neighbor
IP-EIGRP neighbors for process 100
H  Address         Interface  Hold Uptime  SRTT  RTO Q
                               (sec)     (ms)    Cnt Num
1  172.17.1.1      Se0       11 00:11:27  16   200 0 2
0  172.17.2.1      Et0       12 00:16:11  22   200 0 3
```

Fig 4: EIGRP Neighbor Database

C) Access Control List:

Access Control List (ACL) is a security enhancement available for an Azure deployment. An ACL provides the ability to selectively permit or deny traffic for a virtual machine endpoint. This packet filtering capability provides an additional layer of security. For instance, if a file object has an ACL that contains (Alice: read, write; Bob: read), this will give Alice permission to read and write the file and Bob to only read it.

An ACL contains a list of rules. When an ACL is created and applied to a virtual machine endpoint, packet filtering takes place on the host node of the Virtual machine. This prevents the Virtual Machine from spending the precious CPU cycles on packet filtering.

Using Network ACLs, we can do the following:

- Selectively permit and deny incoming traffic based on remote subnet address range to a virtual machine input endpoint.
- Blacklist IP addresses.
- Create multiple rules per VM endpoint.
- Specify up to 50 ACL rules per VM endpoint.
- Specify an ACL for a specific remote subnet address.
- Use rule ordering to ensure the correct set of rules are applied on a given VM endpoint.

Example: Default ACL table:

Rule #	Remote Subnet	Endpoint	Permit/Deny
100	0.0.0.0/0	3389	Permit

Fig 5: ACL table

D) Network Attacks:

There are various types of Network attacks. The network must be able to resist the network attacks. This state of action is always a challenge from hackers to IT professionals.

Some Network attack types are mentioned below:

1. Passive Attack
2. Active Attack
3. Insider Attack
4. Phishing Attack
5. Buffer overflow
6. Hijack attack
6. Spoof overflow
7. Password Attack
8. Close-in Attack etc.

Separate actions are taken in the proposed network to prevent these network attacks.

E) Threats:

Some Network threats are discussed below:

Network Virus: It is an external threat which can enter through unprotected ports and can damage the whole network.

Web server attack: This is an external threat generally to the web servers. If this attack is happened, hackers can hack other systems connected to the network.

Web based attack: This happens due to internal browsing to an external site. This attack can compromise browsing process and affect other internal systems.

E-mail with virus: An external threat which can infect system reading e-mail.

Network User Attack: This is an internal threat where traditional border firewalls become failed.

F) Firewall:

Firewall is used for monitoring operation and to allow or block network traffic on a private network. In the proposed system, a hardware firewall is used to help protecting the campus network security.

G) Implementing VLAN:

The VLAN stands for Virtual Local Area Network. VLANs have become extremely popular on networks of all sizes. VLAN reduces the problem of managing multiple cable plants and switches in a single organization. VLANs create multiple broadcast domains allowing traffic from the domains in remaining isolated at the time of increment of the network`s bandwidth, security and availability.

Here, in this paper, some VLANs have been suggested for a better security of our campus network.

Sl. No.	VLAN ID	VLAN Name
1.	10	Faculty Members
2.	20	Admin Office
3.	25	Accounts Department
4.	30	Cultural Affairs
5.	35	Examination Department
6.	40	Students

Table 1: VLAN ID Suggestion for the proposed network

H) VPN:

A Virtual Private Network is mainly used to extend a private network across a public network like the internet. With the help of this, we can receive and share data across a public network like we are directly connected to that network. By making virtual point-to-point connections, we can establish the VPN easily. Along with providing network flexibility, VPN also maintains the security of the network. In the proposed network, a full tunnel VPN service is there, which is a secured connection to the network from external public

networks.

VI. The Proposed Network

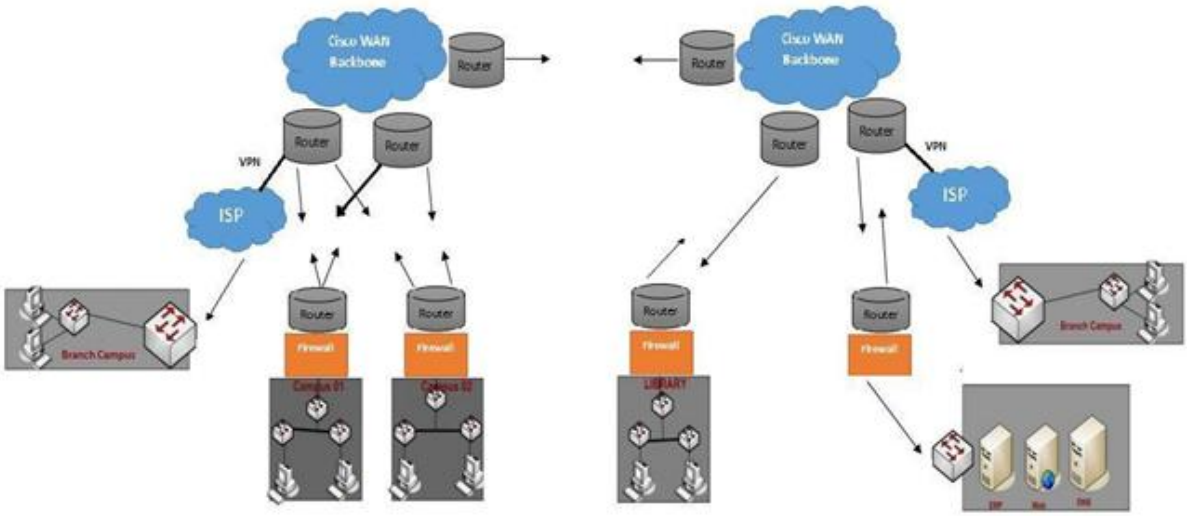

Fig 6: The Proposed Network

VII. Conclusion & Future Scope

Designing and implementing a secured private network in a university is pretty much tough work, which must be done with a lot of patience and skills. The above description is a theoretical concept of a different private network where routing becomes smoother and security is maintained well. The idea is checked and discussed several times and finally it is concluded that it can be successfully implemented for the said purpose. To make more developments in this idea, the concept of Access Control List can be replaced by the concept of Network Security Groups in future. Then the efficiency of the network security will be increased.

References

[1]. "EIGRP, a fast routing protocol based on distance vectors" - R. Albrightson, J. J. Garcia-Luna-Aceves, and J. Boyle.
[2]. "Networking for Global Communications" - Zhou Haijun.
[3]. "Security Problems in Campus Network and Its Solutions", 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam; Department of Computer Science1-2, NIT Agartala, India, 3 National Informatics Centre, India.
[4]. "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.
[5]. "Access Control List" – Wikipedia the free encyclopedia.

BIOGRAPHIES

Joysankar Bhattacharjee, a permanent resident of Agartala, Tripura, India, is a M.Tech. in Electronics & Communication Engineering. Currently he is a visionary entrepreneur in New Delhi, India, working on his own research projects.